ARTIFACT REFERENCE

8.0.0

CONTENTS

Windows

Additional Sources

Android Backups

Description	Android Backups contains information about any backups of Android devices that are recovered from the computer. If an Android backup is recovered during a search, you can search the contents of the backup for additional artifacts.
Recovery method	Parsing

Attribute	Description
File Name	The name of the backup file.
File Path	The path where the backup was stored on the computer.
Encryption	The type of encryption (if any) that was used on the backup.
File System Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time for the AB file from the file system.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time for the AB file from the file system.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time for the AB file from the file system.

Additional Information

Apple Disk Images

Description	Apple disk images are commonly stored as DMG or IMG files. These files are containers that may contain additional items of interest. This artifact identifies any Apple disk image found on the system.
Recovery method	Parsing

Attribute	Description
File Name	The name of the Apple disk image file.
File Path	The path where the Apple disk image was stored on the computer.
File Type	The type of Apple disk image file (DMG or IMG).
File System Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time for the file from the file system.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time for the file from the file system.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time for the file from the file system.

Additional Information

iOS Backups

Description	iOS Backups contains information about any backups of iOS devices that are recovered from the computer. If an iOS backup is recovered during a search, you can search the contents of the backup for additional artifacts.
Recovery method	Parsing

Attribute	Description
Device Phone Name	The name of the iOS device from which the backup originated.
Device Phone Number	The phone number of the iOS device from which the backup originated.
IMEI	The IMEI of the iOS device from which the backup originated.
ICCID	The ICCID of the iOS device from which the backup originated.
Backup File Creation Date/Time	The date and time that the backup was created.
Product Name	The model of the iOS device from which the backup originated.
Product Version	The version of iOS of the device at the time of the backup creation.
Serial Number	The serial number of the iOS device from which the backup originated.

Additional Information

Virtual Machines

Description	Virtual Machine files that have been found on the object being searched.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the virtual machine.
Virtual Machine Software	The software that is associated with the virtual machine.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the virtual machine was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the virtual machine was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the virtual machine was last modified.

Additional Information

Application Usage

Application Install States

Description	Application Install States contains a list of state changes that occur while an application installs or is uninstalled on the computer.

Recovery method	Parsing

Attribute	Description
Action	The type of change that occurred to the application.
Package Name	The internal name of the application.
Date/Time	The date and time that the event occurred.
Path	The file path to the package of the application.

Additional Information

Feature Usage

Description	FeatureUsage is a registry key available in Windows 10 version 1903 and later. It contains information on user activity in the Windows taskbar such as app and tray item clicks.
Recovery method	Parsing

Attribute	Description
Application	The name of the application. This can be an app name, full path, or tray item name.
Badge Update Count	The number of times the notification badge was updated for the application.

Attribute	Description
App Launch Count	The number of times the user started the application pinned to the taskbar.
App Switch Count	The number of times the user switched to the application by clicking it on the taskbar.
Jump View Show Count	The number of times the user opened the Jump List for the application by right-clicking it on the taskbar.
Click Count	The number of times the user clicked on a taskbar item. For example, the clock or Start menu.

Additional Information

Installed Microsoft Programs

Description	Installed Microsoft Programs contains applications installed on the machine which are published by Microsoft.
Recovery method	Parsing

Attribute	Description
Application Name	The name of the installed application.
Company	The publisher listed when the program was installed.
Created Date	The date of installation or most recent update.

Attribute	Description
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the key was last updated in the registry.
Install Size (Bytes)	The estimated install size of the installation.
Version	The publisher provided version number of the application.
Potential Location	The potential location for the application's executable, as determined by the location where the icon for the application was found.
Embedded Signature	Indicates whether the program is digitally signed using an embedded digital signature as opposed to one signed utilizing a security catalog file.
MD5 Hash	The MD5 hash of the program.
Authenticode PE Image Hash	The PE Image hash of the program as read from within the digital signature format, Authenticode, if present. This hash is calculated using a Microsoft specified algorithm and is not equal to the hash of the entire program.
Issuer	The issuer of the digital signature, if present.
Signature	The digital signature of the issuer, if present.
Digest Algorithm	The hash algorithm used to create the digest.
Encryption Algorithm	The algorithm used to sign the digest.

Attribute	Description
Not Before	The Issuer's certificates are not valid before these dates.
Not After	The Issuer's certificates are not valid after these dates.

Additional Information

Installed Programs

Description	Installed Programs contain applications installed on the machine which are not published by Microsoft.
Recovery method	Parsing

Attribute	Description
Application Name	The name of the installed application.
Company	The publisher listed when the program was installed.
Created Date	The date of installation or most recent update.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the key was last updated in the registry.
Install Size	The estimated install size of the installation.

Attribute	Description
(Bytes)	
Version	The publisher provided version number of the application.
Potential Location	The potential location for the application's executable, as determined by the location where the icon for the application was found.
Embedded Signature	Indicates whether the program is digitally signed using an embedded digital signature as opposed to one signed utilizing a security catalog file.
MD5 Hash	The MD5 hash of the program.
Authenticode PE Image Hash	The PE Image hash of the program as read from within the digital signature format, Authenticode, if present. This hash is calculated using a Microsoft specified algorithm and is not equal to the hash of the entire program.
Issuer	The issuer of the digital signature, if present.
Signature	The digital signature of the issuer, if present.
Digest Algorithm	The hash algorithm used to create the digest.
Encryption Algorithm	The algorithm used to sign the digest.
Not Before	The Issuer's certificates are not valid before these dates.
Not After	The Issuer's certificates are not valid after these dates.

Additional Information

McAfee Logs

Description	McAfee Logs identifies and collects any log files created by McAfee Antivirus and McAfee ePO.
Recovery method	Parsing

Attribute	Description
File Name	The name of the log file.
File Path	The path of the log file.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the log file was created.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the log file was last accessed.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the log file was last modified.

Additional Information

Windows Defender Logs

Description	Windows Defender Logs identifies and collects any log files created by Windows Defender and Windows Security Essentials.
Recovery method	Parsing

Attribute	Description
File Name	The name of the log file.
File Path	The path of the log file.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the log file was created.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the log file was last accessed.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the log file was last modified.

Additional Information

Cloud Storage

Carbonite Log File

Description	Carbonite is a cloud based automated backup program that is used for backing up a user's files and folders to the cloud. This search will return which files or folders have been, or are pending to be backed up to the Carbonite cloud.
Recovery method	Carving

Attribute	Description
File Name	The name of the file that was backed up.
File Backup Date/Time - UTC (yyyy-mm-dd)	The date and time when a file was backed up to the Carbonite service.
File Size	The size of the backup file.
Type	The type of the file that was backed up.

Additional Information

Dropbox

Description	Dropbox contains information about files that users uploaded and synced to Dropbox.
Recovery method	Parsing

Attribute	Description
Local File Name	The name of the file on the local machine.
File Path	The path to the local file.
Updated File Name	The filename when updated.
Local Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time on the local machine.
Updated Modified	The last modified time of the updated file.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Local Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the local file.
Local File Size (bytes)	The size of the local file.
Updated File Size (bytes)	The size of the updated file.
Local File Version Id	The file version ID of the local file. This value can be used to determine whether there are any updates that need syncing.
Updated File Version Id	The file version ID of the remote file.

Additional Information

Dropbox Configuration Data

Description	Dropbox Configuration Data contains information about users and the file that are uploaded and synced to Dropbox.
Recovery method	Parsing

Attribute	Description
Dropbox User ID	The Dropbox user ID.
Dropbox Email	The email addressed used with the Dropbox service.

Attribute	Description
Dropbox Folder Path	The folder path to the local Dropbox folder.
Recently Changed Files	A list of recently changed files.

Additional Information

Flickr

Description	This search will recover artifacts left behind when using Flickr to upload files via the web. Recovered data can include file names, dates and times, user IDs, file sizes, URLs to files, descriptions, and more.
Recovery method	Carving

Attribute	Description
Title	The title of the media.
Owner ID	The unique identifier of the Flickr media owner.
Owner Name	The name of the media owner.
URL	The URL to the picture on Flickr.
Media	The type of media uploaded.
Post Date/Time - UTC (yyyy-mm-dd)	The date and time that the media was posted.
Taken Date/Time - Local Time (yyyy-mm-dd)	The date and time that the media was created or taken.
Description	A description of the uploaded media.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Google Drive

Description	Google Drive is a file hosting service that allows users to upload and sync files to a cloud service.
Recovery method	Carving

Attribute	Description
File Name	The name of the file that was backed up.
Author Name	The name of the author of the file.
Author Email	The email address of the author of the file.
File Size (Bytes)	The file size.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the file was modified.
Last Modified Name	The last user to modify the file.
Last Modified Email	The last modifying user's email address.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The last date and time that the file was viewed.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created.

Additional Information

OneDrive

Description	These are artifacts left behind using OneDrive to upload and view files via the web or through the OneDrive desktop application. Data recovered can include file names, dates and times, user IDs, file sizes, sharing settings, and more.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file that was backed up.
File Size (Bytes)	The file size in bytes.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the file was modified.
Owner Name	The name of the owner of the file.
Account Type	The type of the account (Personal or Business).
Account ID	The unique identifer of the owner of the account.
Owner ID	The unique identifer of the owner of the file.
File Path	The path to the file that was backed up.
URL	The URL to access the uploaded file. Usually this is a private URL.

Attribute	Description
Last Modified Name	The last user to modify the file.
Last Modified ID	The last modifying user's OneDrive identifier.

Additional Information

Communication

Adium Chat

Description	Adium is a multi-account chat application on Mac computers. It allows users to connect various accounts such as Google Talk, Facebook, and generic Jabber accounts.
Recovery method	Carving

Attribute	Description
Sender	The sender of the message.
Sender Nickname	The sender's nickname.
Recipient	The message recipient.
Message	The message content.
Message Sent Date/Time UTC (yyyy-mm-dd)	The date and time when the message was sent.

Additional Information

AIM

Description	America OnLine Instant Messenger (AIM) is a desktop chat application that allows AOL account holders to chat with one another and transfer files.
Recovery method	Carving

Attribute	Description
Fragment	An HTML fragment of an AIM message.
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

AIM Chat Messages

Description	America OnLine Instant Messenger (AIM) is a desktop chat application that allows AOL account holders to chat with one another and transfer files.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the AIM chat message.
Recipient	The recipient of the AIM chat message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message	The message body.

Additional Information

Chatroulette

Description	Chatroulette is a web-based video chat service that connects users with random users.
Recovery method	Carving

Attribute	Description
Type	The type of message.
Content	The message content.
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Chatstep Messages

Description	Chatstep Messages contains messages recovered from the Chatstep web portal.
Recovery method	Carving

Attribute	Description
Sender	The message sender's username.
Direction	The direction of the message, if known.
Message	The message body.
Message Sent Time - Local Time	The time when the message was sent or received in local time. There is no date information recovered.
Attachment Name	The name of the attachment.
MIME Type	The MIME type for the attachment.
Sender IP Address	The IP address of the sender.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Discord Logged-in Account

Description	Discord Logged-in Account contains information about the user that is currently logged into Discord on the device. Information about other accounts that were previously logged into are not recoverable.
Recovery method	Parsing

Attribute	Description
User ID	The ID of the logged-in user.
User Name	The name of the logged-in user.
Email	The email address of the logged-in user.
Phone Number	The phone number of the logged-in user.
Locale	The locale of the logged-in user.
User Token	The authentication token of the logged-in user.
Platform	The cloud platform name.

Additional Information

Discord Messages

Description	Discord Messages contains information about messages and calls that are sent and received using Discord. Messages from some channels might be missing if they haven't been cached by the application. This artifact uses

	both parsing and carving techniques to recover messages.
Recovery method	Parsing

Attribute	Description
Sender	The username of the message sender.
Sender ID	The ID of the message sender.
Message	The message content. If the message sent is a sticker, the message will display 'Sticker(sticker name)'.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Last Edited Date/Time - UTC (yyyy-mm-dd)	If the message has been edited then this indicates the date and time when the last edit has occurred.
Message Type	The type of the message (Message or Call).
Channel ID	The ID of the channel that the message was sent in.
Attachment URL	If the message includes an attachment, then this value indicates the saved URL of the attachment.
Attachment Name	If the message includes an attachment, then this value indicates the file name of the attachment.
Embedded Content Title	If the message contains a link, then this then this value indicates the title that's displayed in the link preview.
Embedded Content	If the message contains a link, then this value indicates the descrip-

Attribute	Description
Description	tion that's displayed in the link preview.
Call End Date/Time - UTC (yyyy-mm-dd)	If the message was a call, this indicates the date and time that the call ended.
Pinned	Indicates whether a message is pinned (True or False).
Message ID	The Message ID of the message that this message is replying to.
Mentions	The user mentioned in the message, if present.
In Reply To	The Message ID of the message that this message is replying to.
Reactors	The users who reacted to this message, if any. The order of reactors does not correspond to the reactions used.
Reaction	The emojis that were used to react to the message, if any. If a custom emoji is used, the name of that emoji will be listed instead of the emoji itself.

Additional Information

Discord User

Description	Discord User contains expanded information about each Sender encountered in the Discord Messages artifact.
Recovery method	Parsing

Attribute	Description
User ID	The ID of the user.
User Name	The name of the user.
Name	The global name of the user.
Display Name	The display name of the user.
Bot Account	Indicates whether the user is a bot account.
Avatar	The photo used as the user's Avatar, converted to a JPEG.
Raw Data	The Avatar photo in it's original WebP format.
Platform	The cloud platform name.

Additional Information

Facebook Messenger Calls

Description	Facebook Messenger Calls contains call data recovered from Facebook Messenger.
Recovery method	Parsing

Attribute	Description
User Key	The user key of the call partner. If the call was made in a group chat, this field will be empty.
Thread Key	The thread key of the group where the call was made. If the call was made

Attribute	Description
	in a chat with only one other person, this field will be empty.
Partner Name	The name of the call partner. If the call was made in a group chat, this field will be empty.
Group Name	The name of the group where the call was made. If the call was made in a chat with only one other person, this field will be empty.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the call.
Call Duration	The duration of the call in a friendly text format. This field is left empty if the call wasn't answered.
Call Duration (Seconds)	The duration of the call in seconds. This field is left empty if the call wasn't answered.
Call Type	The type of the call. The call type is either a voice call or a group voice call.
Answered	Indicates whether the call was answered or not.
Direction	The direction of the call.
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).

Additional Information

Facebook Messenger Groups

Description	Facebook Messenger Groups contains data about group chats on Facebook Messenger.
Recovery method	Parsing

Attribute	Description
Application Name	The name of the application that generated the data (Facebook Messenger Desktop).
Thread Key	The thread key of the group.
Group Name	The display name of the group.
Participants	The IDs of the users that are a part of the group.
Participants User Names	The usernames associated with the participants of the group.
Sender(s)	The IDs of the users that recently participated in the group (for example, by sending a message).
Senders User Names	The usernames associated with the respective senders in the group.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The date and time of the last activity recorded in the group.
Message Count	The approximate number of messages in the group.

Additional Information

Facebook Messenger Messages

Description	Facebook Messenger Messages contains messages recovered from Facebook Messenger.
Recovery method	Parsing

Attribute	Description
Sender Name	The display name of the person sending the message.
Sender ID	The user ID of the person sending the message.
Receiver Name	The display name of the person receiving the message.
Group Name	The display name of the group receiving the message.
Receiver ID	The user ID of the person receiving the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time when message was sent.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time the message was deleted from the application.
Text	The text of the message.
Message Type	The type of message that was sent. If multiple attachments were sent together, this fragment indicates the number of attachments.

Attribute	Description
Send State	Represents whether the message was sent, received or queued.
Media Info	The information about the media that is found. This value can be a URL to the media, a file name, or a sticker ID.
Latitude	The latitude portion of the location data that is sent with the message.
Longitude	The longitude portion of the location data that is sent with the message.
Application Name	The name of the application that generated the data (Facebook Messenger Desktop).
Thread ID	The thread ID of the message. This is also the Facebook ID of the remote party.
Message ID	The internal unique message ID.
Message Source	The source of the message creation platform.
Attachment	The recovered attachment. If the attachment is a video, the video gets segmented into multiple files. Each segment gets collected for playback in Magnet AXIOM, but the actual file size might differ from the size that AXIOM reports due to the segmentation.

Additional Information

Facebook Messenger Users Contacted

Description	Facebook Messenger Users Contacted contains information about users contacted from the device using Facebook Messenger.

Recovery method	Parsing

Attribute	Description
User Key	The user key of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
Name	The display name of the user.
Username	The unique identifier of the user.
Profile Image	The profile image of the user.
Profile Picture URL	The URL of the user's profile picture.
Is App User	Identifies whether the user is using Facebook Messenger or not.
Is Friend	Identifies whenever the user is a friend of the local user.
Application Name	The name of the application that generated the data (Facebook Messenger Desktop).
Rank	User's rank within the app.

Additional Information

Google Talk

Description	Google Talk is an instant messaging service that provides both text and

	voice communication.
Recovery method	Carving

Attribute	Description
Message ID	The ID for the message.
Sender	The email address of sender.
Sender ID	The ID of sender.
Recipient	The email address of recipient.
Recipient ID	The ID of recipient.
Message	The content of message.
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

ICQ 10 Messages

Description	ICQ 10 Messages contains messages that the user sent and received using the ICQ 10 messaging application..

Recovery method	Parsing

Attribute	Description
Local User ID	The ICQ User ID of the local user.
Sender ID	The ICQ User ID of the message sender
Sender	The message sender's nickname.
Recipient ID	The ICQ User ID of the message recipient. If the message is part of a group conversation, then it is the ICQ ID of the group.
Recipient	The message recipient's nickname. If the message is part of a group conversation, then it is the name of the group.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Message	The content of the message.
Direction	The direction of the message.
Type	The type of message.
Duration (Seconds)	The duration of a call, if the message type is a call.
Group Chat ID	The ID of the group chat, if the message is part of a group conversation.
Media URL	A media URL link to any attachments sent.

Additional Information

Currently, it's not possible to determine whether the timestamp associated with a message is

Additional Information
the sent or received time. In addition, the recipient in a group conversation is the name of the group when the user first joined the group, and may not represent the current name of the group.

ICQ Messages

Description	ICQ Messages contains messages that the user sent and received using the ICQ messaging application.
Recovery method	Parsing and carving

Attribute	Description
Local User ID	The ID of the local user of the message.
Sender	The sender of the message.
Conversation Partner ID	The ID of the partner.
Sent Date/Time - UTC(yyyy-mm-dd)	The date and time when the message was sent.
Received Date/Time - UTC(yyyy-mm-dd)	The date and time when the message was received.
Message	The message's contents.
Direction	The direction of the message.
Type	The type of message
Status	The sent status of the message.
Group Chat ID	The ID of the group that the message is associated with.

Additional Information

Status will only be retrieved for ICQ 6 and ICQ 7.

iMessage Chats

Description	iChat (now iMessage) is a chat application on Mac that allows users to share files and communicate via text chat, video, and audio. iChat is standard on almost all Mac computers.
Recovery method	Parsing

Attribute	Description
Recipient	The recipient of the message.
Sender	The sender of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message content.
Type	The type of message.
Status	The sent status of the message.

Additional Information

iMessage Messages

Description	iMessage (previously iChat) is a chat application for Apple products that allows users to share files and to communicate via text chat, video, and audio. iMessage is standard on almost all Mac computers and iOS devices.
Recovery method	Parsing

Attribute	Description
Recipient	The recipient of the message.
Sender	The sender of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message content.
Type	The type of message.
Status	The sent status of the message.

Additional Information

IP Addresses - Audio/Video Calls

Description	IP Addresses of web audio/video calls show who a user was communicating with. Each instance of this artifact represents a single hop in the communication chain. By showing the relationship between multiple hops, you can determine where a call originated from and what the final des-

	tination was.
Recovery method	Carving

Attribute	Description
Call ID	The ID of the call.
Message ID	The ID of the message.
Domain	The domain used for the call.
Connection Type	The type of connection.
Origin IP Address	The originating IP address for this hop in the call.
Origin Port	The originating port for this hop in the call.
Destination IP Address	The destination IP address for this hop in the call.
Destination Port	The destination port address for this hop in the call.
Date/Time - UTC (yyyy-mm-dd)	The timestamp associated with this hop in the call.
Remote User ID	The unique ID of the remote user.
Communication Protocol	The communication protocol for this call (either UDP or TCP).
Metadata	Any additional details about the call.

Additional Information

KakaoTalk Chat Rooms - Windows

Description	KakaoTalk Chat Rooms contains a list of all chat rooms that the KakaoTalk has open.
Recovery method	Parsing

Attribute	Description
Chat ID	The ID of the chat room.
Room Name	The name of the room.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the last message was sent to the room.
Last Message	The last message that was sent to the room.
Chat Type	The type of chat room.
Number of Participants	The number of users in the chat room.
Participant IDs	The user IDs of all participants in the chat room.
Link ID	The link ID of the chat room.
Room Status	The status messages for the room.
Room Status Author	The user ID of the last user to change the room status.
Status Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the status message was updated.

Additional Information

If the KakaoTalk data is acquired using a Files and Folders scan, some data might not be available. In order for the email and password decryption option to work correctly, the account in question must be active on Kakao servers. If the account has been deactivated, AXIOM will not be able to obtain the decryption key. In this case, only the UserId decryption option will work.

KakaoTalk Contacts - Windows

Description	KakaoTalk Contacts contains a list of all the users associated with the KakaoTalk account.
Recovery method	Parsing

Attribute	Description
User ID	The user ID.
Account Type	The account type.
Screen Name	The user provided screen name.
Profile Image URL	A URL to the user's profile image.
Status Message	The status message of the contact.
Phone Number	The contact's phone number.
User Name	The known username of the contact.
Nickname	The nickname provided to the contact by the current user.

Attribute	Description
Hidden	Indicates whether or not the contact has been hidden.
Favorite	Indicates whether or not the contact is a favorite.
Link ID	The link ID of the contact.

Additional Information

If the KakaoTalk data is acquired using a Files and Folders scan, some data might not be available. In order for the email and password decryption option to work correctly, the account in question must be active on Kakao servers. If the account has been deactivated, AXIOM will not be able to obtain the decryption key. In this case, only the UserId decryption option will work.

KakaoTalk Messages - Windows

Description	KakaoTalk Messages contains messages sent or received using the KakaoTalk account.
Recovery method	Parsing

Attribute	Description
Sender ID	The ID of the sender.
Message ID	The message ID.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.

Attribute	Description
Message	The content of the message.
Message Type	The type of message.
Attachment	Any attachment information associated with the message.
Attachment URL	The URL that corresponds to the attachment.
Attachment ID	The KakaoTalk generated ID which uniquely identifies this attachment on the local machine.
Deleted	Indicates whether or not the message has been deleted.

Additional Information

If the KakaoTalk data is acquired using a Files and Folders scan, some data might not be available. In order for the email and password decryption option to work correctly, the account in question must be active on Kakao servers. If the account has been deactivated, AXIOM will not be able to obtain the decryption key. In this case, only the UserId decryption option will work.

KakaoTalk Pictures

Description	KakaoTalk Pictures contains the decrypted pictures that have been shared using KakaoTalk. The formats that are supported are described in the Pictures artifacts.
Recovery method	Parsing

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction	The Exif extraction status indicates the level of Exif extraction that was per-

Attribute	Description
Status	formed. Complete indicates that a full Exif extraction was performed. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS latitude coordinates of the camera where the picture was taken (extracted from Exif data).

Attribute	Description
Longitude	The GPS longitude coordinates of the camera where the picture was taken (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the pciture was taken (extracted from Exif data).
Exif Data	A searchable field for all raw exif properties.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

If the KakaoTalk data is acquired using a Files and Folders scan, some data might not be available. In order for the email and password decryption option to work correctly, the account in question must be active on Kakao servers. If the account has been deactivated, AXIOM will not be able to obtain the decryption key. In this case, only the UserId decryption option will work.

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

KakaoTalk Shared Pictures - Windows

Description	KakaoTalk Shared Pictures contains pictures sent or received using the KakaoTalk account. The actual picture content is available if the user downloads the picture locally. If the user does not download the picture locally, the content remains encrypted. If it's possible to decrypt the picture, you can see the decrypted content in KakaoTalk Pictures.
Recovery method	Parsing and carving

Attribute	Description
Message ID	The ID of the message that included the picture.
Chat ID	The ID of the chat room where the picture was shared.
Sender ID	The ID of the sender of the picture.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the picture was sent.
File Size (Bytes)	The size of the picture in bytes.
Thumbnail URL	A URL to a thumbnail of the picture.
Download Location	A filepath location to where the picture was saved.
Download Completed Date/Time - UTC (yyyy-mm-dd)	The date and time when the picture was downloaded.
Attachment URL	The URL that corresponds to the shared picture.
Deleted	Indicates whether or not the picture has been deleted.

Attribute	Description
File Extension	The extension of the picture.
MIME Type	The MIME type of the picture.
Attachment ID	The KakaoTalk generated ID which uniquely identifies this picture on the local machine.

Additional Information
If the KakaoTalk data is acquired using a Files and Folders scan, some data might not be available. In order for the email and password decryption option to work correctly, the account in question must be active on Kakao servers. If the account has been deactivated, AXIOM will not be able to obtain the decryption key. In this case, only the UserId decryption option will work.

LINE Pictures

Description	LINE is a desktop application that allows users to exchange text messages, graphics, video, and audio media. Line also allows users to make free VoIP calls, and hold free audio and video conferences.
Recovery method	Parsing

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.

Attribute	Description
File Extension	The extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.

Attribute	Description
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software that used to create or modify the picture. This could either be the OS version of the phone used to take the picture, or the name of the software that was used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera that was used to take the picture (extracted from Exif data).
Model	The model of the camera that was used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS latitude coordinates of the camera where the picture was taken (extracted from Exif data).
Longitude	The GPS longitude coordinates of the camera where the picture was taken

Attribute	Description
	(extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the picture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Lync / OC Calls

Description	Lync/OC is a business grade communication application created by Microsoft.
Recovery method	Carving

Attribute	Description
Remote Participant Email	The email of the remote participant.
Remote Participant Display Name	The display name of the remote participant.

Attribute	Description
Call Started Date/Time - Local Time (yyyy-mm-dd)	The date and time when the call was started, local to the system.
Call Ended Date/Time - Local Time (yyyy-mm-dd)	The date and time when the call ended, local to the system.
Duration (Seconds)	The duration of the call in seconds.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Lync / OC File Transfers

Description	Lync/OC is a business grade communication application created by Microsoft.
Recovery method	Carving

Attribute	Description
Type	The type of file.
Sender	The sender of the file.
Recipient	The recipient of the file.
File	The file name or path.
File Size (Bytes)	The size of the file.

Attribute	Description
Transfer Event Date/Time - Local Time (yyyy-mm-dd)	The start or end date time of the transfer.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Lync / OC Fragments

Description	Lync/OC is a business grade communication application created by Microsoft.
Recovery method	Carving

Attribute	Description
HTML Fragment	The HTML fragment of the conversation.

Additional Information

Lync / OC Messages

Description	Lync/OC is a business grade communication application created by Microsoft.
Recovery method	Carving

Attribute	Description
Sender Email	The email address of the sender.
Sender Display Name	The display name of the sender.
Body	The body of the message.
Sent Date/Time - Local Time (yyyy-mm-dd)	The date and time when the message was sent, local to the system.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Microsoft Teams Activity

Description	Microsoft Teams Activity contains interactions that occur between users on Teams. These interactions include messages, members added/removed from meetings, and meeting start/end events.
Recovery method	Parsing

Attribute	Description
Conversation ID	The unique identifier of the conversation.
Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was initiated.
Sender ID	The unique identifier of the sender.

Attribute	Description
Sender Display Name	The display name of the sender
Message Type	The type of the interaction.
Content	The content of the message or summary of the interaction.
Metadata	The JSON metadata from the database defining the interaction.

Additional Information

Microsoft Teams Direct Messages

Description	Microsoft Teams Direct Messages contains interactions that occur between users on Teams. These interactions include messages, members added/removed from meetings, and meeting start/end events.
Recovery method	Parsing

Attribute	Description
Sender ID	The unique identifier of the sender.
Sender Display Name	The display name of the sender
Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was initiated.
Content	The content of the message or summary of the interaction.

Attribute	Description
HTML Body	The HTML formatted content of the message.
Message Type	The type of the interaction.
Conversation ID	The unique identifier of the conversation.
Emotion	The emotion reactions to the message.
Metadata	The JSON metadata from the database defining the interaction.

Additional Information

Microsoft Teams Meeting Messages

Description	Microsoft Teams Direct Messages contains interactions that occur between users on Teams. These interactions include messages, members added/removed from meetings, and meeting start/end events.
Recovery method	Parsing

Attribute	Description
Sender ID	The unique identifier of the sender.
Sender Display Name	The display name of the sender
Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was initiated.

Attribute	Description
Content	The content of the message or summary of the interaction.
HTML Body	The HTML formatted content of the message.
Message Type	The type of the interaction.
Conversation ID	The unique identifier of the conversation.
Emotion	The emotion reactions to the message.
Metadata	The JSON metadata from the database defining the interaction.

Additional Information

Microsoft Teams Messages

Description	Microsoft Teams Messages contains information about messages sent and received between Teams members, and are recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Conversation ID	The unique identifier of the conversation.
Message ID	The unique identifier of the current message.
Local User	The username of the target user.
Sender ID	The unique identifier of the sender.

Attribute	Description
Sender Name	The name of the sender.
Recipient Name	The name of the recipient.
Recipient Email	The email of the recipient.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Content Type	The type of content in the message.
Message Text	The message text extracted from the HTML body.
HTML Body	The HTML body of the message.
Parent ID	The ID of the parent conversation.
Attachment URL	The URL of the attachment.
Attachments	The attachments.

Additional Information

Microsoft Teams Topic Messages

Description	Microsoft Teams Topic Messages contains interactions that occur between users in Microsoft Teams spaces, in the Teams section of the application. These interactions include messages, call started and ended logs, and updates to topics.
Recovery method	Parsing

Attribute	Description
Conversation ID	The unique identifier of the topic the message belongs to.
Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was initiated.
Sender ID	The unique identifier of the sender.
Sender Display Name	The display name of the sender
Topic	The name of the topic the message belongs to.
Space	The name of the space the message belongs to.
Space ID	The unique identifier of the space the message belongs to.
Message Type	The type of the message.
HTML Body	The HTML formatted content of the message.
Emotion	The emotion reactions to the message.
Content	The content of the message or summary of the interaction.
Metadata	The JSON metadata from the database defining the interaction.

Additional Information

mIRC Chat Logs

Description	mIRC is a chat client that allows users to communicate and share files on the IRC network.
Recovery method	Carving

Attribute	Description
Fragment	An HTML fragment of a MIRC chat log.
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

MSN Plus!

Description	MSN Plus! is a desktop chat application that allows Microsoft Acccount holders to chat with one another, transfer files and video conference. This is an older version of Windows Live Messenger.
Recovery method	Carving

Attribute	Description
Fragment	An HTML fragment of a MSN Plus! message.

Additional Information

MSN Protocol Fragments

Description	MSN Messenger (also known as Windows Live Messenger) is a desktop chat application that allows Microsoft Account holders to chat with one another, transfer files, and video chat.
Recovery method	Carving

Attribute	Description
Fragment	A fragment of an MSN protocol message.

Additional Information

Omegle

Description	Omegle is a free online chat website that allows users to communicate with strangers without registering.
Recovery method	Carving

Attribute	Description
Type	The type of message.
Message	The content or body of the message.
Source	The location of where the artifact was found.

Attribute	Description
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

ooVoo Chat History

Description	ooVoo is a desktop communication application.
Recovery method	Parsing

Attribute	Description
Message ID	The ooVoo unique message identifier.
Sender User ID	The ooVoo identifier of the sender.
Receiver User ID(s)	The ooVoo identifier of the recipient(s).
Chat Date/Time - UTC (yyyy-mm-dd)	The date and time of the conversation.
Message	The actual message content.
Message Type	The type of message that was sent. Some examples are: Chat, Video, Image, etc.
Message Direction	Indicates whether the message was sent (Outgoing) or received

Attribute	Description
	(Incoming).
Group Name	The name that is associated with a group conversation. If the chat is between two people the name will be empty.
Video URL	The address of the video that was sent in the message.
Image URL	The address of the image that was sent in the message.
Source	The location where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

ooVoo Contact List

Description	ooVoo is a desktop communication application.
Recovery method	Parsing

Attribute	Description
Display Name	The contact display name.
User ID	The contact's unique ooVoo identifier.

Attribute	Description
Status Message	A message set by the contact. This message can contain insight into how the person is feeling or share ideas and thoughts.
Birthday (yyyy-mm-dd)	The contact's birthday.
Phone Number	The contact's phone number.
Password	The contact's password stored as plain text.
Platform	The cloud platform name.

Additional Information

ooVoo Phone Book

Description	ooVoo is a desktop communication application.
Recovery method	Parsing

Attribute	Description
Contact Name	The name of the contact.
Phone Number	The contact's phone number
Source	The location where the artifact was found.

Attribute	Description
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Pal Talk

Description	Pal Talk is a desktop chat client.
Recovery method	Carving

Attribute	Description
Message	The message content.
Source	The location where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Pidgin Accelerators

Description	Pidgin Accelerators contains user-created keyboard shortcuts (accelerators) to perform actions within Pidgin more efficiently.
Recovery method	Parsing

Attribute	Description
Window	An identifier for the application window.
Type	The type of accelerator.
Data	A description of the accelerator that the user created.

Additional Information

Pidgin Accounts

Description	Pidgin Accounts contains user information that's recovered from Pidgin accounts, such as the name, password, and display picture.
Recovery method	Parsing

Attribute	Description
Protocol	The chat protocol of the account.
Name	The name of the account.

Attribute	Description
Password	The password of the account.
Alias	The user's nickname.
Status	The online status of the account.
Image	The user's display picture.

Additional Information

Pidgin Buddies

Description	Pidgin Buddies contains information about a user's Pidgin contacts.
Recovery method	Parsing

Attribute	Description
Name	The name of the contact.
Friends With	The users that the contact is friends with.
Group	The group(s) that the contact belongs to, if any.
Protocol	The contact's chat protocol.
Alias	The contact's nickname.
Last seen Date/Time - UTC (yyyy-mm-dd)	The last date and time that the contact was seen online.
Image	The contact's display picture.

Attribute	Description
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.
Evidence Number	The evidence number of the physical evidence that this artifact was recovered from.

Additional Information

Pidgin Chat

Description	Pidgin Chat contains Pidgin chat messages exchanged between users.
Recovery method	Parsing

Attribute	Description
Participants	The chat participants.
Sender	The sender of the message.
Message Sent Date/Time - Local Time	The date and time that the message was sent.
Message	The message content.
Image	The display picture of the sender, if found locally.
Downloaded Image	The display picture of the sender, downloaded from the Internet.

Attribute	Description
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.
Evidence Number	The evidence number of the physical evidence that this artifact was recovered from.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Pidgin Custom Smileys

Description	Pidgin Custom Smileys contains custom emoticons that a user creates and uses in Pidgin.
Recovery method	Parsing

Attribute	Description
Shortcut	The keyboard shortcut to insert the custom smiley.
Image	The custom smiley image.
Source	The location where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.

Attribute	Description
Evidence Number	The evidence number of the physical evidence that this artifact was recovered from.

Additional Information

Pidgin OTR Fingerprints

Description	Pidgin is a multi-account desktop chat application. It allows users to connect various accounts such as Google Talk, Facebook, and generic Jabber accounts.
Recovery method	Parsing

Attribute	Description
Local User	The local user of the account.
Participant	The chat participant.
Protocol	The chat protocol of the account
Participant Fingerprint	The unique fingerprint belonging to the participant's account, used for Off-the-Record authentication.
Secure Conversation	Indicates whether the users used the Off-the-Record protocol to encrypt messages.

Additional Information

Pidgin OTR Users

Description	Pidgin is a multi-account desktop chat application. It allows users to connect various accounts such as Google Talk, Facebook, and generic Jabber accounts.
Recovery method	Parsing

Attribute	Description
Local User	The local user of the account.
Protocol	The chat protocol of the account.
Instance Tag	A 32-bit value that represents the user's login location. If the user logs in to the same account from multiple locations, each location will have a unique tag to identify it.
Private Key	The local user's private key, used for Off-the-Record encryption.

Additional Information

QQ Chat

Description	QQ is a chat application with a large user base. QQ is extremely popular in Asia and boasts about 800 million users. While the chat logs are encrypted, chat messages can still be recvoered if they are saved to RAM, pagefile.sys, hiberfil.sys and unallocated areas. Because the chat messages are retrieved from volatile locations, not all have a date and time associated with them.

Recovery method	Carving

Attribute	Description
Message	The message content.

Additional Information

Second Life Chat

Description	Second Life is an online virtual world where users can create characters and interact with other users.
Recovery method	Carving

Attribute	Description
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
From User	The sender of the message.
Chat Partner	The conversation partner.
Message	The content of the message.
Source	The location where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.

Attribute	Description
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Signal Messages - Windows

Description	Signal Messages - Windows contains decrypted messages sent or received by a Signal user on Windows.
Recovery method	Parsing

Attribute	Description
Sender	The phone number of the sender.
Recipient(s)	The recipient(s) of the message. If this is not a phone number it will be a UUID tied to the recipient.
Conversation ID	A UUID identifying the conversation.
Conversation Name	The name of the conversation.
Conversation Type	The type of conversation.
Message	The message body.
Sent Date/Time - UTC (yyyy-mm-dd)	The date/time in UTC that the message was sent.

Attribute	Description
Received Date/Time - UTC (yyyy-mm-dd)	The date/time in UTC that the message was received.
Direction	The direction of the message.
File Name	The name of the attached file(s).
File Size (Bytes)	The size of the attached file(s).
File Type	The type of the attached file(s).
File Path	The path for the attached file(s).

Additional Information

Skype Accounts

Description	Information about the Skype accounts that are recovered, such as user info and when the account was created.
Recovery method	Parsing

Attribute	Description
Skype Name	The Skype name of the account.
Display Name	The display name of the account.
Full Name	The full name of the account.
Email(s)	The email of this account.

Attribute	Description
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date when the profile was created.
Last Online Date/Time - UTC (yyyy-mm-dd)	The last time that the account was online.
Birthday (yyyy-mm-dd)	The birthday of the account.
Gender	The gender of the account.
City	The city where the account is located.
State/Province	The state/province where the account is located.
Country	The country where the account is located.
Home Phone	The home phone of this contact.
Office Phone	The office phone of this account.
Mobile Phone	The mobile phone of this account.
Homepage	The homepage of this contact.
About Info	The about info of this contact.
Profile Last Modified On Date/Time - UTC (yyyy-mm-dd)	The date when the profile was last modified.
Mood Text	The text used to express mood.
Last Used On Date/Time - UTC (yyyy-mm-dd)	The last time that the account was used.
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	The time that the avatar was created.
Picture	The avatar for this contact.

Additional Information

Skype Activity

Description	Skype Activity contains interactions that occur between users on Skype. These interactions include messages, group interactions, calls, files sent/received, and SMS. Applies to Skype 8.1 and later.
Recovery method	Parsing and carving

Attribute	Description
Conversation ID	ID of this conversation.
Profile Name	The local user's profile name.
Sender	The username of the sender/initiator of the interaction.
Sender Email	The sender's email as given in the message (if available).
Recipient Name(s)	The recipients or targets of the interaction.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was initiated.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was last updated (for example, when a call ends).
Message Type	The type of the interaction.
Message	The content of the message or summary of the interaction.
Emotion Count	The number of reactions to the interaction (for example, likes,

Attribute	Description
	dislikes, emojis, and so on).
File Name	The name of any attached files associated with the interaction.
File Size (Bytes)	The size in bytes of any attached files.
Attachment	The attachment file (if applicable).
Attachment Data Recovered	Whether the attached file was recovered from the local filesystem.
Thumbnail URL	A URL that directs to the thumbnail picture (if applicable).
Call Duration (Seconds)	The length of the call in seconds (if applicable).
Metadata	The content of the message, if it consisted of interpreted data (that is, XML or JSON data, rather than plain text).

Additional Information

Skype Calls

Description	Information about Skype calls that occur between users.
Recovery method	Parsing and carving

Attribute	Description
Local Username	The user logged into Skype at the time of the call.
Call Initiator	The user who started the call.

Attribute	Description
Initiator Display Name	The display name of the user. This might be different from the user-name.
Recipient(s)	The users who accepted a call from the call initiator and participated in the call for a period of time.
Call Participants	The users who accepted and participated in the call from the call initiator for some duration.
Started Date/Time - UTC (yyyy-mm-dd)	Start time of the call.
Duration	Total duration of the Skype call.
Metadata	Additional details about the call extracted in XML format. This includes the duration of time each participant was in the call.

Additional Information

Skype Chat Messages

Description	Skype messages sent from one user to another.
Recovery method	Parsing and carving

Attribute	Description
Profile Name	Profile name of the caller
Message Sent Date/Time - UTC	The date and time the message was sent

Attribute	Description
(yyyy-mm-dd)	
Author	Author of the message
From Display Name	The display name of who sent the message
Message	The body of the message or a description of the action taken. For example, adding another participant to a group chat or sharing a file or picture.
Attachment Name	The name of the attachment that was sent. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Attachment Size (Bytes)	The size of the attached file, in bytes. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Metadata	Additional details about the action, extracted in its original XML format.
Message Status	The status of the message.
Message Type	Type of message
Chat ID	ID of this chat
Recipient	Recipient of the chat

Additional Information

Skype Chatsync Messages

Description	Skype messages sent from one user to another that are parsed from the chatsync directory.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local Skype user
Chat Initiator	The user that started the conversation
Chat Partner/Group Chat ID	The other user in the chat, or a group chat identifier
Message Type	Indicates the sent status of the message
Message	The content or body of the message
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent

Additional Information

Skype Chatsync Messages Carved

Description	Skype messages sent from one user to another that are carved from the chatsync directory.
Recovery method	Parsing

Attribute	Description
Message Type	Indicates the sent status of the message
Message	The content or body of the message
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Skype Contacts

Description	Information about Skype contacts that are recovered, which may or may not be added contacts.
Recovery method	Parsing and carving

Attribute	Description
Profile Name	Profile name of the user
Skype Name	Skype name of the contact

Attribute	Description
Display Name	Display name of this account
Is Blocked	Is this contact blocked?
Contact Added	Specifies whether the contact is an added contact or just cached into the database (1 if the contact was added, 0 otherwise). Contacts can be cached into the database for a variety of reasons (for example, as a 'suggested contact').
Full Name	Full Name of this account
Birthday (yyyy-mm-dd)	Birthday of this account
Gender	Gender of this account
City	City where this account is located
State/Province	State/Province this account is located
Country	Country this account is located
Home Phone	Home phone of this contact
Office Phone	Office phone of this account
Mobile Phone	Mobile phone of this account
PSTN Number	PSTN number of this contact
Email(s)	Email of this account
Homepage	Homepage of this contact
About Info	About info of this contact
Profile Loaded	Previously called "Profile Created On Date/Time", this attribute rep-

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	resents the date/time when a contact's profile is first created on the user's device. When the profile information is updated by the contact, the date in the database is also updated.
Mood Text	Text used to express mood
Last Online On Date/Time - UTC (yyyy-mm-dd)	Last time the account was online
Last used On Date/Time - UTC (yyyy-mm-dd)	Last time the account was used
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	Avatar created time
Image	Image for this contact

Additional Information

Skype File Transfers

Description	Files that are transferred from one user to another using Skype.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Partner Handle	The user name of the file transfer partner.
Partner Display Name	The display name of the file transfer partner
File Name	The file name being transferred
Type	The type of file being transferred
File Path	The path to the local file
Transferred File	The file that was transferred
File Size (Bytes)	The size of the file being transferred
Bytes Transferred	The number of bytes that were transferred
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date and time the file transfer was started
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date and time the file transfer completed
Status	The status of the file (for example, transfer, transferring or cancelled)

Additional Information

Skype Group Chat

Description	Information about the Skype group chats that a user is a part of.
Recovery method	Parsing and carving

Attribute	Description
Profile Name	The name of the user.
Chat ID	The group chat's unique identifier.
Participants	The participants of the chat.
Posters	The users that have posted to the chat.
Active Members	The currently active users of the group.
Chat name	The name of the chat.
Started Date/Time - UTC (yyyy-mm-dd)	The date and time the chat started.
Last Changed Date/Time - UTC (yyyy-mm-dd)	The date and time the chat was modified.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Skype IP Addresses

Description	IP addresses that are associated with a Skype user account.
Recovery method	Parsing and carving

Attribute	Description
Username	Username of Skype accounts
IP Addresses	IP Addresses for the Skype user
Date/Time - UTC (yyyy-mm-dd)	Date and time
IP Address Type	Type of IP address Local or Public

Additional Information
This artifact is no longer supported as of Skype 7.40.

Skype Media Cache

Description	Media content that gets sent from one Skype user to another.
Recovery method	Parsing

Attribute	Description
Chat ID	The group chat's unique identifier.
Profile Name	The name of the user.
Author	The author of the media message.
Recipient(s)	The recipient(s) of the media message.
From Display Name	The display name of the sender.
Message Sent Date/Time	The Date/Time the media message was sent.
MIME Type	The MIME type of the media sent.

Attribute	Description
File Size (Bytes)	The size of the media file sent in bytes.
Is Thumbnail	Whether the particular media recovered is a thumbnail.
Media URL	The URL of the media as stored in the Skype cloud.
Thumbnail URL	The URL of the thumbnail as stored in the Skype cloud.
Media	The media that was recovered.
Thumbnail	The thumbnail if the media recovered was a video file.

Additional Information

Skype Message History Exports

Description	Skype Message History Exports contains a history of a user's sent and received messages and attachments, as parsed from a message history export.
Recovery method	Parsing

Attribute	Description
Author	The Skype ID of the sender of the message.
Author Name	The display name of the sender of the message.
Recipient(s)	The recipient(s) of the message.
Message Sent Date/Time - UTC	The date and time that the message was sent.

Attribute	Description
(yyyy-mm-dd)	
Message	The body of the message.
Message Type	The data type of the message.
Conversation Name	The name of the group conversation the message was sent in.
Location Address	The name of the location in a geolocation message.
Temp File Name	The name of the attachment as it was downloaded in the export.
Attachment Name	The name of the attachment when it was sent in Skype.
Attachment Size (bytes)	The size of the attachment in bytes.
Attachment	The attachment file.
Local User ID	The Skype ID of the user whose data was exported.
_ThreadID	The Skype ID of the conversation.

Additional Information

Skype SMS

Description	SMS messages that a user sends or recieves using Skype.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Author	The author of the message
Message	The message content.
Target Number(s)	The recipient phone numbers
Status	The status of the message.
Reply-to Number	A phone number the recipients can reply to

Additional Information

Skype Voicemails

Description	Voicemails that a user sends or recieves using Skype.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Partner Handle	The user name of the conversation partner
Partner Display Name	The display name of the conversation partner
Subject	Identifies the subject of the voicemail
Message Sent Date/Time - UTC (yyyy-	The date and time the message was sent

Attribute	Description
mm-dd)	
Duration	The length of the voicemail
Allowed Duration	The maximum length allowed for the voicemail
Size	The size of the recording
Path	The file path of the voicemail
Type	Identifies whether the voicemail was received or sent.
Status	The status of the voicemail, recording or played for example.

Additional Information

Telegram Media - Windows

Description	Windows Telegram Media contains decrypted copies of encrypted cached picture files sent and received in conversations through the Telegram application.
Recovery method	Parsing

Attribute	Description
User ID	The internal User ID which separates one local Telegram account from another.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the encrypted cache file was created.
Picture	The decrypted jpeg data retrieved from the Telegram image cache.

Additional Information

TorChat

Description	TorChat is a chat application that allows users to anonymously chat through the TOR (onion-routed) network. Chat logs are recovered when logging has been used or messages have been delayed on the TOR network.
Recovery method	Parsing and carving

Attribute	Description
Local Date/Time	The local date and time of the message.
Sender	The sender of the message.
Receiver	The receiver of the message.
Message	The message content.

Additional Information

Trillian

Description	Trillian is a multi-protocol chat client for Windows desktop.
Recovery method	Carving

Attribute	Description
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Type	The type of message.
From User	The sender of the message.
To User	The conversation partner.
Message	The content of the message.
Chat Network	The chat network that the message was sent over. Trillian supports many chat networks.
Source	The location where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

WeChat Messages

Description	WeChat Messages contains stored messages for the WeChat application on a computer.
Recovery method	Carving

Attribute	Description
Sender User Name	The user name or ID of the sender, as assigned by the application.
Sender Nick-name	The display name of the sender, as defined by the user.
Recipient User Name	The user name of the person receiving the message.
Recipient Nick-name	The nickname of the person receiving the message.
Group Chat Name	The name of the group chat, if the message is sent in a group chat.
Group Chat ID	The unique ID of the group chat, if the message is sent in a group chat.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was created on the device.
Message	The content of the message. For Location, Notice, and Pay messages, this content will be extracted from XML data. Contact Card messages will dis-

Attribute	Description
	play the XML data for the contact.
XML Data	The raw XML data. Not supported on Computer.
Call Duration (Seconds)	The duration of voice and/or video call in seconds.
Type	The type of the message (Text, Picture, Audio, Friend Request, Contact Card, Video, Animated Emoticon, Location Data, Shared Information, Voice/Video Call, Sight Video, Group Voice/Video Call, Notice, Pay Message, or Location Sharing).
Account	The user name of the account that was used to send the message.
Latitude	The latitude of the location data sent within the message.
Longitude	The longitude of the location data sent within the message.
Attachment	The attachment (such as audio, video) associated with the message.
Attachment Data Recovered	Indicates whether attachment data was recovered (Yes or Null).
Attachment Path	The absolute path to recovered message attachments.
Content Format	The content format of successfully recovered audio file attachments. AXIOM Process will attempt to decode audio from SILK V3 to WAV. Successfully converted attachments are saved and playable in AXIOM Examine. Unconverted attachments are saved in their original format and can be manually decoded using another tool or method.

Additional Information
On OS X / Windows, the MD5 Hashed Partner Username, File, Call Duration, Latitude, Longitude, and Attachment Path attributes are always empty.

WhatsApp Messages - Windows

Description	WhatsApp Messages contains information about the messages that are sent and received by the user. The data in this artifact is carved from RAM and/or unallocated space and can be created by the desktop application or the web.
Recovery method	Carving

Attribute	Description
Chat Type	The audience of the message or call. Individual indicates one-on-one messages/calls, and Group indicates that the message or call involves more than one user.
Sender	The sender of the message. This value is a user ID for individual chats. If the message is recieved from a group, this value can be a group ID, or user ID of the sender. Messages sent by local user usually don't have a user ID.
Recipient	The message recipient. This fragment only used for group chats, using group ID value.
Message	The message text body.
ID	The unique message identifier.

Additional Information

To learn more about artifacts from WhatsApp Messenger, sign in to the Support Portal to read the article Artifact profile: WhatsApp Messenger.

Wickr Me Conversations

Description	Wickr Me Conversations contains details about all the Individual, Group, and Room conversations the local user is a part of.
Recovery method	Parsing

Attribute	Description
Conversation ID	The unique identifier for the conversation.
Participants	The names of all participants in the conversation.
Type	The type of conversation. Individual is used for 1-on-1 or group conversations, and Room is used for room conversations.
Name	The name of the Room.
Description	The description of the Room.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the last message for this conversation was read.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the conversation was last viewed and synced on the device.

Additional Information

To learn more about Wickr Me, see Artifact profile: Wickr Me.

Wickr Me Messages

Description	Wickr Me Messages contains decrypted and decoded messages sent or received by a Wickr Me user on Windows. These messages can include text messages, call logs, transmitted locations, attachments such as pictures and videos, voice messages, and more.
Recovery method	Parsing

Attribute	Description
Sender	The sender's Wickr username.
Recipient(s)	The recipient's Wickr username.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when this message was sent.
Message	The message content.
Message Type	The message type. This value is interpreted from the ZPRIMARYTYPE. This value can be: Text, Call, Attachment, Location, Key Verification, System Message, or Control (Group Conversation Events).
Chat Type	The type of the chat. This value can be Individual, or Room.

Attribute	Description
Room Name	The name of the chat room.
Direction	Indicates whether the message was incoming or outgoing.
Read	Indicates whether or not the message was read.
Call Status	The status of the call, if applicable. This value can be: Started, Completed, Missed, or Cancelled.
Attachment Name	The file name of the attachment included in the message, if applicable.
Attachment Path	The original file path of the encrypted attachment, if applicable.
Attachment	The decrypted attachment file, if applicable (can include photos, video, or voice messages).
Latitude	The latitude of the coordinates (for transmitted locations only).
Longitude	The longitude of the coordinates (for transmitted locations only).

Additional Information

To learn more about Wickr Me, see Artifact profile: Wickr Me.

Wickr Me Users

Description	Wickr Me Users contains details about the users the local user has interacted with in the app.
Recovery method	Parsing

Attribute	Description
User Name	The name of the user.
User ID	The ID of the user.
Starred	Dictates whether the user has been starred or not.
Hidden	Dictates whether the user is hidden/inactive or not.
Blocked	Dictates whether the user is blocked or not.
Bot Account	Dictates whether the user is a bot.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The date and time when the user was last active.
Profile Image	The profile image of the user.

Additional Information
To learn more about Wickr Me, see Artifact profile: Wickr Me.

Windows Live Messenger / MSN

Description	MSN Messenger (Windows Live Messenger) is a desktop chat application that allows Microsoft Acccount holders to chat with one another, transfer files and video conference.
Recovery method	Carving

Attribute	Description
Sender	The MSN Account of the sender.
Recipient	The MSN account of the recipient.
Message Sent Date/Time - UTC (yyy-mm-dd)	The date and time when the message was sent. This information is stored as the local time of the system and cannot be timezone converted.
Message	The content of the chat message.

Additional Information

Windows Live Messenger Chat - Mac

Description	MSN Messenger (Windows Live Messenger) is a desktop chat application that allows Microsoft Acccount holders to chat with one another, transfer files, and video conference.
Recovery method	Parsing

Attribute	Description
Message Sent Date/Time - Local Time (Date Format Unknown)	The date and time when the message was sent. This information is stored as the local time of the system and cannot be timezone converted.
Sender	The sender's name.
Message	The content of the chat message.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Windows Viber Calls

Description	Windows Viber Calls contains details about calls sent or received using the Viber application.
Recovery method	Parsing

Attribute	Description
Partner Phone Number	The number of the person or group that the call was with.
Partner Name	The name of the person or group that the call was with.
Partner Display Name	The display name of the person or group that the call was with.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the call was sent or received.
Direction	The direction of the call (Incoming or Outgoing).
Call Status	The status of the call. This value can be Answered, Unanswered, Missed or Declined.
Duration	The duration of the call.
Call Type	The type of the call. This value can be Audio, Video, or Viber Out.

Additional Information

Windows Viber Chat Messages

Description	Viber Chat Messages contains details about chat messages sent or received using the Viber. This artifact applies to Viber 9.x and lower.
Recovery method	Parsing

Attribute	Description
Partner Phone Number	The phone number of the person (or group) that the local user is chatting with.
Partner Name	The name of the person (or group) that the local user is chatting with.
Partner Display Name	The display name of the person (or group) that the local user is chatting with.
Subject	The subject of a message, currently only videos from a mobile device will have a subject.
Message Body	The body of the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was either sent or received.
Direction	The direction of the message (Incoming or Outgoing).
Read	Indicates whether the message been read by the user on the computer.
File Name	The name of the file attached to the message.
Attachment Path	The path to the attachment included with the message.

Attribute	Description
Attachment	The raw data for the attachment included with the message.
Latitude	The latitude of the user chatting with the local user.
Longitude	The longitude of the user chatting with the local user.

Additional Information

Windows Viber Contacts

Description	Windows Viber Contacts contains details about a user's contacts in the Viber application.
Recovery method	Parsing

Attribute	Description
Name	The name of the contact.
Display Name	The display name of the contact.
Avatar Path	The path to the user's avatar.
Avatar	The users avatar.
Number	The users telephone number.
Number Type	The type of the users number.

Additional Information

Windows Viber Group Members

Description	Viber Group Members contains details about group membership and group metadata for conversations made using Viber. It's important to note that group membership history is not recoverable, so it is hard to be certain of who may have received messages and attachments that were shared in a group chat.
Recovery method	Parsing

Attribute	Description
Member Name	The name of the person that belongs to the group.
Member Phone Number	The phone number of the person that belongs to the group.
Admin	Specifies whether the person has Administrator privileges for the group. Administrators are usually the creators of the group, but they can also be added by another Administrator.
Group Name	The name of the group that the person belongs to. Group names are optional in the Viber application, and if there is no group name this field will be blank.
Group Chat ID	The ID of the group. It can be used to sort or filter the member list to quickly see all members of any particular gorup. It can also be used to cross-reference with messages in the Windows Viber Messages artifact.
Group Type	The type of the group. This value can be Group, Community, or Public Account.

Attribute	Description
Group Tagline	The tagline that is meant to describe the group. This field only applies to Community and Public Account group types.
Group Origin	The country of origin of the group's creator. This field only applies to Community and Public Account group types.

Additional Information

Windows Viber Messages

Description	Viber Messages contains details about messages sent or received using the Viber. This artifact applies to Viber 9.x and higher.
Recovery method	Parsing

Attribute	Description
Sender	The phone number of the person (or group) that the local user is chatting with.
Sender Phone Number	The name of the person (or group) that the local user is chatting with.
Recipient	The display name of the person (or group) that the local user is chatting with.
Recipient Phone Number	The subject of a message, currently only videos from a mobile device will have a subject.

Attribute	Description
Group Chat Name	The name of the group with which the message was shared.
Group Chat ID	The ID of the group. It can be used to cross-reference with members in the Windows Viber Group Members artifact.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was either sent or received.
Message Body	The body of the message.
Subject	The subject of the message. A subject usually appears in various media-type messages.
Type	The type of the interaction. This value can be Message, Picture, Video, Sticker, Attachment, Group Chat Membership, Set Group Name, Set Group Icon, or Set Background.
Direction	The direction of the message (Incoming or Outgoing).
Read	Indicates whether the message has been read by the user on the computer.
File Name	The name of the exchanged file.
Attachment Path	The path to the attachment on the local user's computer. Sometimes the File Name is present but the Attachment Path is empty, which might indicate that an incoming attachment was not downloaded by the local user.
Attachment	The raw data for the attachment included with the message.
Latitude	The latitude of the sender.
Longitude	The longitude of the sender.

Additional Information

World of Warcraft Chat

Description	World of Warcraft (WoW) was created in 2004 by Blizzard Entertainment. It is a massively multiplayer online role-playing game (MMORPG) where users can communicate via chat within the game.
Recovery method	Carving

Attribute	Description
Type	The type of message (private or public).
From Name	The name of the sender.
To Name	The name of the recipient.
Message	The message content.
Channel	The channel that the message was sent over.
Local Player GUID	The local players GUID.
Remote Player GUID	The remote players GUID.
Source	The location where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Yahoo! Diagnostic Chats

Description	Yahoo Messenger Chat is a desktop chat application that allows Yahoo account holders to chat with other Yahoo users.
Recovery method	Carving

Attribute	Description
Local User	The local Yahoo account user.
Sender	The sender of the chat message.
Recipient	The recipient of the chat message.
Chat Sent Date/Time - Local Time	The local date and time that the chat was sent.
Message	The chat message body.
Command	The command associated with the chat message.
Type	The type of the chat message.
Room Name	The name of the chat room.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Yahoo! Messenger (Mac)

Description	Yahoo Messenger Chat is a desktop chat application that allows Yahoo Account holders to chat with other Yahoo users.
Recovery method	Parsing

Attribute	Description
Sender User Name	The Yahoo account of the sender.
Sender Display Name	The display name of the Yahoo account of the sender.
Recipient User Name	The Yahoo account of the receiver.
Recipient Display Name	The display name of the Yahoo account of the receiver.
Message Sent Date/Time - UTC (yyy-mm-dd)	The date and time that the message was sent.
Message	The content of the chat message.

Additional Information

Yahoo! Messenger - Group Chat

Description	Yahoo Messenger Chat is a desktop chat application that allows Yahoo account holders to chat with other Yahoo users.

Recovery method	Carving

Attribute	Description
Username	The Yahoo account of the sender.
Message Sent Date/Time - Local Time	The date and time when the message was sent. This information is stored as the local time of the system and cannot be timezone converted.
Message	The content of the chat message.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Yahoo! Messenger - Non-encrypted Chat

Description	Yahoo Messenger Chat is a desktop application that allows Yahoo account holders to chat with other Yahoo users.
Recovery method	Carving

Attribute	Description
User name	The Yahoo account of the sender.
Message Sent Date/Time - Local	The date and time when the message was sent. This information is stored as the local time of the system and cannot be timezone con-

Attribute	Description
Time	verted.
Sent Message Text	The content of the chat message.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Yahoo! Messenger Chat

Description	Yahoo Messenger Chat is a desktop chat application that allows Yahoo account holders to chat with other Yahoo users.
Recovery method	Carving

Attribute	Description
Local user	The user account of the current system that is being searched.
Sender	The Yahoo account of the sender.
Recipient	The Yahoo account of the receiver.
Message Sent Date/Time - UTC (yyy-mm-dd)	The date and time when the message was sent.
Message	The content of the chat message.

Additional Information

In Yahoo Messenger 11 and later, the user can save messages to the cloud or not at all. In either case, this prevents the recovery of actual message content for those versions of the app.

Yahoo! Messenger Diagnostic Logs

Description	Yahoo Messenger Chat is a desktop chat application that allows Yahoo account holders to chat with other Yahoo users.
Recovery method	Carving

Attribute	Description
Image	An image that was pulled from the diagnostic log.
Log Created Date/Time - Local Time	The date and time that the log entry was logged.
Local User	The local Yahoo account user.
Command	A number that represents a Yahoo diagnostic command.
Type	The type of the command.
Data	The data associated with the command.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Yahoo! Webmail Chat

Description	Yahoo Webmail Chat is a browser chat application that allows Yahoo Account holders to chat with other Yahoo users.
Recovery method	Carving

Attribute	Description
Sender	The sender of the chat message.
Recipient	The recipient of the chat message.
Message	The message being sent.
Status	The status of the webmail message.
Version	The version of the webmail chat.
Vendor ID	The ID of the vendor.
Session ID	The ID of the chat session.

Additional Information

Zoom Chat Messages

Description	Zoom Chat Messages contains details about Zoom chat messages sent outside of a meeting.
Recovery method	Parsing and carving

Attribute	Description
Sender Name	The name of the person who sent the message.
Sender ID	The ID of the person who sent the message.
Buddy ID	The ID of the person or group that the message was sent to.
Recipient Name	The name of the person who received the message.
Recipient ID	The ID of the person who received the message.
Group Chat ID	The ID of the group this message was sent in.
Message ID	The GUID of the message.
Message	The body of the message.
Message Date/Time - UTC (yyyy-mm-dd)	A timestamp that indicates when the message is sent or received, depending on whether the local user is the sender or receiver.
Sender	Indicates whether the message was sent by the local user or a remote user. This value can be Local User or Remote User.
Read	Specifies whether the message has been read (Yes or No).
Message Type	The type of message that was sent. This value can be Message, Picture, File, or Notification.
Attachment Name	The name of the attachment that was sent.
Attachment Local File Path	The local path where the attachment was saved. This is empty if the attachment was not saved.
Attachment	The contents of the attachment if it can be recovered.

Additional Information
Zoom clears its local storage of chat and meeting messages when the user signs out or when the application shuts down. In these cases, local data can't be recovered. However, if the machine is shut down without signing out or exiting the application, this data may still remain on the drive.

Zoom Meeting Messages

Description	Zoom Meeting Messages contains details about Zoom chat messages sent during a meeting.
Recovery method	Parsing and carving

Attribute	Description
Message ID	The GUID of the message.
Sender Name	The name of the person who sent the message.
Sender ID	The ID of the person who sent the message.
Receiver Name	The name of the person who received the message. If blank, the message was sent to everyone in the meeting.
Receiver ID	The ID of the person who received the message. If zero, the message was sent to everyone in the meeting.
Message	The body of the message.
Message Date/Time - UTC (yyyy-mm-dd)	A timestamp that indicates when the message is sent or received, depending on whether the local user is the sender or receiver.

Attribute	Description
Sender	Indicates whether the message was sent by the local user, or a remote user. This value can be Local User or Remote User.
Read	Specifies whether the message has been read (Yes or No).
Message Type	The type of message that was sent.
Conference ID	The ID of the meeting that the message was sent in.

Additional Information
Zoom clears its local storage of chat and meeting messages when the user signs out or when the application shuts down. In these cases, local data can't be recovered. However, if the machine is shut down without signing out or exiting the application, this data may still remain on the drive.

Zoom User Accounts

Description	Zoom User Accounts contains details about the local user's zoom account.
Recovery method	Parsing and carving

Attribute	Description
User ID	The unique identifier for the user.
User Name	The account's username.
Email	The email address associated with the account.

Attribute	Description
First Name	The user's first name.
Last Name	The user's last name.
Phone Number	The user's phone number.
Profile Image URL	The URL to the user's profile picture.
Downloaded Profile Image	The data for the profile picture.

Additional Information
Zoom clears its local storage of chat and meeting messages when the user signs out or when the application shuts down. In these cases, local data can't be recovered. However, if the machine is shut down without signing out or exiting the application, this data may still remain on the drive.

Connected Devices

Latent Wireless Geolocated WiFi Hotspots

Description	Latent Wireless Geolocated WiFi Hotspots contains information about WiFi hotspots that were discovered using a Latent Wireless device. Latent Wireless stores information about the hotspots in a database that Magnet AXIOM can parse for details about each hotspot.
Recovery method	Parsing

Attribute	Description
MAC Address	The MAC address of the detected WiFi hotspot.
First Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was first discovered.
Last Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was last seen.
Strongest Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was detected at its highest strength.
Network Name (SSID)	The SSID of the WiFi hotspot.
Channel	The WiFi hotspot channel.
RSSI	The received signal strength indicator for the WiFi hotspot.
Latitude	The latitude where the WiFi hotspot was detected.
Longitude	The longitude where the WiFi hotspot was detected.
Secure	Indicates whether the WiFi hotspot is secure.

Additional Information

LogMeIn Activity

Description	LogMeIn Activity records connection events that occur using the LogMeIn remote desktop client. These records can include remote sessions and file sharing events.
Recovery method	Parsing

Attribute	Description
Date/Time Local Time	The time in local time when the log line was recorded.
Activity Type	The type of the activity that was recorded. Session type indicates that the event is a remote session. SessionDateReport indicates that the recorded event is a session summary. FileShare type indicates that the recorded event was a file being shared with other users.
Connection Type	The type of connection that was used.
Status	Indicates the status of the file sharing event (only applies to FileShare activities).
Remote IP Address	The public IP address of the client server.
Local IP Address	The public IP address of the host server.
Connection State	The login or logout state of the connection.
OS Version	The OS version of the host.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Remote Desktop Protocol

Description	The Remote Desktop Protocol artifact can indicate whether a device accesses external network devices, or was accessed by external network devices. The data collected by this artifact is recovered from the Windows Event Log, as well as the Windows Registry.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID from the Windows Event Log.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the Registry Key associated with the Remote Desktop Protocol (RDP) connection was modified.
Direction	The direction (outgoing or incoming) of the RDP connection.
Event Description Summary	The description of the event recovered.
Origin Service Name	The windows service or local account that initiated the RDP connection.
Origin Domain Name	The local domain name of the service or user that initiated the RDP connection.
Origin IP Address	The IP address of the device that initiated the RDP connection.

Attribute	Description
Origin Port	The IP Port of the device that initiated the RDP connection.
Destination User Name	The username of the account that was remotely connected to.
Destination Domain Name	The user domain of the account that was remotely connected to.
Destination IP Address	The IP address of the device that was remotely connected to.
Destination Port	The IP Port of the device that was remotely connected to.
Event Data	The raw Windows Event Log data for the RDP connection.

Additional Information

Remote Desktop Protocol Bitmap Cache

Description	Remote Desktop Protocol Bitmap Cache provides a reconstruction of the RDP Bitmap Cache, which gives an indication of what may have been on screen during an RDP session.
Recovery method	Parsing

Attribute	Description
Preview	A reconstructed image of the contents of the Remote Desktop Protocol bitmap cache. The image is produced by concatenating the individual cache bitmap tiles in the order that we find them, so the image is expected to look fragmented.

Additional Information

TeamViewer Activity

Description	TeamViewer Activity contains information about incoming and outgoing remote connections using TeamViewer remote desktop software.
Recovery method	Parsing

Attribute	Description
Computer Name	The name of the local computer.
TeamViewer ID	The TeamViewer ID of the local computer.
Local User	The local computer user that was logged in during the connection.
Direction	The direction (incoming or outgoing) of the connection that the activity was part of.
Remote Computer Name	The name of the remote computer associated with the connection.
Remote TeamViewer ID	The TeamViewer ID of the remote computer associated with the connection.
Session Type	The type of connection (remote control or file transfer).
Date/Time - UTC (yyyy-mm-dd)	The date and time of the activity.
Activity	The TeamViewer activity being reported.

Additional Information

USB Devices

Description	USB Devices contains a history of all USB devices that have been connected to the system.
Recovery method	Parsing

Attribute	Description
Device Class ID	The class ID of the USB device.
Serial Number	The USB device serial number.
Class	The class of the device (USB, USBSTOR).
Last Connected Date/Time - UTC (yyyy-mm-dd)	The date and time when the device was last connected to the computer.
Device Description	The description of the device.
Friendly Name	The friendly name of the device.
Manufacturer	The manufacturer of the device.
Last Assigned Drive Letter	The last drive letter that was assigned to the device by Windows.
Volume GUID	The GUID of the volume.
VSN Decimal	The volume serial number in decimal notation.

Attribute	Description
VSN Hex	The volume serial number in hexadecimal notation.
Associated User Accounts	Any user accounts that have used the device.
First Connected Date/Time - Local Time (yyyy-mm-dd)	The date and time when the device was first connected.
First Connect Since Reboot Date/Time - UTC (yyyy-mm-dd)	The date and time when the device was first connected since the last reboot.
Install Date/Time - UTC (yyyy-mm-dd)	The date and time for each successive update of the device driver.
First Install Date/Time - UTC (yyyy-mm-dd)	The date and time that specifies when the device instance was first installed in the system.
Last Insertion Date/Time - UTC (yyyy-mm-dd)	The date and time when the device was last inserted into the system. This value was added in Windows 8.
Last Removal Date/Time - UTC (yyyy-mm-dd)	The date and time when the device was last removed from the system. This value was added in Windows 8.

Additional Information

Timestamps from USB Devices should always be verified against timestamps from other artifacts in your evidence source. To learn more about verifying timestamps and examining evidence from USB Devices, see Artifact profile: USB Devices.

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Your Phone Contacts

Description	Your Phone Contacts contains information about contacts synced from a mobile device to a computer using Your Phone. The Your Phone application can sync data from Android and iOS devices to computers running Windows 10.
Recovery method	Parsing

Attribute	Description
Display Name	The contact's display name.
Nickname	The contact's nickname.
Phone Number	The contact's phone number.
Type	The type of phone number associated with the contact, for example Home, Mobile, or Business.
Last Time Contacted Date/Time - UTC (yyyy-mm-dd)	The last time that this contact either sent a message to, or received a message from the synced device or local user since the Your Phone application was installed.
Number of Times Contacted	The number of times the synced device or local user either sent a message to, or received a message from the contact since the Your Phone application was installed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that this contact's details were modified.

Additional Information

Your Phone Devices

Description	Your Phone Devices contains information about the devices that are synced to the user's computer by using the Your Phone application.
Recovery method	Parsing

Attribute	Description
Application Version	The version of Your Phone running on the computer.
Last Run Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was last run on the computer.
Device Application Version	The version of the Your Phone companion application running on the device.
Device ID	A GUID identifier generated to uniquely identify devices within the Your Phone application.
Device Name	The name provided by the device and displayed in the user interface when referring to it.
Device Platform	The device's platform (Android or iOS).
Device Messages Synced Date	The date and time when the device last synchronized its messages data with Your Phone.
Computer Messages Synced Date	The date and time when the computer last synchronized its messages data with Your Phone.
Device Contacts Synced Date	The date and time when the device last synchronized its contacts data with Your Phone.

Attribute	Description
Computer Contacts Synced Date	The date and time when the computer last synchronized its contacts data with Your Phone.
Device Photos Synced Date	The date and time when the device last synchronized its picture data with Your Phone.
Computer Photos Synced Date	The date and time when the computer last synchronized its picture data with Your Phone.

Additional Information

Your Phone Pictures

Description	Your Phone Pictures contains information about pictures synced from a mobile device to a computer using Your Phone. The Your Phone application syncs the 25 most recently taken photos from Android and iOS devices to computers running Windows 10.
Recovery method	Not applicable

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.

Attribute	Description
Device ID	A GUID identifier generated to uniquely identify devices synced using the Your Phone application.
Device Name	The name of the device (as provided by the device) which is displayed in the user interface for Your Phone.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial

Attribute	Description
	indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
GPS Lon-	The GPS longitude coordinates of where the picture was taken (extracted

Attribute	Description
gitude	from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS Latitude (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicates whether the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.
Exif Data	A searchable field for all raw exif properties.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Your Phone SMS/MMS

Description	Your Phone SMS/MMS contains information about messages synced from a mobile device to a computer using Your Phone. The Your Phone application can sync data from Android and iOS devices to computers running Windows 10.
Recovery method	Parsing and carving

Attribute	Description
Sender	The phone number that sent the message.
Recipient(s)	The phone number(s) the message was sent to.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message content.
Message Direction	Indicates whether the message was sent or received by the synced device or local user.
Message Type	Indicates whether the message is SMS or MMS.
Message Status	Indicates whether the message has been read.
Attachment Name	The name of the attached file, if applicable (MMS only).

Additional Information

Custom

File Signature Mismatch (Audio)

Description	File Signature Mismatch (Audio) contains identified mismatches between a known file signature header and the extension (or lack thereof) for an audio file. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Container)

Description	File Signature Mismatch (Container) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a container. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Document)

Description	File Signature Mismatch (Document) contains identified mismatches

	between a known file signature header and the extension (or lack thereof) for a document. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Picture)

Description	File Signature Mismatch (Picture) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a picture. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.

Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file. If the MIME type is unknown, this defaults to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file. If the MIME type is unknown, this defaults to application/octet-stream. If there is no file extension, but the MIME type is known, a mismatch is is returned.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Video)

Description	File Signature Mismatch (Video) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a video. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

Documents

CSV Documents

Description	CSV Documents contains CSV documents (.csv) that are located on the system.
Recovery method	Parsing

Attribute	Description
File Name	The name of the CSV document.

Attribute	Description
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last modified.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was created.
File Content	The content of the CSV document.
Size (Bytes)	The size of the CSV document in bytes.
SHA1 Hash	The SHA1 hash of the contents of the document.
MD5 Hash	he MD5 hash of the contents of the document.

Additional Information
For information about supported formats, see Supported media and file types.

Google Docs

Description	Google Docs is a word processing suite available to all Google account holders.
Recovery method	Carving

Attribute	Description
File Name	The name of the file that was backed up.

Attribute	Description
Owner Email	The email address of the author of the file.
Owner Name	The name of the author of the file.
Last Edited Date/Time - UTC (yyyy-mm-dd)	The last date and time when the file was edited.
Last Modified By Local User Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was edited locally.
File Size	The size of the file.
Last Collaborator Name	The name of the last collaborator of the file.
Last Collaborator Email	The email address of the last collaborator of the file.

Additional Information

Hangul Word Processor

Description	Hangul Word Processor specifies information about files created using Hangul Word Processor.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the found file.

Attribute	Description
Password Required	Indicates whether the file requires a password to be opened.
Application Version	The version of the software used to create the file.
Preview Text	A preview of the file content that contains the first 1024 symbols.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was modified on the filesytem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was accessed on the filesytem.
File System Last Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesytem.
Title	The title field of the document.
Subject	The subject field of the document.
Author	The author field of the document.
Date String	The date field of the document.
Keyword	The keyword field of the document.
Additional Information	Any additional information that the author provided for the document. This information appears as the Other field in the software.
Last Saved By	The username of the last user that saved the file.

Attribute	Description
Document Created Date/Time - Local Time (yyyy-mm-dd)	The date and time when the file was originally created.
Preview Image	The preview image of the title page of the file.
File	The contents of the Hangul Word document.
MD5 Hash	A MD5 hash of the Hangul Word document.
SHA1 Hash	A SHA1 hash of the Hangul Word document.

Additional Information

For information about supported formats, see Supported media and file types.
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Microsoft Excel Documents

Description	Microsoft Excel is a spreadsheet processor developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.

Attribute	Description
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Size (Bytes)	The size of the document in bytes.
Saved Size (Bytes)	The size of the document (in bytes) that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title metadata.
Subject	The subject metadata.
Authors	The authors of the document.
Keywords	The keywords metadata in the document.
Comment	The comments metadata.
Last Author	The last author to edit the document.
Last printed Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was created, extracted from metadata within the document.

Attribute	Description
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information
For information about supported formats, see Supported media and file types.

Microsoft Office 365 MRU Document Requests

Description	Includes a user's most recently requested documents in Microsoft Office 365.
Recovery method	Parsing

Attribute	Description
UserID	User ID (InternetUID_LiveID or GUID_ADAL).
Locale	Locale of the current system when the file was requested.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	Date and time when the item was last accessed via web browser or office application.
Path	Path to the document.
Pinned	Indicates if the document has been pinned with a Yes or No value.

Attribute	Description
ServiceName	The name of the servce where the document is hosted.
URL	The Url to the document.
FileName	The file name of the document.
ResourceId	A unique ID for the document.
StorageClass	The type of Storage Host.
Application	The Application used to access the document.

Additional Information

Microsoft Office 365 MRU Documents

Description	Includes a user's most recently accessed documents in Microsoft Office 365.
Recovery method	Parsing

Attribute	Description
User ID	User ID (InternetUID_LiveID or GUID_ADAL).
Locale	Locale of the current system when the file was accessed.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	Date and time when the document was last accessed via web browser or office application.
Path	Path to the document.

Attribute	Description
Pinned	Indicates if the document has been pinned with a Yes or No value.
Service Name	The name of the service where the document is hosted.
URL	The URL to the document.
File Name	The file name of the document.
Resource ID	A unique ID for the document.
Storage Class	The type of storage host.
Application	The Application used to access the document.

Additional Information

Microsoft Office 365 MRU Place Requests

Description	Includes a user's most recently requested folders in Microsoft Office 365.
Recovery method	Parsing

Attribute	Description
UserID	User ID (InternetUID_LiveID or GUID_ADAL).
Locale	Locale of the current system when the folder was requested.

Attribute	Description
Last Accessed Date/Time - UTC (yyyy-mm-dd)	Date and time when the folder was last requested via web browser or office application.
Path	Path to the folder.
Pinned	Indicates if the folder has been pinned with a Yes or No value.
ServiceName	The name of the servce where the folder is hosted.
URL	The Url to the folder.
FileName	The file name of the folder.
ResourceId	A unique ID for the folder.
StorageClass	The type of Storage Host.
Application	The Application used to access the folder.

Additional Information

Microsoft Office 365 MRU Places

Description	Includes a user's most recently accessed folders in Microsoft Office 365.
Recovery method	Parsing

Attribute	Description
UserID	User ID (InternetUID_LiveID or GUID_ADAL).
Locale	Locale of the current system when the place was accessed.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	Date and time when the folder was last accessed via web browser or office application.
Path	Path to the folder.
Pinned	Indicates if the folder has been pinned with a Yes or No value.
ServiceName	The name of the servce where the document is hosted.
URL	The Url to the folder.
FileName	The file name of the folder.
ResourceId	A unique ID for the folder.
StorageClass	The type of Storage Host.
Application	The Application used to access the document.

Additional Information

Microsoft Office Backstage Items

Description	Microsoft Office Backstage Items are items that can be found in the Back-stage View of Microsoft Office applications.
Recovery method	Parsing

Attribute	Description
Item Name	The name of the file or folder.
Item Type	The type of the item (e.g. File, Folder)
File Extension	The file extension
Path	The location at which the original file or folder can be found within.
Author	The author of the file or folder
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file or folder was last modified (extracted from metadata within the file or folder).
Last Read Date/Time - UTC (yyyy-mm-dd)	The date and time when the file or folder was last read from (extracted from the metadata within the parent directory).
Resource ID	The position of the resource in relation to other resources.
Sharing Scope	The scope in which the file or folder has been shared.
Note	Indicates whether the file or folder is a OneNote item.
Remote Address	Indicates whether the file or folder is a remote item.

Additional Information

Microsoft PowerPoint Documents

Description	Microsoft PowerPoint is a presentation creator developed by Microsoft. This table captures documents created with PowerPoint, extracted from the filesystem and carved from unallocated space.

Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
File	The actual file.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Comment	The comments in the metadata of the file.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was last printed, extracted from metadata within the document.

Attribute	Description
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information
For information about supported formats, see Supported media and file types.

Microsoft Word Documents

Description	Microsoft Word is a word processor developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last accessed on the filesystem.

Attribute	Description
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last modified on the filesystem.
Size (bytes)	The size of the document.
Saved Size (bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title metadata.
Subject	The subject metadata.
Authors	The authors of the document.
Keywords	The keywords metadata in the document.
Comment	The comments metadata.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyy-mm-dd)	The date and time when the document was last printed (extracted from metadata within the document).
Last Modified Date/Time - UTC (yyy-mm-dd)	The date and time when the document was last modified (extracted from meta-data within the document).
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created (extracted from metadata within the document).
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Attribute	Description
Source	The location where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information
For information about supported formats, see Supported media and file types.

OpenOffice Calc Documents

Description	OpenOffice Calc Documents are spreadsheets similar to Microsoft Excel spreadsheets, but are created using OpenOffice Calc.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the document.
Created Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the file was created. This data is recovered from the <meta:creation-date> tag found in meta.xml.
Modified Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the file was modified. This data is recovered from the <dc:date> tag found in meta.xml.

Attribute	Description
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was modified. This data is recovered from the local ZIP file header for meta.xml.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Recovered Size (Bytes)	The recovered size of the document in bytes.
Password Required	Indicates whether the document is password protected.
Title	The title meta-data as set by the creator. This data is recovered from the <dc:title> tag found in meta.xml. Note that this value can be different from the name of the document.
Authors	The authors of the document. This data is recovered from the <meta:initial-creator> tag found in meta.xml.
Subject	The subject of the document as set by the creator. This data is recovered from the <dc:subject> tag found in meta.xml.
Keywords	The keywords metadata in the document. This data is recovered from the <meta:keyword> tag found in meta.xml.
Comment	The comments metadata. This data is recovered from the <dc:-

Attribute	Description
	description> tag found in meta.xml.
Editing Cycle	The number of times that the document has been edited. This data is recovered from the <meta:editing-cycles> tag found in meta.xml.
File	The actual file stored as an attachment.

Additional Information
For information about supported formats, see Supported media and file types. Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

OpenOffice Impress Documents

Description	OpenOffice Impress Documents are slide presentations similar to Microsoft PowerPoint presentations, but created using OpenOffice Impress.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the document.
Created Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the file was created. This data is recovered from the <meta:creation-date> tag found in meta.xml.
Modified Date/Time - Local Time (yyyy-mm-	The local date and time when the file was modified. This data is recovered from the <dc:date> tag found in meta.xml.

Attribute	Description
dd)	
Modified Date/Time - UTC (yyyy-mm-dd)	The UTC date and time when the file was modified. This data is recovered from the local ZIP file header for meta.xml.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Recovered Size (Bytes)	The recovered size of the document in bytes.
Password Required	Indicates whether the document is password protected.
Title	The title metadata as set by the creator. This data is recovered from the <dc:title> tag found in meta.xml. Note that this value can be different from the File Name value.
Authors	The authors of the document. This data is recovered from the <meta:initial-creator> tag found in meta.xml.
Subject	The subject of the document as set by the creator. This data is recovered from the <dc:subject> tag found in meta.xml.
Keywords	The keywords metadata in the document. This data is recovered from the <meta:keyword> tag found in meta.xml.

Attribute	Description
Comment	The comments metadata. This data is recovered from the <dc:-description> tag found in meta.xml.
Editing Cycle	The number of times that the document has been edited. This data is recovered from the <meta:editing-cycles> tag found in meta.xml.
File	The actual file stored as an attachment.

Additional Information
For information about supported formats, see Supported media and file types. Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

OpenOffice Writer Documents

Description	OpenOffice Writer Documents are documents similar to Microsoft Word documents, but are created using OpenOffice Writer.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the document.
Created Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the file was created. This data is recovered from the <meta:creation-date> tag found in meta.xml.
Modified Date/Time -	The local date and time when the file was modified. This data is

Attribute	Description
Local Time (yyyy-mm-dd)	recovered from the <dc:date> tag found in meta.xml.
Modified Date/Time - UTC (yyyy-mm-dd)	The UTC date and time when the file was modified. This data is recovered from the local ZIP file header for meta.xml.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Recovered Size (Bytes)	The recovered size of the document in bytes.
Password Required	Indicates if the document is password protected.
Title	The title metadata as set by the creator. This data is recovered from the <dc:title> tag found in meta.xml. Note that this can be different from the File Name value.
Authors	The authors of the document. This data is recovered from the <meta:initial-creator> tag found in meta.xml.
Subject	The subject of the document as set by the creator. This data is recovered from the <dc:subject> tag found in meta.xml.
Keywords	The keywords metadata in the document. This data is recovered

Attribute	Description
	from the <meta:keyword> tag found in meta.xml.
Comment	The comments metadata. This data is recovered from the <dc:-description> tag found in meta.xml.
Editing Cycle	The number of times that the document has been edited. This data is recovered from the <meta:editing-cycles> tag found in meta.xml.
File	The actual file stored as an attachment.

Additional Information

For information about supported formats, see Supported media and file types.
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

PDF Documents

Description	Portable Document Format (PDF) is a file format used to present documents in a manner independent of application software, hardware, and operating systems. This table captures documents in this file format, extracted from the filesystem and carved from unallocated space.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time -	The date and time that the file was created on the filesys-

Attribute	Description
UTC (yyyy-mm-dd)	tem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was created, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was last modified, extracted from metadata within the document.
File	The PDF file.
MD5 Hash	An MD5 hash of the PDF content.
SHA1 Hash	A SHA1 hash of the PDF content.

Additional Information

For information about supported formats, see Supported media and file types.

RTF Documents

Description	The information for each RTF document that was recovered from the search.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the RTF document.
File Size (Bytes)	The size of the RTF document in bytes.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the RTF document was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the RTF document was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the RTF document was last modified.
File Content	The contents of the RTF document.
MD5 Hash	A MD5 hash of the RTF content.
SHA1 Hash	A SHA1 hash of the RTF content.

Additional Information

For information about supported formats, see Supported media and file types.

Text Documents

Description	Text documents (.txt) that are located on the system.
Recovery method	Parsing

Attribute	Description
Filename	The name of the text document.
Size (Bytes)	The size of the text document in bytes.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was created.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.
File Content	The content of the text document.

Additional Information

For information about supported formats, see Supported media and file types.

Email and Calendar

Calendar Events (ICS)

Description	Calendar Events (ICS) contains information about events and appointments that are recovered from calendar .ics files. These files are used by many different email applications, including Outlook, Google Calendar, and Apple Calendar.
Recovery method	Parsing

Attribute	Description
ID	A unique ID for the calendar entry.
Type	The type of event (for example, Event, TODO, or Journal).
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was created.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the event starts.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the event ends.
Summary	A short summary of the event.
Description	A more complete description of the event.

Attribute	Description
Latitude	The latitude coordinates of the event's venue.
Longitude	The longitude coordinates of the event's venue.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was last modified.
Location Name	The name of the venue in which the event is held.
Organizer	The organizer of the calendar event.
Status	The current pending status of the event (for example, NEEDS-ACTION, ACCEPTED, DECLINED, TENTATIVEB, DELEGATED, COMPLETED, or IN-PROGRESS).
URL	The URL that is associated with the event.
Recurrence	Indicates whether the event is recurring.
Attendees	A list of attendees for the event.
Categories	The tags that are associated with the event.
Comment	A comment that the organizer writes for to the user.
Contact Label	A reference of contacts associated with the event.
Resources	A list of resources and equipment required for the event.
Timezone	The timezone in which the event is held.

Additional Information

EML(X) Files

Description	EML(X) Files contains the emails in .eml and .emlx formats, that have been found on the device.
Recovery method	Parsing and carving

Attribute	Description
To	The recipients of the email.
From	The sender of the email.
Date/Time	The date and time that the email was sent or received.
Subject	The subject of the email.
Body	The body of the email.
CC	The recipients that receive the email by CC.
BCC	The recipients that receive the email by BCC.
Headers	The raw email headers.
Importance	The email importance setting.
Last Read Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was last read, if the data is available.
MD5 Hash	An MD5 hash of the email content.
SHA1 Hash	A SHA1 hash of the email content.
Attachment Name(s)	A list of attachments on the email.

Additional Information

Gmail Email Fragments

Description	Gmail Email Fragments contains the Gmail email fragments that were recovered from a Windows or OS X computer.
Recovery method	Parsing

Attribute	Description
HTML Fragment	The HTML fragment of the email.

Additional Information

Gmail Webmail

Description	Gmail is a webmail website that allows users to send and receive emails.
Recovery method	Carving

Attribute	Description
Email(s)	The email addresses involved with the email. If the email status is received it stores the email address of the sender otherwise it stores the emails that the message was sent to.

Attribute	Description
Subject	The subject of the email.
Snippet	A snippet of the message. It displays the first words as they were being displayed in the Gmail Inbox page.
Sent Date/Time - Local Time	The local date and time of when the email was sent. This value is saved in the database as a string, so attempts to sort or filter the column may not behave as expected. Instead of sorting by date, the column sorts alphabetically.
Last Activity Date/Time	The date and time that the latest activity occurred. This value could represent the time that the email was sent or when it was received.
Status	The status of the email. The values can be Sent or Received for emails sent since 2018. If an email was sent before 2018, the possible values are Read or Unread.
Attachments	Information about attachments using the following format: file name (file type - file size).
Confidential	Indicates whether the email was sent in confidential mode.
Duration	For emails that are confidential, this attribute indicates how long that email is valid for (in days). This information is only recovered if all information about the confidential email is available.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Hotmail Webmail

Description	Hotmail is a web-based email client that allows users to send and receive emails. Hotmail was replaced by Outlook.com in 2012.
Recovery method	Carving

Attribute	Description
Type	The type of fragment found. This value can be one of the following: Contacts, Message, Folder view, Inbox Message, Edit Message, Plaintext Message Fragment, or Welcome Page.
HTML Fragment	The HTML fragment that was found.

Additional Information

Hushmail Fragments

Description	Hushmail Fragments contains fragments of messages sent and received using Hushmail. Recovered data can include the email sender, receiver, and message fragments.
Recovery method	Carving

Attribute	Description
Sender	The sender of the email.
Receiver	The receiver of the email.
Fragment	An HTML fragment of the email.

Additional Information

Hushmail Inbox

Description	Hushmail Inbox contains messages sent and received using Hushmail Webmail. Recovered data can include the email sender, receiver, subject, and timestamps.
Recovery method	Carving

Attribute	Description
Sender	The sender of the email.
Receiver	The receiver of the email.
Message Received Date/Time - UTC (yyyy-mm-dd)	The UTC date and time when the email was received.
Message Received Date/Time - Local Time	The local date and time when the email was received.
Subject	The subject of the email.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Mail.ru

Description	Mail.ru is a webmail provider.
Recovery method	Carving

Attribute	Description
Sender	The name of the sender.
Reciever	The name of the receiver.
Message Sent Date/Time - Local Time	The date and time when the message was sent.
Message	The actual message content.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Mail.ru Chat Non-Carved

Description	Mail.ru is a desktop communication application.
Recovery method	Carving

Attribute	Description
Local User	The name of the local user.
Name	The name of the group.
Source	The location where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Mail.ru Contacts

Description	Mail.ru is a desktop communication application.
Recovery method	Parsing

Attribute	Description
Local User	The name of the local user.
First Name	The first name of the contact.
Last Name	The last name of the contact.
Email	The email address of the contact.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The last time that user was seen online.
Locale	The location of the contact.

Additional Information

Mailinator Inbox Access

Description	Mailinator Inbox Access contains instances when a user accesess their Mailinator inbox. Mailinator is webmail service that allows users to send and receive emails anonymously.
Recovery method	Carving

Attribute	Description
Inbox	The inbox that was accessed.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the inbox was accessed.

Additional Information

Mailinator Snippets

Description	Mailinator Snippets contains fragments of email messages that are sent using Mailinator. Mailinator is webmail service that allows users to send and receive emails anonymously.
Recovery method	Carving

Attribute	Description
Sender Name	The name of the sender.
Sender Address	The email address of the sender.
Sender Mailserver IP	The IP of the sender's mail server.
Recipient Address	The email address of the recipient.
Subject	The subject of the email.
Boddy Snippet	A snippet of the email body.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the email was received.

Additional Information

MBOX Emails

Description	MBOX is the default format used in Linux mail clients such as Thunderbird.
Recovery method	Carving

Attribute	Description
Folder Name	The folder where the email is stored.
Sender	The sender of the email.
To	The recipients of the email.

Attribute	Description
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Subject	The subject of the email.
Body	The body of the email.
Date/Time	The date and time the email was sent or received.
Headers	The raw email headers.
Importance	The email importance setting.
Attachments	A list of attachments on the email.

Additional Information

Offline Gmail webmail

Description	Gmail is a webmail website that allows users to send and receive emails.
Recovery method	Parsing

Attribute	Description
From Address	The sender of the email.
To Address(es)	The recipients of the email.

Attribute	Description
cc Address(es)	The recipients of the email that were CC'd.
bcc Address(es)	The recipients of the email that were BCC'd.
Subject	The subject of the email.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was sent or received.
Status	The sent status of the email.
Email Body	The body of the email.

Additional Information

Outlook Appointments

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to appointments scheduled in Outlook.
Recovery method	Parsing

Attribute	Description
Sender Name	The person who requested the appointment.
Sender Exchange Account	The sender's Exchange account name.
Recipients	The recipients of the appointment invitation.
Subject	The subject of the appointment.

Attribute	Description
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the appointment starts.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the appointment ends.
Body	The body of the appointment description.
Recipients CC	The CC'd recipients of the appointment invitation.
Recipients BCC	The BCC'd recipients of the appointment invitation.
Companies	The companies involved in the appointment.
Attachments	The attachments for the appointment.
Locale	The location of the appointment.
Is All-Day Event	Indicates if the appointment is an all-day event.
Is Recurring	Indicates if the appointment is recurring.
Recurrence Pattern Description	Describes the recurrence pattern of the appointment, if applicable.
Sensitivity	Indicates if the appointment is sensitive.
Is Hidden	Indicates if the appointment is hidden.
Is Private	Indicates if the appointment is private.
Priority	The priority of the appointment.
Importance	The appointment importance setting.
MD5 Hash	An MD5 hash of the appointment.
SHA1 Hash	A SHA1 hash of the appointment.

Additional Information

Outlook Contacts

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to contacts stored in Outlook.
Recovery method	Parsing

Attribute	Description
Display Name	The contact's display name.
Customer ID	The customer ID of the contact.
Email Address 1	The contact's primary email address.
Email Display As 1	The display string of the contact's primary email address.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact details were last modified.
Company Name	The contact's company name.
Department Name	The contact's department name.
Title	The contact's job title.
Profession	The contact's profession.
Manager Name	The name of the contact's manager.

Attribute	Description
Office Location	The contact's office location.
Business Address	The physical address of the business.
Business Phone	The contact's business phone number.
Business Phone 2	The contact's secondary business phone number.
Business Fax	The contact's business fax number.
Business Homepage	The website of the contact's business.
Email Display Name 1	The display name of the contact's primary email address.
Email Address 2	The contact's secondary email address.
Email Display As 2	The display string of the contact's secondary email address.
Email Display Name 2	The display name of the contact's secondary email address.
Email Address 3	The contact's tertiary email address.
Email Display As 3	The display string of the contact's tertiary email address.
Email Display Name 3	The display name of the contact's tertiary email address.
Cellular Phone	The contact's mobile phone number.
Home Address	The contact's home address.
Home Phone	The contact's home phone number.

Attribute	Description
Home Phone 2	The contact's secondary home phone number.
Home Fax	The contact's home fax number.
FTP Site	The contact's FTP site.
Body	More information about the contact.
Attachments	Any attachments to the contact entry.
Last Modifier Name	The name of the person who last modified the contact details.
MD5 Hash	An MD5 hash of the contact.
SHA1 Hash	A SHA1 hash of the contact.

Additional Information

Outlook Emails

Description	Microsft Outlook is a personal information manager and email client. This table captures information related to emails sent and received in Outlook.
Recovery method	Parsing

Attribute	Description
Sender Name	The sender of the email.

Attribute	Description
Sender Email	The email address of the sender.
Recipients	The recipients of the email.
Subject	The subject of the email.
Sender Exchange Account	The sender's Exchange account name.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was created.
Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the email synced with the HxStore platform.
Submitted Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was submitted.
Delivered Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was delivered.
Last Modified Date/Time - UTC (yyyy-mm-	The date and time that the email was last modified.

Attribute	Description
dd)	
Body	The body of the email. For HxStore data sources that include email bodies deleted when an account was removed, the displayed value is the path where the email body was located on the file system.
Folder Name	The name of the folder where the email is stored.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Attachments	The list of attachments on the email. If a picture can't be previewed, it will be converted to a file type that can be previewed, and include the suffix 'converted_by_Magnet'. The original file will also be included.
Headers	The raw email headers.
Priority	The priority of the email.
Importance	The importance of the email.
Sensitivity	The sensitivity of the email.
Read	Indicates whether the email was opened and therefore marked as Read. Note that Outlook users can also manually mark emails as either Read or Unread.
MD5 Hash	The MD5 hash of the email.
SHA1 Hash	The SHA1 hash of the email.

Additional Information

Outlook Journals

Description	Microsft Outlook is a personal information manager and email client from Microsoft. This table captures information related to journal entries stored in Outlook.
Recovery method	Parsing

Attribute	Description
Creator Name	The name of the journal entry's creator.
Last Modifier Name	The name of the person who last modified the journal entry.
Subject	The subject of the journal entry.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the journal entry was last modified.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was created.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the journal entry was started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the journal entry was finished.
Type Description	The type of journal entry.
Duration (minutes)	The length of the journal entry, in minutes.
Body	The body of the journal entry.

Attribute	Description
Attachments	The list of attachments on the journal entry.
MD5 Hash	An MD5 hash of the journal entry.
SHA1 Hash	A SHA1 hash of the journal entry.

Additional Information

Outlook Notes

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to notes written and stored in Outlook.
Recovery method	Parsing

Attribute	Description
Creator Name	The name of the user who created the note.
Last Modifier Name	The name of the person who last modified the journal entry.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the note was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the journal entry was last modified.
Body	The body of the note.

Attribute	Description
MD5 Hash	An MD5 hash of the note.
SHA1 Hash	A SHA1 hash of the note.

Additional Information

Outlook Tasks

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to tasks created in Outlook.
Recovery method	Parsing

Attribute	Description
Owner	The owner of the task.
Companies	The company the owner belongs to.
Recipients	The recipients of the task.
Subject	The subject of the task.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the task was last modified.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time that the task was created.
Completed Date (yyyy-mm-dd)	The date the task was completed.

Attribute	Description
Start Date (yyyy-mm-dd)	The date the task was started.
Due Date (yyyy-mm-dd)	The due date of the task.
Status	The status of the task.
Percent Complete	The completeness of the task as a percentage.
Body	The content of the task body.
Attachments	Any attachments related to the task.
Is Complete	Indicates if the task is complete.
Actual Work (Minutes)	The actual amount of time it took to complete the task, in minutes.
Total Work (Minutes)	The total amount of time for the task, in minutes.
Mileage	The mileage that was travelled for the task.
Billing Information	The billing information for the task.
Delegator	The person who delegated this task to the user.
Delgation State	Indicates whether or not the task was delegated.
Creator Name	The name of the person who created the task.
Last Modifier Name	The name of the person who last modified the task.
Is Hidden	Indicates if the task is hidden.
Is Private	Indicates if the task is private.
Is Read-Only	Indicates if the task is readable but not writable.
Sensitivity	Indicates if the task is sensitive.

Attribute	Description
Is Team Task	Indicates if the task is for a team.
Is Recurring	Indicates if the task is recurring.
Recurrence Pattern Description	Describes the recurrence pattern of the task, if applicable.
Is Reminder Set	Indicates if a reminder is set for the task.
Reminder Date/Time - UTC (yyyy-mm-dd)	The date and time of the task reminder, if applicable.
Priority	The priority of the task.
Importance	The importance of the task.
MD5 Hash	An MD5 hash of the task.
SHA1 Hash	A SHA1 hash of the task.

Additional Information

Outlook Web App Email Fragments

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to emails sent and received from Outlook's web application.
Recovery method	Carving

Attribute	Description
Sender	The sender of the email.
Recipients	The recipient(s) of the email.
Subject	The subject of the email.
Server Timestamp	The timestamp of the email on the server.
Is Draft	Indicates if the email is a draft.
Fragment	The recovered raw email fragment.

Additional Information

Outlook Web App Inbox

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to the inbox viewed from Outlook's web application.
Recovery method	Carving

Attribute	Description
Participants	The participants of the email.
Subject	The subject of the email.
Server Timestamp	The timestamp of the email on the server.

Additional Information

Outlook Webmail Inbox

Description	Outlook.com (formerly hotmail.com) is a webmail website that allows users to send and receive emails.
Recovery method	Carving

Attribute	Description
Sender	The sender of the email.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was sent or received.
Displayed Date/Time - Local (yyyy-mm-dd)	The date and time that the user was shown on the webpage.
Subject	The subject of the message.
Status	The sent status of the email.

Additional Information

Windows Mail

Description	Windows Mail contains email messages sent or received using Windows Mail.
Recovery method	Parsing and carving

Attribute	Description
To	The recipients of the email.
From	The sender of the email.
Date/Time	The date and time that the email was sent or received.
Subject	The subject of the email.
Body	The body of the email. For HxStore data sources that include email bodies deleted when an account was removed, the displayed value is the path where the email body was located on the file system.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Headers	The raw email headers.
Importance	The email importance setting.
Read	The read status of the email. This value is displayed for emails from HxStore data sources.
MD5 Hash	An MD5 hash of the email content.
SHA1 Hash	A SHA1 hash of the email content.
Attachments	A list of attachments on the email.

Additional Information

Yahoo! Webmail

Description	Yahoo Mail is a web-based email client that allows users to send and receive emails.
Recovery method	Carving

Attribute	Description
Sender Name	The name of the sender.
Sender Email	The email of the sender.
Receiver Name	The name of the receiver.
Receiver Email	The email of the receiver.
Subject	The email subject.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was sent, received, or drafted.
HTML Fragment	An HTML fragment of the email.
Type	The type of message. Folder Listing indicates that the email was recovered from the Inbox view. Message indicates that the user was looking at an individual email. Compose indicates that the user was composing a message. Inbox Preview indicates that the message was displayed as a preview.

Additional Information

Encryption and Credentials

Encrypted Files

Description	Encrypted Files contains information about any files that have been recovered on the system that are encrypted. This artifact is not available in Magnet IEF.
Recovery method	Parsing

Attribute	Description
File Name	The name of the encrypted file.
File Size (Bytes)	The size of the encrypted file in bytes.
Detected File Type	The detected type of the encrypted file.
File Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the encrypted file was created on the filesystem.
File Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the encrypted file was last modified on the filesystem.
File Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the encrypted file was last accessed on the filesystem.
MD5 Hash	The MD5 hash of the file.
SHA1 Hash	The SHA1 hash of the file.

Additional Information

To learn more, see Search for encrypted files in Magnet AXIOM.

Encryption/Anti-forensics Tools

Description	Encryption/Anti-forensics Tools contains the encryption or anti-forensics tool(s) that have been found in the searched evidence.
Recovery method	Parsing

Attribute	Description
Filename	The name of the executable for the encryption or anti-forensics tool.
Software	The name of the encryption or anti-forensics tool.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the encryption or anti-forensics tool was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the encryption or anti-forensics tool was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the encryption or anti-forensics tool was last modified on the filesystem.

Additional Information

You can find a list of the applications that are supported by this artifact at Encryption/Anti-forensics tools.

Windows Stored Credentials

Description	Windows Stored Credentials recover and decrypt the stored credentials for Windows Users. At this time, only non-domain users are supported.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
Entry ID	The name of the entry.
Description	The description of the entry.
User Name	The username of the user who is associated with the entry.
Password	The password of the entry.
Target Service	The target service of the credential.
Type	The type of credential.
Persistence Level	The persistence level of the credential.
Size (Bytes)	The size of the document in bytes.
File Path	The file path containing the credential.
Current Modified Date/Time - UTC (yyyy-mm-dd)	The modified date and time recovered from the metadata of the file.
File Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created.

Attribute	Description
File Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was modified.

Additional Information

Location and Travel

Google Maps

Description	Google Maps is a free web service that allows users to get directions.
Recovery method	Carving

Attribute	Description
Search Query	The term that was searched for.
Starting Location	The starting location for navigation/directions.
Latitude	The latitude coordinate in decimal degrees.
Longitude	The longitude coordinate in decimal degrees.
Location Type	The type of location associated with the latitude and longitude values. Values can be 'Center of Map', 'Business' or 'Street View'.
Source Address	The source physical address.

Attribute	Description
Destination Address	The user's desired destination.
Route Type	Indicates how the user will travel (e.g. Car, bus, or bike).
Additional Address	Any additional addresses within the navigation.

Additional Information

Google Maps Tiles

Description	Google maps is a free web service that allows users to get directions.
Recovery method	Parsing and carving

Attribute	Description
Image	The actual picture content.
Latitude	The latitude coordinate in decimal degrees.
Longitude	The longitude coordinate in decimal degrees.
X Coordinate	The X coordinate value that Google uses to download the right tile.
Y Coordinate	The Y coordinate value that Google uses to download the right tile.
Zoom Level	The level that the user was zoomed in to the map. This value is the Z coordinate value that Google uses to download the right tile.

Additional Information

Media

AMR Files

Description	AMR Files contains voicemail messages or memos for both iOS and Android.
Recovery method	Carving

Attribute	Description
File Name	The name of the file the AMR was recovered from.
Size (Bytes)	The size of the AMR content.
MD5 Hash	An MD5 hash of the AMR content.
SHA1 Hash	A SHA1 hash of the AMR content.
Audio	The contents of an AMR file.
Media Duration (Seconds)	The duration of the audio clip in seconds.

Additional Information

For information about supported formats, see Supported media and file types. Media duration is calculated from the number of speech frames carved from the AMR data, where each speech frame has a duration of 20ms, as AMR files do not contain metadata for duration.

Audio

Description	Audio contains audio files that are recovered that use the .mp3 or .wav formats.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file.
File Extension	The extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was created.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was last modified.
File Size (Bytes)	The size of the audio file.

Attribute	Description
MD5 Hash	An MD5 hash of the audio content.
SHA1 Hash	A SHA1 hash of the audio content.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the audio clip in seconds (extracted from Exif data).
Exif Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio clip was first recorded (extracted from Exif data).
Exif Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio clip was edited (extracted from Exif data).
Timezone	The timezone setting on the recorder at the time when the audio clip was recorded (extracted from Exif data).
Software	The software used to record or modify the audio clip. This could either be the OS version of the phone used to record the audio clip or the name of the software used to edit the audio clip in post-production (extracted from Exif data).
Latitude	The GPS latitude coordinates of where the audio clip was recorded (extracted from Exif data).

Attribute	Description
Longitude	The GPS longitude coordinates of where the audio clip was recorded (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of where the audio clip was recorded (extracted from Exif data).
Exif Data	A searchable field for all raw Exif properties.

Additional Information
For information about supported formats, see Supported media and file types. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Carved Video

Description	Carved Video contains videos that are recovered using carving. Supported formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. Other container formats can also be recovered provided that their underlying packets are the same as one of the supported formats.
Recovery method	Parsing

Attribute	Description
Content Format	The format of the video.
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).

Attribute	Description
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
File Size (Bytes)	The size of the container and file.
Container Format	The format of the video container.
Saved Video Size (Bytes)	The size of the video that was saved to the database.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Additional Information
As of February 20 2020, this artifact will no longer be included under Videos. Carved Video functionality will be included in the Videos artifact instead.

Pictures

Description	Pictures contains pictures retrieved using either carving or parsing techniques.
Recovery method	Parsing and carving

Attribute	Description
Image	The image data that was recovered.

Attribute	Description
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial

Attribute	Description
	indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time when the picture was being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The latitude coordinate in decimal degrees.

Attribute	Description
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS latitude (extracted from Exif data).
Longitude	The longitude coordinate in decimal degrees.
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicating if the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.
Exif Data	A searchable field for all raw exif properties.

Additional Information

For information about supported formats, see Supported media and file types.
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.
To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

RealPlayer Library Assets

Description	RealPlayer Library Assets contains information about the items that have been added to the library. This artifact can reveal information about the user's interaction with the application.
Recovery method	Parsing

Attribute	Description
Type	The type of asset, such as video, photo, or folder.
Path	The path to the asset.
Title	The asset's title.
Original Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the imported asset was original created.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the asset was added to the library.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the asset was last accessed.

Attribute	Description
Exif Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the imported asset was created according to its file metadata.
Private	Indicates whether the asset is marked private.
Hidden	Indicates whether the asset is hidden.
Artist	The artist name associated with the asset, if applicable.
File Size (Bytes)	The size of the file in bytes.
Audio Format	The format of the asset's audio content (media files only).
Video Format	The format of the asset's video content (video files only).

Additional Information

RealPlayer Video History

Description	RealPlayer Video History contains information about the media files that were played using RealPlayer. This artifact can reveal information about the user's interaction with the application.
Recovery method	Parsing

Attribute	Description
Video URL	The URL of the video that was played, if streamed.
File Path	Th file path of the video, if it was played from the local

Attribute	Description
	filesystem.
File Name	The file name of the video, if it was played from the local filesystem.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time that the video was last viewed.
First Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time that the video was first viewed.

Additional Information

Thumbcache Pictures

Description	Thumbcache Pictures contains thumbnails and picture previews recovered from thumbcache_xx.db files. The artifact also contains metadata that is cross-referenced from the Windows Search Service database (Windows.edb) where possible.
Recovery method	Parsing

Attribute	Description
Thumbnail File	The name of the thumbnail picture as stored in the thumbcache_xx.db file.
Size (Bytes)	The size of the thumbnail picture in bytes.

Attribute	Description
Picture	The thumbnail picture data that was recovered.
File Name	The name of the file or folder that the thumbnail picture represents.
MIME Type	The MIME type of the file that the thumbnail picture represents. If the thumbnail did not come from a file, this value will be blank.
File Path	The path to the file or folder that the thumbnail picture represents.
File Extension	The extension of the file that the thumbnail picture represents. If the thumbnail did not come from a file, this value will be blank.
Original Width	The original width of the picture file that the thumbnail picture represents. If the thumbnail did not come from a file, this value will be blank.
Original Height	The original height of the picture file that the thumbnail picture represents. If the thumbnail did not come from a file, this value will be blank.
Skin Tone Percentage	The calculated percentage of skin tone in the thumbnail picture.
MD5 Hash	An MD5 hash of the thumbnail picture content.
SHA1 Hash	A SHA1 hash of the thumbnail picture content.
PhotoDNA Hash	The hash of the thumbnail picture content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

Videos

Description	Videos contains videos that are recovered using parsing or carving. Supported formats for parsing include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. Supported carving formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. For more information about supported video formats, see Supported media and file types.
Recovery method	Parsing

Attribute	Description
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
File Name	The name of the file.
File Extension	The extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was last accessed.
Last Modified Date/Time - UTC (yyyy-	The date and time when the video was last modified.

Attribute	Description
mm-dd)	
File Size (Bytes)	The size of the video.
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed, including potential metadata located at the end of the video. Partial indicates that only Exif information in the header section of the video file was recovered, which should only occur with very large videos (in excess of the limit set in the options screen). Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The resolution of the video (extracted from Exif data).
Original Height	The resolution of the video (extracted from Exif data).
Exif Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was first recorded (extracted from Exif data).
Exif Modified Date/Time -	The date and time when the video was edited (extracted from Exif data).

Attribute	Description
UTC (yyyy-mm-dd)	
Timezone	The timezone setting on the camera at the time of the video being recored (extracted from Exif data).
Software	The software used to record or modify the video. This could either be the OS version of the phone used to record the video or name of the software used to edit the video in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to record the video (extracted from Exif data).
Model	The model of the camera used to record the video (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to record the video (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS latitude coordinates of the camera where the video was recorded (extracted from Exif data).
Longitude	The GPS longitude coordinates of the camera where the video was recorded (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the video was recorded (extracted from Exif data).
MD5 Hash	An MD5 hash of the video content.

Attribute	Description
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.
Content Format	The format of the carved video.
Container Format	The format of the carved video container.
Saved Video Size (Bytes)	The size of the carved video that was saved to the database.
Exif Data	A searchable field for all raw exif properties.

Additional Information
If AXIOM Process is configured to save a set amount of data from carved videos, any generated MD5 and SHA1 hashes are based on the saved data, not the full video. This behavior might cause issues when searching for known video hashes, as the hash for a carved video will differ from the actual video if it exceeds the size limit set in AXIOM Process. To learn more about Exif data for videos, see Extracting Exif data from videos. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

VLC Recently Played Files

Description	VLC Recently Played Files contains information about the media files that are played using the VLC Media Player. This artifact can reveal information on the user's interaction with the application.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file that was played in the player.
File Path	The file path to the recently played file.
Resume Time (seconds)	The number of seconds played before the media file is paused or stopped. A value of -1 indicates that the file was watched completely. If the duration is less than 10 seconds, the Media Player will always set the value to 0.

Additional Information

Web Video Fragments

Description	This search recovers two distinct types of web-based video. Fragments of Flash video can be left behind by many video streaming sites, such as YouTube. RTMP Frame Fragments are frames left behind by streaming sites using the RTMP protocol (widely used by webcam chat sites, including Chatroulette and Camstumble). In this case, a thumbnail from a recovered video is displayed, as well as any relevant metadata. Videos can be exported to .FLV format to be played. Due to the nature of the data recovered, some video players will have issues playing the exported files. We recommend trying FFmpeg, VLC, and the GOM player.
Recovery method	Carving

Attribute	Description
Preview	A thumbnail preview of the video.

Attribute	Description
Content Recovered	The raw bytes that were recovered.
Metadata	Any metadata about the video.
Recovered Duration	The length of the video that was recovered.

Additional Information

Memory

Active Network Info (sockets)

Description	The Active Network Info (sockets) artifact can be used to detect listening sockets and identify active networks. For more information about the sockets utility, see https://-github.com/volatilityfoundation/volatility/wiki/Command-Reference#sockets.
Recovery method	Volatility

Attribute	Description
Process ID	The process ID (PID).
Local Port	The port that was opened by the socket.
Protocol	The transport layer protocol that the socket is listening for.

Attribute	Description
IP Address	The IP address associated with the socket.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the socket was created.

Additional Information

API Hooks (apihooks)

Description	The API Hooks (apihooks) artifact detects various styles of programming hooks. For more information about the apihooks utility, see https://-github.com/volatilityfoundation/volatility/wiki/Command-Reference-Mal#apihooks.
Recovery method	Volatility

Attribute	Description
Process ID	The process ID (PID).
Process Name	The name of the process where the hook is found.
Hook Mode	The hook mode that was used.
Hook Type	The hook type that was used.
Victim Module	The victim module.
Function	The function that called the hook.

Attribute	Description
Hook Address	The address in memory where the hook is located.
Hooking Module	The hooking module.
Assembly Instructions	The assembly instructions field.

Additional Information

Clipboard (clipboard)

Description	The Clipboard (clipboard) artifact recovers data that the user saves to their clipboard. For more information about the clipboard utility, see https://-github.com/volatilityfoundation/volatility/wiki/Command-Reference-Gui#clipboard.
Recovery method	Volatility

Attribute	Description
Text	The text that was saved to the clipboard.
Data	The hex representation of the data saved to the clipboard.
Session ID	The associated session ID.
Window Station	The window station field.
Format	The format of the data that is saved to the clipboard.
Handle ID	The handle ID field.
Object ID	The object ID field.

Additional Information

Command History (cmdscan)

Description	The Command History (cmdscan) artifact returns a history of commands that are run in the Command Prompt (cmd.exe). These results can help provide insight into an attack on the system. For more information about the cmdscan utility, see https://-github.com/volatilityfoundation/volatility/wiki/Command-Reference#cmdscan.
Recovery method	Volatility

Attribute	Description
Process ID	The process ID (PID).
Process Name	The name of the console host process (either csrss.exe or conhost.exe).
Command History Location	The location in memory where the command history is located.
Application Name	The name of the application (or the process that is using cmd.exe).
Flags	The flags field from cmdscan.
Command Count Total	The total number of commands that are recovered.
Last Added Command Number	The last added command number.

Attribute	Description
Last Displayed Command Number	The last displayed command number.
First Command	The first command.
Command Count Maximum	The maximum number of commands that the console saves (the default is 50).
Handles	The application process handle.
Command Number	The number for the command.
Command	A string that contains the command that was run.

Additional Information

Connection Scan (connscan)

Description	The Connection Scan (connscan) artifact contains information about network connections, both active and terminated. For more information about the connscan utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#connscan.
Recovery method	Volatility

Attribute	Description
Local Address	The local IP address.

Attribute	Description
Remote Address	The remote IP address.
Process ID	The process ID (PID).

Additional Information

Dynamically Loaded Libraries (dlllist)

Description	The Dynamically Loaded Libraries (dlllist) artifact contains information about the files that were loaded into memory. For more information about the dlllist utility, see https://-github.com/volatilityfoundation/volatility/wiki/Command-Reference#dlllist.
Recovery method	Volatility

Attribute	Description
Process Name	
Process ID	The process ID (PID).
File Path	The path to the executable.
Load Count	The load count. This value can help indicate whether the DLL was statically or dynamically loaded.
DLL Path	The path to the DLL.

Additional Information

Files (filescan)

Description	The Files (filescan) artifact contains information about the files that were loaded into memory. For more information about the psxview utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#filescan.
Recovery method	Volatility

Attribute	Description
Pointers	The number of pointers to the file.
Handles	The number of handles to the object.
Permissions	The permissions set on the file.
File Path	The path to the file.
File Name	The name of the file.

Additional Information

Hidden Processes (psxview)

Description	The Hidden Processes (psxview) artifact can help reveal processes that were hidden. For more information about the psxview utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference-Mal#psxview.
Recovery method	Volatility

Attribute	Description
Process ID	The process ID (PID).
Process Name	The name of the process.
Pslist	Indicates whether the process is found in Pslist.
Psscan	Indicates whether the process is found in Psscan.
Thrdproc	Indicates whether the process is found in Thrdproc.
Pspcid	Indicates whether the process is found in Pspcid.
Csrss	Indicates whether the process is found in Csrss.
Session	Indicates whether the process is found in Session.
Deskthrd	Indicates whether the process is found in Deskthrd.
End Date/Time	The date and time when the process ends.

Additional Information

Hidden/Residual Modules (modscan)

Description	The Hidden/Residual Modules (modscan) artifact scans memory for pool tags to reveal unloaded drivers or drivers that have been hidden/unlinked by rootkits. For more information about the modscan utility, see https://-github.com/volatilityfoundation/volatility/wiki/Command-Refer-ence#modscan.
Recovery method	Volatility

Attribute	Description
Driver Name	The name of the driver.
Base Address	The base address for the driver.
Size	The size of the driver.
File Path	The path to the driver.

Additional Information

Hidden/Terminated Processes (psscan)

Description	The Hidden/Terminated Processes (psscan) artifact can help reveal processes that were terminated or were hidden or unlinked by a rootkit. For more information about the psscan utility, see https://-github.com/volatilityfoundation/volatility/wiki/Command-Reference#psscan.
Recovery method	Volatility

Attribute	Description
Physical Offset	
Process Name	
Process ID	The process ID (PID).
Parent Process ID	The parent process ID.

Attribute	Description
PDB	The location of the PDB.
Process Start Date/Time	The date and time when the process started.
Process Exit Date/Time	The date and time when the process exited.

Additional Information

Image Info (imageinfo)

Description	The Image Info (imageinfo) artifact reveals high-level information about the memory image being scanned. For more information about the imageinfo utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#imageinfo.
Recovery method	Volatility

Attribute	Description
Suggested Profiles	The suggested Volatility profiles you should use with this memory image.
KDBG Address	The address for the KDBG structure.
Image Date/Time	The date and time that the image was created.
Image Date/Time - Local Time	The date and time that the image was created in local time.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

LDR Modules (ldrmodules)

Description	The LDR Modules (ldrmodules) artifact can help reveal DLLs that have been hidden with malicious intent. For more information about the ldrmodules utility, see https://-github.com/volatilityfoundation/volatility/wiki/Command-Reference-Mal#ldrmodules.
Recovery method	Volatility

Attribute	Description
Process ID	The process ID (PID).
Process Name	The name of the process.
Base Address	The base address.
In Load	Indicates whether the PE file is found in the Load list.
In Init	Indicates whether the PE file is found in the Init list.
In Memory	Indicates whether the PE file is found in the Memory list.
Mapped Path	The mapped path to the PE file.
Load Path	The path to the Load file.
Init Path	The path to the Init file.
Memory Path	The path to the Memory file.

Additional Information

Loaded Kernel Modules (modules)

Description	The Loaded Kernel Modules (modules) artifact shows the kernel drivers that are loaded on the system. For more information about the modules utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#modules.
Recovery method	Volatility

Attribute	Description
Driver Name	The name of the driver.
Base Address	The base address.
Size	The size of the kernel.
File Path	The path to the kernel.

Additional Information

Malware Finder (malfind)

Description	The Malware Finder (malfind) artifact can help reveal hidden or injected code/DLLs in memory. For more information about the malfind utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference-Mal#malfind.

Recovery method	Volatility

Attribute	Description
Process ID	The process ID (PID).
Process Name	The name of the affected process.
Vad Tag	The VAD tag (virtual address descriptor) for the memory segment.
Protection	The protection level.
Flags	Flags that are set on the memory segment.
Assembly Instructions	The assembly language representation of the memory segment.

Additional Information

Network Connections (connections)

Description	The Network Connections (connections) artifact can be used to recover information about active TCP connections. For more information about the connections utility, see https://-github.com/volatilityfoundation/volatility/wiki/Command-Refer-ence#connections.
Recovery method	Volatility

Attribute	Description
Local IP Address	The local IP address.
Remote IP Address	The remote IP address.
Process ID	The process ID (PID).

Additional Information

Network Connections (sockscan)

Description	The Network Connections (sockscan) artifact can be used to detect sockets used in network connections. For more information about the sockscan utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#sockscan.
Recovery method	Volatility

Attribute	Description
Process ID	The process ID (PID).
Local Port	The local port used by the socket.
Protocol	The transport layer protocol that the socket is listening for.
IP Address	The IP address associated with the socket.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the socket was created.

Additional Information

Network Info (netscan)

Description	The Network Info (netscan) artifact can be used to recover network details from memory, such as TCP or UDP listeners and endpoints. For more information about the netscan utility, see https://-github.com/volatilityfoundation/volatility/wiki/Command-Refer-ence#netscan.
Recovery method	Volatility

Attribute	Description
Protocol	The protocol used for communication.
Local IP Address	The local IP address.
Remote IP Address	The remote IP address.
State	The state of the connection.
Process ID	The process ID (PID).
Owner	The application or process that owns the connection.
Created Date/Time	The date and time that the connection was established.

Additional Information

Open Handles (handles)

Description	The Open Handles (handles) artifact can be used to show the active handles in a process. For more information about the handles utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#handles.
Recovery method	Volatility

Attribute	Description
Process ID	The process ID (PID).
Virtual Offset	The offset in memory.
Handle ID	An identifier for the handle.
Access	The access number.
Handle Type	The type of handle.
Details	Additional details about the handle.

Additional Information

Process Security Identifiers (getsids)

Description	The Process Security Identifiers (getsids) artifact can be used to recover the SIDs (security identifiers) associated with a process. SIDs can be useful in identifying processes that have their privileges escalated with malicious intent. For more information about the getsids utility, see

	https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#getsids.
Recovery method	Volatility

Attribute	Description
Process ID	The process ID (PID).
Application Name	The name of the application that the SID is associated with.
Security ID	The security ID (SID).
Security Identifier	The security identifier level. Some examples include Users, Administrators, or Everyone.

Additional Information

Processes (pslist)

Description	The Processes (pslist) artifact contains information about the processes that are loaded into memory. For more information about the pslist utility, see https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#pslist.
Recovery method	Volatility

Attribute	Description
Process Name	The name of the process.
Process ID	The process ID (PID).
Parent Process ID	The ID of the parent process (PPID).
Number of Threads	The number of threads that the process contains.
Handles	The number of handles that the process has.
Session ID	The session ID for the process.
WoW64 Process	Indicates whether the process is a WoW64 process.
Process Start Date/Time	The time when the process started.
Process Exit Date/Time	The time when the process exited.

Additional Information

Timeline (timeliner)

Description	The Timeline (timeliner) artifact scans a number of different sources in memory, such as processes, event logs, threads, and registry keys, and creates hits to help illustrate a timeline of the events. For more information about the timeliner utility, see https://-github.com/volatilityfoundation/volatility/wiki/Command-Refer-ence#timeliner.
Recovery method	Volatility

Attribute	Description
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the event starts.
Type	The source of the event.
Item Name	The name of the item, or a path to the item.
Details	Additional details about the item.

Additional Information

Operating System

$LogFile Analysis

Description	$LogFile Analysis provides a sequence analysis of the $LogFile data, condensing the data to draw definitive conclusions on file operations (i.e. file creation, deletion, moving, renaming, and writing).
Recovery method	Parsing

Attribute	Description
File Operation	The file operation that occurred.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time that the file operation occurred.
MFT Record Number	The MFT Record number for the file in this operation.

Attribute	Description
MFT Reference Number	The MFT Reference number for the file in this operation.
Update Sequence Number	The Update Sequence Number (USN) associated with this file operation.
Starting LSN	The starting Log Sequence Number (LSN) associated with this operation.
Original Short File Name	The original state of the file name (8.3 filename format).
Original File Name	The original state of the file name (long filename format).
Original MFT Modified Date/Time - UTC (yyyy-mm-dd)	The original state of the MFT Modified Date/Time field as stored in the MFT.
Original Created Date/Time - UTC (yyyy-mm-dd)	The original state of the Created Date/Time field as stored in the MFT.
Original Modified Date/Time - UTC (yyyy-mm-dd)	The original state of the Modified Date/Time field as stored in the MFT.
Original Accessed Date/Time - UTC (yyyy-mm-dd)	The original state of the Accessed Date/Time field as stored in the MFT.
Original Parent MFT Record Number	The original Parent MFT Record number as stored in the MFT.
Original Parent MFT Reference Number	The original Parent MFT Reference number as stored in the MFT.
Current Short File Name	The current state of the file name (8.3 filename

Attribute	Description
	format).
Current File Name	The current state of the file name (long filename format).
Current MFT Modified Date/Time - UTC (yyyy-mm-dd)	The current state of the MFT Modified Date/Time field as stored in the MFT.
Current Created Date/Time - UTC (yyyy-mm-dd)	The current state of the Created Date/Time field as stored in the MFT.
Current Modified Date/Time - UTC (yyyy-mm-dd)	The current state of the Modified Date/Time field as stored in the MFT.
Current Accessed Date/Time - UTC (yyyy-mm-dd)	The current state of the Accessed Date/Time field as stored in the MFT.
Current Parent MFT Record Number	The current Parent MFT Record Number as stored in the MFT.
Current Parent MFT Reference Number	The current Parent MFT Reference Number as stored in the MFT.

Additional Information

.DS_Store Records

Description	.DS_Store Records contains all the records extracted from .DS_Store files found on the computer. Each record represents a property of a file or a folder. The significance of this artifact is an indicator of high likelihood that the user of the computer was aware of these files and folders with a pos-

	sibility of attributing a date to that awareness.
Recovery method	Parsing

Attribute	Description
Record Name	The name of the file or folder as stored in the .DS_Store file.
Record Type	The type of the record, or property, that is being logged in the .DS_Store file for a particular file or folder.
Record Value	The value of the property for the given file or folder.
Record Path	The full path to the file or folder.
.DS_Store Created Date/Time - UTC (yyyy-mm-dd)	The created date of the .DS_Store file from which the record was extracted.
.DS_Store Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date of the .DS_Store file from which the record was extracted.
.DS_Store Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date of the .DS_Store file from which the record was extracted.

Additional Information

In the Apple macOS operating system, .DS_Store (Desktop Services Store) is a hidden file that stores the display information of its containing folder, similar to the file desktop.ini in Microsoft Windows. The file tracks information such as icon positions, view settings, cached file size, cached last modified date, and even the choice of a background image. The .DS_ Store is created and maintained by the Finder application in any folder that it accesses, even

Additional Information
on remote file systems mounted from servers that share files (for example, via Server Message Block protocol or the Apple Filing Protocol). .DS_Store files are also included in archives created by macOS users, such as ZIP files, and they are backed up by some cloud file backup services. This means that the presence of .DS_Store Records artifacts on non-Mac evidence such as Windows, mobile, or cloud indicates that some of the data may have originated or have been accessed from a macOS computer at some point. For more information on .DS_Store files and their forensic significance see: .DS_Stores: Like Shellbags but for Macs.

AmCache Device Containers

Description	AmCache Device Containers contains information recovered from the AmCache about the devices that are connected to the system, such as printers, Bluetooth devices, and storage devices.
Recovery method	Parsing

Attribute	Description
Model Name	The model name for the device.
Model Number	The model number of the device.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the registry key was last updated.
Categories	The category of the device. Some examples are display.monitor, input.mouse, printfax.fax, and printfax.printer.

Attribute	Description
Discovery Method	The DiscoveryMethod property recovered from the registry subkey (value is a string).
Friendly Name	A display name for the device.
Icon	The path to the icon for the device.
Active	Indicates whether or not the device is active.
Connected	Indicates whether or not the device is connected.
Machine Container	Indicates whether or not the device is a machine container.
Networked	Indicates whether or not the device is networked.
Paired	Indicates whether or not the device is paired.
Manufacturer	The device manufacturer.
Model ID	The model ID of the device.
Primary Category	The PrimaryCategory property recovered from the registry sub-key (value is a string).
State	The State property recovered from the registry subkey (value is an integer).

Additional Information

AmCache Driver Binaries

Description	AmCache Driver Binaries contains information recovered from the AmCache about driver binaries on the system. These records can contain

	information about when a driver is signed, the company associated with the driver, and what service it is associated with.
Recovery method	Parsing

Attribute	Description
Driver Name	The name of the driver.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the registry key was last updated.
Driver Last Write Date/Time - UTC (yyyy-mm-dd)	The date and time that the driver was last written to.
Key	The registry key value.
Driver In Box	The DriverInBox property recovered from the registry sub-key (value is a string).
Driver Is Kernel Mode	Indicates whether the driver operates in kernel mode.
Driver Signed	Indicates whether the driver is signed.
Driver Checksum	The checksum of the driver.
Driver Company	The company that produces the driver.
Driver ID	The ID of the driver.
Driver Package Strong Name	The DriverPackageStrongName property recovered from the registry subkey (value is a string).
Driver Timestamp	The DriverTimeStamp property recovered from the registry subkey (value is an integer).

Attribute	Description
Driver Type	The driver type.
Driver Version	The driver version.
Image Size	The size of the driver file.
Inf	The Inf property recovered from the registry subkey (value is a string).
Product	The product that the driver is associated with.
Product Version	The product version.
Service	The service associated with the driver.
Wdf Version	The WdfVersion property recovered from the registry sub-key (value is a string).

Additional Information

AmCache Driver Packages

Description	AmCache Driver Packages contains information recovered from the AmCache about driver packages on the system.
Recovery method	Parsing

Attribute	Description
Key	The registry key value.

Attribute	Description
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key was last updated.
Date	The date of the driver package.
Class	The class of driver.
Directory	The directory where the driver can be located.
Driver In Box	The DriverInBox property recovered from the registry subkey (value is a string).
HWIDs	A list of associated hardware IDs.
Inf	The Inf property recovered from the registry subkey (value is a string).
Provider	The driver provider.
Submission ID	The SubmissionId property recovered from the registry subkey (value is a string).
SYSFILE	The SYSFILE property recovered from the registry sub-key (value is a string).
Version	The driver version.

Additional Information

AmCache File Entries

Description	AmCache File Entries contains information recovered from the AmCache

	about files that are used by executable programs.
Recovery method	Parsing

Attribute	Description
Name	The name of the file.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key was last updated.
File Extension	The extension of the file.
Program ID	The program ID of the program associated with the file.
Key	The registry key value.
Associated Application Name	The name of the application associated with the file.
SHA1 Hash	The SHA1 hash of the file. Note that the SHA1 Hash reported is based on the first 31,457,280 bytes of the executable reported. If the executable size exceeds this, the SHA1 for the complete EXE file on the disk will be different than what is reported by this artifact.
OS Component	Whether or not this file is an operating system component.
Full Path	The full path to the file.

Attribute	Description
Link Date	The link date of the file.
Product Name	The name of the product.
Size	The size of the file.
Version	The version of the file.
Product Version	The product version of the file.
Long Path Hash	The hash of the long path associated with the file.
Binary Type	The BinaryType property recovered from the registry subkey (value is a string).
PE File	Whether or not the file is a portable executable file.
Bin File Version	The binary file version.
Bin Product Version	The binary product version.
Language	The language code of the file.

Additional Information

To learn more about SHA1 hashes, see Understanding SHA1 hashes for AmCache File Entries.

AmCache File Entries - Legacy

Description	AmCache File Entries contains information recovered from the AmCache about files that are used by executable programs. This version of the artifact is for the older, legacy version of the AmCache.
Recovery method	Parsing

Attribute	Description
Name	The name of the file.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key was last updated.
File Extension	The extension of the file.
Program ID	The program ID of the program associated with the file.
Key	The registry key value.
Associated Application Name	The name of the application associated with the file.
SHA1 Hash:	The SHA1 hash of the file.
Full Path	The full path to the file.
Link Date	The link date of the file.
Product Name	The name of the product.
Size	The size of the file.
Version	The version of the file.

Attribute	Description
Product Version	The product version of the file.
Language	The language code of the file.
Volume GUID	The guid of the volume where the file is located.
Publisher	The publisher of the file.
Switch Back Context	The 4 property recovered from the registry subkey (value is an integer).
Description	The description of the file.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created.
Last Modified 2 Date/Time - UTC (yyyy-mm-dd)	The 17 property recovered from the registry subkey (value is a UTC timestamp).
PE Header Field Size Of Image	The field header size of the image for the portable executable.
Hash Of PE Header	The hash of the header of the portable executable.
PE Header Checksum	The checksum of the portable executable header.

Additional Information

AmCache Pnp Devices

Description	AmCache Pnp Devices contains information recovered from the AmCache about plug-n-play devices connected to the system.
Recovery method	Parsing

Attribute	Description
Driver Name	The name of the driver.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the registry key was last updated.
Description	The description of the device.
Key	The registry key value.
Bus Reported Description	The BusReportedDescription property recovered from the registry subkey (value is a string).
Class Value	The class of the device.
Class Guid	The GUID of the device class.
COMPID	The COMPID property recovered from the registry subkey (value is a string).
Container ID	The ID of the device container.
Driver ID	The ID of the driver.
Driver Package Strong Name	The DriverPackageStrongName property recovered from the registry subkey (value is a string).

Attribute	Description
Driver Date	The date of the driver.
Driver Version	The driver version.
Enumerator	The Enumerator property recovered from the registry subkey (value is a string).
HWID	The hardware ID of the device.
Inf	The Inf property recovered from the registry subkey (value is a string).
Install State	The InstallState property recovered from the registry subkey (value is a string).
Manufacturer	The device manufacturer.
Matching ID	The MatchingId property recovered from the registry subkey (value is a string).
Model	The device model.
Parent ID	The ParentId property recovered from the registry subkey (value is a string).
Problem Code	The ProblemCode property recovered from the registry subkey (value is a string).
Provider	The device provider.
Service	The Service property recovered from the registry subkey (value is a string).
STACKID	The STACKID property recovered from the registry subkey (value is a string).

Additional Information

AmCache Program Entries

Description	AmCache Program Entries contains information recovered from the AmCache about the applications that are run on the system.
Recovery method	Parsing

Attribute	Description
Name	The name of the program.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key was last updated.
Install Date	The date the program was installed.
Version	The program version.
Publisher	The program publisher.
Uninstall Date/Time - UTC (yyyy-mm-dd)	The date and time the program was uninstalled.
OS Version At Install Time	The version of the operating system when the program was installed.
Bundle Manifest Path	The path to the bundle manifest.
Hidden Arp	The HiddenArp property recovered from the registry sub-key (value is an integer).

Attribute	Description
Inbox Modern App	The InboxModernApp property recovered from the registry subkey (value is an integer).
Language	The language code of the program.
Manifest Path	The path to the manifest file.
Msi Package Code	The msi package guid.
Msi Product Code	The msi product guid.
Package Full Name	The full name of the package.
Program ID	The ID of the program.
Program Instance ID	The ID of the program instance.
Uninstall Registry Key Path	The path to the uninstall string in the registry.
Root Dir Path	The root directory path of the program.
Type	The type of program.
App Source	The source of the program.
Store App Type	The type of program in the store.
Uninstall String	The string that can be used to uninstall the program.

Additional Information

AmCache Program Entries - Legacy

Description	AmCache Program Entries contains information recovered from the

	AmCache about the applications that are run on the system. This version of the artifact is for the older, legacy version of the AmCache.
Recovery method	Parsing

Attribute	Description
Name	The name of the program.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key was last updated.
Install Date/Time - UTC (yyyy-mm-dd)	The date and time the program was installed.
Version	The program version.
Publisher	The program publisher.
Uninstall Date/Time - UTC (yyyy-mm-dd)	The date and time the program was uninstalled.
Language	The language code of the program.
Msi Package Code	The msi package guid.
Msi Product Code	The msi product guid.
Uninstall Registry Key Path	The path to the uninstall string in the registry.
Install Source	The source of the program installation.
File Entries	The file entries associated with the program.
File Paths	The file paths associated with the program.

Additional Information

AmCache Shortcuts

Description	AmCache Shortcuts contains information recovered from the AmCache about applications and file shortcuts are that are used on the system.
Recovery method	Parsing

Attribute	Description
Key	The name of the registry key.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the registry key was last updated.
Shortcut Path	The path to the shortcut.

Additional Information

Autorun Items

Description	The Autorun Items artifact describes the programs that are configured to run automatically when a certain system event occurs.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the program.

Attribute	Description
File Path	The file path to the program.
Command	The command executed when the trigger condition is met. For run items, this is the raw registry value.
Type	The type of autorun item.
Trigger Condition	The system event condition that triggers the autorun command.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the registry key containing the autorun item was last modified.
Enabled	Indicates whether or not this Autoruns item is enabled.
Embedded Signature	Indicates whether the program is digitally signed using an embedded digital signature as opposed to one signed utilizing a security catalog file.
MD5 Hash	The MD5 hash of the program.
Authenticode PE Image Hash	The PE Image hash of the program as read from within the digital signature format, Authenticode, if present. This hash is calculated using a Microsoft specified algorithm and is not equal to the hash of the entire program.
Issuer	The issuer of the digital signature, if present.
Signature	The digital signature of the issuer, if present.
Metadata	Additional information about the autorun items.

Additional Information

Cortana Person Reminders

Description	Cortana Person Reminders are reminders that can be set for a specific contact. Cortana triggers the reminders when an interaction with that contact occurs, such as when an email is received.
Recovery method	Parsing

Attribute	Description
Title	The title of the reminder.
Contact Name	The name of the contact associated with the reminder.
Status	The status of the reminder. The reminder can be active (either has not been triggered yet or is an ongoing reminder), deleted, or completed.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the person reminder was created.
Last Update Date/Time - UTC (yyyy-mm-dd)	The date and time when the person reminder was last updated.
Completion Date/Time - UTC (yyyy-mm-dd)	The date and time when the person reminder was completed.

Additional Information

Sometimes, the Creation Date / Time might appear to be after other Date / Time data. This behavior occurs if Cortana was disconnected and required the user to log back in. This reset creates a new Creation Time, but other Date / Time data will remain as it was.

Cortana Place Reminders

Description	Cortana Place Reminders are virtual areas that you can define in Cortana to represent a real geographic place. Entering or leaving an area can trigger Cortana to display the reminder.
Recovery method	Parsing

Attribute	Description
Title	The title of the reminder.
Location Name	The name of the location associated with the reminder.
Trigger Condition	The condition under which the reminder will be triggered, either arrival or departure.
Status	The status of the reminder. The reminder can be active (either has not been triggered yet or is an ongoing reminder), deleted, or completed.
Recurrence	The recurrence of the reminder. The reminder can recur on specific days of the week, or every time a user visits that location.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the place reminder was created.
Last Update Date/Time - UTC (yyyy-mm-dd)	The date and time when the place reminder was last updated.
Completion Date/Time - UTC	The date and time when the place reminder was completed.

Attribute	Description
(yyyy-mm-dd)	
Latitude	The latitude coordinates of the place reminder.
Longitude	The longitude coordinates of the place reminder.

Additional Information
Sometimes, the Creation Date / Time might appear to be after other Date / Time data. This behavior occurs if Cortana was disconnected and required the user to log back in. This reset creates a new Creation Time, but other Date / Time data will remain as it was.

Cortana Time Reminders

Description	Cortana Time Reminders are reminders that can be set for a specific time.
Recovery method	Parsing

Attribute	Description
Title	The title of the reminder.
Trigger Date/Time - UTC (yyyy-mm-dd)	The date and time that the time reminder is set to trigger.
Status	The status of the reminder. The reminder can be active (either has not been triggered yet or is an ongoing reminder), deleted, or completed.

Attribute	Description
Recurrence	The recurrence of the reminder. The reminder can recur on specific days of the week.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the time reminder was created.
Last Update Date/Time - UTC (yyyy-mm-dd)	The date and time when the time reminder was last updated.
Completion Date/Time - UTC (yyyy-mm-dd)	The date and time when the time reminder was completed.

Additional Information
Sometimes, the Creation Date / Time might appear to be after other Date / Time data. This behavior occurs if Cortana was disconnected and required the user to log back in. This reset creates a new Creation Time, but other Date / Time data will remain as it was.

Default Browser

Description	This table contains information about the default browser that is set on a computer.
Recovery method	Parsing

Attribute	Description
Program ID	The programmatic identifier of the default browser.
Program Name	The name of the default browser.

Additional Information

File Associations

Description	File Associations contais information about application associations for files. Users or applications can set associations for file types so that when a file of a specified file type is opened, a command gets triggered by Windows.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the program that is run when a file of the specified file type is opened.
File Path	A path to the program that is run when a file of the specified file type is opened.
Command	The command that is executed when a file of the specified file type is opened.
File Type	The file type that triggers the associated command to be executed.
Registry Key	The date and time when the registry key that contains the file association

Attribute	Description
Modified Date/Time - UTC (yyyy-mm-dd)	information was last modified.
Enabled	Indicates whether or not this Autoruns item is enabled.
Embedded Signature	Indicates whether the program is digitally signed using an embedded digital signature as opposed to one signed utilizing a security catalog file.
MD5 Hash	The MD5 hash of the program.
Authenticode PE Image Hash	The PE Image hash of the program as read from within the digital signature format, Authenticode, if present. This hash is calculated using a Microsoft specified algorithm and is not equal to the hash of the entire program.
Issuer	The issuer of the digital signature, if present.
Signature	The digital signature of the issuer, if present.

Additional Information

File System Information

Description	Information pertaining to the File System that was searched
Recovery method	Parsing

Attribute	Description
Volume Serial Number	This field only applies to FAT and NTFS file systems. This is a 32-bit unsigned int value that is stored in Bios Paramter Block (BPB) and is showed in a special hex format ï¿½ XXXX-XXXX (e.g. EABB-6573). For other file systems, the value of this field should show "n/a".
Full Volume Serial Number	This field is a 64-bit volume serial number that is only present in BPB of NTFS file system, such as AABBCCDDEEFF0011. For non-NTFS file systems, "n/a" is displayed for this field.
File System	The type of the file system (e.g. "Microsoft NTFS").
Sectors per cluster	The number of sectors in a file system cluster (e.g. 8).
Starting Sector	The starting sector for this partition.
Ending Sector	The ending sector for this partition.
Total Sectors	Encase shows different values for this field based on how a volume is added to the case. For example, if you add just a volume (e.g. your local C:\ drive), the number of sectors is 12341027. However, if you add your local physical drive 0 to the case and then select your C:\ volume in the "Entries" tree (note that your C drive would most likely have another letter in this tree, such as E:), then the total number of sectors would be one more that the other value (i.e. 123410272). The value shown for this field is taken from BPB, which matches the first value. The other value is shown when the parent physical drive is present probably comes from the partition table, and it counts VBR as well.
Total Capacity	This value is calculated by multiplying the Total Clusters value by the Cluster Size value, which shows the capacity of the file system and not the volume containing it. The size of the volume would be higher than this

Attribute	Description
	value.
Total Clusters	The number of clusters comprising the file system.
Unallocated	The number of unallocated bytes on the file system, which is calculated by multiplying the number of free clusters by the cluster size.
Free clusters	The number of unallocated clusters in the file system.
Allocated	This value is determined by multiplying the allocated clusters by the cluster size.
Volume Name	This is the volume label stored in Volume Boot Record (VBR).
Volume Offset	The offset (in bytes) of the volume containing this file system from beginning of the disk. "0" is displayed if the image and/or drive being searched is the image of one volume. Encase shows the number of sectors for this field instead of the number of bytes.

Additional Information

IME Suggestions (Japanese)

Description	IME Suggestions (Japanese) contains Japanese characters that have been suggested to the user as they use the Input Method Entry (IME) feature in Windows. This feature allows a user to provide a Unicode string and returns the equivalent Japanese characters as a suggestion.
Recovery method	Parsing

Attribute	Description
Created Time/Date - UTC (yyyy-mm-dd)	The date and time when the entry was created.
Candidate 1	The first candidate that's provided in response to the character's typed by the user.
Candidate 2	The second candidate that's provided in response to the character's typed by the user.

Additional Information

Jump Lists

Description	Jump lists are quick lists of recent applications or files that a user launched. The Dest List entries and shortcut entries are combined into a single table showing their joined structure.
Recovery method	Parsing

Attribute	Description
App ID	The unique application identifier generated by Windows based on the install location.
Potential App Name	A potential application name from a list of common applications and install locations.
Linked Path	The path to the target file.

Attribute	Description
Arguments	Any commands being passed to the target file.
Volume Name	The name of the volume where the shortcut resides.
Volume Serial Number	The serial number of the volume.
Target File Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the shortcut target file was created.
Target File Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the shortcut target file was last modified.
Target File Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the shortcut target file was last accessed.
Jump List Type	The type of jump list (Automatic or Custom).
Drive Type	The type of drive for the shortcut.
Target NetBIOS Name	The machine name on the network that the shortcut is on.
Target MAC Address	The MAC address of the volume that the shortcut is on.
Target File Size (Bytes)	The size of the shortcut file.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last time that the shortcut entry was accessed.
Entry ID	The entry ID.
Data	Other data within the shortcut entry.
NetBIOS Name	The machine name on the network.

Attribute	Description
Pin Status	Indicates whether the shortcut was pinned in the Dest List.
Access Count	The number of times a file is accessed through a Jump List.

Additional Information

Keyword Searches

Description	A list of keywords that were searched for on the system.
Recovery method	Parsing

Attribute	Description
Search Term	The term that was searched.
Searched Date/Time - UTC (yyyy-mm-dd)	The date and time that the term was searched.

Additional Information

Known DLLs

Description	Known DLLs is a list of DLLs that have been cached by Windows and are known to be safe. The DLLs are assumed to be located at either the folder path found in DLL Directory or DLL Directory32. The list of Known DLLs

	can be found at the following registry location: SYSTEM\CurrentControlSet\Control\Session Manager\KnownDlls.
Recovery method	Parsing

Attribute	Description
File Name	The filename of the known DLL.
DLL Directory	The value stored under the DllDirectory value in the known DLL registry key.
DLL Directory32	The value stored under the DllDirectory32 value in the known DLL registry key.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the known DLL registry key was last modified.

Additional Information

LNK Files

Description	LNK files are Windows shortcut files that point to other files on the system.
Recovery method	Parsing and carving

Attribute	Description
Linked Path	The path to the target file.
Arguments	Any commands being passed to the target file.
Target File Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the shortcut target file was created.
Target File Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the shortcut target file was last modified.
Target File Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the shortcut target file was last accessed.
Target Attributes	Any file attributes of the target file.
Drive Type	The type of drive for the shortcut.
Volume Serial Number	The serial number of the volume.
Volume Name	The name of the volume where the shortcut resides.
Show Command	Indicates how the shortcut should show the target when opened. The possible values for this field are: SW_SHOWNORMAL, SW_SHOWMAXIMIZED, SW_SHOWMINNOACTIVE, or Unknown.
Net Bios Name	The machine name on the network.
MAC Address	The MAC address of the volume that the shortcut is on.

Attribute	Description
Target File Size (Bytes)	The size of the shortcut file.

Additional Information
LNK files can be shortcuts to executables, media files, or any other type of file on the system. LNK files can be carved from many different areas of the OS, and the forensic importance of each type of LNK file varies from source to source.

MRU Folder Access

Description	The MRU Folder Access artifact contains information about the folders that are accessed by a Windows application using Open/Save browsing dialogs. Windows versions above XP use PIDL to store file path. PIDL paths might contain GUIDs instead of relative path strings. Folder access data cis recovered from the following registry location: Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU (LastVisitedMRU for Windows XP).
Recovery method	Parsing

Attribute	Description
Application Name	Name of the application that was used to access a directory.
Folder Accessed	Full path to the folder that the application accesses while using a Windows dialog (such as an Open/Save dialog).

Attribute	Description
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the MRU registry key was last modified.
Registry Order	Order of recency in which specific directories have being accessed by specific applications. Values occur in an ascending order, with a value of 1 indicating that a directory was accessed the most recently.
Value Name	Name of the value associated with the record within registry key.

Additional Information

MRU Opened/Saved Files

Description	MRU Opened/Saved Files contains information about last files accessed by any application through 'Open File' or 'Save File' dialog window. Windows versions above XP use PIDL to store file path. PIDL paths might contain GUIDs instead of relative path strings. Opened/Saved files data can be found at the following registry location: Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\<subkey> (OpenSaveMRU for Windows XP).
Recovery method	Parsing

Attribute	Description
File Name	Name of the file that was accessed using a Windows dialog (such as an Open/Save dialog)
File Path	Full path to the file.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the mru registry key was last modified.
Registry Order	Order of recency in which specific files were opened or saved by any applications. Values occur in an ascending order, with a value of 1 indicating that a file was opened/saved the most recently.
Value Name	Name of the value associated with the record within registry key.

Additional Information

MRU Recent Files And Folders

Description	The MRU Recent Files And Folders artifact contains information about files that were recently opened or saved and folders that were opened. This data is often related to items found in the Recent folder in the Users directory. Recent files and folders data is recovered from the following registry location: Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs.
Recovery method	Parsing

Attribute	Description
File/Folder Name	Name of the file or folder that was recently accessed.
File/Folder Link	A shortcut file name that is associated with the recently accessed file or folder.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the MRU registry key was last modified.
Registry Order	Order of recency in which specific files or directories have being accessed by any applications. Values occur in an ascending order, with a value of 1 indicating that a file/directory was accessed the most recently.
Value Name	Name of the value associated with the record within registry key.

Additional Information

MRU Run Commands

Description	The MRU Run Commands artifact contains information about commands that a user runs using the Run utility for Windows. Run command data is recovered from the following registry location: Soft-ware\Microsoft\Windows\CurrentVersion\Explorer\RunMRU.
Recovery method	Parsing

Attribute	Description
Run Command	A command string that a user provides in the Windows Run utility. This value can be a folder path, file path, or an command.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the MRU registry key was last modified.
Registry Order	Order of recency in which specific command was run through 'Run' application. Values occur in an ascending order, with a value of 1 indicating that a command was run the most recently.
Value Name	Name of the value associated with the record within registry key.

Additional Information

MUICache

Description	The MUICache artifact contains information about the files that are executed on the system, as parsed from the MUICache registry key.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file that is executed.
File Path	The path to the file that is executed. This value is stored in the Name field of the MUI registry.
Data	Additional information about the file (for example, the name or a description of the application it belongs to).

Additional Information

Network Interfaces (Registry)

Description	Network Interfaces (Registry) contains a list of all of the network interfaces that the image has stored in the registry.
Recovery method	Parsing

Attribute	Description
Description	A brief description of the interface.
MAC Address	The physical MAC address of the interface.
DHCP Enabled?	Indicates whether or not DHCP is enabled on this interface. If DHCP is enabled, this value will be Yes. Otherwise, this value will be No.
IPv4 Address	The IPv4 address of the interface.
IPv4 Subnet Mask	The IPv4 subnet mask of the interface
Lease Obtained Date/Time - UTC (yyyy-mm-dd)	The date and time that the lease was obtained on this interface.
Lease Expires Date/Time - UTC (yyyy-mm-dd)	The date and time that the lease will expire on this interface.
Default Gateway(s)	A comma separated list of the default gateways associated with

Attribute	Description
	this interface.
DHCP Server	A comma separated list of the DHCP servers associated with this interface.
DNS Server(s)	A comma separated list of the DNS servers associated with this interface.
DHCP IPv4 Address	The DHCP assigned IPv4 address of the interface.
DHCP IPv4 Subnet Mask	The DHCP assigned IPv4 subnet mask of the interface.
DHCP DNS Server(s)	A comma separated list of the DHCP assigned DNS servers associated with this interface.
DHCP Default Gateway(s)	A comma separated list of the DHCP assigned default gateways associated with this interface.
DNS Domain	The DNS domain of the interface.
DHCP DNS Domain	The DHCP assigned DNS domain of the interface.

Additional Information

Network Profiles

Description	A list of the saved Network Profiles on a machine.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the saved network profile.
Network Name (SSID)	The name of the network associated with the saved network profile.
Profile Created Date/Time - Local Time (yyyy-mm-dd)	The local date and time that the profile was created.
Last Connected Date/Time - Local Time (yyyy-mm-dd)	The last date and time that the network was connected to.
DNS	The DNS associated with this network connection.
Default Gateway MAC	The default gateway MAC associated with this network connection.
Broadcast SSID	Indicates whether or not this network broadcasts its SSID.
Connection Type	The type of connection, either ESS or IBSS.
Connection Mode	Indicates how the network connects (manual or auto).
Authentication	The authentication mode of the network.
Encryption	The method of encryption used.
Password	The password used to connect to the network.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Network Share Information

Description	Network Share Information provides information about mapped network drives on Windows.
Recovery method	Parsing

Attribute	Description
Network Name	The network share name.
Mapped Drive Letter	The drive letter assigned to the share.
Connection Type	The type of connection to the share.
Provider Name	The share provider.
Account	The account associated with the network share.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the share mapping was last modified.

Additional Information

Network Usage - Application Data

Description	Network Usage Application Data contains information about how an application sends or receives data over the network.
Recovery method	Parsing

Attribute	Description
Process Name	The file name of the executable.
Type	The executable type (Process or App).
First Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the process was first run.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the process was last run.
Last Connected Date/Time - UTC (yyyy-mm-dd)	The date and time when the process last connected to a network.
WiFi Bytes Sent	The number of bytes sent over a WiFi connection.
WiFi Bytes Received	The number of bytes received over a WiFi connection.
Mobile Bytes Sent	The number of bytes sent over a mobile cellular network.
Mobile Bytes Received	The number of bytes received over a mobile cellular network.
Wired Bytes Sent	The number of bytes sent over a wired connection.
Wired Bytes Received	The number of bytes received over a wired connection.

Additional Information

Network Usage - Connections

Description	Network Usage Connections contains information about the networks that a device connects to.
Recovery method	Parsing

Attribute	Description
Network Name	The SSID or mobile network name.
Connection Type	The connection type, such as WiFi or Cellular.
Cell ID/MAC Address	An identifier for the specific access point to the network, which can be either a cell tower identifier or a MAC address.
First Connected Date	The date that the device first connected to this network.
Last Connected Date	The date that the device last connected to this network.

Additional Information

NTFS Timestamp Mismatch

Description	NTFS Timestamp Mismatch reports on files where timestamps may have been modified externally. This artifact checks for cases where the

	$STANDARD_INFORMATION timestamps are older than the equivalent $FILE_NAME timestamps. It also checks for timestamps that have milliseconds set to 0, which may indicate timestomping with an external tool. For an artifact hit to be produced, the created, modified, and MFT modified times all have to be mismatched or have zero milliseconds.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file that has the timestamp mismatch.
MFT Record Number	The MFT record number of the file that has the timestamp mismatch.
Standard_Information Created Date/Time	The created timestamp, parsed from $STANDARD_INFORMATION (0x10).
File_Name Created Date/Time	The created timestamp, parsed from $FILE_NAME (0x30).
Standard_Information Modified Date/Time	The modified timestamp, parsed from $STANDARD_INFORMATION (0x10).
File_Name Modified Date/Time	The modified timestamp, parsed from $FILE_NAME (0x30).
Standard_Information Accessed Date/Time	The accessed timestamp, parsed from $STANDARD_INFORMATION (0x10).
File_Name Accessed Date/Time	The accessed timestamp, parsed from $FILE_NAME (0x30).
Standard_Information MFT Modi-	The MFT modified timestamp, parsed from

Attribute	Description
fied Date/Time	$STANDARD_INFORMATION (0x10).
File_Name MFT Modified Date/Time	The MFT modified timestamp, parsed from $FILE_NAME (0x30).
Reason	Indicates the reason why this file was flagged as a timestamp mismatch.

Additional Information

Operating System Information

Description	This table provides information about the Windows installation.
Recovery method	Parsing

Attribute	Description
Operating System	The operating system.
Version Number	The version number of the operating system.
Installed/Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the operating system was installed or updated.
Product Key	The product key used to license the operating system.
Owner	The owner of the operating system license.
Displayed Computer	The computer name that is displayed to the user of the system. This

Attribute	Description
Name	value is updated every time the system is restarted.
Computer Name	The name of the computer. This value can be can be different than the Displayed Computer Name if the user has changed their computer's name and not updated the system.
Domain	The domain that the computer is currently connected to.
DHCP DNS Server (s)	A comma separated list of the DHCP assigned DNS servers. This fragment represents the Domain Name Server(s) (DNS) provided from the DHCP service. This is stored in the registry as "DhcpNameServer".
Operating System Version	The version of the operating system.
Build Number	The build number of the operating system.
Product ID	The product ID of the operating system.
Last Service Pack	The last service pack that was installed.
Organization	The owner of the operating license organization.
Last Shutdown Date/Time - UTC (yyyy-mm-dd)	The date and time that the operating system was last shut down. In Windows, this comes from the ShutdownTime value which is found in the HKEY_LOCAL_MACHINE\SYSTEM\%ControlSet%\Control\Windows key.
System Root	The path to the system root.
Path	The path.
Last Access Time Enabled	Indicates whether or not Last Accessed Times are updated on this computer. If they are, this value will be 'Yes'. Otherwise, this value

Attribute	Description
	will be 'No'.
Control Set Type	Indicates which control set was used to parse information. The software chooses the control set based on the Current and LastKnownGood subkeys of the HKEY_LOCAL_MACHINE\SYSTEM\Select key. If the Current control set is unavailable, the software uses the LastKnownGood control set.

Additional Information

PowerShell History

Description	The PowerShell History artifact contains a history of PowerShell commands executed on the system.
Recovery method	Parsing

Attribute	Description
User Name	The user that executed the command.
Command	The command text.

Additional Information

Prefetch Files - Windows 8/10

Description	Prefetch files are used to speed up launching of frequently used executables. This table is for Windows 8 and 10.
Recovery method	Parsing and carving

Attribute	Description
Application Name	The application that was run.
Application Path	The original path of the application that was run.
Application Run Count	The number of times that the application was run. On some versions of Windows this count can be zero, while still having run date and time data.
File Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the prefetch file was created.
Last Run Date/Time - UTC (yyyy-mm-dd)	The last date and time that the application was run.
File Hash	A hash of the file name and path, which is included in the file name for the prefetch file.
2nd Last Run Date/Time - UTC (yyyy-mm-dd)	The 2nd last date and time that the application was run.
3rd Last Run Date/Time - UTC	The 3rd last date and time that the application was run.

Attribute	Description
(yyyy-mm-dd)	
4th Last Run Date/Time - UTC (yyyy-mm-dd)	The 4th last date and time that the application was run.
5th Last Run Date/Time - UTC (yyyy-mm-dd)	The 5th last date and time that the application was run.
6th Last Run Date/Time - UTC (yyyy-mm-dd)	The 6th last date and time that the application was run.
7th Last Run Date/Time - UTC (yyyy-mm-dd)	The 7th last date and time that the application was run.
8th Last Run Date/Time - UTC (yyyy-mm-dd)	The 8th last date and time that the application was run.
Volume Name	The name of the first volume.
Volume Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the first volume was created.
Volume 2 Name	The name of the second volume.
Volume 2 Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the second volume was created.

Additional Information

Prefetch Files - Windows XP/Vista/7

Description	Prefetch files are used to speed up launching of frequently used executables. This table is for versions of Windows XP, Vista and 7.
Recovery method	Parsing and carving

Attribute	Description
Application Name	The application that was run.
Application Path	The original path of the application that was run.
Application Run Count	The number of times that the application was run. On some versions of Windows this count can be zero, while still having run date and time data.
File Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the prefetch file was created.
Last Run Date/Time - UTC (yyyy-mm-dd)	The last date and time that the application was run.
File Hash	A hash of the file name and path, which is included in the file name for the prefetch file.
Volume Name	The name of the first volume.
Volume Created	The date and time when the first volume was created.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Volume 2 Name	The name of the second volume.
Volume 2 Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the second volume was created.

Additional Information

Program Compatibility Assistant Records - Windows

Description	Program Compatibility Assistant Records is an artifact that allows users to view a program's execution information.
Recovery method	Parsing

Attribute	Description
File Name	The name of the program that was executed.
File Path	The path of the program that was executed.
Last Execution Date/Time - UTC (yyyy-mm-dd)	The date and time when the program was last executed.
AmCache Program ID	The unique indentifier in AmCache of the program that was executed.

Attribute	Description
File Version	The version of the program that was executed.
Software Vendor Name	The software vendor's name of the program that was executed.
Exit Code Value	The exit code value returned by the program's execution.

Additional Information
This artifact is only supported for Windows 11 operating systems, version 22H2.

Rebuilt Desktops - Windows

Description	Rebuilt Desktops is an artifact that allows users to view an approximation of what a given Windows user's desktop looks like, including wallpapers, monitor configurations, and icon positioning, without having to virtualize the image.
Recovery method	Parsing

Attribute	Description
User Account	The user account that the desktop belongs to.
Wallpaper Path	The path that the wallpaper was located at as identified by the Windows registry.
Background Type	The style of background the user has set, including single wallpaper, wallpaper slideshow, or color.

Attribute	Description
Display Configuration	Indicates whether the user had just a single screen, screens duplicated, or a screen extended across connected monitors.
Monitor Identifier	A record identifier from the Windows Registry that indicates the type of monitors that were connected for a given configuration.
Hidden Items	Indicates whether or not there are items on the desktop that have been manually hidden from view.
Preview	A preview of the rebuilt desktop image.

Additional Information

This artifact is only supported for Windows 10 operating systems. For more information about rebuilt desktops, see support.magnetforensics.com/s/article/Artifact-profile-Rebuilt-Desktops.

Recycle Bin

Description	Recycle Bin displays all items that were moved to the Recycle Bin.
Recovery method	Parsing

Attribute	Description
File Name	The file or folder that was deleted.
Deleted Date/Time - UTC (yyyy-mm-dd)	The local date and time that the folder or file was deleted.
Security Identifier	The Security Identifier of the user who deleted the file or

Attribute	Description
	folder.
Original Path	The original location of the file or folder before deletion.
Type	Specifies whether the deleted item was a file or folder.
Current Location	The current location or the name of the file or folder in the Recycle Bin.
User	The user who deleted the file or folder, if we can retrieve it from the Security Identifier.
File Size (Bytes)	The size of the deleted file.

Additional Information
To learn more about this artifact, see Artifact profile: Recycle Bin.
For information about exporting data from this artifact, see Export Recycle Bin artifacts.

Scheduled Tasks

Description	The Scheduled Tasks artifact contains information about the scheduled tasks that are recovered from the computer. These records can be important to incident response investigations as malware often uses Scheduled Tasks to persist their content on an infected system.
Recovery method	Parsing

Attribute	Description
Name	The display name of the task.
Command	The path to the file used by the action that is performed by the task when it is triggered.
Author	The person who created the task.
Created Date/Time - Local Time	The local date and time of the local machine when the task was created.
Run As	The user account that the task runs as.
Last Run Date/Time - Local Time	The local date and time of the local machine when the task was last run.
Privilege Level	The privilege level that the task runs as. The options are LeastPrivilege and HighestAvailable.
Description	A description of the purpose of the task.
Status	The status of the task at the time of recovery (Ready or Disabled).
Triggers	The actions that must occur for the task to perform its actions.
Actions	The actions the task will perform when it is triggered.
Run Options	The run options of the task.
Hidden	Indicates whether the task is hidden (true or false).
File	The XML markup defining the task.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Shellbags

Description	Windows Shellbags track folder access by keeping logs of the view mode of a folder. If a shellbag record exists for a path, it has been previously viewed.
Recovery method	Parsing

Attribute	Description
Path	The path.
First Interaction Date/Time - UTC (yyyy-mm-dd)	The date and time that the folder was first interacted with.
Last Interaction Date/Time - UTC (yyyy-mm-dd)	The date and time the folder was last interacted with.
Mode	The view mode to which the path is currently set.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the entry on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed time of the entry on the filesystem.
File System Created Date/Time - UTC (yyyy-mm-dd)	The created time of the entry on the filesystem.
MFT Record Number	The MFT Record number of the folder.

Additional Information

Shim Cache

Description	The Shim Cache is used by Windows to track statistics about executables, such as the file path, size, and execution time (varies depending on the version of Windows). Only certain types of executable files are tracked and the data is only as recent as the last system reboot
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
File Path	The path to the file.
Last Run Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last accessed or explored.
Key Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the key was last updated.
File Size (Bytes)	The size of the file, in bytes.
Executed Flag	Indicates whether or not the file is known to have been executed.

Additional Information

SRUM Application Resource Usage

Description	The SRUM Application Resource Usage artifact tracks information about

	an application's resource usage. This artifact indicates the number of CPU cycles an application uses, context switches (foreground to background), and information about input and output operations.
Recovery method	Parsing

Attribute	Description
Entry ID	The entry ID.
Application Name	The name of the application.
Full Path	The full path to the application.
Recorded Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time when the record was recorded in the database.
Security Identifier	The user ID of the account executing the application.
Foreground Cycle Time	The foreground cycle time.
Background Cycle Time	The background cycle time.
Foreground Context Switches	The number of foreground context switches.
Background Context Switches	The number of background context switches.
Foreground Bytes Read	The number of foreground bytes read.
Background Bytes Read	The number of background bytes read.
Foreground Bytes Written	The number of foreground bytes written.
Background Bytes Written	The number of background bytes written.

Attribute	Description
Foreground Read Operations	The number of foreground read operations.
Background Read Operations	The number of background read operations.
Foreground Write Operations	The number of foreground write operations.
Background Write Operations	The number of background write operations.
Foreground Flushes	The number of foreground flushes.
Background Flushes	The number of background flushes.

Additional Information

SRUM Energy Usage

Description	The SRUM Energy Usage artifact contains information about the power expenditure for a device, as recovered from the SRUM database.
Recovery method	Parsing

Attribute	Description
Entry ID	The entry ID.
Recorded Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time when the record was recorded in the database.
Event Date/Time - UTC	The date and time when the event occurred.

Attribute	Description
(yyyy-mm-dd)	
State Transition	The type of state transition that occurred.
Designed Capacity	The original designed capacity of the device.
Full Charged Capacity	The actual full charged capacity of the device.
Charge Level	The current charge level of the device.
Cycle Count	The amount of power expended by the battery over the course of its life. A cycle represents the amount of power that a fully charged battery has.

Additional Information

SRUM Energy Usage (Long Term)

Description	The SRUM Energy Usage (Long Term) artifact contains information about the power expenditure for a device, as recovered from the SRUM database.
Recovery method	Parsing

Attribute	Description
Entry ID	The entry ID.
Recorded Timestamp Date/Time - UTC (yyyy-	The date and time that the record was recorded in the database.

Attribute	Description
mm-dd)	
Active AC Time	The Active AC time.
CS AC Time	The CS AC time.
Active DC Time	The Active DC time.
CS DC Time	The CS DC time.
Active Discharge Time	The Active Discharge time.
CS Discharge Time	The CS Discharge time.
Active Energy	The Active Energy amount.
CS Energy	The CS Energy amount.
Designed Capacity	The original designed capacity of the device.
Full Charged Capacity	The actual full charged capacity of the device.
Cycle Count	The amount of power expended by the battery over the course of its life. A cycle represents the amount of power that a fully charged battery has.

Additional Information

SRUM Network Connections

Description	The SRUM Network Connectivity artifact tracks information about the networks a device connects to and the length of time that it stays connected.
Recovery method	Parsing

Attribute	Description
Entry ID	The entry ID.
Recorded Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was recorded in the database.
Interface Type	The type of interface for the network connection.
Network Name (SSID)	The network name.
Connection Start Date/Time - UTC (yyyy-mm-dd)	The date and time that a connection was made to the network.
Duration (Seconds)	The amount of time (in seconds) connected to the network.

Additional Information

SRUM Network Usage

Description	The SRUM Network Usage artifact contains information about the network activity for a device. This artifact can be useful in data theft investigations because it indicates the individual applications and processes that are responsible for uploading or downloading data.
Recovery method	Parsing

Attribute	Description
Entry ID	The entry ID.

Attribute	Description
Application Name	The application name.
Full Path	The full path to the application.
Recorded Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was recorded in the database.
Security Identifier	The user ID.
Interface Type	The type of interface for the network connection.
Network Name (SSID)	The network name.
Bytes Sent	The number of bytes sent.
Bytes Received	The number of bytes received.

Additional Information

SRUM Push Notification Data

Description	The SRUM Push Notification Data artifact contains information about Windows push notifications sent to the device.
Recovery method	Parsing

Attribute	Description
Entry ID	The entry ID.
Recorded Timestamp Date/Time -	The date and time that the push notification was

Attribute	Description
UTC (yyyy-mm-dd)	recorded in the database.
App ID	The application ID.
Security Identifier	The user ID.
Notification Type	The type of notification.
Payload Size	The size of the notification payload.
Network Type	The type of network.

Additional Information

SSH Authorized Keys

Description	SSH Authorized keys are pre-configured keys used for logging into user accounts.
Recovery method	Parsing

Attribute	Description
Options	The list of options for the authorized key. This may be empty.
Encryption	The type of encryption used for the public key.
Public Key	The encrypted public key.
Comment	The comment added by the user for the authorized key. This may be empty.

Additional Information

SSH Keys

Description	SSH Keys are used to perform secure activities over the internet.
Recovery method	Parsing

Attribute	Description
File Name	The name of the SSH Keys file.
Type	The type of the SSH Key, either Public or Private.
Encryption	The type of encryption used on the SSH Key.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the file system.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the file system.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the file system.
File Content	The contents of the SSH Key file.

Additional Information

SSH Known Hosts

Description	SSH Known Hosts are public keys used to verify the identity of remote hosts. These are often automatically populated when the user connects to a host for the first time, but they can also be added manually.
Recovery method	Parsing

Attribute	Description
Host Names	The name or names of the specified host.
Marker	An optional tag used to indicate whether the host is a certificate authority.
Encryption	The type of encryption used for the public key.
Public Key	The encrypted public key.
Comment	The comment added by the user for the known host. This may be empty.

Additional Information

Startup Items

Description	Startup Items contains the configured auto-run programs for the system at startup.
Recovery method	Parsing

Attribute	Description
Program Name	The name of the program.
Path	The path to the program.
Type	The type of autorun (one of 'Run', 'RunOnce', 'RunOnceEx', or 'Startup').
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the autorun was last modified.
Enabled	Indicates whether or not this Startup item is enabled.
Embedded Signature	Indicates whether the program is digitally signed using an embedded digital signature as opposed to one signed utilizing a security catalog file.
MD5 Hash	The MD5 hash of the program.
Authenticode PE Image Hash	The PE Image hash of the program as read from within the digital signature format, Authenticode, if present. This hash is calculated using a Microsoft specified algorithm and is not equal to the hash of the entire program.
Issuer	The issuer of the digital signature, if present.
Signature	The digital signature of the issuer, if present.

Additional Information

System Services

Description	The System Services artifact lists the current services that exist on the

	system.
Recovery method	Parsing

Attribute	Description
Service Name	The service name.
Service Type	The service type.
Start Type	The service start type.
Service Location	The filepath to the service.
Group	The group the service belongs to.
Display Name	The service display name.
Dependencies	A list of service dependencies.
User Account	The user account to launch the service.
Description	A description of the service.
Service Details	A list of service details.
Hosted	Indicates whether the service is a hosted service (Yes or No).
Hosted Service	The hosted service.
Hosted Service Parameters	The parameters of the hosted service.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the registry key that contains the startup item was last modified.
Error Control	The method of error control for the service.
Tag	The tag for the service.

Additional Information

Timezone Information

Description	Timezone Information contains the timezone information that is stored in the Windows registry.
Recovery method	Parsing

Attribute	Description
Current Control Set	The current control set.
Failure Control Set	The last control set with which the system did not boot correctly.
Last Known Good Control Set	The last control set with which the system booted correctly.
Current Timezone Offset (minutes)	The current timezone offset of the system, in minutes.
Standard Timezone Name	The name of the standard timezone for the system.
Standard Timezone Offset (minutes)	The offset of the standard timezone for the system, in minutes.
Standard Timezone Start Date/Time - Local Time (yyyy-mm-dd)	The date and time when the standard timezone of the system comes into effect.
Daylight Timezone Name	The name of the daylight timezone for the system.

Attribute	Description
Daylight Timezone Offset	The offset of the daylight timezone for the system, in minutes.
Daylight Timezone Start Date/Time - Local Time (yyyy-mm-dd)	The date and time a when the daylight timezone of the system comes into effect.
Display	The name and offset of the currently active timezone, in a readable format.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

User Accounts - Windows

Description	User accounts are pulled from the Windows registry.
Recovery method	Parsing

Attribute	Description
User Name	The username of the account.
Full Name	The user's full name.
Type of User	The type of user (Domain User or Built-in).
Security Identifier	The security identifier of the account.
Relative Iden-	The relative identifier of the account.

Attribute	Description
tifier	
Internet User Name	The internet user name of the account.
Internet UID	The internet UID of the account.
Profile Path	The path to the profile folder.
Last Local Login Date/Time - UTC (yyyy-mm-dd)	The date and time that the local user last logged in. The login time only applies to local logins, not domain users.
Last Password Change Date/Time - UTC (yyyy-mm-dd)	The date and time that the user last changed their password.
Password Required	Indicates whether the account requires a password.
Password Hint	The user's password hint.
LM Hash	The LM hash for the local account password, if one can be recovered.
NTLM Hash	The NTLM hash for the local account password, if one can be recovered.
Account Description	A description of the account.
User Group(s)	Any groups that the user is a part of.

Attribute	Description
Login Script	Any login scripts that get run when logging in as that user.
Last Incorrect Password Login Date/Time - UTC (yyyy-mm-dd)	The date and time that the user last entered the wrong password.
Local Login Count	The number of times that the local user has logged in.
Account Disabled	Indicates whether the account is disabled.
Auto Logon	Indicates whether the user has enabled Auto Logon, which allows them to log in without a password when starting or restarting the computer. Note that even if this setting is enabled, the user still needs to provide a password after sleep and hibernation, and behavior might vary depending on certain admin settings

Additional Information

To learn more about the Password Required field, see Understanding the Password Required field of the User Accounts artifact.

UserAssist

Description	UserAssist contains the applications that are stored in the Microsoft Window's start menu.

Recovery method	Parsing

Attribute	Description
User Name	The name of the user the UserAssist belongs to.
File Name	The name of the application that potentially executed.
Application Run Count	The number of times that the application has been launched from Windows Explorer or the Start menu shortcut.
Last Run Date/Time - UTC (yyyy-mm-dd)	The date and time that the application was last executed.
Focus Count	The number of times that the application was brought in focus by the user. This fragment might be 0 for background applications.
Focus (Seconds)	The amount of time, in seconds, that the application was in focus by the user. In some cases, such as when the user switches between applications, an application can still be receiving focus even if it's being displayed behind another application.

Additional Information

To learn more about UserAssist, see Artifact profile: UserAssist.

UsnJrnl

Description	The UsnJrnl artifact contains a listing of the records found in the $Us-

	nJrnl:$J alternate data stream.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file or directory associated with this record.
Update Sequence Number	The update sequence number of this record.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The standard UTC timestamp of this record.
Reason	Reasons for changes that have accumulated in this file or directory journal record since the file or directory opened.
MFT Record Number	The MFT Record number as stored in the MFT.
MFT Reference Number	The ordinal number of the file or directory for which this record applies.
Parent MFT Record Number	The parent MFT Record number as stored in the MFT.
Parent MFT Reference Number	The ordinal number of the parent directory or file for which this record applies.
File Attributes	The attributes for the file or directory associated with this record.
Source Information	Additional information about the source of the change.
Security ID	The unique security identifier assigned to the file or directory associated with this record.

Additional Information

Windows Event Logs

Description	Event logs are logs of events from any Windows application.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Event Type	The event type associated with the log. Event types are determined by the Event ID and, in some cases, a LoginType property indicated by the Event Data attribute. For example, an RDP event can have a number of different Event IDs, but it must have a LoginType of 10.
Security Identifier	The security user ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the event recovered, if available.
Level	The level of error.

Attribute	Description
Keywords	The event keywords.
Provider Name	The name of the event provider.
Task category	The category that the event falls under.
Computer	The computer that generated the event.
Event Data	Any event data.

Additional Information

Windows Event Logs - Firewall Events

Description	Event logs related to firewall events.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the event recovered, if available.

Attribute	Description
Rule ID	The firewall rule ID associated with the event.
Rule Name	The firewall rule name associated with the event.
Modifying User	The modifying user associated with the event, if applicable.
Modifying Application	The modifying application associated with the event, if applicable.
Direction	The direction (Inbound or Outbound) of the firewall event, if applicable.
Event Data	Any event data.

Additional Information

Windows Event Logs - Networking Events

Description	Event logs related to networking and file share setup events.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.

Attribute	Description
Event Description Summary	The description of the event recovered, if available.
Subject User SID	The SID of the user who initiated the networking event.
Subject Username	The Username of the user who initiated the networking event.
Subject Domain Name	The domain name of the user who initiated the networking event.
Subject ID	The logon id of the user who initiated the networking event.
Network Share	The network share associated with the event.
Local File Path	The local file path of the network share associated with the event.
Network Name SSID	The SSID of the wifi network, if any, associated with the networking event.
Adapter Name	The local machine's network adapter, associated with the networking event.
Local MAC Address	The mac address of the local machine's network adapter, associated with the networking event.
Unique Device Identifier	The device identifier of the local machine associated with the networking event.
Event Data	Any event data.

Additional Information

Windows Event Logs - Office Alert Events

Description	Event logs related to Microsoft Office alerting events.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the event recovered, if available.
Application Name	The name of the Office application sending the alert.
Message	The short description of the alert.
Content	An unknown data value. This is often a number (such as an error code).
Version	The office application version.
Event Data	Any event data.

Additional Information

Windows Event Logs - Scheduled Task Events

Description	Event logs related to scheduled task events that are from any Windows application.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the event recovered, if available.
Task Name	The name of the task associated with this log.
User Name	The username, if any, associated with this log.
Event Data	Any event data.

Additional Information

Windows Event Logs - Script Events

Description	Event logs related to WMI or Powershell events.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the event recovered, if available.
Security User ID	The SID of the user associated with the powershell event.
User Name	The username associated with the event.
Computer Name	The computer name associated with the event.
Process ID	The ID of the process, if any, associated with the event.
Command	The command or query, if any, associated with the event.
Event Data	Any event data.

Additional Information

Windows Event Logs - Service Events

Description	Event logs related to service events that are from any Windows application.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the event recovered, if available.
Service Name	The name of the service associated with this log.
Service File Name	The filename associated with the service referenced.
Service Type	The service type associated with this log.
Service Start Type	The startup type referenced in this event.
Service Account	The account corresponding to this service event.
Event Data	Any event data.

Additional Information

Windows Event Logs - Storage Device Events

Description	Event logs related to storage device events for external storage devices.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the event recovered, if available.
Action	The action performed with the storage device, either 'Connected' or 'Disconnected'.
Total Capacity (Bytes)	Total capacity of the attached storage device, in bytes. If this field is 0, this device was disconnected.
Manufacturer	The manufacturer of the attached storage device.
Model	The model of the attached storage device.
Serial Number	The serial number of the attached storage device.
Parent ID	The Parent ID of the attached storage device.
Volume Serial Number	A list of Volume Serial Numbers of the attached storage device.
Event Data	Any event data.

Additional Information

Windows Event Logs - System Events

Description	Event logs related to networking and file share setup events.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the event recovered, if available.
Subject User SID	The SID of the user who initiated the event.
Subject Username	The Username of the user who initiated the event.
Subject Domain Name	The domain name of the user who initiated the event.
Subject ID	The logon id of the user who initiated the event.
Process Name	The name of the process associated with the event.
Process ID	The id of the process associated with the event.
Object ID	The registry object identifier associated with the event.
Object	The registry object value associated with the event.
Event Data	Any event data.

Additional Information

Windows Event Logs - User Events

Description	Event logs related to user events that are from any Windows application.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the event recovered, if available.
Logon Type	The logon type associated with the log.
Subject Username	The subject username.
Subject Domain Name	The subject domain name.
Subject User SID	The subject user security identifier.
Target Username	The target username
Target Domain Name	The target domain name.
Target User SID	The target user security identifier.
Event Data	Any event data.

Additional Information

Windows Event Logs - User PNP Events

Description	Event logs related to user PNP events that are from any Windows application.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the recovered event, if available.
Service Name	The name of the service that was added.
Driver Name	The name of the driver that was installed.
Driver Version	The version of the driver that was installed.
Driver Company	The company that produced the driver that was installed.
Driver Type	The description of the device for which the driver was installed.
Event Data	Any event data.

Additional Information

Windows Logon Banner

Description	This table contains the legal text a user must acknowledge in order to logon to the computer. This table contains legal text found in the group policy or that was set manually.
Recovery method	Parsing

Attribute	Description
Legal Caption	The caption for the legal text that will be displayed to the user before they can logon to the computer.
Legal Text	The legal text being displayed to a user before they can logon to a computer.

Additional Information

Windows Notification Center

Description	The Windows Notification Center provides real-time notifications of events as they occur, such as received emails, calendar appointments, and more.
Recovery method	Parsing

Attribute	Description
Title	The title of the notification center popup.
Subtext	The subtext of the notification center popup.
Message	The message text of the notification center popup.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the notification was received.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the notification expires.

Additional Information

Windows Search - Calendar

Description	Windows Search - Calendar contains information related to Outlook Events and Appointments that were indexed in the Windows Search results. Indexed items are files that existed on a computer at some point in time, but it's not guaranteed that a user interacted with these files.
Recovery method	Parsing

Attribute	Description
Title	The title of the Outlook event.
File Path	The path to the calendar event within the Outlook inbox.

Attribute	Description
Organizer Name	The name of the event organizer.
Duration	The duration of the calendar event, in minutes.
Is Recurring	A value indicating if this event is recurring.
Location Name	The location or locations of the event.
Reminder Date/Time - UTC	The date and time that a reminder will be sent for this meeting.
Attendees	A list of required attendees for the event.
Optional Attendees	A list of optional attendees for the event.
Reources	Any resources allocated to the event, such as rooms or equipment.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the search result was last modified.

Additional Information

Windows Search - Contact

Description	Windows Search - Contact contains information related to Outlook Contacts that were indexed in the Windows Search results. Indexed items are files that existed on a computer at some point in time, but it's not guaranteed that a user interacted with these files.
Recovery method	Parsing

Attribute	Description
Display Name	The contact's display name.
Email Address	The contact's primary email address.
Email Address 2	The contact's secondary email address.
Company	The contact's company name.
Department	The contact's department name.
Job Title	The contact's job title.
Profession	The contact's profession.
Office Location	The contact's office location.
Business Address Street	The street address of the contact's business.
Business Address City	The city of the contact's business address.
Business Address Postal Code	The postal code, ZIP code etc. of the contact's business address.
Business Phone	The contact's business phone number.
Business Fax	The contact's business fax number.
Business Homepage	The website of the contact's business.
Mobile Phone	The contact's mobile phone number.
Work Phone	The contact's work phone number.
Home Address Street	The street address of the contact's home.
Home Address City	The city of the contact's home address.
Home Address Postal Code	The postal code, ZIP code etc. of the contact's home

Attribute	Description
	address.
Home Phone	The contact's home phone number.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the search result was last modified.

Additional Information

Windows Search - Document

Description	Windows Search - Document contains information related to document searches that were indexed in the Windows Search results. Indexed items are files that existed on a computer at some point in time, but it's not guaranteed that a user interacted with these files.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the document.
File Extension	The file extension of the document.
File Path	The path to the document.
Last Author	The last author of the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created.

Attribute	Description
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last printed.
Saved Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last saved.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the search result was last modified.
Owner	The owner of the document.
Type	The type of document.
Computer Name	The name of the computer.
Content	The body of the document, if full text indexing is enabled.

Additional Information

Windows Search - Image

Description	Windows Search - Image contains information related to image searches that were indexed in the Windows Search results. Indexed items are files that existed on a computer at some point in time, but it's not guaranteed that a user interacted with these files.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the image.
File Extension	The file extension of the image.
File Path	The path to the image.
File Size (Bytes)	The file size of the image file.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the image was modified.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the image was accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the image was created.
Taken Date/Time - UTC (yyyy-mm-dd)	For images that originated from a camera, the date and time when the picture was taken.
Horizontal Resolution	The number of pixels per inch in an image, measured from left to right.
Vertical Resolution	The number of pixels per inch in an image, measured from top to bottom.
Original Width	The number of pixels in an image, from left to right.
Original Height	The number of pixels in an image, from top to bottom.
Latitude	The latitude of the device when the image was captured.
Longitude	The longitude of the device when the image was captured.
Make	The make of the device that captured the image.

Attribute	Description
Model	The model of the device that captured the image.
Owner	The owner of the image.
Type	The image format.
Computer Name	The name of the computer.

Additional Information

Windows Search - Internet Explorer

Description	Windows Search - Internet Explorer contains information related to Internet Explorer searches that were indexed in the Windows Search results. Indexed items are files that existed on a computer at some point in time, but it's not guaranteed that a user interacted with these files.
Recovery method	Parsing

Attribute	Description
Target	The target URL of the search result.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Visit Count	The number of times the webpage was visited.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the search result was last modified.

Additional Information

Windows Search - Outlook

Description	Windows Search - Outlook contains information related to Outlook emails that were indexed in the Windows Search results. Indexed items are files that existed on a computer at some point in time, but it's not guaranteed that a user interacted with these files.
Recovery method	Parsing

Attribute	Description
Sender Name	The sender of the email.
Sender Email	The email address of the sender.
Recipient(s)	The recipients of the email.
Subject	The subject of the email.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was received.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the email was sent.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Attachment Name(s)	The file names attached to the email.
Modified Date/Time - UTC (yyyy-	The date and time the search result was last mod-

Attribute	Description
mm-dd)	ified.
File Path	The name of the folder where the email is stored.
Content	The content of the email item, if full text indexing is enabled.

Additional Information

Windows Timeline Activity

Description	Windows Timeline Activity contains information about application usage, such as application start and end times, and duration of usage.
Recovery method	Parsing and carving

Attribute	Description
Application Name	The name of the executable reporting the timeline data.
Display Name	The title bar display text.
Content	The content that the executable was displaying.
Activity Type	The activity type.
Focus (Seconds)	The number of seconds that the user was engaged with the application.

Attribute	Description
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the activity started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the activity ended.
Activity ID	The ID of the activity.
Platform	The platform related to the executable.
Created Time/Date - UTC (yyyy-mm-dd)	The date and time when the entry was created.
Created In Cloud Date/Time - UTC (yyyy-mm-dd)	The date and time when the activity was recorded in the cloud.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the entry was last modified.
Last Modified On Client Date/Time - UTC (yyyy-mm-dd)	The date and time when the activity was last modified on the client.
Original Last Modified On Client Date/Time - UTC (yyyy-mm-dd)	The original date and time when the activity was last modified on the client.
Local Only	Indicates whether or not the activity only occured locally.

Additional Information

Peer-to-Peer

Ares Download Folder

Description	Ares Download Folder contains the locations where Ares saves its downloads for each user on the system.
Recovery method	Parsing

Attribute	Description
Download Folder	The location that Ares is saving its downloads to.

Additional Information

Ares Downloads

Description	Ares is a peer-to-peer file sharing application.
Recovery method	Carving

Attribute	Description
Title	The title of the media.
Artist	The artist of the media.
Album	The album of the media.

Attribute	Description
Type	The genre of the media.
Language	The language of the media.
Year	The year that the media was created.
URL	The URL to the file.
Comment	Any comments about the file.
Downloaded Date/Time - Local Time (yyyy-mm-dd)	The local date and time of the system when the file was downloaded.
Available for Download by Other Users	Indicates whether or not other users can download this file.
Corrupt	Indicates whether or not the file is corrupt.
SHA1 Hash	The SHA1 hash of the file.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Ares Incomplete Downloads

Description	Ares is a peer-to-peer file sharing application.
Recovery method	Carving

Attribute	Description
Title	The title of the media.
Artist	The artist of the media.
Album	The album of the media.
Type	The genre of the media.
Language	The language of the media.
Year	The year the media was created.
URL	The URL to the file.
Comment	Any comments about the file.
Keyword Genre	The genre of the media.
Subfolder	The subfolder where the file was downloaded.
Download Start Date/Time - Local Time (yyyy-mm-dd)	The local date and time of the system when the file was downloaded.
SHA1 Hash	The SHA1 hash of the file.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Ares Search Keywords

Description	Ares is a peer-to-peer file sharing application.
Recovery method	Carving

Attribute	Description
Search Keyword	The keyword that was searched for.

Additional Information

Ares Shared Files

Description	Ares is a peer-to-peer file sharing application.
Recovery method	Carving

Attribute	Description
Title	The title of the media.
Artist	The artist of the media.
Album	The album of the media.
Type	The genre of the media.
Language	The language of the media.
Year	The year the media was created.
URL	The URL to the file.
Comment	Any comments about the file.
File Size (Bytes)	The size of the file.
Video Info	Any information about the file if it is a video.
Corrupt	Indicates whether or not the file is corrupt.
SHA1 Hash	The SHA1 hash of the file.

Additional Information

Bitcoin Address

Description	Bitcoin wallet is an application that generates and stores private keys, and communicates with peers on the Bitcoin network to enable transactions.
Recovery method	Carving

Attribute	Description
Address	The Bitcoin address.
Label	Any labels that were applied to this address by the user.
Status	Indicates whether or not the address is listed in the thread pool.
Public Key	The public key.
Encrypted Private Key	The encrypted private key.

Additional Information

Bitcoin Debug Logs

Description	Bitcoin Debug Logs contain events related to bitcoin transactions performed by the user.
Recovery method	Carving

Attribute	Description
Event Type	The type of event that occurred in the log.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time the log event occurred.
Wallet Path	The path to the bitcoin wallet.
Transaction ID	The transaction identifier related to this event.

Additional Information

Bitcoin Logged Queries

Description	Bitcoin is a widely-used digital currency based on advanced encryption techniques. This search will return the Bitcoin addresses stored by the most common Bitcoin application, as well as transaction queries logged by older versions. These values are used to query Bitcoin servers for transaction history.
Recovery method	Carving

Attribute	Description
Query Type	The type of query on the network that was made (may or may not relate to the local user's activity).
Object ID	The ID of the transaction or block that was queried.
Query Date/Time - UTC (yyyy-mm-dd)	The date and time of the query.

Additional Information

Cryptocurrency Clients

Description	Cryptocurrency Clients searches the system for known client applications that are used to transfer cryptocurrencies. Finding these applications can be helpful to investigations where cryptocurrency transactions might have been made using these applications.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file that matched for known crypto-currency clients.
Software	The name of the cryptocurrency client software.
Created Date/Time - UTC (yyyy-mm-dd)	The MAC creation time for the cryptocurrency client executable.
Accessed Date/Time - UTC (yyyy-mm-dd)	The MAC access time for the cryptocurrency client executable.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The MAC modified time for the cryptocurrency client executable.

Additional Information

You can find a list of the cryptocurrency client applications that are supported by this artifact at Cryptocurrency client applications.

Cryptocurrency Wallets

Description	Cryptocurrency Wallets searches the system for known cryptocurrency wallet formats. Recovering wallets can be helpful in an investigation where cryptocurrency transactions might have been made on the system and stored in the associated wallet.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file that matched for known cryptocurrency wallets.
File Type	The name of the cryptocurrency client software that created or manages the wallet.
Created Date/Time - UTC (yyyy-mm-dd)	The MAC creation time for the cryptocurrency wallet file.
Accessed Date/Time - UTC (yyyy-mm-dd)	The MAC access time for the cryptocurrency wallet file.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The MAC modified time for the cryptocurrency wallet file.

Additional Information

You can find a list of the known cryptocurrency wallet formats that are supported by this artifact at Cryptocurrency wallet formats.

eMule Clients.met Records

Description	This search parses files used by the P2P file sharing application Emule. It will parse the following files: known.met, emfriends.met, clients.met, StoredSearches.met, sharedfiles.dat, shareddir.dat, and AC_SearchString-s.dat. Information recovered varies from file to file, but all fields available in each file format are recovered. Of particular evidential interest are the known.met, emfriends.met, StoredSearches.met, and AC_SearchString-s.dat files.
Recovery method	Parsing and carving

Attribute	Description
Client Hash	The hash of the client.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The last time that the client was seen online.
Uploaded Bytes	The number of bytes uploaded to that client.
Downloaded Bytes	The number of bytes downloaded from that client.

Additional Information

eMule EmFriends.met Records

Description	This search parses files used by the P2P file sharing application, Emule. It

	will parse the following files: known.met, emfriends.met, clients.met, StoredSearches.met, sharedfiles.dat, shareddir.dat, and AC_SearchString-s.dat. Information recovered varies from file to file, but all fields available in each file format are recovered. Of particular evidential interest are the known.met, emfriends.met, StoredSearches.met, and AC_SearchString-s.dat files.
Recovery method	Parsing and carving

Attribute	Description
Friend Name	The name of the friend on eMule.
Last Used IP	The last IP address of that user.
Last Used Port	The last port used by that user.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The last time the friend was seen online.
Last Chatted Date/Time - UTC (yyyy-mm-dd)	The last date and time there was a conversation with the friend.

Additional Information

eMule GUIDs

Description	This search parses files used by the P2P file sharing application, Emule. It will parse the following files: known.met, emfriends.met, clients.met, StoredSearches.met, sharedfiles.dat, shareddir.dat, and AC_SearchString-

	s.dat. Information recovered varies from file to file, but all fields available in each file format are recovered. Of particular evidential interest are the known.met, emfriends.met, StoredSearches.met, and AC_SearchString-s.dat files.
Recovery method	Parsing and carving

Attribute	Description
Network	The type of network.
GUID	The GUID for the eMule Network.

Additional Information

eMule Known.met Records

Description	This search parses files used by the P2P file sharing application, Emule. It will parse the following files: known.met, emfriends.met, clients.met, StoredSearches.met, sharedfiles.dat, shareddir.dat, and AC_SearchString-s.dat. Information recovered varies from file to file, but all fields available in each file format are recovered. Of particular evidential interest are the known.met, emfriends.met, StoredSearches.met, and AC_SearchString-s.dat files.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file on the KAD network.
File Size (Bytes)	The total size of the file (in bytes).
Temp File Name	The name of the local .part file.
Last Written Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last written or fully downloaded.
Last Posted Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was posted or should be reposted on the KAD network.
Last Shared Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last shared.
Requests Total	The number of total requests from the other users in the KAD network.
Requests Accepted	The number of accepted requests from other users in the KAD network.
Bytes Uploaded	The number of bytes downloaded by other users in the KAD network.
Upload Priority	The priority of the upload. eMule sets this value to Auto by default. The priorty can be changed manually by the user.
Artist	The name of the artist (for media files).
Album	The name of the album (for media files).
Title	The title (for media files).
Length	The length of the media file in seconds.
Bitrate	The bitrate of the media file.

Attribute	Description
Codec	The codec of the media file.
File Type	The type of the file, such as images, videos, or documents.
File Hash	The eD2K has value of the original file.

Additional Information

eMule Search Keywords

Description	This search parses files used by the P2P file sharing application Emule. It will parse the following files: known.met, emfriends.met, clients.met, StoredSearches.met, sharedfiles.dat, shareddir.dat, and AC_SearchString-s.dat. Information recovered varies from file to file, but all fields available in each file format are recovered. Of particular evidential interest are the known.met, emfriends.met, StoredSearches.met, and AC_SearchString-s.dat files.
Recovery method	Parsing and carving

Attribute	Description
Search Keyword	The keyword that was searched for.

Additional Information

eMule Shared Files

Description	This search parses files used by the P2P file sharing application Emule. It will parse the following files: known.met, emfriends.met, clients.met, StoredSearches.met, sharedfiles.dat, shareddir.dat, and AC_SearchString-s.dat. Information recovered varies from file to file, but all fields available in each file format are recovered. Of particular evidential interest are the known.met, emfriends.met, StoredSearches.met, and AC_SearchString-s.dat files.
Recovery method	Parsing and carving

Attribute	Description
File	A user's file.
Shared Status	Identifies whether or not the file is shared on the eMule network.

Additional Information

eMule Shared Folders

Description	This search parses filesused by the P2P file sharing application Emule. It will parse the following files: known.met, emfriends.met, clients.met, StoredSearches.met, sharedfiles.dat, shareddir.dat, and AC_SearchString-s.dat. Information recovered varies from file to file, but all fields available in each file format are recovered. Of particular evidential interest are the known.met, emfriends.met, StoredSearches.met, and AC_SearchString-s.dat files.

Recovery method	Parsing and carving

Attribute	Description
Shared Folder	The name of the shared folder.

Additional Information

eMule StoredSearches.met Records

Description	This search parses files used by the P2P file sharing application Emule. It will parse the following files: known.met, emfriends.met, clients.met, StoredSearches.met, sharedfiles.dat, shareddir.dat, and AC_SearchString-s.dat. Information recovered varies from file to file, but all fields available in each file format are recovered. Of particular evidential interest are the known.met, emfriends.met, StoredSearches.met, and AC_SearchString-s.dat files.
Recovery method	Parsing and carving

Attribute	Description
Search Expression	The keyword that was searched for.
Special Title	An alternate title for the file.
Name of Matched File	The name of the file that was found.

Attribute	Description
Hash of Matched File	The hash of the file that was found.
File Type	The type of file that was found.
File Rating	The file's rating on the eMule network.

Additional Information

Frostwire

Description	Frostwire contains files and torrents downloaded with Frostwire version 5.
Recovery method	Parsing and carving

Attribute	Description
Torrent Name	The name of the torrent file.
Total Size (Bytes)	The total size of all files contained within the torrent.
Number of Pieces	The number of pieces needed to download the torrent. This value does not reflect the number of files in the torrent.
Creation Date/Time - UTC (yyyy-mm-dd)	The creation date and time of the original torrent file.
Created By	The original author of the torrent file.
File Download Progress	The names of all files within the torrent along with their current

Attribute	Description
	download progress.
Download Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the download was started.
Download Completed Date/Time - UTC (yyyy-mm-dd)	The date and time that the download was completed.
Tracker Data	The list of IP addresses and ports connected when downloading the torrent.

Additional Information

Frostwire.props Files

Description	This search finds fragments of Frostwire.props files. These files contain configuration data for the Frostwire peer to peer file sharing client and can include geo-locations, recent downloads, and many other useful items.
Recovery method	Carving

Attribute	Description
Fragment	The file contents.

Additional Information

Gigatribe Chat Messages

Description	This search will recover Gigatribe chat messages saved by Gigatribeï¿½ (versions 2 and 3). These logs are created when a user uses the chat feature of Gigatribe. Due to the way searches for these chat messages are performed, they can be recovered even if the log file has been deleted or a portion of the log file has been corrupted or overwritten. The chat messages can also be recovered from live memory dumps.
Recovery method	Carving

Attribute	Description
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
From ID/Name	The unique ID or name of the user that sent the message.
To ID/Name	The unique ID or name of the user who received the message.
Message	The content of the message.
Type	The visibility type of the message (Private or Public).

Additional Information

Gigatribe Shared Files

Description	Gigatribe is a peer-to-peer file sharing network that allow users to download files from other users.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the file being shared.
File/Folder	This value is either File or Folder.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created.
Folder Name	The name of the folder that contains the file.
Folder Source	The source of the folder.
Sub Directories	Indicates whether or not the source has sub directories.
Shared with group	Indicates whether or not the source is shared with groups.
Access	The file access permissions.
Available from HTTP	Indicates whether the file is available via URL or not.
Folder Creation Date/Time - UTC (yyyy-mm-dd)	The date and time that the folder was created.

Additional Information

Limerunner Shared Files

Description	Limewire is a P2P file sharing application.
Recovery method	Parsing

Attribute	Description
Filename	The name of the file being shared.
Shared	Indicates whether or not the file is shared.
Base32 Hash Value	The base32 hash of the file.
SHA1 Hash Value	The SHA1 hash of the file.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time when the file was modified.
Additional Source	The additional source.

Additional Information

Limewire Shared Files

Description	This search finds fragments of Limewire.props files. These files contain configuration data for the Limewire peer to peer file sharing client and can include geo-locations, recent downloads, and many other useful items.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the file being shared.
Shared	Indicates whether or not the file is shared.
Base32 Hash Value	The base32 hash of the file.
SHA1 Hash Value	The SHA1 hash of the file.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time when the file was modified.
Additional Source	

Additional Information

Limewire v5.x Searches

Description	Limewire v5.x Searches contains search keywords left behind in live memory by Limewire. Search keywords or terms that are recovered have an associated number indicating how many search results were returned for that search term at the time that the keyword was left in memory. The recovered search terms are search keywords that were entered by the local user. Other search keywords that were passed through the client (such as incoming searches) from other clients on the P2P network are not recovered.
Recovery method	Parsing and carving

Attribute	Description
Search Keyword	The keyword searched.
Search Category	The category searched. This field displays one of the following values: All, Images, Videos, Documents, Audio, Program, or Other.
Number of Search Results	The number of search results found for the specific search keyword in the search category.

Additional Information

Limewire/Frostwire 4.x Searches

Description	Limewire/Frostwire 4.x Searches contains search keywords entered by the local user and left behind in live memory by Limewire. Search keywords that are recovered have an associated number indicating how many search results were returned for that search term at the time the keyword was left in memory. Other search keywords that were passed through the client (such as incoming searches) from other clients on the P2P network are not recovered.
Recovery method	Parsing and carving

Attribute	Description
Search Keyword	The keywords searched.
Number of Search Results	The number of search results found for the specific search keyword in the search category.

Additional Information

Limewire.props Files

Description	This search finds fragments of Limewire.props files. These files contain configuration data for the Limewire peer to peer file sharing client and can include geo-locations, recent downloads, and many other useful items.
Recovery method	Parsing and carving

Attribute	Description
Fragment	The file contents.

Additional Information

Luckywire Shared Files

Description	Luckywire is a P2P file sharing application.
Recovery method	Parsing

Attribute	Description
Filename	The name of the file.
Shared	Indicates whether or not the file is shared.

Attribute	Description
Base32 Hash Value	The base32 hash of the file.
SHA1 Hash Value	The SHA1 hash of the file.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the file was modified.
Additional Source	The additional source.

Additional Information

Shareaza GUIDs

Description	The GUIDs used by Shareaza. Shareaza is a peer-to-peer file sharing client that runs under Microsoft Windows. It supports supports the gnutella, Gnutella2 (G2), eDonkey, BitTorrent, FTP, HTTP and HTTPS network protocols.
Recovery method	Parsing

Attribute	Description
Gnutella GUID	The GUID used for Gnutella.
Bittorrent GUID	The GUID used for Bittorrent.

Additional Information

Shareaza Library Files

Description	The files in the Shareaza library.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
Folder	The location of the file on.
Created Date/Time - UTC (yyy-mm-dd)	The date and time when the file was created.
Shared	Indicates whether the file is shared or not. This value can be explicit, or it can be inherited from a parent folder. The possible values include Yes, No, Inherited (Yes), Inherited (No), and Inherited (Unknown).
File Size (Bytes)	The size of the file in bytes.
MD5 Hash	The MD5 hash of the file.
SHA1 Hash	The SHA1 hash of the file.
Hits	The number of times that the file has appeared in other user's search results.
Uploads	The number of times that the file has been uploaded to other users.
File Rating	The average rating of the file.
Comment	The comments left on the file by Shareaza users.

Additional Information

Shareaza Search Keywords

Description	Shareaza is a peer-to-peer file sharing client that runs under Microsoft Windows. It supports supports the gnutella, Gnutella2 (G2), eDonkey, BitTorrent, FTP, HTTP and HTTPS network protocols.
Recovery method	Parsing and carving

Attribute	Description
Search Keyword	The keyword that was searched for.

Additional Information

Shareaza Search Results

Description	The results from a search conducted in Shareaza.
Recovery method	Parsing

Attribute	Description
Search Keyword	The keyword that was searched for.
Name	The file name of the search result.

Attribute	Description
URL	The URL to the peer serving the file.
File Size (Bytes)	The size of the file in bytes.
MD5 Hash	The MD5 hash of the file.
SHA1 Hash	The SHA1 hash of the file.

Additional Information

Torrent Active Transfers

Description	Torrent Active Transfers contains information about the torrents that are active on the user's system.
Recovery method	Parsing

Attribute	Description
Torrent Name	The name of the torrent file.
Potential App Name	The name of the application that the torrent was potentially downloaded with.
Download Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the torrent file download was started.
Download Completed Date/Time - UTC (yyyy-mm-dd)	The date and time when the torrent file download was completed.

Attribute	Description
Download URL	The URL to download the torrent.
Downloaded Bytes	The total number of bytes that were downloaded.
Download Location	The location on the disk to where the torrent was downloaded.
Bytes Uploaded	The total number of bytes that the system has uploaded for this torrent.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the active transfer was last modified.

Additional Information

Torrent Feeds

Description	Torrent Feeds contains information about RSS feeds that a user subscribes to, which contains torrents available for download.
Recovery method	Parsing

Attribute	Description
Feed Name	The name of RSS subscription feed.
Feed URL	The URL of the RSS subscription feed.
Torrent Name	The name of the torrent available for download from the feed.

Attribute	Description
Download URL	The URL to download the torrent.
Description	A description of the contents of the torrent.
Published Date/Time - UTC (yyyy-mm-dd)	The date and time when the torrent feed item was published.
Status	The donwload status of the feed item (Downloaded or Not Downloaded).

Additional Information

Torrent File Fragments

Description	Torrent File Fragments contains data that is carved or parsed from .torrent files that are used to download torrents from various networks on the Internet.
Recovery method	Carving

Attribute	Description
Name	The name of the torrent file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the torrent file was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the torrent file was modified.

Attribute	Description
Torrent Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the torrent file was originally created.
Torrent Files	The files that are listed in the torrent to be downloaded.

Additional Information

Usenet Binary Files

Description	This search recovers uuencoded (ENC) encoded files that are used to transfer files on newsgroups (USENET). These files can have a wealth of header information and can be split into multiple files. Recovered files can be reconstructed in the Refined Results category in Report Viewer/AXIOM Examine. You can rebuild the files by clicking each item, or by right-clicking and selecting 'Rebuild All'.
Recovery method	Carving

Attribute	Description
Message ID	The message identifier of the Usenet file being downloaded.
Organization	A string that describes the organization of the message sender or machine the file was on.
Posted Date/Time -	The date and time when the file was originally posted on the Usenet.

Attribute	Description
Local Time	
Subject	The subject of the message.
Newsgroup	The list of newsgroups to which the message belongs.
From	The email of the user who sent the message.
Path	The path that the message took to get to the local system.
Keywords	The keywords that describe the message.
Description	A description of the message.
Original File Name	The original file name that is contained in the message.
Image	The actual image.
File Part	If a Usenet file is too large, it will be separated into pieces. This column will indicate which piece of the file was recovered.
Original File Size (Bytes)	The size of the file.
Received File Size (Bytes)	The number of bytes that have been downloaded.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Social Networking

Bebo Live Chat

Description	Bebo Live Chat contains messages sent or received in Bebo live chat. Information found within these attributes can include the status of the message, the date and time, the sender's username, the target's username, and the message itself.
Recovery method	Carving

Attribute	Description
Status	The sent status of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Source ID	The account of the source.
Target ID	The account of the target.
Message	The content of the chat message.

Additional Information

Facebook

Facebook, being one of the most popular social networking sites in the world, presents numerous opportunities for gathering evidence. You can recover messages that are sent and received,

status updates and wall posts, and pages and pictures that the user views. On mobile devices, you can also recover user profiles and contacts.

Facebook can provide background information about a user, as well as evidence of who they are communicating with or associated with. Status and location updates can provide details about where a user has been and what they've been doing.

Forensic notes

The Facebook Pictures artifact represents cached pictures found on the system that originated from Facebook. When caching pictures, Facebook names the pictures using a particular format which allows forensic tools to know that they come from Facebook. These pictures can be user profile pictures, friends' pictures, or any other picture that gets cached while browsing Facebook.

Artifacts

Related resources

How important are Facebook artifacts?

Recovering Facebook artifacts

Facebook Chat

Description	Facebook Chat contains chat messages sent and received using Facebook Chat.
Recovery method	Carving

Attribute	Description
Profile ID	The Facebook profile ID of the sender.
Message ID	The unique ID for a specific chat message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Sender ID	The Facebook ID of the sender.
Downloaded Sender Image	The profile picture of the sender, downloaded from the Internet based on the Sender ID.
Sender Name	The name of the sender.
Receiver ID(s)	The Facebook IDs of all the receivers of the message.
Downloaded Receiver Image	The profile picture of the receiver, downloaded from the Internet based on the Receiver ID.
Receiver Names(s)	The name of the receiver.
Message	The content of the chat message.
Sender Offline	The online status of the sender.

Additional Information

Facebook Email Snippets

Description	Facebook Email Snippets contains snippets of email messages sent using Facebook.
Recovery method	Carving

Attribute	Description
Subject	The subject of the email.
Snippet	A text snippet of the body of the email.
Original Author	The author of the email.
Recent Author	The most recent author of the email.
Time Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the email was last updated.
Thread ID	The conversation ID.

Additional Information

Facebook Email

Description	Facebook Email contains email messages sent using Facebook.
Recovery method	Carving

Attribute	Description
Logged-In User ID	The unique Facebook ID of the user that is currently logged in.
Downloaded Logged-In User Image	The profile picture of the sender, downloaded from the Internet based on the Logged-In User ID value.
Author ID	The unique Facebook ID of the author of the email.
Downloaded Author Image	The profile picture of the sender, downloaded from the Inter-

Attribute	Description
	net based on the Author ID value.
Author Name	The name of the author.
Recipient(s)	The names of the recipients.
Subject	The subject of the email.
Time Rendered - Local Time (yyyy-mm-dd)	The time that was rendered in the web browser when the user viewed the email.
Time Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the email was last updated.
Original Author	The first author of the email.
Message	The content of the email message.
Thread ID	The unique ID that represents the email trail.
Mobile	Indicates whether this email was sent from a mobile device.
Attachments	Indicates whether this email has attachments.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Facebook Pages

Description	Facebook Pages contains the content of the Facebook webpages that are cached.

Recovery method	Carving

Attribute	Description
Fragment	An HTML fragment of a Facebook webpage.

Additional Information

Facebook Status Updates/Wall Posts/Comments

Description	Facebook Status Updates/Wall Posts/Comments contains information about Facebook status updates, wall posts, and comments that are cached.
Recovery method	Carving

Attribute	Description
Sender ID	The Facebook ID of the sender.
Downloaded Sender Image	If Downloading Images from Web is enabled, the sender's profile picture can be fetched using the Facebook Graph API.
Sender Name	The name of the sender.
Receiver ID	The Facebook ID of the receiver.
Downloaded Receiver Image	If Downloading Images from Web is enabled, the receiver's profile picture can be fetched using the Facebook Graph API.

Attribute	Description
Receiver Name	The name of the receiver.
Status Update / Wall Post / Comment	The content of the status update, wall post, or comment.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time of the post.

Additional Information

Google+ Chat

Description	Google+ is a web-based social network that allows users to communicate publicly, share photos and videos and also message privately.
Recovery method	Carving

Attribute	Description
Type	Indicates whether or not the message is a sent or received message.
Email	The email address associated with the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The content of the message.

Additional Information

Instagram Pictures

Description	Instagram is a social media website where users share pictures.
Recovery method	Carving

Attribute	Description
Profile Image	The profile picture of the poster.
Downloaded Profile Image	The profile image of the poster, downloaded from the Internet.
User ID	The user ID of the poster.
User Name	The username of the poster.
Instagram Image	The picture that was posted, if found locally.
Downloaded Instagram Image	The picture that was posted, downloaded from the Internet.

Additional Information

Instagram Posts

Description	Instagram is a social media website where users share pictures.
Recovery method	Carving

Attribute	Description
Profile Image	The profile picture of the poster.
Download Profile image	The profile image of the poster, downloaded from the Internet.
Text	The content of the post.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the post was created.
User ID	The user ID of the poster.
User Name	The username of the poster.
Posted Image	The picture that was posted, if found locally.
Downloaded Posted Image	The picture that was posted, downloaded from the Internet.

Additional Information

LinkedIn Emails

Description	LinkedIn Emails contains carved emails that have been sent or received on LinkedIn. These email fragments can include sender and recipient names, subject, date and time, and the full message. Please note that, depending on the browser, these emails might be compressed and are decompressed as they are viewed.
Recovery method	Carving

Attribute	Description
Fragment	An HTML fragment of the email.

Additional Information

MySpace Chat - Messages

Description	MySpace Chat Messages contains messages sent or received in MySpace live chat. Information found within these attributes can include the status of the message, the date and time, the sender ID, the target ID, and the message itself. Some user info is also recoverable, such as the real name or username associated to a MySpace ID, image URL, and other information. This information is saved to a User Info report. This has been discontinued as of 2010.
Recovery method	Carving

Attribute	Description
Source ID	The account of the source.
Target ID	The account of the target.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The contents of the chat message.
Status	The sent status of the message.

Additional Information

MySpace Chat - User Info

Description	MySpace is a social networking website popular with music lovers.
Recovery method	Carving

Attribute	Description
User ID	The MySpace user ID.
UserName	The username used on MySpace.
Group	The group that the user is associated to (if applicable).
Image	The user's display picture.

Additional Information

MySpace Inbox Messages

Description	MySpace Inbox Messages contains sessages sent or received in MySpace live chat. Information found within these attributes can include the status of the message, the date and time, the sender ID, the target ID, and the message itself. Some user info is also recoverable, such as the real name or username associated to a MySpace ID, image URL, and other information. This information is saved to a User Info report. This has been discontinued as of 2010.

Recovery method	Carving

Attribute	Description
Sender	The sender of the message.
Subject	The subject of the message.
Message	The contents of the chat message.

Additional Information

Sina Weibo Carved Searches

Description	Sina Weibo is a Chinese microblogging (weibo) website. Akin to a hybrid of Twitter and Facebook, it is one of the most popular websites in China. This table carves for a user's searches.
Recovery method	Carving

Attribute	Description
Search Term	The term that was searched.

Additional Information

Sina Weibo Microblogs

Description	Sina Weibo is a Chinese microblogging (weibo) website. Akin to a hybrid of Twitter and Facebook, it is one of the most popular websites in China. This table captures microblogging information.
Recovery method	Carving

Attribute	Description
Nickname	The blogger's nickname.
User ID	The user ID of the blogger.
Downloaded Profile Picture	The profile picture of the user, downloaded from the Internet based on the user ID.
Microblog Text	The content of the blog.
Posted From URL	The URL from which the blog was posted.

Additional Information

Sina Weibo Search History

Description	Sina Weibo is a Chinese microblogging (weibo) website. Akin to a hybrid of Twitter and Facebook, it is one of the most popular websites in China. This table captures a user's searches that have been parsed from the filesys-tem.
Recovery method	Parsing

Attribute	Description
Search Term	The term that was searched.

Additional Information

Twitter

Description	Twitter is a social networking website that allows users to share status messages, known as tweets.
Recovery method	Carving

Attribute	Description
Name	The full name of the user.
Screen Name	The Twitter handle of the user (e.g. @username).
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the tweet was created.
Tweet Text	The content of the tweet.
In Reply To	Indicates whether the tweet was a reply to another user.
Status ID	The unique identifier for the tweet.
Tweet Source	The type of device or application that was used to create the tweet.
Geo	The geo-location of the user when they posted the

Attribute	Description
	tweet.
Retweeted	This identifies whether the tweet was a retweet.
Profile Img URL	The URL link to the profile picture of the user.

Additional Information

VK Wall Posts

Description	VK Wall Posts contains the wall postings on social networking site VK.-com.
Recovery method	Carving

Attribute	Description
Author	The author of the wall post.
Wall Text	The content of the wall text.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message Relative Timestamp	A relative timestamp for the VK wall post.

Additional Information

VK Web Messages

Description	VK Web Messages contains a combination of both VK instance messages and sent and received messages.
Recovery method	Carving

Attribute	Description
Message Sender	The sender of the message.
Message	The content of the message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message Relative Timestamp	A relative timestamp for the VK message.

Additional Information

Volatile Artifacts

Active Connections

Description	Active Connections contains a list of all active and inactive connections, as well as the TCP and UDP ports the device is currently listening to.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
Protocol	The protocol used for the connection (UDP/TCP).
Local Address	The local address of the connection. This value can either be IPv4 or IPv6.
Local Port	The port that the connection is originating from.
Remote Address	The remote address of the connection. This value can either be IPv4 or IPv6.
Remote Port	The port that the connection is heading to.
State	The state of the connection.
Process ID	The process ID of the connection.

Additional Information

DNS Cache

Description	DNS Cache contains a list of all the cached DNS Records for the device.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-	The date and time that the information was cap-

Attribute	Description
dd)	tured.
Record Name	The name of the DNS record.
Record Type	The DNS record type.
Record Type ID	The DNS record type's ID.
Length	The length of the record in bytes.
Record Value	The value of the DNS record.

Additional Information

Linux Active Users

Description	Active Users contains details of logged on users.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
User Name	The owner of the process.
TTY	Abbreviation of teletype, used to pass data to system and display.
From	IP address or machine name from where the artifact was found (optional).

Attribute	Description
Idle Time	The amount of time the user has been idle.
Login	The time the user logged in (linux and mac).
JCPU	The total run time of all system processes attached to the user's terminal.
PCPU	Elapsed time for the user's current process.
WHAT	The file name or folder location.

Additional Information

Linux Firewall Rules

Description	Linux Firewall Rules contains a list of all firewall rules applied on Linux endpoint.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
Zone	The name of the zone. A network zone defines the level of trust for network connections.

Attribute	Description
Target	Default behavior that handles incoming traffic that is not further specified. There options are - default, ACCEPT, REJECT, and DROP.
ICMP Block Inversion	When enabled, all ICMP message types are blocked, except for those in the ICMP block list.
Interfaces	The network interfaces associated with the zone.
Sources	To route incoming traffic into a specific source, add the source to the zone. The source can be an IP address or an IP mask in the Classless Inter-domain Routing (CIDR) notation.
Services	The list of the services added to the zone. This opens all necessary ports and modifies other settings according to the service definition file.
Ports	The list of open ports added to the zone.
Protocol	The list of protocols to allow traffic through the firewall.
Forwarded	Whether Intra Zone forwardng is enabled or not.
Masquerade	Whether IP masquerading is enabled or not. IP masquerading is a process where one computer acts as an IP gateway for a network.
Forward Ports	The list of rules to forward the port traffic.
Source Ports	The list of sources used by zone to sort and route the incoming traffic.
ICMP Blocks	Blocks selected Internet Control Message Protocol (ICMP) messages.
Rich Rules	The rich rules extends the elements (service, port, icmp-block, masquerade, forward-port and source-port) with additional source and destination addresses, logging, actions and limits for logs and actions. It can also be used for host or network white and black listing.

Additional Information

Mac Active Users

Description	Active Users contains details of logged on users.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
User Name	The owner of the process.
TTY	Abbreviation of teletype, used to pass data to system and display.
From	IP address or machine name from where the artifact was found (optional).
Idle Time	The amount of time the user has been idle.
Login	The time the user logged in (linux and mac).
WHAT	The file name or folder location.

Additional Information

Network ARP Info

Description	Network ARP info contains a list of cached Address Resolution Protocol (ARP) entries.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
Local IP Address	Local IP address for the ARP cache entry.
Local MAC Address	Local MAC Address for the ARP cache entry.
Type	Type of ARP cache entry.
Seconds since ARP entry used	Number of seconds since the ARP entry was used. Fragment only populated for Linux.
Seconds since ARP entry confirmed	Number of seconds since the ARP entry was confirmed. Fragment only populated for Linux.
Seconds since ARP entry updated	Number of seconds since the ARP entry was updated. Fragment only populated for Linux.

Additional Information

Network Shares

Description	Network Shares contains a list of all of resources that are shared on the endpoint.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
Name	The network name of the shared resource.
Path	The path of the directory to be shared.
Description	A description of the shared resource. Fragment only populated for Windows.
Share State	Indicates the state of the shared resource: Pending, Online, or Off-line. Fragment only populated for Windows.
Shadow Copy Enabled	Indicates whether shadow copies are enabled. Fragment only populated for Windows.
Enabled Protocols	A list of enabled data transfer protocols for this share point. Fragment only populated for Mac.
Data Transfer Protocol	Indicates the data transfer protocol of the share point: afp, ftp, or smb. Fragment only populated for Mac.
Record Name	The name of the share point when using the specified data transfer protocol. Fragment only populated for Mac.

Attribute	Description
Sharing Enabled	Indicates whether sharing is enabled. Fragment only populated for Mac.
Guest Access Enabled	Indicates whether guest access is enabled. Fragment only populated for Mac.
Read Only (Yes/No)	Indicates whether the share point is read only. Fragment only populated for Mac.
Inherit Privileges Enabled	Indicates whether inherit privileges are enabled. Fragment only populated for Mac.

Additional Information

Prefetch List

Description	Prefetch List contains a list of all prefetch files populated on the endpoint.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
File Path	The absolute file path of the prefetch file.

Additional Information

Running Processes

Description	Running Processes contains a list of all processes currently running on the endpoint.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
Process Name	The name of the process.
Process ID	The process ID (PID).
User Name	The owner of the process.
Session ID	The associated session ID.
Session Name	The name of the associated session.
Memory Usage (KB)	The amount of memory used by the process, indicated in KB.
CPU Time (dd.HH:mm:ss.ff)	The amount of time that the CPU has been running the process. Shown in dd.HH:mm:ss.ff format.
Command Line Call	The call to the command line that started the process.
Status	The status of the process.
Parent Process ID	The ID of the parent process (PPID).

Additional Information

Scheduled Jobs

Description	Scheduled Jobs contains a list of all scheduled jobs created using WMIC or the AT utility on the endpoint.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
Node	The name of the endpoint where the job is scheduled to run.
Command	The name of the command, batch program, or binary file and command-line parameters that the schedule service uses to invoke the job.
Days Of Month	Days of the month when a job is scheduled to run.
Days Of Week	Days of the week when a job is scheduled to run.
Description	A short textual description of the job.
Interact With Desktop	If true, the specified job is interactive and allows a user to give input to a scheduled job while it is running.
Job ID	The identifier number of the job.
Job Status	Status of execution the last time this job was scheduled to run.
Name	The label by which the job is known.

Attribute	Description
Owner	The user who submitted the job.
Priority	The importance of a job's execution.
Run Repeatedly	If True, a scheduled job runs repeatedly on specific days of the week or month.
Start Time	The time the job is scheduled to run. The format is: '********HHMMSS.MMMMMM(+-)OOO'.

Additional Information

Services

Description	Service List contains a list of all services currently running on the end-point.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
Service Name	The name of the service.
State	The state of the service.
Process ID	The process ID (PID).
Description	The description of the service.

Additional Information

Windows Active Users

Description	Active Users contains details of logged on users.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
User Name	The owner of the process.
Session Name	The name of the associated session.
ID	The associated session ID.
State	The state of the service.
Idle Time	The amount of time the user has been idle.
Logon Time	The time the user logged on on windows.

Additional Information

Windows Firewall Rules

Description	Windows Firewall Rules contains a list of all firewall rules applied on Windows endpoint.

Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
Rule Name	The name of the firewall rule.
Description	The description of the firewall rule.
Rule Enabled	Whether the rule is enabled and applied by Windows Firewall or not.
Direction	The direction (Inbound or Outbound) of the rule.
Profiles	The network location/profile the rule is applied to: private, public, or domain.
Grouping	The group the rule belongs to. Generally, the group describes the app or the Windows feature the rule belongs to.
Local Address	The local IP addresses to which the rule applies.
Local Port	The local ports to which the rule applies.
Remote Address	The remote IP addresses to which the rule applies.
Remote Port	The remote ports to which the rule applies.
Protocol (Type,Code)	The communication protocol to which the rules applies like TCP or UDP. In case of ICMPv4 or ICMPv6 protocol types, (Type, Code) shows ICMP message types to which the rules applies.

Attribute	Description
Edge Traversal	Edge traversal allows the computer to accept unsolicited inbound packets that have passed through an edge device, such as a network address translation (NAT) router or firewall.
Program Name	The complete path to the program to which the rule applies.
Services	The service to which the rule applies.
Interface Type	The interface types to which the rules applies.
Security	Authentication setting the rule is applied to: NotRequired, Authenticate, AuthEnc, AuthDynEnc, AuthNoEncap.
Rule Source	The source of the rule.
Action	The action can Allow or Block based on what the rule is supposed to do.

Additional Information

Web Related

360 Safe Browser Archived Keyword Search Terms

Description	360 Safe Browser is a web browser developed by Qihoo.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword that was searched.
URL	The URL that was invoked because of the search.

Additional Information

360 Safe Browser Archived Web History

Description	360 Safe Browser Archived Web History contains all of the websites the user has gone to, along with when they last visited the site, and how often they have visited the site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the website the user visited.
Title	The title of the website that the user visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the user last visited the website.
Visit Count	The number of times that the user has visited the website.
Typed Count	The number of times that the user has manually typed the website's URL.
ID	The 360 Safe Browser identifier of the website.

Additional Information

360 Safe Browser Autofill

Description	360 Safe Browser Autofill contains all of the values that the user has saved to fill in fields at a later date and time.
Recovery method	Parsing

Attribute	Description
Name	The name of the field to fill in.
Value	The value to perform the fill in with.
Count	The number of times that the autofill has been used.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was first created.

Additional Information

360 Safe Browser Autofill Profiles

Description	360 Safe Browser Autofill Profiles contains all of the profiles that are used to represent a person.
Recovery method	Parsing

Attribute	Description
Name	The name that the person goes by or uses.
Email	The email address to use to contact the person.
Number	The telephone number to use to contact the person.
Company	The company the person works at.
Address Line 1	The first line of the person's address (e.g. 123 Fake Street, Fake Town, Fake Country).
Address Line 2	The second line of the person's address (e.g. Suite 123 or Apt. 123).
City	The city that the person lives in.
State	The state or province that the person lives in.
Zipcode	The ZIP Code that the person lives in.
Country	The country that the person lives in.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the person modified the profile.

Additional Information

360 Safe Browser Bookmarks

Description	360 Safe Browser Bookmarks contains all of the websites the user has bookmarked.
Recovery method	Parsing

Attribute	Description
Title	The title of the website.
URL	The URL of the website.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was last modified.
Is Folder	Indicates whether the bookmark is a folder. The possible value for this field are Yes, No, or Invalid.
Parent Folder	The parent folder of the bookmark.

Additional Information

360 Safe Browser Cache Records

Description	360 Safe Browser Cache Records contains all of the files and their information that has been cached by the browser.
Recovery method	Parsing

Attribute	Description
URL	The URL that the file was downloaded from.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.

Attribute	Description
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was first visited.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The last time that the local cache was synced with the web-server.
File Type	The type of cache file.
Content Size (Bytes)	The size of the cache file.
Image	If the content file is an image, it will be displayed here.
Content	If the file is not an image, such as a JavaScript file, the raw bytes will be stored here.

Additional Information

360 Safe Browser Cookies

Description	360 Safe Browser Cookies contains all of the cookies saved to the browser.
Recovery method	Parsing

Attribute	Description
Host	The host that created the cookie.
Name	The name of the cookie.

Attribute	Description
Value	The cookie value.
Accessed Date/Time - UTC(yyyy-mm-dd)	The date and time that the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was created.
Expiration Date/Time - UTC(yyyy-mm-dd)	The date and time that the cookie expires.

Additional Information

360 Safe Browser Current Downloads

Description	360 Safe Browser Current Downloads contains all of the files currently being downloaded.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file being downloaded.
Download Source	The source URL where the file was downloaded.
Saved To	The local file location.
State	The current state of the download.

Attribute	Description
Opened By User	Indicates whether the downloaded file was opened by the user.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Bytes Downloaded	The number of bytes download.
File Size (Bytes)	The size of the file being downloaded, in bytes.

Additional Information

360 Safe Browser Current Session

Description	360 Safe Browser Current Session contains all of the sessions that are currently in use by the browser.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - (UTC)(yyyy-mm-dd)	The date and time that the URL was last visited.

Attribute	Description
Visit Count	The number of times the user accessed the URL.

Additional Information

360 Safe Browser Current Tabs

Description	360 Safe Browser Current Tabs contains all of the open tabs in the browser.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - (UTC)(yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.

Additional Information

360 Safe Browser FavIcons

Description	360 Safe Browser FavIcons contains all of the icons that belong to common webpages the user goes to.
Recovery method	Parsing

Attribute	Description
Page URL	The URL of the webpage.
Icon URL	The URL to the icon image.
Last Updated Date/Time - UTC(yyyy-mm-dd)	The last date and time when the icon was updated.
State	The current state of the download.
Opened By User	Indicates whether the downloaded file was opened by the user.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Bytes Downloaded	The number of downloaded bytes.
File Size (Bytes)	The size of the file being downloaded, in bytes.

Additional Information

360 Safe Browser History Index

Description	360 Safe Browser History Index contains the browsing history of the user.
Recovery method	Parsing

Attribute	Description
Page URL	The webpage URL.
Title	The title of the webpage.
Visited on Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Body	The HTML body of the webpage.

Additional Information

360 Safe Browser Last Session

Description	360 Safe Browser Last Session contains all of the sessions that were last open.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.

Attribute	Description
Title	The title of the webpage.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time that the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

360 Safe Browser Last Tabs

Description	360 Safe Browser Last Tabs contains all of the tabs that were last open.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time that the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

360 Safe Browser Logins

Description	360 Safe Browser Logins contains all of the logins for websites the user has saved.
Recovery method	Parsing

Attribute	Description
User Name	The username for the webpage.
Password	The password for the login of the webpage.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the login information was created.
URL	The URL to the webpage.

Additional Information

360 Safe Browser Saved Credit Cards

Description	360 Safe Browser Saved Credit Cards contains all of the credit card information the user has saved.
Recovery method	Parsing

Attribute	Description
GUID	The identifier of the credit card.
Name On Card	The name on the credit card.
Expiry Date	The date the credit card is supposed to expire in format 'month-year'.
Card Number	The number of the credit card.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the credit card information was last modified.

Additional Information

360 Safe Browser Shortcuts

Description	360 Safe Browser Shortcuts contains all of the shortcuts used by 360 Safe Browser for user entered URLs.
Recovery method	Parsing

Attribute	Description
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.

Attribute	Description
Last Access Date/Time - (UTC) (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the webpage.
Times Used	The number of times that the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (Typed URL or Bookmark).

Additional Information

360 Safe Browser Top Sites

Description	360 Safe Browser Top Sites contains all of the websites the user goes to most often.
Recovery method	Parsing

Attribute	Description
URL	The URL to the webpage.
Title	The title of the webpage.
Last Updated Date/Time - (UTC)	The last time that the information for the top site

Attribute	Description
(yyyy-mm-dd)	was updated.
Thumbnail	The thumbnail of the webpage.

Additional Information

360 Safe Browser Web History

Description	360 Safe Browser Web History contains all of the websites the user has gone to.
Recovery method	Parsing and carving

Attribute	Description
Date Visited Date/Time - (UTC) (dd/MM/yy)	The date and time that the URL was first visited.
URL	The URL that was accessed by the user.
Title	The title of the webpage.
Visit Count	The number of times the user accessed the URL.
Typed Count	The number of times the user has navigated to this page by typing in the address.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition

Attribute	Description
	type is 'link'.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time that the URL was last visited.

Additional Information

360 Safe Browser Web Visits

Description	360 Safe Browser Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Title	The title of the webpage that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a

Attribute	Description
	user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

Ashley Madison/Backpage Ads/Craigslist Ads/Plenty of Fish

Description	Ashley Madison/Backpage Ads/Craigslist Ads/Plenty of Fish contains recovered webpages from pagefile.sys.
Recovery method	Carving

Attribute	Description
Fragment	The fragment that was extracted.
Source	The location where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Bing Toolbar - Map History

Description	Bing Toolbar Map History contains information about maps and locations that were searched for using the Bing Toolbar.
Recovery method	Parsing

Attribute	Description
Location History	The previous location of the map.
Default Location	The default location of the map.
Default lat/long	The default latitude and longitude of the default location.
Show Traffic	Indicates whether the Show Traffic feature was turned on (True or False).
Default Zoom Level	The default zoom level for the map.
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Bing Toolbar - Search History

Description	Bing Toolbar Search History contains information about the search history for the Bing Toolbar.
Recovery method	Parsing

Attribute	Description
Search Term	The keyword that was searched for.
Search Date/Time - UTC (yyyy-mm-dd)	The date and time that the keyword search was conducted.
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Chrome

Google Chrome is free web browser developed by Google and is available on all major operating systems, for both mobile and desktop. As of 2016, Chrome usage represents over 70% of the world's total browser traffic.

Analyzing the websites a user visits and the time the visits occur can provide valuable insights about a user. One notable feature that Google Chrome has is that it allows users to sync their

bookmarks, browsing history, and more across multiple platforms and devices by using cloud sync accounts.

Forensic notes

Web Visits vs Web History

Chrome has two distinct artifacts that are very similar nature: Chrome Web Visits and Chrome Web History. Both of these artifacts are recovered from the History database. Chrome Web History is parsed from the URLS table and only contains information for the last visited date of a particular website. Chrome Web Visits can contain multiple entries for the same website, giving the examiner a more complete look at browser usage if the user visited a website multiple times. For example, if a user visits www.magnetforensics.com six times, the Chrome Web History artifact displays only the last time the site is visited, while the Chrome Web Visits artifact potentially displays records for all six instances. Chrome Web Visits was added in a later version of Chrome than Chrome Web History.

Carved web history

The Chrome / 360 Safe Browser / Opera Carved Web History is essentially the same as Chrome Web History except that it's recovered using carving and you may find additional deleted hits with it. The 360 Safe and Opera browsers are included in this artifact because when the data is carved, it's not possible to tell which browser the hit comes from as they're all formatted the same way.

Autofill and profile data

Chrome stores field data that the user has previously input as autofill and profile settings. For example, if you visit magnetforensics.com and login to the customer portal, browsers automatically save your username (and other details) so that you don't have to type it in each time you visit the site. This data is helpful for recovering usernames and other information that your user has filled out on various sites.

Sessions and tabs

When the system has an active session available, Chrome stores the browsing activity as the Chrome Current Session and any tabs that are open as Chrome Current tabs. The previous session and tabs are maintained in Chrome Last Session and Chrome Last Tabs so that the user can restore the last session and tabs if Chrome is closed.

Artifacts

Related resources

Artifact profile: Google Chrome

How does Chrome's 'incognito' mode affect digital forensics?

Forensic email analysis: browser artifacts you may find on a PC or laptop

Chrome Affiliations

Description	Chrome Affiliations contains information about visited pages and the domains their affiliated domains. Typical examples are; login page, advertiser, or CDN affiliated with a larger domain.
Recovery method	Parsing

Attribute	Description
Name	The name of the website visited.
URL	The url of the page visited.
Domain	The domain the visited page is affiliated with.

Attribute	Description
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time of the last visit to the affiliated url.

Additional Information

Chrome Archived Keyword Search Terms

Description	Chrome Archived Keyword Search Terms contains keyword search terms that were archived by the browser.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Chrome Archived Web History

Description	Chrome Archived Web History contains an archived history of old

	webpage visits.
Recovery method	Parsing

Attribute	Description
URL	The URL where the archived web history is located.
Title	The title of the archived web history.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.
Visit Count	The total visits to this URL.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
ID	The ID for the web history archive.

Additional Information

Chrome Autofill Profiles

Description	Chrome Autofill Profiles contains profiles that Chrome uses to fill in forms with saved values.
Recovery method	Parsing

Attribute	Description
Name	The name for the autofill profile.
Email	The email used in the the autofill profile.
Number	The phone number used in the autofill profile.
Company	Th company name used in the autofill profile.
Address Line 1	The address Line 1 used in the autofill profile.
Address Line 2	The address Line 2 used in the autofill profile.
City	The city used in the autofill profile.
State	The state used in the autofill profile.
Zipcode	The Zipcode used in the autofill profile.
Country	The country used in the autofill profile.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the profile was last modified.

Additional Information

Chrome Autofill

Description	Chrome Autofill contains records of the autofill values that Chrome saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time that the autofill was last used.

Additional Information

Chrome Bookmarks

Description	Chrome Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was added.
Parent	The name of the parent folder of the bookmark.

Additional Information

Chrome Cache Records

Description	Chrome Cache Records contains content that Chrome downloads and caches to speed up rendering times. Cached content can include pictures, text, HTML, JavaScript, and more.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached item.
Website	The website visted.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was first visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the record was last modified.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the cache was last synced with the server.
State	The state of the record. This may be Normal (Live), Doomed (Marked for Deletion), or Evicted (Deleted).
File Type	The type of file that was cached.
Content Size (Bytes)	The size of the cached file.
Picture	The cached picture if the file type is a picture. Otherwise, this

Attribute	Description
	column is empty.
Content	The cached file contents if the file type is not a picture. Otherwise, this column is empty.
File Name	The file name of the cached item.
MD5 Hash	An MD5 hash of the cached item if it is a picture. Otherwise, this column is empty.
SHA1 Hash	A SHA1 hash of the cached item if it is a picture. Otherwise, this column is empty.
PhotoDNA Hash	The hash of the cached item for PhotoDNA if it is a picture. Otherwise, this column is empty.

Additional Information

Chrome Cookies

Description	Chrome Cookies contains cookies that Chrome downloads from the Internet that contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	The domain of the cookie.
Name	The name of the cookie.

Attribute	Description
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Chrome Current Session

Description	Chrome Current Session contains information about the browser session that's currently underway.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.

Attribute	Description
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Current Tabs

Description	Chrome Current Tabs contains information about the tabs that are open in the current browser session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.

Additional Information

Chrome Downloads

Description	Chrome Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the download.
Download Source	The URL of the file that was downloaded.
Saved To	The location where the download was saved to.
State	The state of the download.
Opened	Indicates whether the download is opened by the user.
Start Time Date/Time - UTC (yyyy-mm-dd)	The download start time.
End Time Date/Time - UTC (yyyy-mm-dd)	The download end time.
Bytes Downloaded	The bytes that were downloaded.
File Size(Bytes)	The file size of the download.

Additional Information

Chrome Extensions

Description	Chrome Extensions contains information about the extensions that a user has installed on their computer.
Recovery method	Parsing

Attribute	Description
Application Name	The name of the Chrome plugin or extension.
Version	The version number of the plugin or extension.
Description	The description of the plugin or extension.
Install Date/Time - UTC (yyyy-mm-dd)	The install time in the Chrome/Webkit time.
State	The state of the plugin or extension on the google account (Enabled or Disabled).
Permissions	The list of permissions that the plugin or extension has, as recorded in the 'manifest.json' file.
Active Permissions	The list of active permissions that the plugin or extension has, as recorded in the 'Preferences' file.
Granted Permissions	The list of all granted permissions that the plugin or extension has, as recorded in the 'Preferences' file.
Withholding Permissions	States whether the permissions are being withheld, as recorded in the 'Preferences' file.
Installed by OEM	States whether the plugin or extension is installed by OEM (True

Attribute	Description
	or False).
Installed by Default	States whether the plugin or extension is installed by default (True or False).
From Bookmark	States whether the plugin or extension was installed from a bookmark (True or False).
From Webstore	States whether the plugin or extension was installed from the chrome webstore (True or False).
Author	The author.
Homepage	The homepage.

Additional Information

Chrome FavIcons

Description	Chrome FavIcons contains the favicons that Chrome displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite or bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Icon URL	The icon URL of the favicon.

Attribute	Description
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.
Icon	A preview of the favicon.

Additional Information

Chrome GPU Cache Records

Description	Chrome GPU Cache Records contains content that Chrome downloads and caches to speed up rendering times. Cached content can include textures, shader code, and other graphics related content.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached item.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was first visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the record was last modified.
State	The state of the record. This may be Normal (Live), Doomed (Marked for Deletion), or Evicted (Deleted).

Attribute	Description
Content Size (Bytes)	The size of the cached file.
Content	The cached file contents.

Additional Information

Chrome History Index

Description	Chrome History Index contains an index of the webpages the user has visited in the past.
Recovery method	Parsing

Attribute	Description
Page URL	The URL of the webpage.
Title	The title of the webpage.
Visited On Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was visited.
Body	A snippet of the webpage.

Additional Information

Chrome Keyword Search Terms

Description	Chrome Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Chrome Last Session

Description	Chrome Last Session contains information about the previous browser session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.

Attribute	Description
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Last Tabs

Description	Chrome Last Tabs contains information about the tabs that were open during the previous session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Logins

Description	Android Chrome Logins contains login information that a user provides in Chrome. Passwords are often encrypted, so you might not be able to recover them unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username of the login.
Password	The password of the login.
GUID	The GUID of the login found in the keychain.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the login was created.
Last Login Date/Time - UTC (yyyy-mm-dd)	The date and time when the login was last used successfully. If the login is unsuccessful for the page or account, this date and time will not be updated.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the login was last modified.
URL	The URL of the login page.

Additional Information

Chrome Media History

Description	Chrome Media History contains information about media that a user viewed.
Recovery method	Parsing

Attribute	Description
URL	The URL of the media page.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the media.
Played Seconds	The duration of the media file that has been played, in seconds.
Media Duration	The full duration of the media file, in seconds.
Current Position	The position in the video when the user stopped watching, in seconds.
Origin Link	The root URL of the media that was viewed.
Thumbnail URL	The thumbnail URL of the media that was viewed.

Additional Information

Chrome Saved Credit Cards

Description	Chrome Saved Credit Cards contains information about the credit cards that a user has saved to their device.
Recovery method	Parsing

Attribute	Description
Name On Card	The name of the person on the credit card.
Card Number	The number on the credit card.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was last modified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time that the credit card autofill information was last used.
GUID	An ID for the credit card.
Expiry Date	The date that the credit card is supposed to expire in month-year format.

Additional Information

Chrome Shortcuts

Description	Chrome Shortcuts contains all of the shortcuts used by Google Chrome for user entered URLs.
Recovery method	Parsing

Attribute	Description
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - UTC (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the webpage.
Times Used	The number of times that the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is link.
Type	The type of shortcut, such as typed url or bookmark.

Additional Information

To learn more about the Transition Type fragment, sign in to the Support Portal to read the article Google Chrome transition types.

Chrome Sync Accounts

Description	Chrome Sync Accounts contains information about the Chrome accounts that a user has logged in with. Chrome syncs data to the cloud so that a user can log in on multiple devices.
Recovery method	Parsing

Attribute	Description
Sync Id	The unique ID for the account that's used to sync data to the cloud.
Account Name	The name of the sync account.
Google Account	The GAIA ID of the sync account.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the sync account was synced.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the sync account was created.
Profile Picture URL	The profile picture URL of the sync account.
Active	Indicates whether or not the sync account is active.

Additional Information

Chrome Sync Data

Description	Chrome Sync Data contains information about the data that Chrome has synced to a user's account in the cloud.
Recovery method	Parsing and carving

Attribute	Description
Name	The name of the sync key.

Attribute	Description
Local Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the local system.
Server Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the server.
Local Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the local system.
Server Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the server.
Type	The type of data that is synced, such as bookmarks, favicons, type URLs, and more.
Parsed Content	The type parsed data.
Favicon Image	The actual favicon image.

Additional Information

Chrome Top Sites

Description	Chrome Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the site.
Title	The title of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Rank	A ranking of the website, in terms of how frequently it was visited. A value of 1 indicates the most frequent and values increment to 8 as frequency decreases. A value of -1 indicates a site that the user manually added to the list of top sites.
Thumbnail	The thumbnail of the site.

Additional Information

Chrome Web History

Description	Chrome Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.

Attribute	Description
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Chrome Web Visits

Description	Chrome Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Attribute	Description
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is link.
Visit Source	The source of the visit.

Additional Information
To learn more about the Transition Type fragment, sign in to the Support Portal to read the article Google Chrome transition types.

Edge Archived Keyword Search Terms

Description	Edge Archived Keyword Search Terms contains keyword search terms that were archived by the browser.
Recovery method	Parsing and carving

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Edge Cache Data

Description	Edge Cache Data contains information about cached data that was saved during browsing.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
URL	The URL of the cached data source.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when cached data was saved on the machine.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when cached data was modified on the source side.
File Type	The file type.
Visit Count	The number of times that the current cached file was accessed.
Content Size (Bytes)	The size of the cached file in bytes.
Image	The content of the file as an image, if the file is a supported image type.
File	The content of the file in raw bytes.
Original Path	The original absolute path to the cached file stored in the database.
Relative Path	A relative path to the file based on the location of the WebCache database. Doesn't exist is displayed if the file is not found.

Additional Information
This artifact allows an investigator to see the content a user views, it's origin, and how often the content is reused by the browser. By clearing the cache, the user can effectively delete these records. In some cases, records do not get deleted from the database, but in cases where the files are deleted, the original files cannot be restored.

Edge Extensions

Description	Edge Extensions contains information about the extensions or plugins installed in the user's Edge browser.
Recovery method	Parsing and carving

Attribute	Description
Package Name	The package name for the extension.
Application Name	The name of the extension.
Version Number	The most recent version number of the extension.
Created Date/Time - UTC (yyyy-mm-dd)	The time when this extension was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent time that the AppxManifest file for the extension was accessed (most likely the same as created time).
Last Modified Date/Time - UTC (yyyy-mm-dd)	The most recent time when the extension was updated.

Additional Information
Deleted and removed extensions can't be acquired, as all of this data is fully deleted from the browser when the user deletes an extension.

Edge Favorites

Description	Edge Favorites contains information about the websites a user favorites while browsing.
Recovery method	Parsing and carving

Attribute	Description
Favorite Name	The name given to the favorite.
Is Folder	Indicates whether the item is a folder or a URL for a website. This value is Yes if the item is a folder, and No if the item is a URL.
URL	The URL of the favorite.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the favorite was last modified.
Favicon URL	The URL of the favicon for the website.

Additional Information
This artifact allows an investigator to see the content a user views, it's origin, and how often the content is reused by the browser. By clearing the cache, the user can effectively delete these records. In some cases, records do not get deleted from the database, but in cases where the files are deleted, the original files cannot be restored.

Edge Keyword Search Terms

Description	Edge Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing and carving

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Edge Last Session

Description	Edge Last Session contains information about the last snapshot Edge took of the user's browsing session.
Recovery method	Parsing and carving

Attribute	Description
Page URL	The URL of the webpage.
Page Title	The title of the webpage.
Image	The browser generated snapshot of the page.
Body	The HTML body that was saved from the page.

Additional Information
At certain time intervals, Edge takes a snapshot of the user's browsing session. Using this artifact, an investigator is able to see exactly what the user was looking at, at the time of snapshot. The time interval between snapshots is unknown. Due to the interval, it's possible for a tab to be opened and closed quick enough that the tab isn't included in a snapshot.

Edge Reading Lists

Description	Edge Reading Lists contains collections of websites that the user has saved for offline viewing.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the Reading List page.
URL	The URL of the Reading List page.
Source Address	Other source information for the Reading List page.
Picture Path	A file path to pictures associated with the Reading List

Attribute	Description
	page.
Deleted	Indicates whether the user has deleted the Reading List page.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the Reading List page was added.
Last Access Date/Time - UTC (yyyy-mm-dd)	The date and time when the Reading List page was last accessed.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the Reading List page was updated.

Additional Information

Edge Top Sites

Description	Edge Top Sites lists the websites that the user visits frequently in the Edge browser. Top Sites can also be removed or added by the user.
Recovery method	Parsing and carving

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the page was added as a top site.
Updated Date/Time - UTC (yyyy-mm-	The date and time that the top site was updated.

Attribute	Description
dd)	
Favicon URL	The URL of the favicon for the top site.
Title	The title of the top site.
URL	The URL of the top site.

Additional Information

Edge/Internet Explorer 10-11 Content

Description	Edge/Internet Explorer 10-11 Content contains content that the browser caches, including webpages, pictures, and other resources.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
URL	The URL of the cache record.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.
Last Modified by Web Server Date/Time - UTC	The last time that the content was modified on the web server. This time is reflective of when the website created the content on the page and can be before the system being examined was built.

Attribute	Description
(yyyy-mm-dd)	
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time that the content was created on the local system.
Access Count	The number of times that the content was accessed through the web browser.
Filename	The filename of the cached content.
File Size (Bytes)	The size of the cache file.
Image	If the content is an image, it will be displayed here.
Content	If the file is not an image, such as a javascript file, the raw bytes will be stored here.

Additional Information

Edge/Internet Explorer 10-11 Cookies

Description	Edge/Internet Explorer 10-11 Cookies contains site usage information that websites send to the browser when a user visits their sites.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.

Attribute	Description
User	The local user on the system.
URL	The URL that the cookie is for.
Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.
Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time that the cookie was updated by the website at the URL visited.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Access Count	The number of times that the cookie was accessed.
Filename	The filename of the cookie.
File Size (Bytes)	The size of the cookie.

Additional Information

Edge/Internet Explorer 10-11 Daily/Weekly History

Description	Edge/Internet Explorer 10-11 Daily/Weekly History contains websites that a user visits using Internet Explorer, which are recovered from the daily/weekly history.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
URL	The URL that was accessed by the user.
User	The local user on the system.
Accessed Date/Time - Local (yyyy-mm-dd)	The most recent visit to the URL.
Access Count	The number of times that the website was accessed.
Browser Source	The directory of the browser from where the history is extracted from.

Additional Information
At the end of the week, all the daily .dat records are bundled into a weekly history and a new daily .dat file is created. This table represents a good secondary source for evidence if the main history is missing details or records.

Edge/Internet Explorer 10-11 Dependency Entries

Description	Edge/Internet Explorer 10-11 Dependency Entries contains a history of the websites that the browser is required to load in order to render a page.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.

Attribute	Description
URL	The URL visited by the user.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.

Additional Information
Records for this artifact are similar to the main history, the difference being that this artifact also includes dependencies for viewed websites (for example, if a viewed website contains pictures stored on another website).

Edge/Internet Explorer 10-11 Downloads

Description	Edge/Internet Explorer 10-11 Downloads contains information about the files that a user downloads using the browser.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
URL	The URL of the downloaded file.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last time that the user accessed the downloaded URL.
Redirect URL	The previous URL that led the user to the downloaded URL.
Download Location	The local path where the file was saved.

Attribute	Description
Temporary Download Location	The local path where the file was saved temporarily (usually while downloading).

Additional Information
Internet Explorer 9 introduced a new integrated download manager which stores the details of downloaded files in a new download INDEX.DAT file. This file has a different structure to the standard INDEX.DAT files.

Edge/Internet Explorer 10-11 Main History

Description	Edge/Internet Explorer 10-11 Main History contain records of the websites that a user visits using Internet Explorer, which are recovered from the main history.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
URL	The URL that was accessed by the user.
User	The local user on the system.
Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.
Page Title	The title of the webpage.

Attribute	Description
Access Count	The number of times that the website was accessed.
Browser Source	The directory of the browser from where the history is extracted from.

Additional Information
The access count does not always accurately represent the real access count. These values should only be used as an estimate.

Firefox Add-ons

Description	Firefox Add-ons contains the add-ons from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
Name	The name of the add-on.
Version	The version the add-on.
Installed Date/Time - UTC (yyyy-mm-dd)	The date and time when the add-on was installed.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the add-on was updated.
Extension Enabled	Indicates whether the add-on is enabled by the

Attribute	Description
	user.
Description	The description of the add-on.

Additional Information

Firefox Bookmarks

Description	Firefox Bookmarks contains the bookmarks from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
URL	The URL of the website that was bookmarked.
Added Date/Time - UTC (yyyy-MM-dd)	The date and time that the bookmark was created.
Last Modified Date/Time - UTC (yyyy-MM-dd)	The date and time that the field was last modified.
Title	The title of the bookmark.
Bookmark Type	The type of bookmark (Bookmark Item or Bookmark Folder).

Additional Information

Firefox Cache Records

Description	Firefox Cache Records contains all of the cached entries in the Firefox Cache Map.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached entry.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cached entry was created.
MIME Type	The MIME type of the cached data.
Content Size (Bytes)	The content size of the cached data.
Image	The image that should one be associated with the cached entry.
Content	The content that should any be associated with the cached entry.

Additional Information

Firefox Cookies

Description	Firefox Cookies contains the cookies from the Firefox web browser on a device.

Recovery method	Parsing

Attribute	Description
Host	The host domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-MM-dd)	The date and time that the cookie was last accessed.
Created Date/Time - UTC (yyyy-MM-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-MM-dd)	The date and time when the cookie will expire, if it is set to expire.
Path	The path to the cookie.

Additional Information

Firefox Downloads

Description	Firefox Downloads contains the downloads from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file being downloaded.
Download Source	The URL of the file being downloaded.
Start Date/Time - UTC (yyyy-MM-dd)	The date and time when the download was started.
End Date/Time - UTC (yyyy-MM-dd)	The date and time when the download was ended.
Saved To	The path to where the file was downloaded to.
Temp Path	The path to where the file was saved during downloading.
State	The state of the download can be Download In Progress, Download Complete, Download Stopped, or Download Paused.
Referrer	If the webpage used a mirror for downloading, this value is the path to the original download URL.

Additional Information

Firefox FavIcons

Description	Firefox FavIcons contains the favicons from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
URL	The URL of the icon.

Additional Information

Firefox FormHistory

Description	Firefox FormHistory contains the form history from the Firefox web browser on a device.
Recovery method	Parsing and carving

Attribute	Description
Field Name	The name of the field.
Value	The value of the field.
First Used Date/Time - UTC (yyyy-MM-dd)	The date and time that the field was first used.
Last Used Date/Time - UTC (yyyy-MM-dd)	The date and time that the field was last used.
Times Used	The number of times that the field has been used.
ID	The unique ID of the field.

Additional Information

Firefox Input History

Description	Firefox Input History contains the input to forms from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
URL	The URL that the input was given to.
Input	The value that was given.
Use Count	The number of times that the input has been used.
ID	The unique ID of the input.

Additional Information

Firefox Logins

Description	Firefox Logins contains login information for websites that a user logs in to using the browser.
Recovery method	Parsing

Attribute	Description
URL	The URL of the login page.

Attribute	Description
Username	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the data was created.

Additional Information

Firefox Private Browsing History

Description	Firefox Private Browsing History contains the URLs that were loaded during a Private Browsing session from the Firefox web browser on a device.
Recovery method	Carving

Attribute	Description
URL	The URL.

Additional Information

Firefox SessionStore Artifacts

Description	Firefox SessionStore Artifacts contains the webpages from the last active session from the Firefox web browser on a device.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the webpage.
URL	The URL of the webpage.
Referrer URL	The URL of the webpage, if the webpage was a redirect.

Additional Information

Firefox Web History

Description	Firefox Web History contains the webpages from the last active session from the Firefox web browser on a device.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the webpage.
Last Visited Date/Time - UTC (yyyy-MM-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage.
Visit Count	The number of times that the webpage has been visited.
Typed	Indicates whether the user typed the URL (Yes or No).

Additional Information

Firefox Web Visits

Description	Firefox Web Visits contains all of the non-archived URL visits for Firefox.
Recovery method	Parsing

Attribute	Description
URL	The URL that was visited.
Title	The title of the page that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the page was visited.
Typed	Indicates whether the user typed the URL (Yes or No).
Transition Type	Identifies how the transition to the page happened.

Additional Information

Flash Cookies

Description	This artifact has been deprecated and is no longer supported in AXIOM. Flash cookies are Internet browser cookies that are saved when a user

	watches a flash video (e.g. YouTube).
Recovery method	Carving

Attribute	Description
Cookie Name	The name of the cookie.
Content	The flash content of the cookie. This content is essentially serialized ActionScript code. Primitive values such as integers and strings are shown, as well as more complicated data structures such as objects and arrays. A complex data structure's value is shown only once, along with an "object ID" that gets generated. For all subsequent references to that structure in the content, it's referred to by the generated object ID.
Domain	The domain or host that created the cookie.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Google Analytics First Visit Cookies

Description	Google Analytics First Visit Cookies contains information about Google

	Analytics first-visit cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Creation DateTime	The date and time when the site was first visited.
Most Recent Visit Date/Time	The date and time of the most recent session.
2nd Most Recent Visit Date/Time	The date and time of the previous session.
Hits	The number of visits.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics First Visit Cookies Carved

Description	Google Analytics First Visit Cookies Carved contains information about Google Analytics first-visit cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Creation DateTime	The date and time when the cookie was created.
Most Recent Visit Date/Time	The date and time of most recent session.
2nd Most Recent Visit Date/Time	The date and time of the previous session.
Hits	The number of visits.

Additional Information

Google Analytics Referral Cookies

Description	Google Analytics Referral Cookies contains information about Google Analytics referral cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Cookie Source	The source URL used to reach the site.
Host	The domain of the URL.
Update Date/Time	The last time that the cookie was updated.
Campaign	The method of referral.
Access Method	Indicates whether the site was accessed organically or was referred.

Attribute	Description
Keyword	The keywords used to arrive at the site.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics Referral Cookies Carved

Description	Google Analytics Referral Cookies Carved contans information about Google Analytics referral cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Cookie Source	The source URL used to reach the site.
Host	The domain of the URL.
Update Date/Time	The last time that the cookie was updated.
Campaign	The method of referral.
Access Method	Indicates whether the site was accessed organically or was referred.
Keyword	The keywords used to arrive at the site.

Additional Information

Google Analytics Session Cookies

Description	Google Analytics Session Cookies contains information about Google Analytics session cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start time of the current sesion.
Outbound Link Events Left	
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics Session Cookies Carved

Description	Google Analytics Session Cookies Carved contains information about Google Analytics session cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start date and time of the current sesion.
Outbound Link Events Left	

Additional Information

Google Analytics URLs

Description	Google Analytics URLs contains URLs that are discovered in other artifacts that are related to Google Analytics.
Recovery method	Carving

Attribute	Description
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	The domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.

Attribute	Description
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics URLs Carved

Description	Google Analytics URLs Carved contains information about Google Analytics URLs that are recovered using carving.
Recovery method	Carving

Attribute	Description
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	The domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.

Attribute	Description
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.

Additional Information

Google Toolbar

Description	The Google toolbar is a browser add-on where a user can perform Google searches. While there are many different features to the Google Toolbar, search history is the focus. Search history can be either typed or done by autocomplete. It's also possible to determine where the user's search comes from, whether it is Google Search, YouTube, Google Maps, Google News, etc.
Recovery method	Parsing

Attribute	Description
Search	The keyword that was searched for.
Search Type	The type of Google search that the user completed (pictures, web, etc.).

Additional Information

Internet Explorer Cache Records

Description	Internet Explorer Cache Records contains temporary Internet files that are written locally when the user views pages from the Internet.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the cache record.
User	The local user.
Last Modified by Web Server Date/Time - UTC (yyyy-mm-dd)	The last time that the content was modified on the web server. This time is reflective of when the website created the content on the page, and this can be from before the system being examined was built.
Last Checked by Local Host Date/Time - UTC (yyyy-mm-dd)	The date and time that the content was checked for recency on the local system.
Cache Retrieval Count	The number of times that the cache record was requested by the browser.
Filename	The name of the file.
File Type	The filename of the cached content.
Content Size (Bytes)	The size of the cached file.

Attribute	Description
Image	If the content file is an image, it will be displayed here.
Content	If the file is not an image, such as a JavaScript file, the raw bytes will be stored here.

Additional Information

Internet Explorer Cookie Records

Description	Internet Explorer Cookie Records contains site usage information that web-sites send to the browser when a user visits their sites.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that created the cookie.
User	The user of the system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL was accessed.
Last Modified by Web Server Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL record was modified.
Visit Count	The number of times that the URL was vis-ited.
Web Page Title	The title of the webpage.
File Name	The name of the cookie file.

Additional Information

Internet Explorer Cookies

Description	Internet Explorer Cookies contains site usage information that websites send to the browser when a user visits their sites.
Recovery method	Parsing

Attribute	Description
Host	The host that created the cookie.
Name	The name of the cookie.
Value	The cookie value.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Flags	The flags associated with the cookie.

Additional Information

Internet Explorer Downloads

Description	Internet Explorer Downloads contains information about the files that a

	user downloads using the browser.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL for the file download.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was downloaded.
Status	The download status.
Saved To	The local path where the file was saved.
Referrer URL	The previous URL that led the user to the download URL.
File Size (Bytes)	The size of the file in bytes.
Source IP	The IP address of the download URL.

Additional Information

Internet Explorer Favorites

Description	Internet Explorer Favorites contains webpages that the user has set as a favorite.
Recovery method	Parsing and carving

Attribute	Description
Favorite Name	The name of the favorite as it shows up in Internet Explorer.
URL	The URL of the favorite.
Modified Date/Time - UTC (yyyy-mm-dd)	The last time that the user modified the favorite.
User	The user to whom the favourite belongs.
Favorites Root Location	The local path that is the root storage point for the favorite.
Folder Structure	The folder structure under which the favorite will show up in Internet Explorer.
Icon URL	The URL of the icon for the favorite if an icon does exist.

Additional Information

Internet Explorer InPrivate/Recovery URLs

Description	Internet Explorer InPrivate/Recovery URLs contains URLs visited during InPrivate browsing that are saved in Internet Explorer recovery files (used to recover tabs in the event of a crash).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that was visited.
File Create Date/Time - UTC (yyyy-mm-dd)	The date and time that the Internet record was created.
Description	The title of the website.
Local MAC address	The MAC address of the local machine.

Additional Information

Internet Explorer Leak Records

Description	Internet Explorer Leak Records contains browser history records that are scheduled for deletion.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL visited.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL record was modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL was accessed.
Visit Count	The number of times that the URL was visited.

Additional Information

LEAK artifacts are created when an error occurs while the system attempts to delete a record and the Temporary Internet File is unavailable for some reason.

Internet Explorer Main History

Description	Internet Explorer Main History contains websites that a user visits using Internet Explorer, which are recovered from the main history.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that was visited.
User	The local user.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Last visited (2nd Timestamp) Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Web Page Title	The webpage title.

Additional Information

Internet Explorer PrivacIE Records

Description	Internet Explorer PrivacIE Records contains websites that a user visits while having the privacy settings turned on.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL visited.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL record was modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL was accessed.
Visit Count	The number of times that the URL was visited.

Additional Information

Internet Explorer Typed URLs

Description	Internet Explorer Typed URLs contains URLs that the user types directly into the address bar for Internet Explorer.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that was typed into the address bar.
Last Entered Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last typed.

Additional Information
This includes data that a user pastes into the address bar, as well as instances when a user starts typing in the address bar and clicks on a suggestion from the browser. You may also see local paths and network locations here when the user types a location in Windows Explorer.

Internet Explorer Weekly History

Description	Internet Explorer Weekly History contains websites that a user visits using Internet Explorer, which are recovered from the weekly history.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that was visited.
User	The local user.
Last Visited Date/Time (local time) (yyyy-mm-dd)	The date and time that the URL was last visited. This date is local to the machine that visited the website.
Weekly History File Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the weekly history file was created.

Attribute	Description
Visit Count	The number of times that the user accessed the URL.
Web Page Title	The webpage title.

Additional Information
At the end of the week, all the daily .dat records are bundled into a weekly history and a new daily .dat file is created. This table represents a good secondary source for evidence if the main history is missing details or records.

Magnet Web Page Saver Captured HTML

Description	This table contains information on the HTML of a webpage captured by Magnet Web Page Saver.
Recovery method	Parsing

Attribute	Description
URL	The URL of the captured webpage.
Web Page Title	The title of the webpage.
Captured Date/Time	The date and time when the webpage was captured.
MD5 Hash	The MD5 hash of the captured HTML body.
HTML Source	The HTML source of the captured webpage.

Additional Information

Magnet Web Page Saver Captured Media

Description	This table contains information on the media of a webpage captured by Magnet Web Page Saver.
Recovery method	Parsing

Attribute	Description
URL	The URL of the captured webpage.
Resource URL	The URL of the captured media.
Captured Date/Time	The date and time when the webpage was captured.
MD5 Hash	The MD5 hash of the captured media.

Additional Information

Magnet Web Page Saver Captured Webpage

Description	This table contains information on the screenshots of a webpage collected by Magnet Web Page Saver.
Recovery method	Parsing

Attribute	Description
URL	The URL of the captured webpage.

Attribute	Description
Web Page Title	The title of the webpage.
Captured Date/Time	The date and time when the webpage was captured.
MD5 Hash	The MD5 hash of the screenshot of the captured webpage.

Additional Information

Malware/Phishing URLs

Description	Malware/Phishing URLs contains records that are believed to be either malware or phishing related URLs.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the website.
URL	The URL of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact that the URL belongs to.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Opera Archived Keyword Search Terms

Description	Opera is a web browser developed by Opera Software, and opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Keyword Search Term	The keyword that was searched.
URL	The URL that was invoked by the search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Opera Archived Web History

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Date Visited	The date and time when the URL was first visited.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
URL	The URL that was accessed by the user.
Title	The title of the webpage.
Visit Count	The number of times that the user accessed the URL.
Typed Count	The number of times the user has navigated to this page by typing in the address.
Transition Type	Describes how the browser navigated to a particular URL on a particular visit. For example, if a user visits a page by clicking a link on another page, the transition type is "Link".
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.

Additional Information

Opera Autofill Profiles

Description	Opera is a web browser developed by Opera Software, and uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Name	The name of the user.
Email	The user's email.
Number	The user's phone number.
Company	The user's company.
Address Line 1	The user's address.
Address Line 2	The user's address.
City	The user's city.
State	The user's state.
Zipcode	The user's ZIP Code.
Country	The user's country.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the autofill profile was last modified.

Additional Information

Opera Bookmarks

Description	Opera is a web browser developed by Opera Software, and uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Name	The name of the bookmark.
URL	The URL that was bookmarked.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Parent	The parent bookmarks folder (if applicable).
Type	The type of bookmark.

Additional Information

Opera Cache Records

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that the file was downloaded from.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was first visited.

Attribute	Description
Last Sync Date/Time - UTC (yyyy-mm-dd)	The last time that the local cache was synced with the web-server.
File Type	The type of cache file.
Content Size (Bytes)	The size of the cache file.
Image	If the content file is an image, it will be displayed here.
Content	If the file is not an image (e.g. a javascript file), the raw bytes will be stored here.

Additional Information

Opera Cookies

Description	Opera is a web browser developed by Opera Software, and uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Host	The host that created the cookie.
Name	The name of the cookie.
Value	The cookie value.

Attribute	Description
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie expires.
Path	The path to the cookie.

Additional Information

Opera Current Session

Description	Opera is a web browser developed by Opera Software, and Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Visit Count	The number of times that the user accessed the

Attribute	Description
	URL.
Redirect URL	The URL to use to redirect, if applicable.

Additional Information

Opera Current Tabs

Description	Opera is a web browser developed by Opera Software, and Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect, if applicable.

Additional Information

Opera Downloads

Description	Opera is a web browser developed by Opera Software, and uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file being downloaded.
Download Source	The source URL where the file was downloaded.
Saved To	The local file location.
State	The current state of the download.
Opened By User	If the downloaded file was opened by the user.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Bytes Downloaded	The number of bytes downloaded.
File Size (Bytes)	The total file size in bytes.

Additional Information

Opera History Index

Description	Opera is a web browser developed by Opera Software, and uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Page URL	The webpage URL.
Title	The title of the webpage.
Visited On Date/Time - UTC (yyyy-mm-dd)	The date and time tha the URL was last visited.
Body	The HTML body of the webpage.

Additional Information

Opera Keyword Search Terms

Description	Opera Keyword Search Terms contains information about the keyword search terms that a user entered.
Recovery method	Parsing and carving

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Opera Last Session

Description	Opera is a web browser developed by Opera Software, and uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect, if applicable.

Additional Information

Opera Last Tabs

Description	Opera is a web browser developed by Opera Software, and uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL used to redirect, if applicable.

Additional Information

Opera Logins

Description	Opera is a web browser developed by Opera Software, and uses the Blink

	layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL the autofill was extracted from.
User Name	The username to be auto-populated.
Password	The password that was remembered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the autofill was saved.

Additional Information

Opera Media History

Description	Opera Media History contains information about media that a user viewed.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the media page.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.

Attribute	Description
Title	The title of the media.
Played Seconds	The duration of the media file that has been played, in seconds.
Media Duration	The full duration of the media file, in seconds.
Current Position	The position in the video that the user stopped watching, in seconds.
Origin Link	The root URL of the media that was viewed.
Thumbnail URL	The thumbnail URL of the media that was viewed.

Additional Information

Opera Saved Credit Cards

Description	Opera is a web browser developed by Opera Software, and uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
GUID	A unique identifier for the credit card.
Name On Card	The name on the credit card.

Attribute	Description
Expiry Date	The date the credit card is supposed to expire in format 'month-year'.
Card Number	The credit card number.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the credit card information was modified.

Additional Information

Opera Search Field History

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Search Entries	The term that was searched for.

Additional Information

Opera Shortcuts

Description	Opera Shortcuts contains all of the shortcuts used by Opera for user entered URLs.
Recovery method	Parsing and carving

Attribute	Description
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - (UTC) (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the webpage.
Times Used	The number of times that the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

Additional Information

Opera Top Sites

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time when the top site was updated.
Thumbnail	A thumbnail of the webpage.

Additional Information

Opera Typed History

Description	Opera is a web browser developed by Opera Software. Web history are recently visited webpages. Opera stores a user's browsing history so that he or she can view it later. This search carves and parses web history from the Opera web browser, including the typed history (i.e. URLs or search terms entered by the user). The entire history file is not required; single records can be carved from live RAM captures and unallocated clusters, and so on.

Recovery method	Parsing and carving

Attribute	Description
Last Typed Date/Time - UTC (yyyy-mm-dd)	The last date and time that the content was typed.
Typed URL/Data	The content that was typed. This could be a URL or other data.
Type	The type of content that was typed (e.g. URL).

Additional Information

Opera Web History

Description	Opera is a web browser developed by Opera Software. Web history are recently visited webpages. Opera stores a user's browsing history so that he or she can view it later. This search carves and parses web history from the Opera web browser, including the typed history (i.e. URLs or search terms entered by the user). The entire history file is not required; single records can be carved from live RAM captures and unallocated clusters, and so on.
Recovery method	Parsing and carving

Attribute	Description
Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the user visited the website.
URL	The URL accessed.
Title	The webpage title.
Visit Count	The number of times that the user has gone to the website.
Typed Count	The number of times that the user has typed out the website.

Additional Information

Pornography URLs

Description	Pornography URLs contains records that are believed to be pornography related URLs.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the website.
URL	The URL of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.

Attribute	Description
Artifact	The name of the artifact that the URL belongs to.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information
For a list of the URLs that are targeted by this artifact, see Pornography domains.

Rebuilt Webpages

Description	Rebuilt Webpages contains the data that allows for the reconstruction of webpages.
Recovery method	Not applicable

Attribute	Description
Page Title	The title.
URL	The URL.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the original record was created.
Domain	The domain.
Cache Table	The table the data to re-construct the page came from.
Cache RowID	The row ID in the table that constructed the rebuilt webpage.

Additional Information

Safari Bookmarks

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to webpages that have been bookmarked.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the bookmarked webpage.
Title	The title of the bookmarked webpage.
Type	The type of bookmark (for example, Bookmark, Favorite, and Folder)
Read	No data is populated for this fragment on Windows.
Added Date/Time - UTC (yyyy-mm-dd)	Indicates the date and time that the bookmark was added.
Last Visited Date/Time - UTC (yyyy-mm-dd)	No data is populated for this fragment on Windows.
Modified Date/Time - UTC (yyyy-mm-dd)	Indicates the date and time that the bookmark was modified.

Attribute	Description
Locally Added	Indicates whether the bookmark was created on the local device or a synced device with the same Apple ID. This data is not always available for every bookmark on Windows.

Additional Information

Safari Cache Records

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to webpages that have been cached on the local system.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL from which the file was downloaded.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cache file was created.
File Type	The type of the cached file.
Content Size	The size of the cached file.
Image	If the content file is an image, it will be displayed in this column.
Content	If the file is not an image (e.g. if it is a javascript file), the raw file content will be stored here.

Additional Information

Safari Downloads

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to files that have been downloaded from Safari.
Recovery method	Parsing and carving

Attribute	Description
Download URL	The URL of the downloaded file.
Saved to Path	The local path where the download was saved.
Download Start Date/Time - UTC (yyyy-mm-dd)	The date and time the download started.
Download End Date/Time - UTC (yyyy-mm-dd)	The date and time the download finished.
Download Identifier	The unique identifier for the download.
Amount Downloaded (Bytes)	The number of bytes downloaded.
Size of Download (Bytes)	The size of the download in bytes.

Additional Information

Safari History

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures history entries which have been parsed from the filesystem.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of a visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Redirect URL	The URL that the user was redirected to.
Title	The title of the webpage.
Visit Count	The number of times that the URL was visited.
Visit Source	Indicates whether the website was viewed on the local device or on a synced device.

Additional Information

Safari iCloud Devices

Description	Safari iCloud Devices contains information about the devices that are synced to an iCloud account. Each device can access any browser tabs that are synced to the account.

Recovery method	Parsing and carving

Attribute	Description
Unique Device Identifier	A unique ID for the device that is accessing the tab.
Device Name	The name of the device that is linked to the iCloud account.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the device first synced to the iCloud account.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the device last synced with the iCloud account.

Additional Information

Safari iCloud Tabs

Description	Safari iCloud Tabs contains information about tabs that have been opened in the browser and synced to an iCloud account. Synchronized tabs are available to any device that logs in to the iCloud account.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the tab.

Attribute	Description
URL	The URL address of the tab.
Unique Device Identifier	A unique ID for the device that is accessing the tab.
Device Name	The name of the device that is accessing the tab.
Tab ID	The unique ID of the tab.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was last modified.
Modified By	The name of the device that last modified the tab.
Close Requested	Indicates whether a close request has been opened for the tab.
Close Request Date/Time - UTC (yyyy-mm-dd)	The date and time when the close request was created.

Additional Information

Safari Last Session

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to the user's last session with Safari.
Recovery method	Parsing and carving

Attribute	Description
Tab URL	The webpage URL.
Tab Title	The title of the webpage.

Additional Information

Safari Top Sites

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to the user's top sites.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Feed Last Update Time	The date and time that the top site content was last updated.
Feed URL	The URL of the RSS feed.

Additional Information

SharePoint Discussions

Description	This table captures information related to discussions held on SharePoint.
Recovery method	Carving

Attribute	Description
Subject	The subject of the discussion.
Discussion Link	A link to the discussion.
Fragment	A fragment of the discussion.
Modified Date/Time - Local Time	The date and time when the content was last modified.
Created By	The user who created the content.
Creator Link	A link to the user that created the content.
Reply Count	The number of replies in the discussion.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

SharePoint Recycle Bin

Description	This table captures information about content in a SharePoint recycle bin.

Recovery method	Carving

Attribute	Description
Name	The name of the file in the recycle bin.
Type	The type of the file in the recycle bin.
Original Location	The file's original location.
Creator Name	The user who created the file.
Creator Email Address	The email address of the user who created the file.
Deleted Date/Time - Local Time	The date and time that the file was deleted.
Size	The size of the file.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

SharePoint Shared Documents

Description	This table captures information related to shared documents stored on SharePoint.
Recovery method	Carving

Attribute	Description
Content Type	The type of the content.
Content Name	The name of the conten.t
Content Link	A link to the content.
Modified Date/Time - Local Time	The date and time when the content was last modified.
Modified By	The user that modified the content.
Modified By Link	A link to the user who modified the content.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

WebKit Browser Session/Tabs (Carved)

Description	WebKit Browser Sessions/Tabs contains information about the browser sessions and tabs that the user has open, while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. The usage of other browsers, such as Firefox and Safari, aren't likely to appear under this artifact.
Recovery method	Carving

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

WebKit Browser Web History (Carved)

Description	WebKit Browser Web History contains information about the websites that a user visits while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. The usage of other browsers aren't likely to appear under this artifact, however, some URLs found by other browsers may also be found by this artifact.
Recovery method	Carving

Attribute	Description
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that this webpage was last visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

XBox 360 Internet Explorer Cache Records

Description	Internet explorer is a Windows-based desktop application for browsing the internet. All Windows computers are pre-loaded with this web-browser as the default internet browser.
Recovery method	Carving

Attribute	Description
URL	The URL of the cache record.
User	The local user.
Last Modified by Web Server	The last time that the content was modified on the web server. This time is reflective of when the website created the content on the page

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	and can be before the system being examined was built.
Last Checked by Local Host Date/Time - UTC (yyyy-mm-dd)	The date and time that the content was checked for recency on the local system.
Cache Retrieval Count	The number of times that the item was retrieved from the cache.
Filename	The name of the file.
File Type	The filename of the cached content.
Content Size (Bytes)	The size of the cache file.
Image	If the content file is an image, it will be displayed here.
Content	If the file is not an image, as in the case of a JavaScript file for example, the raw bytes will be stored here.

Additional Information

XBox 360 Internet Explorer Daily History

Description	Internet explorer is a Windows-based desktop application for browsing the Internet. All Windows computers are pre-loaded with this web-browser as the default Internet browser.
Recovery method	Carving

Attribute	Description
URL	The URL that was visited.
User	The local user.
Last Visited Date/Time (local time) (yyyy-mm-dd)	The local date and time that the URL was last visited.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time that the URL was last visited.
Visit Count	The number of times that the URL was visted.
Web Page Title	The webpage title.

Additional Information

XBox 360 Internet Explorer Favorites/Recent/Featured Items

Description	Internet explorer is a Windows-based desktop application for browsing the Internet. All Windows computers are pre-loaded with this web-browser as the default Internet browser.
Recovery method	Carving

Attribute	Description
URL	The URL of the item.
Display Name	The name of the item.

Additional Information

XBox 360 Internet Explorer Weekly History

Description	Internet explorer is a Windows-based desktop application for browsing the Internet. All Windows computers are pre-loaded with this web-browser as the default Internet browser.
Recovery method	Carving

Attribute	Description
URL	The URL that was visited.
User	The local user.
Last Visited Date/Time (local time) (yyyy-mm-dd)	The local date and time that the URL was last visited.
Weekly History File Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the weekly history file was created.
Visit Count	The number of times that the URL was visited.
Web Page Title	The webpage title.

Additional Information

XBox Internet Explorer Main History

Description	Internet explorer is a Windows-based desktop application for browsing the Internet. All Windows computers are pre-loaded with this web-browser as the default Internet browser.
Recovery method	Carving

Attribute	Description
URL	The URL that was visited.
User	The local user.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time that the URL was last visited.
Last Visited (2nd Timestamp) Date/Time - (UTC) (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the URL was visted.
Web Page Title	The webpage title.

Additional Information

YARA Rules

YARA Rule Matches

Description	The YARA artifact contains information about files and processes that matched with conditions specified in a YARA rule.
Recovery method	Parsing

Attribute	Description
File Name	The name and extension of the file whose content matched with the condition(s) from the YARA rule. The value is blank if the match came from a process (executable/application that was loaded into memory at the time of the memory dump) during memory analysis using the Comae plugin option.
File size (bytes)	The size of the file in bytes. The value is blank if the match came from a Process.
Process Name	The name of the process that matched with the condition(s) from the YARA rule. The value is blank if the match came from a file.
Process ID	The ID of the process (PID). The value is blank if the match came from a File.
Matched rule set(s)	List of the paths and respective YARA rule sets that had a match.
Matched rule	The YARA rule name that a match was found for.
Matching conditions	List of conditions for the YARA rule that had a match.

Additional Information

Android

Advanced Search Tools

Dynamic Application Finder

Description	Artifacts found using the Dynamic Application Finder vary depending on your case's evidence. To learn more, see Processing details > Find more artifacts in the AXIOM User Guide.
Recovery method	Parsing

Attribute	Description

Additional Information

Application Usage

Activity Manager History

Description	Activity Manager History contains a list of recent activity manager events, identified by the package name that triggered the event.
Recovery method	Parsing

Attribute	Description
Date/Time - Local Time (yyyy-mm-dd)	The date and time of the activity.
Type	The type of activity.
Event	The name of the event.
Package Name	The name of the package that triggered the event.
Process ID	The process ID of the package.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Android Application Roles

Description	Android Application Roles contains a list of the default set application for specific functions in Android.
Recovery method	Parsing

Attribute	Description
Package Name	The internal name of the application.
Role	The role assigned to the application.

Additional Information

Android Device Information

Description	Android Device Information contains the phone identification values.
Recovery method	Parsing

Attribute	Description
User ID	The unique number identifying the device user or profile in the file system.
User Name	The name for the device user or profile.
Type of User	The user type for the device user or profile.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the non primary user or profile was created.
Last Login Date/Time - UTC (yyyy-mm-dd)	The date and time that the user or profile was logged into.
Icon	The icon for the user or profile of the device.
Device ID	The unique identifier that is displayed when rooting the device.
IMSI	The IMSI associated with the device.
IMEI	The IMEI associated with the device.
MEID	The MEID associated with the device.
ICCID	The ICCID associated with the device.
Serial Number	The serial number associated with the device.
Manufacturer	The manufacturer of the device.

Attribute	Description
Model	The model of the device.
Product Name	The secret codename that the manufacturer gave to the device.
Advertising ID	The advertising ID of the primary user account.
Chip Name	The name of the processor within the device.
Bootloader	The bootloader associated with the device.
SIM Card State	The state of the SIM card when the device was acquired (for example, READY).
Service Provider Country Code	The country code associated with the service provider of the device.
Mobile Country Code	The mobile country code of the provider of the SIM.
Mobile Network Code	The mobile network code of the provider of the SIM.
Service Provider Name	The name of the SIM service provider.
Device Phone Number	The phone number of the device.
Device Phone Type	The type of radio used to transmit voice calls (for example, GSM)
OS Version	The Android OS version of the device.
Build Fingerprint	The Android build fingerprint of the device.
Voice Mail Identifier	The alphabetic identifier associated with the voice mail number.
Voice Mail Number	The phone number the device calls to access voice mail.

Attribute	Description
Current Network Country ISO Code	The ISO country code of the network that the device was registered on during acquisition.
Current Network Operator Name	The name of the network operator that the device was registered on during acquisition.
Network Type	The type of network that the device was registered on during acquisition.
Host Name	The hostname associated with the device.
Device Software Version	The software version of the device.
Security Patch	The current installed security patch of the device.
Roaming	Indicates whether the device was considered to be roaming during acquisition.
MAC Address	The WiFi hardware address of the device.
Bluetooth Address	The Bluetooth hardware address of the device.
Bluetooth Name	The Bluetooth name that appears upon pairing the device.
Timezone	The timezone for the device.
User Full Data Backup Eligible	Indicates whether or not the user is eligible for full data backup for the device.
Network Location Opt In	Indicates whether or not the user has opted in to network location services for the device.
Location Services Enabled	Indicates whether or not the user has allowed Google services to use location data for the device.
Mock Locations Allowed	Indicates whether or not mock locations have been enabled on

Attribute	Description
	the device.
Home Screen Wallpaper	The wallpaper used on the home screen for the device user or profile.
Lock Screen Wallpaper	The wallpaper used on the lock screen for the device user or profile.

Additional Information

Android Usage History

Description	Android Usage History contains information about the usage and activity of applications that are running on the device.
Recovery method	Parsing

Attribute	Description
Event Name	The category of event that is occurring.
Package Name	The package name defined by the publisher/developer of the application (for example, com.example.mypackage).
Event	The event that is running within the application.
Event Date/Time - UTC (yyyy-	The last time that the event was actively being engaged either by a user or by the system.

Attribute	Description
mm-dd)	
Last Active Date/Time - UTC (yyyy-mm-dd)	The last time that the package was active on the device.
Last System Active Date/Time - UTC (yyyy-mm-dd)	The last time that the package was being utilized on or by the system.
Total Time (Seconds)	The amount of time that the application/package was open and being interacted with by the user.
Type	The type of event representing a state of change, for example, configuration change or shortcut invocation. For a complete list of events, visit https://developer-.android.com/reference/android/app/usage/UsageEvents.Event.

Additional Information

Android Usage History (Dumpsys)

Description	Android Usage History (Dumpsys) contains information about the usage and activity of applications running on the device, recovered using the dumpsys utility. The dates and times that were recovered by this artifact reflect the local time of the device.

Recovery method	Parsing

Attribute	Description
Event Name	The category of event that is occurring.
Package Name	The package name that was defined by the publisher/developer of the application (for example, com.example.mypackage).
Event	The event that is running within the application.
Configuration	The Android configuration that is currently active.
Time Range - Local Time (yyyy-mm-dd)	The time range that the data was aggregated within.
Total Time (Seconds)	The amount of time that the application/package was open and being interacted with by the user.
Event Date/Time - Local Time (yyyy-mm-dd)	The last time that the event was actively being engaged either by a user or by the system.
Last Active Date/Time - Local Time (yyyy-mm-dd)	The last time that the package was active on the device.
Last System Active Date/Time -	The last time that the package was being utilized on or by the system.

Attribute	Description
Local Time (yyyy-mm-dd)	
Type	The type of event representing a state of change, for example, configuration change or shortcut invocation. For a complete list of events, visit https://developer-.android.com/reference/android/app/usage/UsageEvents.Event.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Android User Dictionary

Description	Contains the shortcuts and words the user has on his or her device.
Recovery method	Parsing

Attribute	Description
Word	A word entered by a user to auto-complete a shortcut (a desired word or phrase). For example, a user may type the word, "Hello," prompting the shortcut, "Hello World."
Shortcut	The symbols that the user types to cause the word to be written.

Additional Information

Application Activity - Android

Description	Application Activity represents the applications that are active in the background of the operating system.
Recovery method	Parsing

Attribute	Description
Package Name	The application package name.
First Active Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was first active.
Last Active Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was last active.
Last Moved Date/Time - UTC (yyyy-mm-dd)	The date and time when the application last changed positions in the list of running applications. An application moves to the front of the list when it starts.
Application Activity	The activity the application is performing.
Application Data	The application data.

Attribute	Description
Origin Activity	The Android activity where the currently running activity originated from. For example, if the current activity describes opening a website in the browser, the origin activity might be from a messaging application where the link was opened from.
Device User ID	A unique user ID associated with the user account.
Preview	The snapshot preview of the active application.

Additional Information

Application Permissions - Android

Description	Application Permissions contains information about the application permissions that a user has granted or declined.
Recovery method	Parsing

Attribute	Description
Package Name	The package that requests the permission.
Permission	The permission name.
Allowed	Indicates whether the package is allowed to use the service/permission.

Additional Information

Application Power Usage

Description	Application Power Usage represents the amount of battery power consumed by each application since the device's last full charge.
Recovery method	Parsing

Attribute	Description
Application Name	The application package name.
Application ID	The unique ID associated with the application package.
Power Usage	The amount of power (in mAh) that the application consumes.

Additional Information

Application Runtime Permissions

Description	Application Runtime Permissions contains information about the application permissions that a user has granted or declined while the application is running.
Recovery method	Parsing

Attribute	Description
Package Name	The package that requests the permission.

Attribute	Description
Permission	The permission name.
Allowed	Indicates whether the package is allowed to use the service/permission.

Additional Information

Device Health Services Application Usage

Description	Device Health Services Application Usage provides information about the applications that were used on the device, including each time the same application was used, within a recorded interval.
Recovery method	Parsing

Attribute	Description
Package Name	The bundle name of the application used.
Recorded Date/Time - UTC	The date and time when the application was used.

Additional Information

Device Health Services Battery Usage

Description	Device Health Services Battery Usage provides information about when the user was charging their device and what the battery level percentage

	was at that time. This artifact also includes the timezone that the device was set to at that time.
Recovery method	Parsing

Attribute	Description
Battery Level	The current battery level percentage of the device.
Charging	Indicates whether the device is charging rapidly, slowly, wirelessly, or is not charging at all.
Battery Saver	Indicates whether or not the device is set to use battery saver mode.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time when the battery data was recorded.
Timezone	The timezone the device is currently set to.

Additional Information

Device Reset/Activation Times

Description	Device Reset/Activation Times contains the approximate reset or wipe and activation date times on a device. It's extremely important to compare this data to other data on the device. For more information: https://the-binaryhick.blog/2021/08/19/wipeout-detecting-android-factory-resets/.
Recovery method	Parsing

Attribute	Description
Device ID	The unique identifier that is displayed when rooting the device.
Reset/Activation	Indicates whether the time is a reset or activation time.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the reset or activation of the device.

Additional Information

Digital Wellbeing Events

Description	Digital Wellbeing Events contains information about events that are tracked by the Digital Wellbeing app. Events describe state changes such as when an application pauses or resumes. Digital Wellbeing is a system application that's available on most Android 9 and 10 devices. The app is used to track events and provide the user with options to limit their usage of applications and set up a sleep schedule to reduce device usage.
Recovery method	Parsing

Attrib-ute	Description
Event ID	The unique ID of the event.
Event	The date and time of the event.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Package Name	The package name of the application associated with the event.
Event Type	An event representing a state change in the application associated with the event. The Event Type is based on the Usage Events Android source code and is described in full detail from the provided source URL: https://android-.google-source.-com/-platform/frameworks/base/+/master/core/java/android/app/usage/UsageEvents.java
Source Package Name	The package name of the application that triggered the event. The application that triggers the event can be different from the application that the event is associated with. For example, opening one application might cause an activity in a tracked application to pause.

Additional Information

Digital Wellbeing Limits

Description	Digital Wellbeing Limits is used for restricting the amount of time for application usage. An application is suspended once the time limit has been reached.
Recovery method	Parsing

Attribute	Description
Package Name	The package name of the application.
Time Limit (m)	The time limit configured for the application, in minutes (converted from milliseconds).
Suspended	Indicates whether the application is currently suspended.

Additional Information

Google Play Application Details

Description	Google Play Application Details contains more detailed information about the applications that a user has downloaded from Google Play. This information includes when the user last installed or updated an application, and how the user was referred to the application.
Recovery method	Parsing

Attribute	Description
Package Name	The package name of the application that is installed.
Title	The name of the application as it is currently represented in the Google Play Store.
Account	The signed in Google Play Store account that is used to install the application.
Last Updated Date/Time	The date and time when the application was last updated through the Google Play Store.
Downloaded Date/Time	The date and time when the application was last downloaded through the Google Play Store.
Download Request Date/Time	The date and time when the application was last requested for installation through the Google Play Store.
First Install Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was first installed through the Google Play Store.
Update Discovered Date/Time	The last time Google Play discovered an available update for the installed application.
Automatically Update	Indicates whether the application is set to automatically update in Google Play.
Referrer	The original source that referred the user to the application in Google Play.

Additional Information

Google Play Installed Applications

Description	Google Play Installed Applications lists each of the applications that were downloaded and installed from Google Play.
Recovery method	Parsing

Attribute	Description
Package Name	The package name of the application that is installed.
Account	The signed in Google Play Store account that is used to install the application.
Purchased Date/Time	The time that the application was purchased from the Google Play Store.

Additional Information

Google Play Searches

Description	Google Play Searches contains the search queries that a user has performed in Google Play, and the date and time of when they were performed.
Recovery method	Parsing

Attribute	Description
Search Query	The search query entered by the user.
Query Date/Time	The date and time when the user made the search.

Additional Information

Installed Applications

Description	Installed Applications contains a list of all of the applications on an Android device, including their versions.
Recovery method	Parsing

Attribute	Description
Package Name	The internal name of the application.
Display Name	The display name of the application.
AXIOM Supported	The application that the data was recovered from, as defined by AXIOM artifact processing.
Icon	The icon for the application.
Platform	The platform of the application.
Type	The type of application (either System or User).
Installed	The date and time when the application was installed.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the application was last updated.
Display Version	The display version of the application.
Internal Version	The internal version of the application.
Secondary Package Names	If known by AXIOM, other internal names of the application, which are not the primary Package Name.
Application UID	The unique identifier of the application. Some applications reference a UID in their data instead of a package name. You can cross-reference this value with an application package name. Note that this attribute applies to Android only.
AppSource	The path of where the .app file application is located for the installed application.
Application Data	The path, or paths of where the user data is stored for the installed application
User Accessible Application	Whether it is a third party application, or a native application that can be executed by the user.

Additional Information

Note that different file paths from the Application Data attribute could contain similar content. This may occur when one file path is a symbolic link to another on the same device, linking between the original file and a copy created by a backup image.

Privacy Dashboard

Description	Privacy Dashboard is an Android system application that displays 24 hours of permission access by device applications for the user to see.
Recovery method	Parsing

Attribute	Description
Package Name	The unique identifier of the application accessing the permission.
Permission	The permission requested by the application. This may include: Location, Microphone and/or Camera.
Attribution Tag	An optional value set by the application developer which indicates why the application needs to access the permission.
Duration (Seconds)	The amount of time the application accessed the Microphone or Camera, measured in seconds.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the application accessed the permission on the device.

Additional Information

Samsung Device Health Services Battery Statistics

Description	Samsung Device Health Services Battery Statistics provides information about the applications that were used on the device, including each time the same application was used, within a recorded interval. This artifact also contains details about how the user used the applications, and for how long.
Recovery method	Parsing

Attribute	Description
Application UID	The unique identifier of the application. You can match the UID to the package name, found in the Installed Applications Artifact.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was used.
Power Usage	How much of the device's battery power the app consumed while it was running.
Awake Duration	The duration, in seconds, that the app was awake.
Mobile Packets	The number of data packets that the app sent or received via cellular signal.
WiFi Packets	The number of data packets that the app sent or received via WiFi signal.
GPS Duration	The duration in milliseconds that the app used GPS.
Camera Duration	The duration in milliseconds that the app used the device's camera.

Attribute	Description
Close Count	The number of times the app crashed or was forcibly closed.
Audio Duration	The duration in milliseconds that the app played audio on the device
Focus Duration	The duration in milliseconds that the app was in focus, or in the foreground, of the device.
Background Duration	The duration in milliseconds that the app was running in the background of the device.

Additional Information

Samsung Device Health Services CPU Data

Description	Samsung Device Health Services CPU Data provides information about the processes that were running on the device, including each time period a process was running. This artifact also contains details about how much CPU usage a process had.
Recovery method	Parsing and carving

Attribute	Description
Application UID	The unique identifier of the application. You can match the UID to the package name, found in the Installed Applications artifact.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the process started running.

Attribute	Description
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the process stopped running.
Process Name	The name of the process.
Process Usage	The CPU usage of the process, in bytes.

Additional Information

Samsung Device Health Services Network Statistics

Description	Samsung Device Health Services Network Statistics provides information about the applications or services that were using the network on the device, including the time period when each application or service was running. This artifact also contains details about how much data the application or service used on the network.
Recovery method	Parsing

Attribute	Description
Package Name	The name of the application package or service that is using the network.
Network Usage	The network usage of the application or service, in bytes.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the application or service started running.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the application or service stopped running.

Additional Information

Samsung Digital Wellbeing Events

Description	Samsung Digital Wellbeing Events contains information about events that are tracked by the Samsung Digital Wellbeing app. Events describe state changes such as when an application pauses or resumes. Samsung Digital Wellbeing is a system application that's available only on Samsung devices and replaces the native Android Digital Wellbeing app. The app is used to track events and provide the user with options to limit their usage of applications and set up a sleep schedule to reduce device usage.
Recovery method	Parsing

Attribute	Description
Event ID	The unique ID of the event.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time of the event.
Package Name	The package name of the application associated with the event.
Event	An event representing a state change in the application associated with the event.

Attribute	Description
Type	The Event Type is based on the Usage Events Android source code and is described in full detail from the provided source URL: https://android-.google-source.-com/-platform/frameworks/base/+/master/core/java/android/app/usage/UsageEvents.java
Source Package Name	The package name of the application that triggered the event. The application that triggers the event can be different from the application that the event is associated with. For example, opening one application might cause an activity in a tracked application to pause.
Application Category	The package name may have an associated category assigned to its package name that may help describe how the application is typically used. Some examples of descriptions can be values such as: 'Social', 'Game', Shopping and Food'.

Additional Information

Cloud Storage

Android Dropbox

Description	Android Dropbox contains Dropbox file information recovered from a Kindle device.
Recovery method	Parsing

Attribute	Description
File Path	The path to the file.
Updated Modified Date/Time - UTC (yyyy-mm-dd)	The updated date and time that the file/folder was modified.
Local Modified Date/Time - UTC (yyyy-mm-dd)	The local date and time that the file/folder was modified.
Updated File Name	The name of the file/folder being updated.
Displayed Modified Date/Time	The displayed modified date and time.
Local File Size (Bytes)	The size of the file on the local machine.
Updated File Size (Bytes)	The updated size of the file.
Favorited	Indicates whether or not the file has been favorited.
File Version	The file version.

Additional Information

Android Dropbox Account Info

Description	Android Dropbox Account Info contains Dropbox account information recovered from a Kindle device.
Recovery method	Parsing

Attribute	Description
Email	The email address associated with the account.
User ID	The Dropbox user account ID.
Display Name	The Dropbox user account display name.
Country	The country that the user account is set for.

Additional Information

MEGA Accounts

Description	MEGA Accounts contains information about the accounts that the local user has logged in with on the device.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the local user.
Email Address	The email address of the local user.
First Name	The first name of the local user.
Last Name	The last name of the local user.

Additional Information

MEGA Chat

Description	MEGA Chat contains messages sent and received by the local user.
Recovery method	Parsing

Attribute	Description
Sender ID	The ID of the sender.
Sender Email	The email address of the sender.
Recipient ID(s)	The user ID(s) of the recipient(s).
Recipient Email(s)	The email address of the recipient of the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message Body	The body of the message.
Message Type	The type of the message.
Attachment Name	The file name of the attachment in a message.
File	The attachment in the message. For video files, the preview might only be a thumbnail of the original video.

Additional Information

MEGA Contacts

Description	MEGA Contacts contains information about MEGA users that have com-

	municated with the local user account.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the contact.
Email Address	The email address of the contact.
First Name	The first name of the contact.
Last Name	The last name of the contact.

Additional Information

Communication

AIM Buddies

Description	Contains the AIM buddies that were recovered from an Android device.
Recovery method	Parsing

Attribute	Description
User AIM ID	The AIM ID of the local user.
Buddy Name	The name of the buddy.

Attribute	Description
Buddy Display ID	The display ID of the buddy.
Buddy AIM ID	The AIM ID of the buddy.
Buddy Icon URL	The URL of the buddy's icon.
Downloaded Buddy Icon	The dowloaded icon of the buddy.
Buddy Group	Identifies if the row is a buddy or group chat. The possible values are Buddies or groupcht.
Group Chat ID	The ID of the group chat, if applicable.

Additional Information

AIM Messages

Description	Contains the AIM messages that were recovered from and Android device.
Recovery method	Parsing

Attribute	Description
Sender	The AIM ID of the sender of the message
Receiver	The AIM ID of the user receiving the message or the group chat ID if in a chat.

Attribute	Description
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Message	The message that was sent/received.
Latitude	The latitude of the message sender.
Longitude	The longitude of the message sender.

Additional Information

Android Burner Conversations

Description	Android Burner Conversations contains the Burner conversations that were recovered from an Android device.
Recovery method	Parsing

Attribute	Description
Burner Number	The Burner number on the device that is a part of the conversation.
Conversation Partner	The phone number of the other person in the conversation.
Message	The last message of the conversation.
Account Num-ber	The Burner ID on the device that is a part of the conversation.

Attribute	Description
Conversation Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message in the conversation.
Conversation Name	The name of the conversation.
Type	The type of the last interaction in the conversation. The possible values are Outgoing Text Message, Incoming Text Message, Incoming Phone Call, Missed Incoming Phone Call, Outgoing Phone Call, and Incoming Voice Mail.
Voice Mail URI	The URI to the voice mail, if applicable.

Additional Information

Android Burner Numbers

Description	Android Burner Numbers contains the Burner numbers that were recovered from an Android device.
Recovery method	Parsing and carving

Attribute	Description
User ID	The ID of the user's Burner account.

Attribute	Description
Burner ID	The ID of the Burner number.
Burner Number	The phone number that was generated by Burner.
Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time when the Burner number was updated.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the Burner number was generated.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the Burner number will expire.
About	Information about the Burner number.

Additional Information

Android Call Logs

Description	Android Call Logs contains information about the phone calls that occur using the Android Phone application.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Partner	The phone number of the conversation partner.

Attribute	Description
Partner Name	The name of the conversation partner.
Direction	The direction of the call (Incoming or Outgoing).
Call Status	The status of the call (Answered, Unanswered, Missed or Declined).
Call Date/Time - UTC (yyyy-mm-dd)	The date/time of the call.
Call End Date/Time - UTC (yyyy-mm-dd)	The date and time when the call ended. This value is calculated by adding the Call Duration to the Call Date/Time.
Call Duration	The duration of the call in one of the following formats: HH:MM:SS (hours, minutes, seconds) or DD:HH:MM:SS (days, hours, minutes, seconds).
Partner Location	The location of the other participant of the call, can be a province or state.
Service Provider Country Code	The country code of the service provider that handled the call.
ICCID	The ICCID number of the SIM card inside the device.
Message	Up to 50 characters of logged text message content on Samsung devices.

Additional Information

Android Call Logs (UFED Agent)

Description	Android Call Logs (UFED Agent) contains calling logs from the Phone application on Android. These logs are recovered from <incoming_calls>, <outgoing_calls>, <missed_calls>, <unknown_calls> tags found in a UFED Report.xml.
Recovery method	Parsing

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Type	The type of call (Incoming, Outgoing, or Missed). This data is retrieved from the <incoming_calls>, <outgoing_calls>, <missed_calls>, <unknown_calls> tags in a UFED Report.xml.
Partner Phone Number	The phone number of the conversation partner. This data is retrieved from the <number> tag within each call element in a UFED Report.xml.
Partner Name	The name of the conversation partner. This data is retrieved from the <name> tag within each call element in a UFED Report.xml.
Call Date/Time - UTC (yyyy-mm-dd)	The date/time of the call. This data is retrieved from the <timestamp> tag within each call element in a Report.xml.
Call End Date/Time - UTC (yyyy-	The date and time when the call ended. This value is calculated by adding the Call Duration to the Call Date/Time.

Attribute	Description
mm-dd)	
Call Duration	The duration of the call in one of the following formats: HH:MM:SS (hours, minutes, seconds) or DD:HH:MM:SS (days, hours, minutes, seconds). This data is retrieved from the <duration> tag within each call element in a Report.xml.

Additional Information

Android Contacts

Description	Android Contacts contains contact information from a recovered Android device.
Recovery method	Parsing and carving

Attribute	Description
Display Name	The display name of the contact.
Phone Number(s)	The phone number of the contact.
Email Address(es)	The email address of the contact.
Address	The postal address of the contact.
Website	The website of the contact.
Starred	Indicates whether or not the contact has been starred.

Attribute	Description
Deleted	Indicates whether or not the contact has been deleted.
Last Time Contacted Date/Time - UTC (yyyy-mm-dd)	The last date and time when the contact was contacted.
Number of Times Contacted	The number of times that the contact has been contacted.
Total Contact Call Duration (Seconds)	The sum of the call durations for a given contact.
Notes	Notes associated with the contact.
Source Account Name(s)	The name of the account.
Source Account Type(s)	The type of account that the contact information is for.
Image	The image associated with the contact.

Additional Information

Android Contacts (UFED Agent)

Description	Android Contacts (UFED Agent) contains information recovered from the Contacts application on Android. These contacts are recovered from <contacts> tag found in a UFED Report.xml.
Recovery method	Parsing

Attribute	Description
Contact Name	The name of the contact. This data is retrieved from the <name> tag within contact elements in a UFED Report.xml.
Phone Numbers	The phone number of the contact. This data is retrieved from the <phone_number> tags within the contact elements in a UFED Report.xml.
Email Address(es)	Any email addresses associated with the contact. This data is retrived from the <extra_field> tags within the contact elements in a UFED Report.xml.
Company	The company name of the contact. This data is retrived from the <extra_field> tags within the contact elements in a UFED Report.xml.
Address	The mailing address of the contact. This data is retrieved from the <extra_field> tags within the contact elements in a UFED Report.xml.
Source Account Type(s)	The source from where the contact information is saved (that is, whether the contact is saved to the SIM card, the device, or another account). This data is retrieved from the <memory> tag within the contact elements in a UFED Report.xml.
Notes	The data from the notes field for the contact. This data is retrieved from the <extra_field> tag within calendar elements in a UFED Report.xml.
Additional Data	Any additional data that is recovered that's related to the contact. This field is in XML format as the data recovered is directly from the Report.xml without any further interpretation.

Additional Information

Android Facebook Messenger Attachments

Description	Android Facebook Messenger Attachments contains information about files shared within Facebook Messenger. Picture and video files are valuable when investigating a suspect's computer for illicit content. Media content can help an examiner identify victims in cases of child abuse material and exploitation. In a corporate environment, pictures can contain scans of confidential documents, easily shared through file sharing.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the file.
Attachment Type	The type of media file (for example: Image, Audio, Video).
Attachment	The attachment file.
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).

Additional Information

Android Google Hangouts Messages

Description	Android Google Hangouts Messages contains the messages from Google

	Hangouts from an Android device.
Recovery method	Parsing

Attribute	Description
Sender Phone ID	The identifier of the device for who sent the message.
Sender Full Name	The full name of the sender who sent the message.
Sender Fall-back Name	The name of the sender, if they don't have a full name.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Recipient Phone ID	The identifier of the recipient of the message.
Recipient Full Name	The full name of the recipient of the message.
Recipient Fall-back Name	The name of the recipient, if they don't have a full name.
Message	The body of the message.
Message Type	The type of the message. The message type value can be 'Sent Message', 'Received Message', 'Participant joined/left the Hangout', 'Video Chat Started', 'Video Chat Ended', 'History Turned Off', 'History Turned On', 'Par-

Attribute	Description
	ticipant left the Hangout', or 'Participant joined the Hangout'.
Sender Profile Photo URL	The URL to the profile photo of the sender of the message.
Recipient Profile Photo URL	The URL to the profile photo of the recipient of the message.
Remote Attachment URL	The URL to the attachment of a message.
Attachment Type	The type of the attachment.
Latitude	The latitude of the message. It has not been determined whether this is the sender of the message, the recipient of the message, or just where the device received the message.
Longitude	The longitude of the message. It has not been determined whether this is the sender of the message, the recipient of the message, or just where the device received the message.
Location URL	The URL to a location on Google maps of the image.
Location Thumbnail URL	The URL to a thumbnail picture of the location of the message on Google Maps.

Additional Information

Android Kik Messenger Attachments

Description	Android Kik Messenger Attachments contains the attachments of messages from Kik Messenger from an Android device.
Recovery method	Parsing

Attribute	Description
Media ID	The ID of the attachment.
Attachment	The attachment.
File Metadata	Any metadata from the file.

Additional Information

Android Kik Messenger Contacts

Description	Android Kik Messenger Contacts contains information about a user's Kik Messenger contacts.
Recovery method	Parsing

Attribute	Description
Contact ID	The ID of the contact.
Display Name	The display name of the contact.

Attribute	Description
Local Name	The local name of the person on the device.
User Name	The username of the contact.
Photo Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the contact's profile photo.
Photo URL	The URL to the profile photo of the contact.
Group Member	Indicates whether the contact is a member of a group (Yes or No).
Blocked	Indicates whether the contact is blocked by the local user.

Additional Information

Android Kik Messenger Messages

Description	Android Kik Messenger Messages contains Kik Messenger messages that were sent or received by the local user.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Partner	The person the local user sent a message to or received a message from.

Attribute	Description
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the message.
Message Body	The body of the message.
Message Status	The status of the message. The possible values are Trying to establish connection, Message has been sent to recipient, Message has been delivered to recipient, Message has been read by recipient and Unknown message status.
Message Type	The type of the message. The possible values are Message Received, Message Sent and Unknown Message Type.
Media ID	The ID of the attachment.
Media Info	The description of the attached media.
Attachment	The attachment sent with the message.

Additional Information

Android Messages

Description	SMS/MMS messages sent and received using Android Messages.
Recovery method	Parsing and carving

Attribute	Description
Sender	The name of the sender or the phone number if the name is not available.
Sender Phone Number	The phone number of the sender.
Recipient	The recipient of the message.
Message Sent Date/Time	The date and time when the message was sent.
Message Received Date/Time	The date and time when the message was received.
Message	The content of the message.
Message Status	The read status of the message.
Message Type	The message type. An example of message type is Text/plain.
Message Direction	Indicates whether the message was sent by or recieved on the local user's device.
Attachment Path	The path of an attachment.
Attachment Data Recovered	Indicates whether attachment data was recovered (Yes or No).
Subject	The optional subject line provided for an MMS message.
Target File Size (Bytes)	The size of attachments.
Latitude	The latitude associated with a location message.
Longitude	The longitude associated with a location message.
Avatar Path	The path to the contact icon used for the sender.

Additional Information

Android MMS

Description	MMS messages sent or received using an Android device. These messages are recovered from mmssms.db.
Recovery method	Parsing and carving

Attribute	Description
Sender	The phone number of the device that sent the message.
Recipient(s)	The phone numbers of the devices that received the message.
Message Direction	Indicates whether the message was incoming or outgoing. If the direction is not recognized, the value will be an integer.
Original Transmit Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was first sent from the sender.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent (only for outgoing messages).
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received (only for incoming messages).
Message	The message body of the MMS message.
Attachments	The file names of all recovered attachments.
Attachment Data Recovered	Indicates whether attachment data was recovered (Yes, No, or Partial).

Additional Information

Android MMS (UFED Agent)

Description	Android MMS (UFED Agent) contains MMS messages sent or received using the Messages app on Android. These messages are recovered from <mms_messages> tags found in a UFED Report.xml
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Partner Name	The name of the person who communicated with the local user. This data is retrieved from the <to> or <from> tags within mms_message elements in a UFED Report.xml.
Partner Phone Number	The phone number of the person who communicated with the local user. This data is retrieved from the <to> or <from> tags within mms_message elements in a UFED Report.xml.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the message, though it is unclear whether this represents the sent or received time. This data is retrieved from the <timestamp> tag within mms_message elements in a UFED Report.xml.
Subject	The subject of the message. This data is retrieved from the <subject> tag within mms_message elements in a UFED Report.xml.
Message	The body of the message, excluding any attachments. This data is retrieved

Attribute	Description
	from the <body> tag within mms_message elements in a UFED Report.xml.
Message Direction	The direction of the message relative to the Local User. This data is retrieved from the <to> or <from> tags within mms_message elements in a UFED Report.xml.
Message Status	The status of the message. This data is retrieved from <status> tag within mms_message elements in a UFED Report.xml. However, if the value in the <folder> tag is Draft, this attribute will indicate Draft.
Priority	The priority of the message. This data is retrieved from <priority> tags within mms_message elements in a UFED Report.xml.
Attachment Name(s)	The attachment file name. This data is recovered from the <attachments> tag within mms_message elements in a UFED Report.xml.
Attachment	The attachment file.

Additional Information

Android Sim Card Information

Description	Android SIM Card Information is information about the device's SIM card that is recoverable if the user has the Android Messages application installed on the device.
Recovery method	Parsing

Attribute	Description
ICCID	The ICCID (Integrated Circuit Card Identifier) is a serial number stored in the SIM card.
Service Provider Name	The name of the mobile service provider.
Phone Number	The phone number associated with the SIM card.
IMSI	The IMSI (International Mobile Subscriber Identity) is a unique number identifying a GSM (Global System for Mobile Communications) subscriber.

Additional Information

Android SMS

Description	SMS messages sent using the Messages app on Android.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Partner	An identifier for the person who communicated with the local user.
Received Date/Time-(UTC)(dd/MM/yyyy)	The time the message is received.
Sent Date/Time-(UTC)(dd/MM/yyyy)	The time the message is sent. This value will also display the time when the message has a direction of queued, failed or outbox.

Attribute	Description
Original Transmit Date/Time-(UTC) (dd/MM/yyyy)	Original transmit timestamp.
Message	The message body of the SMS message.
Message Direction	Indicates whether the message was incoming or outgoing.
Application	The application from which the message was sent.

Additional Information

Android SMS (UFED Agent)

Description	Android SMS (UFED Agent) contains SMS messages sent or received using the Messages app on Android. These messages are recovered from <sms_messages> tags found in a UFED Report.xml.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Partner Name	The name of the person who communicated with the local user. This data is retrieved from the <name> tag within sms_message elements in a UFED Report.xml.
Partner	The phone number of the person who communicated with the local user.

Attribute	Description
Phone Number	This data is retrieved from the <number> tag within sms_message elements in a UFED Report.xml.
Message Date/Time - UTC (yyyy-mm-dd)	A date and time associated with the message, though it is unclear whether this represents the sent or received time. This data is retrieved from the <timestamp> tag within the sms_message elements in a UFED Report.xml.
Message	The message content for the message. This data is retrieved from the <text> tag within sms_message elements in a UFED Report.xml.
Message Direction	The direction of the message (either incoming or outgoing). This data is retrieved from the <type> tag within sms_message elements in a UFED Report.xml.
Message Status	The status of the message. Values can be Read, Unread, or Sent. This data is retrieved from the <status> tag within sms_message elements in the UFED Report.xml.
SMSC	The Short Message Service Center (SMSC) associated with the message. This data is retrieved from the <smsc> tag within sms_message elements in a UFED Report.xml.

Additional Information

Android SMS/MMS

Description	SMS and MMS messages sent or received using an Android device. These messages are recovered from mmssms.db.
Recovery method	Parsing and carving

Attribute	Description
Sender	The phone number of the device that sent the message.
Recipient(s)	The phone number(s) of the device(s) that received the message.
Message	The message that was sent.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent (only for out-going messages).
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received (only for incoming messages).
Original Transmit Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was first sent from the sender.
Direction	Indicates if the message is incoming, outgoing, draft, out-box, failed, queued, unknown, or alert.
Status	The status of the message.
Type	Whether the message was SMS or MMS.
Attachments	The file names of all recovered attachments.
Attachment Data Recovered	Indicates whether attachment data was recovered (Yes, No, or Partial).
Application	The application from which the message was sent.
Date/Time - UTC (yyyy-mm-dd)	The date and time when message was either sent or received.

Additional Information

Android SMS/MMS (Content Provider)

Description	SMS/MMS messages sent or received using an Android device. Data for this artifact is recovered during the acquisition process using an Android Content Provider.
Recovery method	Parsing

Attribute	Description
Participants	The phone numbers of the people in the conversation.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was either received if it was incoming or sent if it was outgoing.
Original Transmit Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was first sent from the sender to the local user.
Message	The message body of the MMS message.
Message Status	The status of the message.
MIME Type	The MIME type for the attachment.
Attachment	The recovered attachment.

Additional Information

Android SMS/MMS (Google Play Services)

Description	SMS and MMS messages sent or received using an Android device. These

	messages are recovered from icing_mmssms.db.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Partner	An identifier for the person who communicated with the local user.
Sent Date/Time - UTC (yyyy-mm-dd)	The time the message is sent.
Received Date/Time - UTC (yyyy-mm-dd)	The time the message is received.
Message	The message body of the SMS message.
Message Type	The type of message. Possible values are MMS and SMS.
Message Direction	Indicates whether the message was incoming, outgoing, draft, sent, outbox, failed, or queued.
Message Status	The status of the message (Read or Unread).
Date/Time - UTC (yyyy-mm-dd)	The date and time when message was either sent or received.

Additional Information

Android TextNow Calls

Description	Android TextNow Calls contains information about calls and voicemails that are sent and received through the TextNow application.
Recovery method	Parsing and carving

Attribute	Description
Call Type	The type of call or voicemail.
Direction	Whether the call was incoming or outgoing.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the call or voicemail.
Duration (Seconds)	The duration of the call.
Contact ID	The ID of the other call participant.
Contact Type	The other participant's contact type.
Conversation Partner	The name of the other call participant.
Voicemail URL	The URL of the voicemail.
Message Status	The status of the message ('Read' or 'Unread').
Attachment Path	The voicemail attachment path.

Additional Information

If the Contact Name cannot be determined, the Local Contact Key may be used to locate the corresponding entry in the iOS TextNow Contacts artifact.

Android TextNow Chat

Description	Android TextNow Chat contains chat messages that are sent and received through the TextNow application.
Recovery method	Parsing and carving

Attribute	Description
Message	The body of the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Contact ID	The ID of the other message participant.
Contact Type	The other participant's contact type.
Message Partner	The phone number or username of the other participant.
Message Type	The type of message.
Message Direction	Whether the message was incoming or outgoing.
Group Name	The group name, if the message was sent to a group chat.
Message Status	The status of the message ('Read' or 'Unread').
Attachment Path	The attachment path.
Attachment	The attachment.

Additional Information

If the Contact Name cannot be determined, the Local Contact Key may be used to locate the corresponding entry in the iOS TextNow Contacts artifact.

Android TextNow Contacts

Description	Android TextNow Contacts contains the application, phone, email and group contacts that a user has in the TextNow application.
Recovery method	Parsing

Attribute	Description
Contact ID	The name of the contact.
Contact Type	The contact's type.
Contact Name	The display name contact.

Additional Information

Android TextNow Groups

Description	Android TextNow Groups contains membership information for TextNow group chats.
Recovery method	Parsing and carving

Attribute	Description
Contact ID	The ID for the group.
Group	The name of the group.

Attribute	Description
Member Name	The username of a group member.
Type	The group member's contact type.
Display Name	The display name of the group member.
Contact Uri	The Android resource URI of the group member.

Additional Information

Android TextNow Profile

Description	Android TextNow Profile contains TextNow user profiles and application preference settings.
Recovery method	Parsing and carving

Attribute	Description
First Name	The first name of the TextNow user.
Last Name	The last name of the TextNow user.
Email	The email of the TextNow user.
User Name	The username of the TextNow user.
Phone Number	The phone number of the TextNow user.
Signature	The signature automatically appended to the end of each TextNow message sent by the user.

Attribute	Description
Last Number Called	The last number called using the TextNow application by the user.
TextNow Credit	The TextNow credit held by the user.
Balance	The TextNow cash balance held by the user.

Additional Information

Android TigerText Messages

Description	Android TigerText Messages contains messages from the TigerText Android application.
Recovery method	Parsing

Attribute	Description
Sender Display Name	The display name of the message sender.
Sender First Name	The first name of the message sender.
Sender Last Name	The last name of the message sender.
Sender Email	The email address of the message sender.
Sender Phone Number	The phone number of the message sender.
Recipient Display Name	The display name of the message recipient.

Attribute	Description
Recipient First Name	The first name of the message recipient.
Recipient Last Name	The last name of the message recipient.
Recipient Email	The email address of the message recipient.
Recipient Phone Number	The phone number of the message recipient.
Message Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message Expiry Date/Time - UTC (yyyy-mm-dd)	The date and time that the message will expire.
Message Text	The text content of the message.
Message Recalled	Whether the message was recalled. This value is 'True' for recalled, and 'False' for not recalled.
Attachment Type	The file type of the attachment (if any).
Attachment	Attachment data.
Message Status	The status of the message (sent, delivered or read).

Additional Information

BlackBerry Messenger Contacts

Description	Contains the BBM Contacts recovered from an Android device.
Recovery method	Parsing

Attribute	Description
BlackBerry PIN	Contains the contacts BlackBerry PIN.
Display Name	Contains the contacts display name.
Personal Message	Contains the contacts personal message.
Personal Message Last Update Date/Time - UTC (yyyy-mm-dd)	The data and time the contacts personal message was updated.
Avatar	The contacts avatar.
Avatar Content Type	The avatar content type. An example is 'image/jpeg'
Locale	The contacts location.
Timezone	The contacts timezone.

Additional Information

BlackBerry Messenger File Transfers

Description	Contains the BBM File Transfers recovered from an Android device.
Recovery method	Parsing

Attribute	Description
BlackBerry PIN	BlackBerry PIN of the contact who the transfer is with.
Display Name	Display name of the contact who the transfer is with.

Attribute	Description
Transfer Date/Time - UTC (yyyy-mm-dd)	The date and time the transfer took place.
Transfer Direction	Indicates whether a file was sent or received.
Transfer State	Indicates whether a file transfer is 'Pending Approval' or 'Complete'.
Local File Path	The path on the device to the data transferred.
Content Type	The type of data that was transferred.
Transfer Description	Description of what is being transferred.
Attachment	The file that was transferred.
Total Transfer Size (Bytes)	The number of bytes the transferred file is.
Bytes Transferred	The number of bytes that were transferred.

Additional Information

BlackBerry Messenger Invitations

Description	BlackBerry Messenger Invitations contains BBM invite requests recovered from an Android device.
Recovery method	Parsing

Attribute	Description
BlackBerry PIN	The BlackBerry PIN of the user sending the invite request.
Display Name	The display name of the user sending the invite request.
Local Email Address	The local email address of the user.
Remote Email Address	The remote email address of the user.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date/time when the invite was sent/received.
Direction	This column states if the invite is a received invite or a sent invite.
Invitation Status	Contains the status of the invite request. The value can be Pending Approval or Unknown.
Invite Method	The method used for sending the invite request. The value can be Via PIN or Unknown.
Subject	The subject used for the invite request.
Greeting	The message sent with the invite request.

Additional Information

BlackBerry Messenger Locations

Description	BlackBerry Messenger Locations contains BBM locations recovered from an Android device.
Recovery method	Parsing

Attribute	Description
BlackBerry PIN	The BlackBerry PIN of the location sender.
Display Name	The display name of the location sender.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date/time when the location was sent/received.
Message Type	Indicates whether the message was sent or received.
Location Name	The name of the location
Latitude	The latitude of the location
Longitude	The longitude of the location
Altitude (meters)	The altitude of the location.
Accuracy (meters)	The accuracy in meters.
Street	The street address of the location.
City	The city of the location.
State/Province	The state/province of the location.
Country	The country of the location.
ZIP/Postal Code	The postal code/ZIP of the location.

Additional Information

BlackBerry Messenger Messages

Description	Contains the BBM messages recovered from an Android device.
Recovery method	Parsing and carving

Attribute	Description
Conversation ID	The conversation identifier.
BlackBerry PIN	The BlackBerry PIN of who sent the message to the device or who's receiving a message from the device.
Display Name	The display name of who sent the message to the device or who's receiving a message from the device.
Participants	The display names of the people in the conversation.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent/received.
Message Content	The message sent/received.
Message Type	Contains the type of message that was sent. This can be one of the following: Message, Ping, File, Picture, Notification, Location.
Message Status	The status of the message (received or sent).
Message State	Contains the state of the message. This can be one of the following: 'Sent', 'Undelivered', 'Delivered, Unread', 'Read'.
Attachment	The attachment that was sent/received.

Additional Information

BlackBerry Messenger Profile

Description	Contains the BBM Profiles recovered from an Android device.
Recovery method	Parsing

Attribute	Description
BlackBerry PIN	The BlackBerry PIN associated with the profile.
Display Name	The display name associated with the profile.
Personal Message	The profiles personal message.
Personal Message Last Update Date/Time - UTC (yyyy-mm-dd)	The date and time the profile message was last updated.
Avatar	The profiles avatar.
Avatar Content Type	The avatar content type. An example is 'image/jpeg'.
Locale	The location of the profile.
Timezone	The timezone of the profile.
Keeps Chat History	Indicates whether or not the user keeps chat history.

Additional Information

Burner Contacts

Description	Burner Contacts contains information about a subject's Burner Contacts, as recovered from their Android device.
Recovery method	Parsing

Attribute	Description
Contact ID	The ID of the contact.
Contact Name	The name of the contact.
Phone Number	The phone number of the contact.
Burner ID	The ID of the Burner application associated with the contact.
Date/Time Created - UTC (yyyy-mm-dd)	The date and time when the contact was created.

Additional Information

Burner Messages

Description	Burner Messages contains information about messages and calls that are sent and received using Burner.
Recovery method	Parsing

Attribute	Description
Sender	The phone number of the sender.
Recipient	The phone number of the recipient.
Message	The body of the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Direction	Indicates whether the message was incoming or out-going.
Message Type	The type of message.
Media URL	The URL to the media file attached to the message.
Voicemail URL	The URL of the voicemail.

Additional Information

Burner Numbers

Description	Burner Numbers contains information about the burner numbers that the local user created.
Recovery method	Parsing

Attribute	Description
Burner ID	The ID of the Burner number.

Attribute	Description
Burner Number	The Burner phone number.
Display Name	The display name associated with the Burner number.
Created Date/Time	Indicates when the Burner number was created.
Expiration Date/Time	Indicates when the number will expire.
Mobile Phone	The phone number used to sign in to the Burner App.
User ID	The user id of the signed in user.

Additional Information

Cake Local User Account

Description	Cake Local User Account contains information about the logged in local user.
Recovery method	Parsing

Attribute	Description
Local User ID	The unique ID of the local user.
Local User Display Name	The display name of the local user.
Gender	The gender of the local user.
Birthday	The birthday of the local user.
Email Address	The email address of the local user.

Additional Information

Cake Messages

Description	Cake Messages contains messages sent and received by the local user.
Recovery method	Parsing

Attribute	Description
Sender ID	The unique user ID of the sender.
Sender Display Name	The display name of the sender.
Recipient ID	The Cake ID of the message recipient. If the chat type is Group chat, the recipient ID is the group ID.
Recipient Display Name	The display name of the message recipient. If the chat type is Group chat, the recipient display name is the group display name.
Message	The body of the message.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was created.
Chat Type	The type of chat where the message was sent (Group chat or One to one).
Picture URL	The URL of the picture, if one is attached to the message.
File	The attachment file.

Additional Information

Chatous Chat Messages

Description	Chatous Chat Messages contains messages that were sent and received using the Chatous application.
Recovery method	Parsing

Attribute	Description
Sender	The display name of the user who sent the message (Local User if it was the local user).
Recipient	The display name of the user who received the message (Local User if it was the local user).
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The body of the message.
Attachment Name	The name of the attachment that was sent.
Attachment Data Recovered	Indicates whether attachment data was recovered (Yes or No).

Additional Information

Chatous Chat Partners

Description	Chatous Chat Partners contains information about the users that the local user has communicated with.
Recovery method	Parsing

Attribute	Description
Screen Name	The name of the chat partner.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message in the chat.
Age	The age of the chat partner.
Gender	The gender of the chat partner. A blank value indicates that the chat partner is the Team Chatous account.
Locale	The location of the chat partner.
About	A summary of the chat partner.
Tag	The tag that matched the local user and the chat partner for a chat.
Profile Tags	The hashtags that the chat partner uses to describe themselves.

Additional Information

Discord Channels

Description	Discord Channels contains information about each of the channels joined or hosted by the local user account.
Recovery method	Parsing

Attribute	Description
Channel Name	The name of the channel.
Channel ID	The ID of the channel.
Server ID	The ID of the server hosting the channel.
Topic	The optional topic text for the channel.
Category	The parent category for the channel.
Channel Type	The type of channel (Text or Voice.)

Additional Information

Discord Logged-in Account

Description	Discord Logged-in Account contains information about the user that is currently logged into Discord on the device. Information about other accounts that were previously logged into are not recoverable.
Recovery method	Parsing

Attribute	Description
User ID	The ID of the logged-in user.
User Name	The name of the logged-in user.
Email	The email address of the logged-in user.
Phone Number	The phone number of the logged-in user.
Locale	The locale of the logged-in user.
User Token	The authentication token of the logged-in user.
Platform	The cloud platform name.

Additional Information

Discord Messages

Description	Discord Messages contains information about messages and calls that are sent and received using Discord. Messages from some channels might be missing if they haven't been cached by the application. This artifact uses both parsing and carving techniques to recover messages.
Recovery method	Parsing and carving

Attribute	Description
Sender	The username of the message sender.
Sender ID	The ID of the message sender.

Attribute	Description
Message	The message content. If the message sent is a sticker, the message will display 'Sticker(sticker name)'.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Last Edited Date/Time - UTC (yyyy-mm-dd)	If the message has been edited then this indicates the date and time when the last edit has occurred.
Message Type	The type of the message (Message or Call).
Channel ID	The ID of the channel that the message was sent in. This attribute is always empty for Android.
Attachment URL	If the message includes an attachment, then this value indicates the saved URL of the attachment. This attribute is always empty for Android.
Attachment Name	If the message includes an attachment, then this value indicates the file name of the attachment. This attribute is always empty for Android.
Embedded Content Title	If the message contains a link, then this then this value indicates the title that's displayed in the link preview.
Embedded Content Description	If the message contains a link, then this value indicates the description that's displayed in the link preview. This attribute is always empty for Android.
Call End Date/Time -	If the message was a call, this indicates the date and time that the call ended.

Attribute	Description
UTC (yyyy-mm-dd)	
Pinned	Indicates whether a message is pinned (True or False). This attribute is always empty for Android.
Message ID	The Message ID of the message that this message is replying to. This attribute is always empty for Android.
Mentions	The user mentioned in the message, if present. This attribute is always empty for Android.
In Reply To	The Message ID of the message that this message is replying to. This attribute is always empty for Android.
Reactors	The users who reacted to this message, if any. The order of reactors does not correspond to the reactions used. This attribute is always empty for Android.
Reaction	The emojis that were used to react to the message, if any. If a custom emoji is used, the name of that emoji will be listed instead of the emoji itself. This attribute is always empty for Android.

Additional Information

Discord Servers

Description	Discord Servers contains information about the servers which host Discord channels.
Recovery method	Parsing

Attribute	Description
Server	The name of the server hosting the channel.
Server ID	The ID of the server hosting the channel.
Owner ID	The ID of the owner hosting the server.
Joined Date/Time - UTC (yyyy-mm-dd)	The date and time that the local user joined the server.

Additional Information

Facebook Messenger Calls

Description	Facebook Messenger Calls contains call data recovered from Facebook Messenger. Provides useful background information on a suspect, including who he or she is communicating or associated with. Status and location updates in social media can also provide location information about the suspect.
Recovery method	Parsing and carving

Attribute	Description
User Key	The user key of the call partner.
Thread Key	The thread key of the group where the call was made.
Partner Name	The name of the call partner. If the call was made in a group chat, this field will be empty.

Attribute	Description
Group Name	The name of the group where the call was made. If the call was made in a chat with only one other person, this field will be empty.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the call.
Call Duration	The duration of the call in a friendly text format. This field is left empty if the call wasn't answered.
Call Duration (Seconds)	The duration of the call in seconds. This field is left empty if the call wasn't answered.
Call Type	The type of the call. The call type is either a voice call or a group voice call.
Answered	Indicates whether the call was answered or not.
Direction	The direction of the call.
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).

Additional Information

Facebook Messenger End-to-End Encrypted Chats

Description	Facebook Messenger End-to-End Encrypted (E2EE) Chats contains messages recovered from Facebook Messenger E2EE chats on the device.
Recovery method	Parsing

Attribute	Description
Sender Name	The display name of the person sending the message.
Recipient Name	The display name of the person receiving the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message	The text of the end-to-end encrypted message.
Direction	The direction of the message (Incoming or Outgoing) relative to the local user's device.

Additional Information

Facebook Messenger Groups

Description	Facebook Messenger Groups contains data about group chats on Facebook Messenger. Provides useful background information on a suspect, including who he or she is communicating or associated with. Status and location updates in social media can also provide location information about the suspect.
Recovery method	Parsing and carving

Attribute	Description
Group Name	The display name of the group.
Participants User Names	The user names of the users that are a part of the group.

Attribute	Description
Participants	The user IDs of the group members.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The date and time of the last activity recorded in the group.
Senders User Names	The user names of the users that recently participated in the group.
Sender(s)	The IDs of the users that recently participated in the group (for example, by sending a message).
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
Message Count	The approximate number of messages in the group.
Thread Key	The thread key of the group.

Additional Information

Facebook Messenger Messages

Description	Facebook Messenger Messages contains messages recovered from Facebook Messenger. Provides useful background information on a suspect, including who he or she is communicating or associated with. Status and location updates in social media can also provide location information about the suspect.
Recovery method	Parsing and carving

Attribute	Description
Sender Name	The display name of the person sending the message.
Sender ID	The user ID of the person sending the message.
Receiver Name	The display name of the person receiving the message.
Group Name	The display name of the group receiving the message.
Receiver ID	The user ID of the person receiving the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time when message was sent.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time the message was deleted from the application.
Text	The text of the message.
Message Type	The type of message that was sent. If multiple attachments were sent together, this fragment indicates the number of attachments.
Send State	Represents whether the message was sent, received or queued. This field is always empty for Android.
Media Info	The information about the media that is found. This value can be a URL to the media, a file name, or a sticker ID.
Latitude	The latitude portion of the location data that is sent with the message.
Longitude	The longitude portion of the location data that is sent with the message.

Attribute	Description
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
Thread ID	The thread ID of the message. This is also the Facebook ID of the remote party.
Message ID	The internal unique message ID.
Message Source	The source of the message creation platform.
Attachment	The recovered attachment. If the attachment is a video, the video gets segmented into multiple files. Each segment gets collected for playback in Magnet AXIOM, but the actual file size might differ from the size that AXIOM reports due to the segmentation.

Additional Information

Facebook Messenger Users Contacted

Description	Facebook Messenger Users Contacted contains information about users contacted from the device using Facebook Messenger. Status and location updates in social media can provide detail on where the suspect has been. In addition, this artifact provides background information on a suspect,including who he or she is communicating or associated with.
Recovery method	Parsing and carving

Attribute	Description
User Key	The user key of the user.
First Name	the first name of the user.
Last Name	The last name of the user.
Name	The display name of the user.
Username	The unique identifier of the user.
Profile Image	The profile image of the user.
Profile Picture URL	The URL of the user's profile picture.
Is App User	Identifies whether the user is using Facebook Messenger or not.
Is Friend	Identifies whenever the user is a friend of the local user.
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
Rank	User's rank within the app.

Additional Information

Glide Messages

Description	Glide Messages contains messages sent and received by the local user.
Recovery method	Parsing

Attribute	Description
Sender ID	The unique user ID of the sender.
Sender Name	The name of the sender.
Recipient ID(s)	The Glide IDs of the message recipients.
Recipient Name(s)	The names of the message recipients.
Message	The body of the message.
Message Type	The type of message.
Created Date/Time	The date and time when the message was created.
Read	The read status of the message.
Media URL	The URL to any media that's attached to the message.
Chat Type	The type of chat where the message was sent (group or oneToOne).

Additional Information

Glide Users

Description	Glide Users contains information about the contacts that the local user has added using Glide. The local user's contact information is also recovered by this artifact.
Recovery method	Parsing

Attribute	Description
User ID	The unique ID of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
Email Address	The email address of the user.
Gender	The gender of the user.
Account Type	The type of account associated with the user.
Last Seen Date/Time	The last time the user was seen online.

Additional Information

Google Duo Activity

Description	Google Duo Activity contains details about audio calls, video calls, and messages sent and received by the user.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message or call.
Recipient(s)	The recipient(s) of the message or call. The recipients of a group call are the users who joined the call. If no one joined the group call, this fragment will be empty.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	The date and time of the message or call.
Activity Type	The type of activity. Possible values include Audio Call, Video Call, and Message.
Direction	The direction of the activity.
Call Status	The status of the call. Possible values include Answered, Not Answered, and Rejected.
Call Duration (Seconds)	The duration of the call.
Message ID	The ID of the message (if the Activity Type is Message).
Message	The content of the message.
Attachment Name	The name of the attachment from the message.
Reaction	The reaction to a message. You can associate the reaction to the message through the Message ID. In the Google Duo app, the reaction is overlaid on the message, but in AXIOM Examine, the reaction is presented on its own.
Attachment	The attachment from the message.

Additional Information

Google Duo Group Calls

Description	Google Duo Group Calls contains details about the video calls made and received by the user.
Recovery method	Parsing

Attribute	Description
Session ID	The session ID of the group call.
Call Status	The status of the call. 'Incoming Initiated' indicates an incoming call request, 'Incoming Cancelled' indicates that the caller cancelled the request before connecting, and 'Call' indicates an incoming call that was connected or an outgoing call that is unknown if any participants joined the call.
Caller	The phone number of the caller.
Recipient(s)	The recipients of the call.
Call Date/Time - UTC (yyyy-mm-dd)	The date and time of the call.
Call Duration (Seconds)	The duration of the call.
Call Type	The type of call.

Additional Information

Google Duo Groups

Description	Google Duo Groups contains membership information of Google Duo Groups.
Recovery method	Parsing

Attribute	Description
Group Chat ID	The ID of the group.
Group Name	The display name of the group.
Group Member Name(s)	The display names of the group members.
Group Member ID(s)	The IDs of the group members.

Additional Information

Google Hangouts Cached Images

Description	Google Hangouts Cached Images contains the cached images from Google Hangouts from an Android device.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the cached image.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	The date and time of the image. The significance of the date and time is unknown to us.
Image	The cached image.

Additional Information

Google Hangouts Voice Calls

Description	Google Hangouts Voice Calls contains a history of voice calls between the local user and other users.
Recovery method	Parsing

Attribute	Description
Phone Number	The phone number of the call participant.
Call Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the call started.

Additional Information

Google Meet Meeting History

Description	Google Meet Meeting History contains the meetings that any local user on the device has joined.

Recovery method	Carving

Attribute	Description
Meeting ID	The unique ID for the meeting.
Meeting Code	The code that was used to join the meeting.
URL	The URL for the meeting.
Joined Date/Time - UTC (yyyy-mm-dd)	The date and time that the local user joined the meeting. This value is only available in newer versions of Google Meet starting with version 2022.3.6.433612476.
Joined Date/Time - Local Time	The local date and time that the local user joined the meeting.
Type	Whether the local user created or joined the meeting.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

GroupMe Accounts

Description	GroupMe Accounts contains information about the accounts that the local user has logged in with on the device.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the local user.
Display Name	The display name of the local user.
Email Address	The email address of the local user.
Phone Number	The phone number of the local user.
Created Date/Time	The date and time that the account was created (specific to iOS).
Login Date/Time	The date and time that the account was logged in on the device (specific to Android).
Profile Picture URL	The URL of the profile picture of the local user.
Password/Token	The local user password/token.
Platform	The cloud platform name.

Additional Information

GroupMe Contacts

Description	GroupMe Contacts contains information about a user's contacts.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the contact.
Display Name	The display name of the contact.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact was added.

Additional Information

GroupMe Groups

Description	GroupMe Groups contains information about the groups that the logged-in user is a member of.
Recovery method	Parsing

Attribute	Description
Group	The group number.
Group Name	The name of the group.
Topic	The topic of the group.
Creator ID	The creator identifier of the group.
Created Date/Time	The date and time when the group was created
Group Member ID(s)	The IDs of all of the group's participants.
Group Member Name(s)	The names of all of the group's participants.

Additional Information

GroupMe Messages

Description	GroupMe Messages contains the messages sent and received using

	GroupMe.
Recovery method	Parsing

Attribute	Description
Sender Name	The name of the message sender.
Sender ID	The user ID of the message sender.
Recipient Name(s)	The user name(s) of the message recipient(s).
Recipient ID(s)	The user ID(s) of the message recipient(s).
Sent Date/Time	The date and time when the message was sent.
Message	The message text.
Photo URL	The URL to the photo associated with the message.
Video URL	The URL to the video associated with the message.
Locale	The name of the location in the location data sent with the message.
Latitude	The latitude part of location data sent with the message.
Longitude	The longitude part of location data sent with the message.
Event	The event sent with the message.
Document Title	The document details sent with the message.
Poll	The poll details sent with the message.

Additional Information

Gtalk Contacts

Description	Gtalk Contacts contains contact information that was recovered from Gtalk.
Recovery method	Parsing

Attribute	Description
Username	The username/Gmail address of the contact.
Nickname	The nickname of the contact.
Local Account	The user account of the user logged into Gtalk.

Additional Information

Gtalk Messages

Description	Gtalk Message contains the details of messages that were recovered from Gtalk.
Recovery method	Parsing

Attribute	Description
Sender	The user who sent the message.
Receiver	The user who received the message.

Attribute	Description
Local User	The local user ID.
Date/Time - UTC (yyyy-mm-dd)	The timestamp for the message.
Message	The message that was sent.
Sent/Received	The type of the message.

Additional Information

Houseparty Messages

Description	Houseparty Messages contains messages recovered from Houseparty.
Recovery method	Parsing

Attribute	Description
Sender	The username of the person sending the message.
Recipient	The username of the person receiving the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The content of the sent message.
Read Status	Indicates whether or not the message has been read.

Additional Information

Houseparty Users

Description	Houseparty Users contains information about the users that were contacted from the device using Houseparty.
Recovery method	Parsing

Attribute	Description
User Name	The username of the user.
Full Name	The full name of the user.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the user account was created.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the user account was last updated.

Additional Information

imo Contacts

Description	imo Contacts contains information about a user's contacts.
Recovery method	Parsing

Attribute	Description
User ID	The unique user ID of the contact.

Attribute	Description
Display Name	The display name of the contact.
Name	The full name of the contact.
Phone Number	The phone number of the contact.
Number of Times Contacted	The number of times that the local user initiates contact (by message or call) with the contact.

Additional Information

imo Messages

Description	imo Messages contains information about sent and received messages and calls made using the imo application.
Recovery method	Parsing

Attribute	Description
Local User	Indicates the local user identifier of the account.
Remote User ID	The user ID of the remote conversation partner.
Remote User Display Name	The display name of the remote conversation partner.
Direction	The direction of the message.
Message	The message content.

Attribute	Description
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message Type	The type of the message (either call or message).
Attachment Path	The path to locate any attachments on the device.
Attachment	The attachment on the device.

Additional Information

IP Addresses - Audio/Video Calls

Description	IP Addresses of web audio/video calls show who a user was communicating with. Each instance of this artifact represents a single hop in the communication chain. By showing the relationship between multiple hops, you can determine where a call originated from and what the final destination was.
Recovery method	Carving

Attribute	Description
Call ID	The ID of the call.
Message ID	The ID of the message.
Domain	The domain used for the call.
Connection Type	The type of connection.

Attribute	Description
Origin IP Address	The originating IP address for this hop in the call.
Origin Port	The originating port for this hop in the call.
Destination IP Address	The destination IP address for this hop in the call.
Destination Port	The destination port address for this hop in the call.
Date/Time - UTC (yyyy-mm-dd)	The timestamp associated with this hop in the call.
Remote User ID	The unique ID of the remote user.
Communication Protocol	The communication protocol for this call (either UDP or TCP).
Metadata	Any additional details about the call.

Additional Information

Jott Groups

Description	Jott Groups contains information about the groups that the Jott user is a member of.
Recovery method	Parsing

Attribute	Description
Group Chat ID	The ID of the group chat.

Attribute	Description
Group Name	The display name of the group.
Participants	The users that are a part of the group.
Picture Path	The path to the group's picture, if one exists.

Additional Information

Jott Messages

Description	Jott Messages contains information about the messages sent or received by the Jott user.
Recovery method	Parsing

Attribute	Description
Sender	The username of the person sending the message.
Recipient	The username of the person receiving the message, or the group chat ID if the message is being sent to a group.
Message	The message being sent.
Direction	The direction of the message being sent.
Read Status	Indicates whether or not the message has been read.
Group Chat	Indicates whether or not this is a group chat.
Sent Date/Time - UTC	The date and time when the message was sent.

Attribute	Description
(yyyy-mm-dd)	
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received.
Attachment Path	The path to the attachment, if one exists.

Additional Information

KakaoTalk Browsing History

Description	KakaoTalk Browsing History contains the web browsing history on any links visited within the KakaoTalk application.
Recovery method	Parsing

Attribute	Description
URL	The URL of the webpage link opened in KakaoTalk.
Title	The title of the webpage link opened in KakaoTalk.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage link was accessed in KakaoTalk.

Additional Information
Sometimes, the web browsing history is duplicated in the database this artifact is recovered from. This behavior is expected, though the cause is unknown. The duplicated data and its associated timestamps are identical.

KakaoTalk Calls

Description	KakaoTalk Calls contains audio calls and/or video calls sent or received using KakaoTalk.
Recovery method	Parsing and carving

Attribute	Description
Call Status	Information about the call.
Duration (Seconds)	The duration of the call in seconds.
Sender ID	The KakaoTalk ID of the sender.
Sender Name	The name of the sender.
Chat ID	The ID of the KakaoTalk chat room session.
Call Type	Indicates whether the call was a voice call or a video call.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the call was made.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time that the call was deleted from the application.
Direction	Indicates whether the call was incoming or outgoing.

Additional Information
Call Status and Sender information are not available for deleted calls.

KakaoTalk Chat Rooms

Description	KakaoTalk Chat Rooms contains KakaoTalk chat rooms that the user participates in.
Recovery method	Parsing

Attribute	Description
Group Chat ID	The ID of the KakaoTalk chat room session.
Other Participants	The names or KakaoTalk IDs of the other chat room participants.
Chat Type	The type of chat room session.
Last Message	The last message sent by any participant in the chat room session.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the chat room session was last updated.
Unsent Message	Messages that the local user has written, but not sent to the chat room.
Group Name	The name of the group, if the chat room session is a group chat.
Invitation Status	The status of any invitations to the chat room.

Additional Information

KakaoTalk Detected Wifi

Description	KakaoTalk Detected Wifi contains the network name of any WiFi networks detected by KakaoTalk.
Recovery method	Parsing

Attribute	Description
Network Name (SSID)	The network name.

Additional Information
As of KakaoTalk 8.4.0, the data in this artifact is no longer available.

KakaoTalk Friends

Description	KakaoTalk Friends contains the user's KakaoTalk friends and contacts.
Recovery method	Parsing

Attribute	Description
ID	The KakaoTalk ID of the friend.
Name	The friend's name.
Contact Name	The friend's full contact name.
Nickname	The friend's nickname as set by the local user.

Attribute	Description
Status Message	The status message of the friend.
Favorite	Indicates whether the friend has been marked as a favorite.
Hidden	Indicates whether the friend has been hidden in the local user's application.
Phone Number	The friend's phone number.
Profile Picture URL	The URL for the friend's profile picture.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the friend's account was created.
User ID	The friend's KakaoTalk user ID.
Group Chat ID	The chat room session IDs that the friend shares with the local user.

Additional Information

KakaoTalk Messages

Description	KakaoTalk Messages contains messages sent or received using KakaoTalk.
Recovery method	Parsing and carving

Attribute	Description
Sender ID	The KakaoTalk ID of the sender.
Sender Name	The name of the sender.
Message	The message contents.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was created.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was deleted from the application.
Chat ID	The ID of the KakaoTalk chat.
Message Type	The type of the message sent.
Message Direction	Indicates whether the message was sent or received.
Additional Information	Additional information attached to the message.
Latitude	The latitude of location type messages.
Longitude	The longitude of location type messages.
Attachment	The attachment sent with the message.
Attachment Name	The file name of the attachment sent with the message.
Attachment Path	The file path of the attachment sent with the message.

Additional Information

Message and Sender information are not available for deleted messages.

LINE Chats

Description	LINE Chats contains the chats that the local user is a part of.
Recovery method	Parsing

Attribute	Description
Participants	The users in the chat (other than the local user).
Chat Name	The name of the chat.
Owner	The owner of the chat.
Last Message	The last message that was sent in the chat.
Sender	The user who sent the last message.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the last message was received.
Message Count	The number of messages that were sent in the chat.
Read Count	The number of messages that were read in the chat by the local user.

Additional Information

LINE Contacts

Description	LINE Contacts contains the user's LINE contacts.
Recovery method	Parsing

Attribute	Description
Line ID	The LINE ID of the contact.
Name	The name of the LINE contact.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the user contact was added.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact was last updated.
Status Message	The status of the contact.
Hidden	Indicates whether the contact has been marked as hidden.
Favorite	Indicates whether the contact has been marked as favorite.

Additional Information

LINE Messages

Description	LINE Messages contains messages that were sent and received through LINE on Android.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the message. The sender value can be the sender's

Attribute	Description
	name or Local User.
Recipient(s)	The recipient(s) of the message.
Message Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was created.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The body of the message.
Message Type	The type of the message. The Message Type value can be Audio, Call, Contact Card, File, Location, Note, Picture, Sticker, or Text.
Contact Card Name	The first and last name of the contact.
Read Count	The number of times that the message has been read.
Location Address	The address of the location.
Latitude	The latitude of the location when message type is Location.
Longitude	The longitude of the location when the message type is Location.
Audio Length (Seconds)	The length of the audio in seconds when the message type column is Audio.
Call Duration (Seconds)	The duration of the call in seconds when the message type is Call.
File Attachment	The name of the file that's sent when the message type is File.
File Size (Bytes)	The size of the file sent in bytes.

Attribute	Description
Attachment	The attachment sent with the message. For messages with a message type of "Video", the attachment might only be a thumbnail of the original video.
Thumbnail	A thumbnail of the image (if available).

Additional Information

LINE Pictures

Description	LINE Pictures contains pictures originating from LINE.
Recovery method	Parsing

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed	The last accessed date and time of the picture in the file system.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken

Attribute	Description
	(extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture, or the name of the software that was used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Longitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Exif Data	A searchable field for all raw exif properties.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.

Attribute	Description
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Mail.Ru Agent Contacts

Description	Mail.Ru Agent Contacts contains contact info for the Agent application on Android.
Recovery method	Parsing

Attribute	Description
Contact ID	The user ID of contact.
Display Name	The display name of contact.
Account Type	The type of the contact. The value can be Agent ID or Agent Channel.
Local User ID	The unique ID of the local user.

Additional Information

Mail.Ru Agent Messages

Description	Mail.Ru Agent Messages contains messages sent or received by the Agent user on Android.
Recovery method	Parsing

Attribute	Description
Local User ID	The unique ID of the local user.
Remote User ID	The user ID of the remote participant of the chat.
Remote Participant Display Name	The display name of remote participant.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was created.
Message	The content of the message.
Type	The type of the message. The value can be Text Message, Voice Call, Video Call or File Transfer.
Duration (Seconds)	The duration of voice or video call.
Direction	The direction of the message.
File Name	The file name of the attachment.
File	The attachment associated with the message.

Additional Information

Mail.Ru Agent User Accounts

Description	Mail.Ru Agent User Accounts contains information about the Agent user accounts that are saved locally on the Android device.
Recovery method	Parsing

Attribute	Description
User ID	The unique ID of the local user.
Active	Whether or not the account is currently logged in.
First Name	The first name of the account.
Last Name	The last name of the account.
Display Name	The display name of the account.
Birthday	The birthday of the account.
Phone Number	The phone number of the account.
Gender	The gender of the account.
Home Address	The home address of the account.

Additional Information

ooVoo Chat History

Description	ooVoo Chat History contains the chat history between the data owner and

	their contacts.
Recovery method	Parsing

Attribute	Description
Message ID	The ooVoo unique message identifier.
Sender User ID	The ooVoo identifier of the sender.
Receiver User ID(s)	The ooVoo identifier of the recipient(s).
Chat Date/Time - UTC (yyyy-mm-dd)	The date and time of the conversation.
Message	The actual message content.
Message Type	The type of message that was sent. Some examples of message type are chat, video, and image.
Message Direction	Indicates whether the message was sent (Outgoing) or received (Incoming).
Group Name	The name that is associated with a group conversation. If the chat is between two people the name will be empty.
Video URL	The address of the video that was sent in the message.
Image URL	The address of the image that was sent in the message.
Source	The location where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

ooVoo Contact List

Description	ooVoo Contact List contains the list of contacts that the data owner has on ooVoo.
Recovery method	Parsing

Attribute	Description
Display Name	The contact display name.
User ID	The contact's unique ooVoo identifier.
Status Message	A message set by the contact. This message can contain insight into how the person is feeling, as well as their ideas and thoughts.
Birthday (yyyy-mm-dd)	The contact's birthday.
Phone Number	The contact's phone number.
Password	The contact's password stored as plain text.
Platform	The cloud platform name.

Additional Information

ooVoo Phone Book

Description	ooVoo Phone Book contains the name and phone number of contacts from the data owner's iOS device.
Recovery method	Parsing

Attribute	Description
Contact Name	The name of the contact.
Phone Number	The contact's phone number.
Source	The location where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

QQ File Transfers

Description	QQ File Transfers contains file transfers recovered from the QQ application.
Recovery method	Parsing

Attribute	Description
Local User ID	The local user ID who the file was transferred with.
Chat Partner / Group Chat ID	The unique ID of the chat partner or group the file was transferred with.
Partner Display Name	The name displayed for the partner the file was transferred with.
Server Date/Time - UTC (yyyy-mm-dd)	The server date and time that the file was transferred.
Direction	Sent/Received: Indicates the direction of the file transfer relative to the local user.
File Name	The file name of the file transferred.
File Path	The file path of the file transferred.
File Size (bytes)	The size of the file transferred.
MD5 Hash	The MD5 hash of the file.
SHA1 Hash	The SHA1 hash of the file.

Additional Information

QQ Local Users

Description	QQ Local Users contains local users recovered from the QQ application.
Recovery method	Parsing

Attribute	Description
Local User ID	The user ID of the local user.
Local User Display Name	The name displayed for the local user.
Country	The country of the user.
City	The city of the user.
Age	The user's age in years.
Birthday (yyyy-mm-dd)	The user's birthday in YYYY-MM-DD format.
Email	The user's email address.

Additional Information

QQ Messages

Description	QQ Messages contains messages stored by the QQ application.
Recovery method	Parsing

Attribute	Description
Local User ID	The unique ID of the local user.
Local User Display Name	The name displayed for the local user.
Chat Partner / Group Chat ID	The unique ID of the chat partner or group.
Sender User ID	The unique ID of the sender.

Attribute	Description
Sender Display Name	The name displayed for the sender.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the message.
Message	The text of the message.
Type	The type of content in the message.
Sent/Received	Indicates whether the message is incoming or outgoing (Sent or Recieved).
Read	Indicates whether the message has been read (Read or Unread).

Additional Information

Samsung Messages

Description	Samsung Messages is an application that is installed by default on Samsung Android devices and is used for sending SMS and MMS messages.
Recovery method	Parsing

Attribute	Description
Conversation Partner	The phone number of the other person in the conversation.
Contact Name	The name of the contact. This will display if we can get the contact name from the file contact_simple_name.dat.xml.

Attribute	Description
Group Member(s)	The list of phone numbers that are part of the group mass message chat.
Message	The message body text.
Subject	The subject of the message.
Message Received Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was originally meant to be received.
Message Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was created on the device, in both cases where it was either sent or received on the device.
Scheduled Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was scheduled by the local user to be sent.
Group Chat ID	The unique identifier for a group mass message sent by the local user.
Message ID	The message identifier. Some messages will have the same message identifier indicating they are part of the same message.
Message Type	Indicates whether the message is SMS or MMS.
Message Direction	Indicates whether the message was sent or received on the local user's device.
IMSI	The international mobile subscriber identity of the local device's SIM card.
Read	Indicates whether or not the message has been read by the local user.

Attribute	Description
Content Type	The content MIME type of the message.
File Name	The name of the file.
File Path	The local file path of the file sent or received.
URL	The URL of the website previewed in the message.
Description	The description of the website previewed in the message.
Title	The title of the website previewed in the message.
Search Query	This is an automatic search query result given when the web preview for a location or URL is sent in the message.
Attachment	The attachment associated with the message.

Additional Information

Samsung Text Message Logs

Description	Text message logs recovered from a Samsung Android device.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where data was recovered from.
Partner	An identifier for the person who communicated with the local user.
Partner Name	The name of the partner, as set by the local user.

Attribute	Description
Direction	The direction of the message, relative to the local device (Incoming or Outgoing).
Date/Time - UTC (yyyy-mm-dd)	The date and time of the text message.
Message Content	The text message content.
Subject	The subject of the text message. If message type is MMS this field has a value, otherwise is empty.
Message Type	The type of message. This can be 'SMS' or 'MMS'.

Additional Information

Session Communities

Description	Session Communities contains information about the open session groups that the local user has joined.
Recovery method	Parsing

Attribute	Description
Group Name	The name of the session community.
URL	The URL for the community.
Description	The description of the session community.
User Count	The number of users in the session community.

Additional Information

Session Groups

Description	Session Groups specifies each of the Session groups that the local user is a member of.
Recovery method	Parsing

Attribute	Description
Group Name	The name of the group.
Group ID	The ID of the group.
Group Member(s)	The member name(s) of the group.
Group Member ID(s)	The member ID(s) of the group.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the group was created.

Additional Information

Session Messages

Description	Session Messages contains information about the messages and calls that are exchanged between the local user and other users on an Android device.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message.
Sender ID	The ID of the message sender.
Recipient	The message recipient.
Recipient ID	The ID of message recipient.
Message	The content of the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received.
Type	The type of the message.
Direction	The direction of the message (Incoming or Outgoing).
Attachment Name	The name of the message attachment if one was sent.
Attachment	The content of the attachment if one was sent.
Expiration (dd hh:mm:ss)	The expiration policy that was set on the conversation at the time of sending the message.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the message is set to expire.

Additional Information

Session Users

Description	Session Users contains information about the users the local user has associated with through communities, group chats, or direct messages.
Recovery method	Parsing

Attribute	Description
User ID	The user ID.
Display Name	The display name of the user.
Local User	Indicates with 'Yes' if the user is the local user. Otherwise, the field is empty.
Display Name Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the display name was last modified by the user.

Additional Information

Signal

Signal is an encrypted messaging and voice calling application that's available for Android and iOS. The application enables a user to send content (messages, pictures, and videos) to other users and to groups of users. Signal also includes the capability for users to set a password on the application to protect their data.

The content shared between a user and their contacts can be valuable information, as well as the phone numbers of group members and the names of local users. In an investigation, this information can offer insight into the purpose of a suspect's interactions and can be used to

identify users who have been in contact with a suspect. Other information can also be recovered, such as message timestamps and shared location messages. This information can be used in piecing together a timeline of a suspect's activity, or for determining their previous whereabouts.

Signal for Android

Even though Signal uses encryption to protect its data, it's still possible to recover useful artifacts from Android and iOS devices. In cases where the user doesn't set a password, application data can often be recovered and decrypted. Even if decryption is not possible, group and user information, and information about messages can still be recovered (excluding the actual message and attachment content). In addition, latitude and longitude from location messages are also recoverable (these are messages that a user sends that includes their current location).

For instances when the user does set a password, you can provide a list of potential Signal account passwords in AXIOM Process or IEF to use as the key for decrypting the data. Once decrypted, message content and attachments are made available.

Artifacts

Signal Group Members

Signal Local User

Signal Messages

Signal Conversations - Android

Description	Signal Conversations contains information about the group or individual conversations that the local user has participated in.
Recovery method	Parsing

Attribute	Description
Partner Phone Number	The phone number of the partner for individual conversation.
Partner Display Name	The display name of the partner for individual conversation.
Group Name	The name of the group for group conversation.
Group Member Phone Number(s)	The list of phone numbers for the group members.
Group Member(s)	The list of display names for the group members.
Group Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the group was created.
Message Count	The number of messages in the conversation.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the last message in the conversation was sent or received, to the nearest second.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The date and time when the conversation was last viewed by the local user.
Snippet	The short preview of the last message in a conversation.
Type	The type of the last message in the conversation.
Pinned	Indicates if the conversation has been pinned by the local user.
Archived	Indicates if the conversation has been archived by the local user.
Group Avatar	The avatar of the group.

Additional Information

Signal Group Members

Description	Signal Group Members specifies the members from each of the Signal groups that the local user is a member of.
Recovery method	Parsing

Attribute	Description
Group Member	The phone number of the group member.
UUID	The unique user ID associated with group member.
Group Name	The name of the group.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the group was created (Empty for Android).
Group Avatar	The avatar of the group.

Additional Information

Signal Groups

Description	Signal Groups contains information about the members of groups
Recovery method	Parsing

Attribute	Description
Group Name	The name of the group.

Attribute	Description
Group ID	The ID of the group.
Group Member(s)	The user names of the group members.
Group Member Phone Number (s)	The phone numbers of the group members.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the group was created (empty for Android).
Group Avatar	The avatar of the group.

Additional Information

Signal Local User

Description	Signal Local User contains information about the local user account.
Recovery method	Parsing

Attribute	Description
Local User	The name of the local user.
Avatar	The avatar used by the local user account (empty for Android).

Additional Information

Signal Messages - Android

Description	Signal Messages contains information about the messages and calls that are exchanged between the local user and other users.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message.
Sender Name	The name of the sender.
Recipient	The phone number or group ID of the recipient.
Recipient Name	The name of the recipient or the name of the group.
Partner	The partner of the call.
Message	The content of the message. For Group Update type messages, a System Message prefix is attached which tries to imitate a Signal message although the wording might vary.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the the message was first attempted to be sent.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received.

Attribute	Description
Type	The type of message.
Direction	The direction of the message.
Read	Indicates whether or not the message has been read by the local user.
Metadata	The information about current members of a group. This information may not appear in the Signal application but is recorded in the database as a system log. It might be useful to determine if a user is in a group even if the user never actively participated.
Attachment	The attachment of the message.
File Name	The name of the attachment file.
File Path	The path where the attachment file is located.
Story ID	The record ID of the Story hit, if the message is a reply to a story.
MIME Type	The MIME type of the attachment.
Latitude	The latitude of the message.
Longitude	The longitude of the message.

Additional Information

Some Group Update messages might remain encoded. If you notice this issue, contact Magnet Technical Support to request that a new encoding type gets added to this artifact.

Signal Stories

Description	Signal Stories contains information about stories that are posted, viewed,

	or exchanged between the local user and other users on an Android device.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the story.
Recipient(s)	The story recipient(s)
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the story was created.
Story ID	The record ID of the story hit.
Uploaded Date/Time - UTC (yyyy-mm-dd)	The date and time when the story attachment was uploaded if one was added.
Recipient Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the recipient received the story.
Read Date/Time - UTC (yyyy-mm-dd)	The earliest date and time when the story was read (only available on iOS).
Direction	The direction of the story (incoming or outgoing).
Content Type	The content type of the story, such as 'text/html', 'image/jpeg', 'video/mp4', etc.
Story Name	The name of the story (only available on iOS).
Text	The text content of the story if the content type was text.

Attribute	Description
Caption	The caption of the story.
Attachment Name	The name of the story attachment if one was added.
Attachment	The content of the attachment if one was sent.

Additional Information

Signal Users

Description	Signal Users lists all of the users and profiles present in the application.
Recovery method	Parsing

Attribute	Description
Phone Number	The phone number associated with the user.
UUID	The unique user ID (UUID) associated with the user.
Full Name	The full name of the user, as stored by the Signal application.
Profile Name	The profile name of the user. This is usually a nickname.
Family Name	The last name of the user.
Type of User	The type of the user.
Local User	Indicates whether the user is logged into the device.
Avatar	The user's avatar.

Additional Information

Skype Accounts

Description	Skype Accounts contains information about the Skype accounts that are recovered, such as user information and when the account was created.
Recovery method	Parsing and carving

Attribute	Description
Skype Name	The Skype name of the account.
Display Name	The display name of the account.
Full Name	The full name of the account.
Email(s)	The email of this account.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date when the profile was created.
Last Online Date/Time - UTC (yyyy-mm-dd)	The last time that the account was online.
Birthday (yyyy-mm-dd)	The birthday of the account.
Gender	The gender of the account.
City	The city where the account is located.
State/Province	The state/province where the account is located.
Country	The country where the account is located.
Home Phone	The home phone of this contact.
Office Phone	The office phone of this account.

Attribute	Description
Mobile Phone	The mobile phone of this account.
Homepage	The homepage of this contact.
About Info	The about info of this contact.
Profile Last Modified On Date/Time - UTC (yyyy-mm-dd)	The date when the profile was last modified.
Mood Text	The text used to express mood.
Last Used On Date/Time - UTC (yyyy-mm-dd)	The last time that the account was used.
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	The time that the avatar was created.
Picture	The avatar for this contact.

Additional Information

Skype Activity

Description	Skype Activity contains interactions that occurred between users on Skype. These interactions include messages, message drafts, group interactions, calls, sent/received files, and SMS. This information is recovered for Skype 8.1 and later.
Recovery method	Parsing and carving

Attribute	Description
Conversation ID	The ID of this conversation.
Profile Name	The local user's profile name.
Sender	The username of the sender/initiator of the interaction.
Sender Email	The sender's email as given in the message (if available).
Recipient(s)	The recipients or targets of the interaction.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the interaction was initiated.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the interaction was last updated (for example, when a call ends).
Message Type	The type of the interaction.
Message	The content of the message or a summary of the interaction. Drafted messages will begin with [Draft].
Emotion Count	The number of reactions to the interaction. Reactions include likes, dislikes, emojis and more.
File Name	The name of any attached files associated with the interaction.
File Size (Bytes)	The size in bytes of any attached files.
Attachment	The attachment associated with the activity.
Attachment Data Recovered	Indicates whether the attached file was recovered from the local filesystem.
Thumbnail URL	A URL that directs to the thumbnail picture (if applicable).
Call Duration (Seconds)	The length of the call in seconds (if applicable).

Attribute	Description
Metadata	The content of the message, if it consisted of interpreted data (XML or JSON data, rather than plain text).

Additional Information

Skype Calls

Description	Skype Calls contains information about Skype calls that occur between users.
Recovery method	Parsing and carving

Attribute	Description
Local Username	The user logged into Skype at the time of the call.
Call Initiator	The user who started the call.
Initiator Display Name	The display name of the user. This might be different from the user-name.
Recipient Name(s)	The users who accepted a call from the call initiator and participated in the call for a period of time.
Call Participants	The users who accepted and participated in the call from the call ini-tiator for some duration.
Started Date/Time - UTC (yyyy-mm-	The start time of the call.

Attribute	Description
dd)	
Duration	The total duration of the Skype call.
Metadata	Additional details about the call extracted in XML format. This includes information on the amount of time that each participant was in the call.

Additional Information

Skype Chat Messages

Description	Skype Chat Messages contains Skype messages sent from one user to another.
Recovery method	Parsing and carving

Attribute	Description
Chat ID	The ID of the chat.
Profile Name	The profile name of the caller.
Author	The author of the message.
Recipient(s)	The recipient(s) of the chat.
From Display Name	The display name of the message sender.
Message Sent	The date and time that the message was sent.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Message	The body of the message or a description of the action taken. For example, adding another participant to a group chat or sharing a file or picture.
Attachment Name	The name of the attachment that was sent. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Attachment Size (bytes)	The size of the attached file, in bytes. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Metadata	Additional details about the action, extracted in its original XML format.
Message Status	The status of the message.
Message Type	The type of message.

Additional Information

Skype Chatsync Messages

Description	Skype Chatsync Messages contains Skype messages that were sent from one user to another, and that are parsed from the chatsync directory.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of this message.
Chat Partner / Group Chat ID	The other part of this message.
Chat Initiator	The initiator of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The content or body of the message.
Message Type	The type of the message.

Additional Information

Skype Contacts

Description	Skype Contacts contains information about Skype contacts that are recovered, which may or may not be added contacts.
Recovery method	Parsing and carving

Attribute	Description
Profile Name	The profile name of the user.
Skype Name	The Skype name of the contact.
Full Name	The full Name of this account

Attribute	Description
Display Name	The display name of this account.
Email(s)	The email of this account.
Last Online Date/Time - UTC (yyyy-mm-dd)	The last time that the account was online.
Is Blocked	Indicates whether the contact is blocked.
Contact Added	Specifies whether the contact is an added contact or just cached into the database (1 if the contact was added, 0 otherwise). Contacts can be cached into the database for a variety of reasons (for example, as a suggested contact).
Birthday (yyyy-mm-dd)	The birthday of this account.
Gender	The gender of this account.
City	The city where this account is located.
State / Province	The state/province where this account is located.
Country	The country where this account is located.
Home Phone	The home phone of this contact.
Office Phone	The office phone of this account.
Mobile Phone	The mobile phone of this account.
PSTN Num-	The PSTN number of this contact.

Attribute	Description
ber	
Homepage	The homepage of this contact.
About Info	The about info of this contact.
Profile Loaded Date/Time - UTC (yyyy-mm-dd)	Previously called Profile Created On Date/Time, this attribute represents the date and time when a contact's profile is first created on the user's device. When the profile information is updated by the contact, the date in the database is also updated.
Mood Text	The text used to express mood.
Last Used On Date/Time - UTC (yyyy-mm-dd)	The last time that the account was used.
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	The time that the avatar was created.
Image	The image for this contact.

Additional Information

Skype Emotions

Description	Skype Emotions contains the reactions of users to Skype messages.
Recovery method	Parsing and carving

Attribute	Description
Emotion	The type of emotion that the user reacted to the message with. The emotion is displayed using the shortcut from Skype (for example, cwl represents the emotion Crying With Laughter).
Message Content	The content of the message that the user reacted to. If the content of the message is plain text, this attribute matches the "Message" attribute from the "Skype Activity" artifact. Otherwise, this attribute matches the "Metadata" attribute.
Skype Name	The Skype name of the user who reacted to the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the user reacted to the message.

Additional Information

Skype File Transfers

Description	Skype File Transfers contains files that are transferred from one user to another using Skype.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Partner Handle	The username of the file transfer partner.
Partner Display Name	The display name of the file transfer partner.
File Name	The name of the file that was being transferred.
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the file transfer was started.
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date and time when the file transfer was completed.
File Path	The path to the local file.
Transferred File	The file that was transferred.
Type	The type of file that was being transferred.
File Size (Bytes)	The size of the file being transferred.
Bytes Transferred	The number of bytes that were transferred.
Status	The status of the file (for example, transfer, transferring or cancelled).

Additional Information

Skype Group Chat

Description	Skype Group Chat contains information about the Skype group chats that a user is a part of.

Recovery method	Parsing and carving

Attribute	Description
Chat ID	The group chat's unique identifier.
Profile Name	The name of the user.
Participants	The participants of the chat.
Posters	The users that have posted to the chat.
Active Members	The currently active user's of the group.
Started Date/Time - UTC (yyyy-mm-dd)	The date and time that the chat started.
Chat Name	The name of the chat.
Last Changed Date/Time - UTC (yyyy-mm-dd)	The date and time that the chat was modified.

Additional Information

Skype IP Addresses

Description	Skype IP Addresses contains the IP addresses that are associated with a Skype user account.
Recovery method	Parsing and carving

Attribute	Description
Username	The username of Skype accounts.
IP Address	The IP address for the Skype user.
Date/Time - UTC (yyyy-mm-dd)	The date and time.
IP Address Type	The type of IP address (Local or Public).

Additional Information

Skype Notifications

Description	Skype Notifications contains notifications that were shown to users on Skype.
Recovery method	Parsing and carving

Attribute	Description
Read	Indiactes whether the user has read the notification.
Conversation ID	The ID of this conversation.
Profile Name	The local user's profile name.
Sender	The username of the sender/initiator of the interaction.
Recipient(s)	The recipients or targets of the interaction.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the interaction was initiated.

Attribute	Description
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the interaction was last updated (for example, when a call ends).
Message Type	The type of the interaction.
Message	The content of the message or summary of the interaction.
Emotion Count	The number of reactions to the interaction. Reactions include likes, dislikes, emojis, and more.
File Name	The name of any attached files associated with the interaction.
File Size (Bytes)	The size in bytes of any attached files.
Attachment	The attachment file (if applicable).
Attachment Data Recovered	Indicates whether the attached file was recovered from the local filesystem.
Thumbnail URL	A URL that directs to the thumbnail picture (if applicable).
Metadata	The content of the message, if it consisted of interpreted data (XML or JSON data, rather than plain text).

Additional Information

Slack Accounts

Description	Slack Accounts contains account information on accounts signed onto the local device.
Recovery method	Parsing

Attribute	Description
User	The local user account that is signed onto the device.
Display Name	The local user display name of the account that is signed onto the device.
Email Address	The local user email address of the account that is signed onto the device.
User ID	The Slack local user ID of the account that is signed onto the device. This unique identifier is tied to the Slack workspace that the account is a member of. If an account is signed into multiple Slack workspaces, then there will be a Slack ID generated per workspace.
Account Creation Date/Time (yyyy-mm-dd)	The account creation date/time.
Last Accessed Date/Time	The date/time that the account was last accessed on the device.
Password/Token	The password/token of the account that is signed onto the device.
Group ID	The group ID of the Slack workspace that the account is a member of.
Group Name	The group name of the Slack workspace that the account is a member of.
Domain	The domain of the Slack workspace that the account is a member of.
Service	The Android package ID or Apple bundle ID of the service that the account was used for.

Additional Information
After a user signs out of their Slack Account on the device, Slack deletes all of the account information, including data in the accounts_manager database. If a Slack Account is acquired when the user is signed out, this this data will likely not be acquired.

Slack Channel Messages

Description	Slack Channel Messages contains messages sent or received in channels in the user's Slack workspace.
Recovery method	Parsing

Attribute	Description
Workspace ID	The unique identifier for the slack workspace.
Sender	The name or user ID of whoever sent the message.
Channel Name	The name of the channel that the message was sent to.
Message	The message text.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message Status	The delivered status of the message.

Additional Information

Slack Channels

Description	Slack Channels contains information about each of the channels and conversations that exist in a user's Slack workspace.
Recovery method	Parsing

Attribute	Description
Channel Name	The name of a channel or message group.
Channel ID	The ID of a channel or message group.
Workspace ID	The unique identifier for the Slack workspace.
Created By	The name or user ID of whoever created the channel.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the channel was created.
Topic	The topic text for the channel.
Topic Author	The name or user ID of whoever last wrote the topic text.
Channel Type	The type of channel (Public, Private, General, Single User DM, or Multi User DM.)
Last Read Date/Time - UTC (yyyy-mm-dd)	The date and time when the channel was last read.
Member	Represents whether or not the local user is a member of the channel.
Starred	Represents whether or not the local user has starred the channel.

Additional Information

Slack Direct Messages

Description	Slack Direct Messages contains information about direct messages sent or received in 1:1 chats or group chats.
Recovery method	Parsing

Attribute	Description
Workspace ID	The unique identifier for the slack workspace.
Sender	The name or user ID of whoever sent the message.
Recipient(s)	The names or user IDs of the message recipients.
Message	The message text.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message Status	The delivered status of the message.

Additional Information

Slack Files

Description	Slack Files contains information about any files that have saved to the

	Slack workspace. Files may or may not have been shared with other users.
Recovery method	Parsing

Attribute	Description
Workspace ID	The unique identifier for the slack workspace
Title	The title given to the file.
File Name	The name of the file.
Created By	The name or user ID of whoever created the file.
Permanent Link	A permalink to the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was uploaded
FileSize	The size of the file
Deleted	Represents whether or not the file has been deleted.

Additional Information

Slack Users

Description	Slack Users contains information about each user in the Slack workspace.
Recovery method	Parsing

Attribute	Description
Workspace ID	The unique identifier for the slack workspace.
Full Name	The full name of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
User Name	The unique user name of the user.
Display Name	The slack display name of the user.
Email	The user email.
Phone Number	The user phone number.
Member ID	The user ID.
Title	The user title.
Status Message	The status message for the user
Account Type	The type of account the user has.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the user was last updated.
Timezone	The timezone that the user is in.

Additional Information

Snapchat Accounts Information - Android

Description	Snapchat Accounts Information - Android contains information about the

	accounts that the user has logged in on the device with.
Recovery method	Parsing and carving

Attribute	Description
User ID	The unique user identifier of the account, useful for identifying who may own an account across devices.
User Name	The username of the user.
Display Name	The display name of the user.
Email Address	The email address of the user.
Phone Number	The phone number of the user.
Country	The location of the user, specified by country.
Birthday	The birthday of the user.
Last Login Date	The most recent date and time that the user used the application.
Account Creation Date/Time	The date and time that the user created the account.

Additional Information

Snapchat Cached Videos

Description	Snapchat Cached Videos contains the videos sent to the user.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file.
File Extension	The extension of the file.
Image	A generated thumbnail of the video.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the video file was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the video file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the video was last written to.
Skin Tone Percentage	The amount of skin tone found in the video.
File Size (Bytes)	The size of the video in bytes.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Additional Information

Snapchat Chat Messages

Description	Snapchat Chat Messages contains the chat messages sent between users.

Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the message.
Recipient(s)	The recipient(s) of the message.
Message ID	The ID of the message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the chat message.
Message	The content of the message.
Type	The type of the message. This value can be one of the following: Snap, Text, Media, Voice, Emoji, Call/Deleted message/Mini/Game (Snapchat removed Mini/Game feature in early 2023), Screenshot, Unsuccessful voice call, Unsuccessful video call, or Spotlight.
Saved By Sender	Whether the message was saved by the sender (Yes or No).
Saved By Recipient	Whether the message was saved by the recipient (Yes or No).
Released By Recipient	Whether the recipient let the chat message be deleted (Yes or No).
Message Status	The status of the message.

Attribute	Description
Skin Tone Percentage	The percentage of the image that is skin tone.
MD5 Hash	The MD5 hash of the image.
SHA1 Hash	The SHA1 hash of the image.
Attachment	The attachment associated with the chat message. The attachment recovery might depend on if the user saved the media to the chat.
Chat ID	The ID of the Snapchat conversation.

Additional Information

Snapchat Contacts

Description	Snapchat Contacts contains information about the user's Snapchat friends as well as contact information from the user's device that was requested by the Snapchat application.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username of the contact.
Display Name	The display name of the contact on the local device.
Phone Number	The contact's phone number.

Attribute	Description
User ID	The unique user identifier of the contact, useful for identifying who may own an account across devices.
Local User	Indicates whether the listed user account is the local account on the device. This is empty if the local user could not be determined.
Legacy User Name	The username that the contact previously used.
Added Them Date/Time - UTC (yyyy-mm-dd)	The date and time that the local user on the device added the contact.
Added Me Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact added the local user on the device.
Contact Type	Indicates the type of contact. App Native indicates that the contact is a Snapchat user, while Device Native indicates that the contact is from the user's device.

Additional Information

Snapchat Event Logs - Android

Description	Snapchat Event Logs - Android contains the events performed by the user.
Recovery method	Parsing and carving

Attribute	Description
Event	The event that the user performed.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time that the event occurred.
Event Parameters	The parameters of the performed event.

Additional Information

Snapchat Friends - Android

Description	Snapchat Friends - Android contains the friends of the user.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username of the friend.
Display Name	The name that is displayed for that friend on the local device.
Added Them Date/Time - UTC (yyyy-mm-dd)	The date and time that the friend added the user on the device.
Added Me Date/Time - UTC (yyyy-mm-dd)	The date and time that the user on the device added the friend.

Additional Information

Snapchat Group Members

Description	Snapchat Group Members contains information about participants of the groups that the local user is a member of.
Recovery method	Parsing and carving

Attribute	Description
Group Chat ID	The ID of the group.
Group Name	The name of the group.
Group Member	The user name of the group participant.
User ID	The ID of the group participant.
Added Date/Time - UTC	The date and time that the participant joined the group.
Deleted	Whether the participant left the group (Yes or No)

Additional Information

Snapchat Memories

Description	Snapchat Memories contains pictures and videos that the Snapchat user saves as a memory.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The ID of the memory.
User ID	The ID of the user.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the snap was originally taken.
Timezone	The time zone of the device when the original snap was taken, or when the media was moved from the device's gallery to the My Eyes Only section of the application.
Type	Indicates whether the memory is saved as a regular snap or My Eyes Only, the latter being password protected.
Media Type	The media type, either a picture or video.
Duration (Seconds)	The duration of time before the snap expires.
Attachment URL	The url of the memory.
Attachment	The attachment for the memory, if it's not a picture.
Latitude	The latitude of the location where the snap was originally taken.
Longitude	The longitude of the location where the snap was originally taken.
Size (Bytes)	The encrypted size of the snap media. Any overlay that was added to the snap is not included when determining the size of the snap media.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.

Attribute	Description
Attachment Path	The file path of the media attachment on the device.
Skin Tone Percentage	The percentage of the picture that appears to be skin tone. Any overlay that was added to the snap is not included when calculating the skin tone.
MD5 Hash	The MD5 hash of the decrypted media. Any overlay that was added to the snap is not included when creating the hash signature.
SHA1 Hash	The SHA1 hash of the decrypted media. Any overlay that was added to the snap is not included when creating the hash signature.
PhotoDNA Hash	The PhotoDNA hash of the image.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

Snapchat Photo Transfers - Android

Description	Snapchat Photo Transfers - Android contains attributes of the photos sent between users.
Recovery method	Parsing and carving

Attribute	Description
Sender	The person that sent the photo.
Receiver	The person that received the photo.

Attribute	Description
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the photo was sent/received.
Was Viewed	Indicates whether or not the receiver has viewed the sent photo.
Type	The type specifies if the photo was sent or received.
Send Succeeded	Whether the message was successfully sent to the recipient.
Screenshot Taken	Indicates if a screenshot was taken or not.
Photo Id	The identifier of the photo.

Additional Information

Snapchat Received Images - Android

Description	Snapchat Received Images - Android contains the photos that the user on device has received.
Recovery method	Parsing and carving

Attribute	Description
Image	The actual picture content.
Snapchat Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time of the picture according to Snapchat.

Attribute	Description
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the picture was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time whent he picture was created.
Size (Bytes)	The size of the picture
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Skin Tone Percentage	The percentage of the image that is skin tone.
MD5 Hash	The MD5 hash of the image.
SHA1 Hash	The SHA1 hash of the image.
PhotoDNA Hash	The PhotoDNA hash of the image.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

Snapchat Received Snaps - Android

Description	Snapchat Received Snaps - Android contains Snaps containing pictures and videos that have been sent to the local user.
Recovery method	Parsing

Attribute	Description
Sender	The user who sent the snap.
Picture	A picture or thumbnail of the video that was received as the snap.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the snap was sent.
Media Type	Whether the snap was a picture or video snap.
Skin Tone Percentage	The percentage of the video snap that contains what appears to be visible skin.
Status	The status of the snap.
Display Time (seconds)	Indicates how long the snap can be viewed for, in seconds.
Broadcast URL	The URL of a broadcasted snap.
Broadcast Text	The text of a broadcasted snap.

Additional Information

Snapchat Sent Snaps - Android

Description	Snapchat Sent Snaps - Android contains the snaps that have been sent by the user.
Recovery method	Parsing and carving

Attribute	Description
Recipient	The recipient of the snap.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the snap was sent.
Status	The status of the snap.

Additional Information

Snapchat Stories - Android

Description	Snapchat Stories - Android contains information about Snapchat Stories that are recovered, along with any decrypted media content.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username of the owner of the story.
Display Name	The display name of the owner of the story.
Caption	The caption text associated with the story.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the story was first posted.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time when the local user viewed the story.
Expiration Date/Time - UTC	The date and time when the story expires.

Attribute	Description
(yyyy-mm-dd)	
Screenshot Taken	Indicates the number of screenshots that the local user takes of the story.
Display Time (seconds)	The duration of the snap story.
Attachment Path	The path to an encrypted attachment.
Media URL	A URL to the location of the attachment. The URL will expire after some time.
Picture	The decrypted picture attachment.
Attachment	The decrypted attachment (if it's not a picture).

Additional Information

TamTam Messenger Channels - Android

Description	TamTam Messenger Channels contains messages that belong to channel conversations recovered from the local device (the channel type must be User Channel or Default Channel).
Recovery method	Parsing

Attribute	Description
Sender	The name of the channel in which the message originated.

Attribute	Description
Sender ID	The TamTam ID of the channel in which the message originated.
Recipient	The display name of the owner contact that received the message.
Recipient ID	The TamTam ID of the owner contact that received the message
Message	The content of the message. If the messages is a contact share, this attribute displays the text from the VCard.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the message.
Status	The delivery status of the message: Sent or Received.
Channel Type	The classification of the Channel. Channels created by TamTam users are displayed as 'User Channel' whereas 'Default Channel' describes channels that are created and managed by Tamtam. TamTam user are automatically signed up to some of these channels upon application download.
Message Type	The type of message content (Text, Picture, Audio, Video, File, Call, Geo Location or Contact Share). If the message is not in one of these formats, this attribute is empty.
Latitude	The latitude coordinate, if the message type is Geo location.
Longitude	The longitude coordinate, if the message type is Geo location.
Attachment URL	A URL for any attachments that are sent or received. Attachments can be downloaded from this URL. However, to recover pictures properly, you must append '&fn=w_1440' manually to the end of the URL.
Attachment	The locally stored attachment, if the attachment was sent by the local user.

Additional Information

In TamTam Messenger 3.0.0, video attachments aren't always available. To learn more, see Reviewing video files from TamTam Messenger v3.0.0.

TamTam Messenger Contacts

Description	TamTam Messenger Contacts displays information about the TamTam contacts associated with the local user's account (including the local user).
Recovery method	Parsing

Attribute	Description
Contact ID	A unique ID for the contact.
Profile Name	The profile name of the contact.
Website URL	The contact's TamTam website URL, if one exists.
About Info	Information that the user has provided about their self.
Avatar URL	A URL to the user's profile picture. A termination '&fn=w_1440' should be manually added to the URL to properly display the picture.
Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the contact was updated on the local device. If the contact was not added by the local user, this does not display a value. Some contacts might be stored on the local user's device and may have not been added to their contact list. For example, this might occur when the local user belongs to a group but does not have all of the group participants as contacts. In these cases, TamTam adds the group contacts to the application database but they won't automatically be updated.

Additional Information

TamTam Messenger Conversations - Android

Description	TamTam Messenger Conversations contains information about all the chats recovered from the local device (includes individual, group, and channel messages).
Recovery method	Parsing

Attribute	Description
Chat Type	The type of conversation (Individual, Group, User Channel and Default Channel). Individual indicates one-to-one conversations, while Group indicates many-to-many conversations. User Channel indicates a one-to-many conversation created by a TamTam user. Default Channels are one-to-many conversations created and managed by TamTam.
Chat ID	A unique ID for the conversation.
Participants	A list of the participants that belong to the conversation. User Channels only display the local user as a participant whereas Default Channels do not display any participants.
Chat Name	The name of the conversation (only available in Groups and Channels).
Description	The description of the conversation (only available in Groups and Channels)
Address URL	The URL for the channel's webpage. Users can sign up to the channel using this page if the channel is public.

Additional Information

TamTam Messenger Groups - Android

Description	TamTam Messenger Groups contains all messages that belong to group conversations recovered from the local device.
Recovery method	Parsing

Attribute	Description
Sender	The display name of the contact who sent the message.
Sender ID	The TamTam ID of the contact who sent the message. If the contact ID is not recovered, this attribute displays the chat ID of the conversation that the message belongs to.
Recipient	The name of the owner user who received the message.
Recipient ID	The TamTam ID of the owner user who received the message.
Message	The content of the message. If the messages is a contact share, this attribute displays the text from the VCard.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the message.
Status	The delivery status of the message: Sent or Received.
Message Type	The type of message content (Text, Picture, Audio, Video, File, Call, Geo

Attribute	Description
	Location or Contact Share). If the message is not in one of these formats, this attribute is empty.
Latitude	The latitude coordinate, if the message type is Geo location.
Longitude	The longitude coordinate, if the message type is Geo location.
Attachment URL	A URL for any attachments that are sent or received. Attachments can be downloaded from this URL. However, to recover pictures properly, you must append '&fn=w_1440' manually to the end of the URL.
Attachment	The locally stored attachment, if the attachment was sent by the local user.

Additional Information
In TamTam Messenger 3.0.0, video attachments aren't always available. To learn more, see Reviewing video files from TamTam Messenger v3.0.0.

TamTam Messenger Messages - Android

Description	TamTam Messenger Messages contains all individual messages (one-to-one) recovered from the local device.
Recovery method	Parsing

Attribute	Description
Sender	The display name of the contact who sent the message.

Attribute	Description
Sender ID	The TamTam ID of the contact who sent the message. If the contact ID is not recovered this attribute displays the chat ID of the conversation that the message belongs to.
Recipient	The display name of the contact, group or channel that received the message.
Recipient ID	The TamTam ID of the contact, group or channel that received tha message.
Message	The content of the message. If the messages is a contact share, this attribute displays the text from the VCard.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the message.
Status	The delivery status of the message: Sent or Received.
Message Type	The type of message content (Text, Picture, Audio, Video, File, Call, Geo Location or Contact Share). If the message is not in one of these formats, this attribute is empty.
Latitude	The latitude coordinate, if the message type is Geo location.
Longitude	The longitude coordinate, if the message type is Geo location.
Attachment URL	A URL for any attachments that are sent or received. Attachments can be downloaded from this URL. However, to recover pictures properly, you must append '&fn=w_1440' manually to the end of the URL.
Attachment	The locally stored attachment, if the attachment was sent by the local user.

Additional Information

In TamTam Messenger 3.0.0, video attachments aren't always available. To learn more, see Reviewing video files from TamTam Messenger v3.0.0.

Telegram Chats - Android

Description	Information about the conversations that the suspect participates in using the Telegram application.
Recovery method	Parsing

Attribute	Description
Chat ID	The ID of the chat.
Chat Type	The type of the chat.
Chat Name	The name of the chat.
Unread Count	The number of unread messages.
Last Message ID	The ID of the last message in the chat.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message in the chat.
User ID	The ID of the other user in the chat.
RSA Key	The RSA key of the chat, if it is encrypted.
RSA Key Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the RSA key was created.

Additional Information

This table doesn't contain any of the actual text from the conversations that occur. However, the table does contain some useful metadata about group chats such as the RSA ID.

Telegram Contacts - Android

Description	Information about a subject's contacts that are displayed in Telegram. The application pulls the list of potential contacts from Android Contacts, meaning that these users may or may not be Telegram users.
Recovery method	Parsing

Attribute	Description
User ID	The ID of the user.
First Name	The user's first name.
Last Name	The user's last name.
Phone Number	The phone number associated with the user's account.
Second Phone Number	The second phone number associated with the user's account. If there is no second phone associated with the account, this value is the same as the above Phone column.
Deleted	Whether the suspect marked the user's information for deletion.

Additional Information

Telegram Messages - Android

Description	Individual chat messages that are sent and received using the Telegram application.
Recovery method	Parsing

Attribute	Description
Partner	The name of the conversation partner. In case the name is not available or the user was deleted, it displays the Telegram ID of the partner (or conversation ID).
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the message was created on the local device.
Message Body	The body of the message.
Chat Type	The type of chat that the message belongs to.
Direction	The direction of the message.
Action	The action that occurred.
Type	The type of the message that was sent or received. This value can be one of the following: Text, Completed Call, Geo Location, Service, Video call, Photo, Video, Application, Document, Sticker.
Call Duration (Seconds)	The duration of the call.

Attribute	Description
Latitude	The latitude of a location message.
Longitude	The longitude of a location message.
Local Media Path	The path to the content of the media file on the local phone.
Original File Name	The original file name of the media file. This name is unlikely to match the Local Media Path file as Telegram renames the media file with a unique name.
Attachment	The attachment sent with the message.

Additional Information

Telegram Users - Android

Description	Information about the users that a subject has interacted with using Telegram.
Recovery method	Parsing

Attribute	Description
User ID	The ID of the user.
First Name	The user's first name.
Last Name	The user's last name.

Attribute	Description
User Name	The user's user name.
Phone Number	The phone number associated with the user's account.
Last Seen Date/Time	The date and time of the user's last seen.
Profile Image	The profile image of the user.
Contact Added	Indicates whether the subject has added the user as a contact.
Deleted	Indicates whether the contact was deleted by the subject.
Verified	Indicates whether the user has verified their account.
Bot Account	Indicates whether the user is a bot account.
Mutual Contact	Indicates whether the subject has a mutual contact with the user.
Self Contact	Indicates whether the contact is the subject's own user account.

Additional Information

Textfree Attachments

Description	Textfree Attachments contains Attachments from the Android Textfree application.
Recovery method	Parsing and carving

Attribute	Description
Message ID	The ID of the message.
Media URL	The URL from where the media could originaly be downloaded.
Type	The type of media (including picture, voicemail and video).
Preview	The binary data of the attachment. If the attachment is a video, the preview is a frame from the video.
Metadata	Any metadata associated with the attachment. An example of this is VoiceMailDuration.
Media ID	The internal ID used by the application. This value may point to other places where the attachment is used and/or contained.

Additional Information
The Metadata column is always empty for the Android version of the application.

Textfree Contacts

Description	Textfree Contacts contains contacts from the Android Textfree application.
Recovery method	Parsing and carving

Attribute	Description
First Name	The first name of the contact.
Last Name	The last name of the contact.

Attribute	Description
Company Name	The company name of the contact.
Phone Numbers	All phone numbers associated with the contact.
Email(s)	All emails associated with the contact.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the contact was modified.
Contact ID	The internal ID used by the application. This value may point to other places where the attachment is used and/or contained.

Additional Information
Company Name, Email(s), Last Modified Date/Time will always be empty for the Android version of the application.

Textfree Groups

Description	Textfree Groups contains information about group chats from the Android Textfree application.
Recovery method	Parsing

Attribute	Description
Group	The group number.
Group Phone Number	The phone number of the group.

Attribute	Description
Group Member Name(s)	The names of all of the group participants.
Group Member Phone Number(s)	The phone numbers of all of the group participants.

Additional Information
The Group Name column will always be empty for the Android version of the application.

Textfree Messages / Calls

Description	Messages from the Android Textfree application.
Recovery method	Parsing and carving

Attribute	Description
Sender	The name of the sender.
Sender ID	The ID of the sender.
Recipient(s)	The name(s) of the recipient(s).
Recipient ID(s)	The ID(s) of the recipient(s). This value may contain the contact's phone number.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that is associated with the message.
Message	The content of the message.
Type	The type of the message (e.g., Message, Call).
Chat Type	The type of the chat (e.g., Individual, Group).

Attribute	Description
Direction	The direction of the message (e.g., Outgoing, Incoming).
Call Duration (Seconds)	The call duration in seconds, if the message is a call.
Message Status	The read status of the message (e.g., Read, Unread).
Attachment Type	The type of media file attached (e.g., jpeg, png, wav).
Attachment	The media attached to the message.
Media URL	The URL where the media might have originally been downloaded from.

Additional Information

TextMe Calls

Description	TextMe Calls contains information about the calls that the suspect participates in using the TextMe application.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the call.
Sender Phone Number	The phone number of the sender.
Recipient	The recipient of the call.

Attribute	Description
Recipient Phone Number	The phone number of the recipient.
Display Name	The chosen display name for the call participant.
Call Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the call was initiated.
Call End Date/Time - UTC (yyyy-mm-dd)	The date and time when the call ended.
Direction	The direction of the call, either incoming or outgoing.
Status	Whether the call was unanswered, answered, or if the caller left a voicemail.
Call Type	Indicating if the call was an audio call or video call. In later versions of TextMe, this indicates whether the call was 'in', 'out' or 'missed'.
Voicemail	The associated voicemail message.

Additional Information

In some versions of TextMe, call logging does not behave as expected. If a suspect sends or receives a call, a database entry is created as normal. If another call occurs with the same user, without there being any messages in between, the timestamps from the first call are overwritten in the database with the timestamps from the second call. This behavior makes it seem as if the first call never occurred. The timestamps are repeatedly overwritten for each call until a message is sent, at which point a new database entry can be created for the next new call.
For Android TextMe Calls, it is not possible to determine the display name of the recipient, so the 'Display Name' column will always be empty.

TextMe Messages

Description	TextMe Messages contains individual chat messages that are sent and received using the TextMe application.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the message.
Sender Phone Number	The phone number of the sender.
Recipient(s)	The user name(s) of the recipient(s).
Recipient Phone Number	The phone number(s) of the recipient(s).
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent, regardless of whether the message was sent or received.
Message	The body of the message.
Direction	Whether the message was sent or received.
Status	Whether the message was unsent, sent, delivered, or read.
Attachment Name	The name of the attachment, if one exists (can be pictures, videos, or URL links).
Attachment Path	The file path of the attachment, if one exists.
Attachment Type	The file type of the attachment, if one exists.
Attachment	The attachment data.
Group Name	The display name of the group.

Additional Information

TextPlus Activity

Description	TextPlus Activity contains information about messages and calls from TextPlus on an Android device.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the activity.
Recipient	The recipient of the activity.
Date/Time	The date and time when the activity happened.
Activity Type	The type of the activity, which is either Message or Call.
Message Body	If the activity type is Message, the text of the message is displayed.
Call Duration (Seconds)	If the activity type is Call, the duration of the call in seconds is displayed.
Attachment URL	The URL associated with the attachment sent in the activity, if one exists. For some activities, access this URL in the browser to visualize the attachment content.

Additional Information

TextPlus Calls

Description	TextPlus Calls contains call information from TextPlus data on an Android device.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username of the TextPlus account.
User	The identifier for the recipient of the call. This could be a GUID or phone number depending on the TextPlus version.
Display Name	The display name of the TextPlus account.
Conversation Name	The name of the conversation.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the call was made.
Call Duration (Seconds)	The duration of the call.
Call Type	The type of the call. This value can be missed, outgoing, or incoming.
Answered	Indicates whether the call was answered or not.
Attachment URL	The URL associated with the voicemail attached to the call.

Additional Information

TextPlus Logged In Account

Description	TextPlus Logged In Account contains information about the user currently logged into TextPlus on an Android device.
Recovery method	Parsing and carving

Attribute	Description
User Name	The name of the logged in user.
Display Name	The display name of the logged in user.
Phone Number	The phone number of the logged in user.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the logged in account was created.
Gender	The gender of the logged in user.
Last Known Location Latitude	The latitude of the last known location the app was used.
Last Known Location Longitude	The longitude of the last known location the app was used.
Last Known Location Date/Time - UTC (yyyy-mm-dd)	The date and time of the last known usage of the app.

Additional Information

TextPlus Messages

Description	TextPlus Messages contains message information from TextPlus data on an Android device.
Recovery method	Parsing and carving

Attribute	Description
Sender Name	The sender of the message.
Sender	The identifier for the sender of the message. This could be a GUID or phone number depending on the TextPlus version.
Recipient Name	The recipient of the message.
Recipient	The identifier for the recipient of the message. This could be a GUID or phone number depending on the TextPlus version.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent or received.
Message Body	The text contents of the message.
Message Type	Indicates if the message is incoming, outgoing, or an unknown message type.
Status	Indicates if the message was read ('Read'), unread ('Unread') or has an unknown status.

Additional Information

TextPlus Users

Description	TextPlus Users contains information about users that have interacted with the local user on an Android device.
Recovery method	Parsing

Attribute	Description
User ID	The unique user ID of a user that was interacted with by the local user.
Conversation ID	The unique identifier of the conversation that the user is a part of. This may list multiple identifiers of conversations the user is a part of.
Conversation Name	The unique name of the conversation that the user is a part of. This may list multiple names of conversations the user is a part of.
Conversation Type	The local user may have interacted with another user in one or more ways: One to One, Call, Group Chat. This may help identify which conversation to focus on and may provide importance of the interaction.
Local User ID	The user ID of the local user.
Local Username	The username of the local user.

Additional Information

Touch Experiences

Description	Touch Experiences contains experiences in the Android Touch application. Similar to photo albums on Facebook except more private, users can post

	media to an experience and share it with friends, who can comment on the posted media and share media of their own.
Recovery method	Parsing

Attribute	Description
Experience Name	The name of the experience.
Experience Members	All of the members in the experience.
Experience Owner	The user who created the experience.
Author	The author of the post.
Experience Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the experience was created.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the post was sent/received.
Comment	A comment on the content of the experience. This comment can be seen by other users viewing the experience.
Media URL	The URL of a media item posted to the experience.
Downloaded Image	The raw content of the media in the post, downloaded from the URL specified in 'Media URL'.
Status	The status of the post. Describes whether it was sent or received, and whether or not it was viewed/downloaded by the local user.

Additional Information

Touch Friends

Description	Touch Friends contains contact information for friends of the local user in the Android Touch application.
Recovery method	Parsing

Attribute	Description
Touch ID	The friend's unique Touch ID.
First Name	The friend's first name.
Last Name	The friend's last name.
Avatar URL	The URL of the friend's avatar.
Downloaded Image	The raw content of the friend's avatar, downloaded from the URL specified in 'Avatar URL'.

Additional Information

Touch Local User

Description	Touch Local User contains contact information for the local user in the Android Touch application.
Recovery method	Parsing

Attribute	Description
Touch ID	The local user's unique Touch ID.
First Name	The local user's first name.
Last Name	The local user's last name.
Email	The local user's email.
Phone Number	The local user's phone number.
Avatar URL	The URL of the local user's avatar.
Downloaded Image	The raw content of the local user's avatar, downloaded from the URL specified in 'Avatar URL'.
Country Code	The country code of the local user.

Additional Information

Touch Messages

Description	Touch Messages contain messages that were sent and received in the Android Touch application.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message.
Recipients	The recipient(s) of the message. In a group conversation, recipients will be

Attribute	Description
	in a comma-delimited list.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The content of the message.
Message Type	A phrase describing the content of the message. The possible values are 'Text', 'Image', 'Audio', 'Video', and 'Profile Picture Changed'.
Message Status	The status of the message. This value describes whether the message was sent or received by the local user, and describes the interactions that the user has had with it: whether or not it was viewed, or, in the case of media, whether or not it was downloaded.
Media URL	The URL of the media in the message, if it contains video, audio or an image.
Downloaded Image	The raw content of the media in the message, downloaded from the URL specified in 'Media URL'.
Local Media Path	The path to the content of the media in the message on the local phone.

Additional Information

Verizon Messages Messages

Description	Verizon Messages contains information about the messages sent or

	received by the local user.
Recovery method	Parsing

Attribute	Description
Sender	The phone number of the device that sent the message.
Recipient(s)	The phone numbers of the devices that received the message.
Message Direction	Indicates whether the message was incoming or outgoing. If the direction is not recognized, the value will be an integer.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The text for the message.
Attachment Name	The attachment file name.

Additional Information

Viber Messages

Description	Viber Messages contains details about sent/received Android Viber messages.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the message.
Sender Name	The name of the person who sent the message.
Recipient(s)	The recipient(s) of the message. In a group chat, the recipients will be shown as a comma-delimited list.
Recipient Screen Name (s)	The screen name(s) of the person(s) who received the message.
Participant	The contact name of one of the participants of the record. It is up to the investigator to determine if this is the local user, or that of the chat partner.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message that was sent. If the message type was a call this will identify if the call was outgoing, incoming or a missed call. For locations the message is a google maps link to the sent location. For images the message can be empty or a blurb of text.
Chat Type	The type of conversation where the message originates from (Group chat or One-to-one).
Type	The type of message that was sent. Possible values include Text, Sticker, Call, Video, Location, Notification, and Image.
Message Status	The status of the message. This can be one of the following: 'Sent / Failed', 'Sent / Not Delivered', 'Sent / Delivered', or 'Received'.
Attachment	The attachment file name, as stored in the application.

Attribute	Description
Name	
File Attachment	The attachment file name, as named by the user.
File Size (Bytes)	The size of the file.
State	The state of the attachment. This can be one of the following: Complete / Pending, Downloading, or Incomplete Upload / Incomplete Download.
Secret Chat	Indicates whether a message is sent in a secret chat (Yes if true).
Expiration (dd hh:mm:ss)	If the message is a secret chat message, this value represents the time limit that the message can be visible for before it disappears. The value is converted from seconds and reported as a timestamp in dd:hh:mm:ss format.
Repeat Count	If the message was a call, the number of times that the call was repeated.
File Path	If the message included an attachment, the path to the attachment on the local phone, in the form of a URL.
Location Address	The address for the location that was sent.
Latitude	The map latitude location information.
Longitude	The map longitude location information.
Nearby Locations	The locations that are geographically close to the user when they use the Share Location feature within the application (these locations are cached even if a location is not actually shared).
Attachment	The attachment, as stored in the application.

Additional Information

WeChat Friends

Description	WeChat Friends contains stored contact information for the WeChat application on Android.
Recovery method	Parsing and carving

Attribute	Description
Username	The unique username of the friend.
Nickname	The nickname of the friend.
Gender	The friend's gender.
Phone Number	The friend's phone number.
Email	The friend's email address.
Full Name	The friend's full name.
Participants	A list of the participants that belong to the chat room.
Original Location	The geolocation that is configured from a list of countries and cities when the user creates their account. This is not a real-time location.
Profile Picture URL	The profile picture URL of the friend.

Additional Information

WeChat Messages

Description	WeChat Messages contains stored messages for the WeChat application on Android.
Recovery method	Parsing and carving

Attribute	Description
Sender User Name	The user name or ID of the sender, as assigned by the application.
Sender Nick-name	The display name of the sender, as defined by the user.
Recipient User Name	The user name of the person receiving the message.
Recipient Nick-name	The nickname of the person receiving the message.
Group Chat Name	The name of the group chat, if the message is sent in a group chat.
Group Chat ID	The unique ID of the group chat, if the message is sent in a group chat.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was created on the device.
Message	The content of the message. For Location, Notice, and Pay messages, this content will be extracted from XML data. Contact Card messages will dis-

Attribute	Description
	play the XML data for the contact.
XML Data	The raw XML data for Picture, Location, Notice, and Pay messages.
Call Duration (Seconds)	The duration of voice and/or video call in seconds.
Type	The type of the message (Text, Picture, Audio, Friend Request, Contact Card, Video, Animated Emoticon, Location Data, Shared Information, Voice/Video Call, Sight Video, Group Voice/Video Call, Notice, Pay Message, or Location Sharing).
Account	The user name of the account that was used to send the message.
Latitude	The latitude of the location data sent within the message.
Longitude	The longitude of the location data sent within the message.
Attachment	The attachment (such as audio, video) associated with the message.
Attachment Data Recovered	Indicates whether attachment data was recovered (Yes or Null).
Attachment Path	The absolute path to recovered message attachments.
Content Format	The content format of successfully recovered audio file attachments. AXIOM Process will attempt to decode audio from SILK V3 to WAV. Successfully converted attachments are saved and playable in AXIOM Examine. Unconverted attachments are saved in their original format and can be manually decoded using another tool or method.

Additional Information

WhatsApp

WhatsApp is a cross-platform mobile messaging app that is owned by Facebook and has over a billion registered users as of 2016. Magnet tools support the recovery of messages, contacts, and attachments from WhatsApp conversations on both Android and iOS devices.

Information from these artifacts can help investigators identify who a user communicates with, what they talk about, and the possible whereabouts of a user and their contacts.

WhatsApp for Android

There are two SQLite databases that contain a user's WhatsApp for Android data: msgstore.db and wa.db. The msgstore.db contains details on any chat conversations between a user and their contacts, and wa.db stores information on the WhatsApp user's contacts. The msgstore.db contains two tables: messages and chat_list. The messages table contains the following information and more: the contact's phone number, message contents, message statuses, timestamps, and details about attachments included in the message. The chat_list table contains a list of the phone numbers that the user communicated with, which may or may not represent actual contacts in the application. A list of the user's contacts can be found in the wa.db table.

You can access these databases if you have physical access to the device (that is, the device is unlocked or rooted). If you don't have physical access to the device, you can also get WhatsApp data from an SD card backup. However, with SD card backups, the msgstore.db is encrypted and you require the database decryption key to gain access. Another option is to acquire and decrypt a user's WhatsApp backups from the cloud (Google Drive). To perform a cloud acquisition, you need the following information: the user's Google username and password, multi-factor authentication details (if MFA is enabled), the phone number associated with the account, and the backup decryption key. You can provide this data to AXIOM Examine to acquire and decrypt the backup.

Artifacts

WhatsApp Accounts Information

WhatsApp Chats

WhatsApp Contacts

WhatsApp Groups

WhatsApp Live Locations

WhatsApp Messages

WhatsApp Profile Pictures

WhatsApp User Profiles

Resources

Acquire and decrypt a WhatsApp backup using a recovered decryption key

Digital Forensics: Artifact Profile – WhatsApp Messenger

WhatsApp Accounts Information - Android

Description	WhatsApp Accounts Information - Android contains the login information for the user's account, including the private key used for authentication.
Recovery method	Parsing

Attribute	Description
WhatsApp Name	The WhatsApp username that is associated with the account.
Phone Number	The phone number used to register the account.
Private Key	The decryption key of the account.

Additional Information

WhatsApp Chats - Android

Description	WhatsApp Chats - Android contains information about chat sessions that occur between the local user and another user or group. This artifact indicates the IDs of each participant as well as information about unread messages and the time when the last message was sent.
Recovery method	Parsing

Attribute	Description
Individual Chat Name	If the chat is with an individual, this value indicates the name of the participant.
Group Chat Name	If the chat is a group chat, this value indicates the name of the group.
Chat ID	The ID of the individual or group involved in the chat.
Phone Number	The phone number associated with an individual contact.
Last Message	The text body of the last message sent in the chat.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the last message in the chat was sent.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the conversation was created.
Unread Message Count	The number of unread messages in the chat.
Missed Call Count	The number of missed calls in the chat.

Additional Information

WhatsApp Contacts - Android

Description	WhatsApp Contacts - Android contains contacts that were added to WhatsApp by the local user.
Recovery method	Parsing

Attribute	Description
Image	The actual picture content.
ID	The unique identifier for the contact.
Phone Number	The contact's phone number.
Display Name	The contact's full name.
Given Name	The contact's given (i.e. first) name.
Family Name	The contact's family (i.e. last) name.
WhatsApp Name	The contact's name that is displayed to other users.
Status	The contact's status message.
Status Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the status message was updated.
Is WhatsApp User	Identifies whether the user is using WhatsApp or not.
Frequently Contacted	Indicates whether this contact is contacted frequently by the user.

Additional Information

To learn more about artifacts from WhatsApp Messenger, sign in to the Support Portal to read the article Artifact profile: WhatsApp Messenger.

WhatsApp Groups - Android

Description	WhatsApp Groups - Android contains information about the WhatsApp Group chats that the user participates in.
Recovery method	Parsing and carving

Attribute	Description
Picture	The profile picture associated with this group.
Group Chat ID	The unique identifier for group chats. The Group Chat ID format is creator phone number-creation epoch time@g.us.
Group Name	The name of the group that is seen by users in the chat list and the conversation view.
Description	The description of the group.
Admin IDs	The IDs of the administrators of the group chat.
Admin Names	The names of the administrators of the group chat.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the group was created.
Group Member(s)	The list of contact IDs for the members of the group.

Additional Information

WhatsApp Live Locations - Android

Description	WhatsApp Live Locations- Android captures Live Locations that are shared with the local device user. The coordinates in each result represent the sender's last shared location. Once a Live Location expires, it is no longer recoverable.
Recovery method	Parsing

Attribute	Description
ID	The user ID of the contact that is sharing their live location.
Phone Number	The phone number of the contact.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the live location coordinate was captured.
Latitude	The latitude associated with the live location.
Longitude	The longitude associated with the live location.
Speed (m/s)	The speed of the contact at the time the live location was captured.
Direction	The direction of travel for the contact at the time the live location was captured.

Additional Information

WhatsApp Messages - Android

Description	WhatsApp Messages - Android contains messages that were sent and received using WhatsApp.
Recovery method	Parsing and carving

Attribute	Description
Sender	The phone number of the message sender.
Sender Nick-name	The name of the message sender, retrieved from display_name.
Recipient	The phone number of the message recipient.
Recipient Nick-name	The name of the message recipient, retrieved from display_name.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message Received Date/Time - UTC (yyyy-mm-dd)	The date and time the message was received locally.
Recipient Received Date/Time -	The date and time the message was received by the remote recipient.

Attribute	Description
UTC (yyyy-mm-dd)	
Server Received Date/Time - UTC (yyyy-mm-dd)	The date and time the message was received by the server.
Message	The message text.
Type	The format of the message or the MIME type of the media attachment.
Chat Type	Defines the audience for the message/call. 'Individual' indicates one-on-one messages/calls, 'Group' indicates that the message/call involves more than one user, and 'Broadcast' indicates a message with multiple recipients.
Media Duration (Seconds)	The duration of the attached media.
Call Duration (Seconds)	The duration of the audio/video call.
Message Status	The sent/received status.
Latitude	The latitude of the location from which the message was sent.
Longitude	The longitude of the location from which the message was sent.
Attachment	The media attached to the message.
Media URL	The source URL of the attached media.

Attribute	Description
Starred	Indicates whether the user bookmarked (or 'starred') a message.
Forwarded	Indicates whether the user forwarded a message to another conversation

Additional Information
Some WhatsApp Message Status and Date / Time values might appear differently in carved versus parsed items. This behavior is expected, and occurs due to the database containing multiple tables with the same schema and messages. This data cannot be deduplicated. To learn more about artifacts from WhatsApp Messenger, sign in to the Support Portal to read the article Artifact profile: WhatsApp Messenger.

WhatsApp Profile Pictures - Android

Description	WhatsApp Profile Pictures - Android contains profile pictures that WhatsApp uses that are stored locally.
Recovery method	Parsing

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created	The created date/time of the picture in the file system.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed. "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).

Attribute	Description
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera that was used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Longitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).

Attribute	Description
Exif Data	A searchable field for all raw exif properties.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

WhatsApp User Profiles - Android

Description	WhatsApp User Profiles - Android contains profile information about the local WhatsApp user.
Recovery method	Parsing

Attribute	Description
Image	The user's profile image.
WhatsApp Name	The WhatsApp username that is associated with the account.

Attribute	Description
Phone Number	The phone number used to register the account.
Status	The current status that the user shares
Version	The version of the WhatsApp application.
Latitude	The latitude associated with the last location the user shared.
Longitude	The longitude associated with the last location the user shared.
Private Key	The decryption key of the account.

Additional Information

Wickr Me

Wickr Me is a private messaging application for iOS and Android, which provides end-to-end encryption of user communications, including texts, audio and video calls, transmitted locations and more. To ensure the security of your messages, Wickr Me encrypts every sent message with a unique key and gives you the option to control how long these messages will remain available to a recipient once read.

The content of a suspect’s sent and received messages can be valuable to an investigation, as well as their username and the usernames of their recipients. Other information can also be recovered, such as the date and time of when messages were sent, delivered and read, and a suspect's shared locations. This information can offer insight into the purpose of a suspect’s interactions, identify users who have been in contact with a suspect, and can be used to piece together a timeline of a suspect’s activity.

Decrypting messages

On Android, Wickr Me application data is stored in the SQLite database (wickr_db), which is fully encrypted using SQLCipher. Magnet AXIOM Process will search .wic files and Android system files for the components needed to recover the database decryption key.

Artifacts

Wickr Me Messages

Wickr Me Conversations

Description	Wickr Me Conversations contains details about all the Individual, Group, and Room conversations the local user is a part of.
Recovery method	Parsing

Attribute	Description
Conversation ID	The unique identifier for the conversation.
Participants	The names of all participants in the conversation.
Type	The type of conversation. Individual is used for 1-on-1 or group conversations, and Room is used for room conversations.
Name	The name of the Room. Only populated if the conversation is in a room.
Description	The description of the Room. Only populated if the conversation is in a room.
Last Message	The date and time when the last message in this conversation

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	was sent.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the conversation was last synced on the device.

Additional Information
To learn more about Wickr Me, see Artifact profile: Wickr Me.

Wickr Me Messages

Description	Wickr Me Messages contains decrypted and decoded messages sent or received by a Wickr Me user on Android. These messages can include text messages, call logs, transmitted locations, attachments such as pictures and videos, voice messages, and more.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender's Wickr username.
Recipient(s)	The recipient's Wickr username.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when this message was sent.

Attribute	Description
Message	The message content.
Message Type	The message type. This value is interpreted from the ZPRIMARYTYPE. This value can be: Text, Call, Attachment, Location, Key Verification, System Message, or Control (Group Conversation Events).
Chat Type	The type of the chat. This value can be Individual, or Room.
Room Name	The name of the chat room.
Direction	Indicates whether the message was incoming or outgoing.
Read	Indicates whether or not the message was read.
Call Duration (Seconds)	The duration of the call in seconds.
Call Status	The status of the call, if applicable. This value can be: Started, Completed, Missed, or Cancelled.
Attachment Name	The file name of the attachment included in the message, if applicable.
Attachment Path	The original file path of the encrypted attachment, if applicable.
Attachment	The decrypted attachment file, if applicable (can include photos, video, or voice messages).
Latitude	The latitude of the coordinates (for transmitted locations only).
Longitude	The longitude of the coordinates (for transmitted locations only).

Additional Information

To learn more about Wickr Me, see Artifact profile: Wickr Me.

Wickr Me Users

Description	Wickr Me Users contains details about the users the local user has interacted with in the app.
Recovery method	Parsing

Attribute	Description
User Name	The name of the user.
User ID	The ID of the user.
Starred	Dictates whether the user has been starred or not.
Hidden	Dictates whether the user is hidden or not.
Blocked	Dictates whether the user is blocked or not.
Bot Account	Dictates whether the user is a bot.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The date and time when the user was last active.
Profile Image	The profile image of the user.

Additional Information

To learn more about Wickr Me, see Artifact profile: Wickr Me.

Zalo Contacts

Description	Zalo Contacts contains the user's Zalo contacts.
Recovery method	Parsing

Attribute	Description
User Name	The contact's username.
User ID	The contact's unique user ID.
Profile Picture URL	The contact's profile picture URL.
Gender	The contact's gender.
Phone Number	The contact's phone number.
Birthday (yyyy-mm-dd)	The contact's birthday.
Status	The contact's status message.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact was last active.
Is Friend	If the contact is friends with the user.
Type	The contact's type of account.

Additional Information

Zalo Groups

Description	Zalo Groups contains Zalo groups that the user participates in.
Recovery method	Parsing

Attribute	Description
Name	The name of the group.
ID	The unique ID of the chat group.
Created By	The username of the person who created the chat room.
Group Member(s)	The usernames of all of the members in the group.
Number of Participants	The number of participants in the group.

Additional Information

Zalo Messages

Description	Zalo Messages contains messages or calls sent or received using Zalo.
Recovery method	Parsing

Attribute	Description
Sender User Name	The username of the person sending the message.
Recipient User	The username of the person receiving the message.

Attribute	Description
Name	
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent on the device.
Direction	The direction that the message was sent.
Message	The content of the message.
Picture	Any picture attachments in the message.
Attachment	Any non-picture attachments in the message, including audio and video.
Duration (Seconds)	The duration of calls.
Status	The status of calls. The status of some calls is ambiguous as it's not possible to distinguish whether calls are accepted or ended by the user receiving the call.
Message Type	The type of message. The different message types include text, audio, video and more.
Latitude	The latitude data sent within a message.
Longitude	The longitude data sent within a message.
Media URL	The URL of additional media attachments.
Attachment Path	The absolute path to recovered attachments in a message.

Additional Information

Zalo Profiles

Description	Zalo Profiles contains profile information of the local Zalo user.
Recovery method	Parsing

Attribute	Description
User Name	The user's username.
User ID	The user's unique user ID.
Profile Picture URL	The user's profile picture URL.
Gender	The user's gender.
Birthday (yyyy-mm-dd)	The user's birthday.
Phone Number	The user's phone number.
Status	The user's status message.

Additional Information

Zello Messages

Description	Zello Messages provides information about the various messages the user has sent and received on the app.
Recovery method	Parsing

Attribute	Description
Sender	The display name of the user who sent the message (Local User if it was the local user).
Recipient	The display name of the user who received the message (Local User if it was the local user).
Message	The content of the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Direction	Indicates whether the message was incoming or outgoing.
Message Type	The type of message. This can include Alert, Audio Message, Location, Message, Picture, or the actual value with "not parsed" indicated in brackets.
Read	Indicates whether or not the message has been read.
Attachment	The recovered picture attachment.
Latitude	The latitude portion of the location data that is sent with the message.
Longitude	The longitude portion of the location data that is sent with the message.

Additional Information

Zello Profiles

Description	Zello Profiles provides information about the various profiles and channels the user has interacted with on the app.

Recovery method	Parsing

Attribute	Description
User Name	The user name for the profile, this will be empty for channel profiles.
Name	The display name for the profile, this will be empty for channel profiles.
Created Date/Time - UTC (yyyy-mm-dd)	The data and time when the profile was created.
Channel Name	The name of the channel, this will be empty if the profile is not a channel.
Channel Type	The type of the channel, this will be empty if the profile is not a channel.
Location Name	The name of the profile location.
Website	The website field for the profile.
About	The about field for the profile
Profile Picture URL	A URL corresponding to the profile image for the profile.

Additional Information

Zoom Channels

Description	Zoom Channels contains information about the channels that the local user

	participates in.
Recovery method	Parsing

Attribute	Description
Channel ID	The ID of the channel.
Channel Name	The display name of the channel.
Owner ID	The ID of the Zoom user that created the channel.
Participant IDs	The IDs of the participants of the channel.
Participants User Names	The names of the participants of the channel.
Description	A description of the channel, as provided by the creator of the channel.

Additional Information

Zoom Chat Messages

Description	Zoom Chat Messages contains details about Zoom chat messages sent outside of a meeting.
Recovery method	Parsing and carving

Attribute	Description
Sender Name	The name of the person who sent the message.
Sender ID	The ID of the person who sent the message.
Buddy ID	The ID of the person or group that the message was sent to.
Recipient Name	The name of the person who received the message.
Recipient ID	The ID of the person who received the message.
Group Chat ID	The ID of the group this message was sent in.
Message ID	The GUID of the message.
Message	The body of the message.
Message Date/Time - UTC (yyyy-mm-dd)	A timestamp that indicates when the message was sent or received, depending on whether the local user was the sender or receiver.
Sender	Whether the message was sent by the local user or a remote user.
Read	Specifies whether the message has been read. The displayed value is either 'Yes' or 'No'.
Message Type	The type of message that was sent. The message types are 'Message', 'Picture', 'File', or 'Notification'.
Attachment Name	The name of the attachment that was sent.
Attachment Local File Path	The local path where the attachment was saved. This is empty if the attachment was not saved.
Attachment	The contents of the attachment if it can be recovered.

Additional Information

The Attachment Name column is always empty on Android.

Zoom Contacts

Description	Zoom Contacts contains information about a user's Zoom contacts.
Recovery method	Parsing and carving

Attribute	Description
Buddy ID	The user ID of the contact.
Email	The email address of the contact.
Display Name	The display name of the contact.
Description	A description of the contact, as provided by that user.
Personal Meeting ID	An ID that can be used to start up a meeting with the contact.
Region	The default country or region where the contact is located.

Additional Information

Zoom Meeting Messages

Description	Zoom Meeting Messages contains details about Zoom chat messages sent during a meeting.
Recovery method	Parsing and carving

Attribute	Description
Message ID	The GUID of the message.
Sender Name	The name of the person who sent the message.
Sender ID	The ID of the person who sent the message.
Receiver Name	The name of the person who received the message. If blank, the message was sent to everyone in the meeting.
Receiver ID	The ID of the person who received the message. If zero, the message was sent to everyone in the meeting.
Message	The body of the message.
Message Date/Time - UTC (yyyy-mm-dd)	A timestamp that indicates when the message was sent or received, depending on whether the local user was the sender or receiver.
Read	Specifies whether the message has been read. The displayed value is either 'Yes' or 'No'.
Message Type	The type of message that was sent.
Conference ID	The ID for the meeting the message was sent in.

Additional Information

Zoom User Accounts

Description	Zoom User Accounts contains details about the local user's zoom account.
Recovery method	Parsing and carving

Attribute	Description
User ID	The unique identifier for the user.
User Name	The username of the account.
Email	The email address associated with the account.
First Name	The first name of the user.
Last Name	The last name of the user.
Phone Number	The phone number of the user.
Profile Image URL	The URL to the profile picture of the user.
Downloaded Profile Image	The data for the profile picture.

Additional Information

Connected Devices

Amazon Alexa Audio Activity

Description	Contains details about audio activity detected by the Amazon Alexa application.
Recovery method	Carving

Attribute	Description
Text	The spoken audio as interpreted by the Alexa applic-

Attribute	Description
	ation.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the audio was recorded.
Resource URL	The web resource URL for the audio file.

Additional Information
The data in this artifact is retrieved from the application's cached data and may not represent a complete record of the user's activities. Accessing the web resource URL requires the user's Alexa login credentials.

Amazon Alexa Cached Audio

Description	Contains attached audio files recovered from the Amazon Alexa application.
Recovery method	Parsing

Attribute	Description
Audio	An audio file containing voice commands spoken by the user.

Additional Information
The data in this artifact is retrieved from the application's cached data and may not represent a complete record of the user's activities.

Amazon Alexa Device Information

Description	Contains details about Alexa-enabled devices.
Recovery method	Carving

Attribute	Description
Device Name	The name of the device.
Customer ID	The Amazon customer identifier.
Device Type	The type of device.
Serial Number	The serial number of the device.
MAC Address	The MAC address of the device.
Network Name (SSID)	The network name to which the device is connected.
ZIP/Postal Code	The ZIP or postal code associated with the device.

Additional Information

The data in this artifact is retrieved from the application's cached data and may not represent a complete record of the user's activities.

Amazon Alexa Tasks

Description	Contains details about shopping lists or other tasks tracked by the Amazon Alexa application.
Recovery method	Parsing and carving

Attribute	Description
Text	The spoken task as interpreted by the Alexa application.
Type	The type of task.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the task was last updated.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the task was created.
Customer ID	The customer ID of the task creator.
Completed	Whether the task has been completed.
Deleted	Whether the task has been deleted.
Similar Text	Text that's similar to the text for the task, as determined by the Alexa application.
Resource URL	The web resource URL for the audio file.

Additional Information

The data in this artifact is retrieved from the application's cached data and may not represent a complete record of the user's activities. Accessing the audio resource URL requires the user's Alexa login credentials.

Amazon Alexa User

Description	Contains details about user accounts recognized by the Amazon Alexa application.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username for the account.
Email	The email associated with the account.
Device Name	The name of the device.
Customer ID	The Amazon customer identifier.

Additional Information
The data in this artifact is retrieved from the app's cached data and may not represent a complete record of the user's activities.

Amazon Alexa Web Resource

Description	Contains details about Amazon API resources contacted by the Alexa application.
Recovery method	Carving

Attribute	Description
Resource URL	The URL for the web resource.
Type	The type of data available from the resource.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the resource request was made.

Additional Information

The data in this artifact is retrieved from the application's cached data and may not represent a complete record of the user's activities. Accessing the web resource URL requires the user's Alexa login credentials.

Android Cache.Cell

Description	Android Cache.Cell contains cached cell base station data recovered from an Android device.
Recovery method	Parsing

Attribute	Description
Key	The cell identifier. This identifier is constructed like [MCC]:[MNC]:[LAC]:[cell ID].
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time when the information was gathered.
Range	The distance the phone is away from the cell base station.
Confidence	The confidence of the data.
Latitude	The latitude of the cell base station.
Longitude	The longitude of the cell base station.

Additional Information

Android Cache.Wifi

Description	Android Cache.Wifi contains the cached WiFi access points recovered from an Android device.
Recovery method	Parsing

Attribute	Description
Key	The WiFi access point MAC address.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time when the information was gathered.
Range	The distance the phone is away from the access point.
Confidence	The confidence of the data.
Latitude	The latitude of the access point.
Longitude	The longitude of the access point.

Additional Information

Arlo Secure Cached Media

Description	Arlo Secure Cached Media contains the cached media files that have been found inside the Arlo Secure application.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
MIME Type	The MIME type of the media.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the media file.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
MD5 Hash	An MD5 hash of the picture content.
SHA1 Hash	A SHA1 hash of the picture content.
PhotoDNA Hash	The hash of the picture content for PhotoDNA.

Attribute	Description
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Exif Data	A searchable field for all raw Exif properties.

Additional Information

Arlo Secure Device Information

Description	Arlo Secure Device Information contains information about the Arlo home security device.
Recovery method	Parsing

Attribute	Description
Device ID	The unique number identifying the device.
Device Name	The name that the user assigned to the device.
Device Type	The type of the device.
Serial Number	The serial number of the device.
Device Hardware Version	The hardware version of the device.

Attribute	Description
Device Software Version	The software version of the device.
Interface Version	The interface version of the device.
Connection State	The connection state of the device.
Permissions	The user permissions on the device.
Timezone	The timezone set for the device.
User ID	The unique number identifying the device user.
Cloud ID	The unique cloud number identifying the device in the file system.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the device was set up.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the device was modified by the software, not by the user.
Connection Type	The connection type of the device.
Network Name (SSID)	The network name that the device was connected to.
IP Address	The IP Address of the device.

Additional Information

Arlo Secure User Information

Description	Arlo Secure User Information contains information about user accounts linked to the Arlo home security devices. Please note that latitude and lon-

	gitude values are based on the address location entered by the user, and do not necessarily reflect GPS reported device locations.
Recovery method	Parsing

Attribute	Description
User ID	The unique number identifying the user.
First Name	The first name of the user.
Last Name	The last name of the user.
Email Address	The email address associated with the user account.
Address	User provided full address of the camera.
Latitude	User provided latitude address of the camera.
Longitude	User provided longitude address of the camera.
Location Type	The type of location that the user has specified, such as Residential.
Location Name	The user given name of the location.
Device ID	The list of unique numbers identifying the devices of the user.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the user account was created.

Additional Information

Blink Cached Media

Description	Blink Cached Media contains the cached media files that have been found inside the Blink application.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
MIME Type	The MIME type of the media.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the media file.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.

Attribute	Description
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
MD5 Hash	An MD5 hash of the picture content.
SHA1 Hash	A SHA1 hash of the picture content.
PhotoDNA Hash	The hash of the picture content for PhotoDNA.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Exif Data	A searchable field for all raw Exif properties.

Additional Information

Blink Device Information

Description	Blink Device Information contains information about the Blink home security device.
Recovery method	Parsing

Attribute	Description
Device ID	The unique number identifying the device.
Device Name	The name that the user assigned to the device.
Device Type	The type of the device.
Serial Number	The serial number of the device.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the device was set up.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the device was modified by the software, not by the user.

Additional Information

Blink User Information

Description	Blink User Information contains information about the Blink user of the home security device.
Recovery method	Parsing

Attribute	Description
User ID	The unique number identifying the device user.
Email Address	The email address associated with the user account.
Phone Number	The masked phone number associated with the user account (for example, +1******1234).

Additional Information

Bluetooth Devices

Description	Bluetooth Devices contains information about the Bluetooth devices that the iOS device has paired with.
Recovery method	Parsing

Attribute	Description
MAC Address	The MAC address of the device.
Name	The name that has been assigned to the device.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The last date and time when the device was seen in UTC time.
Last Seen Date/Time - Local Time (yyyy-mm-dd)	The last date and time when the device was seen in Local time.
Major Device Class	The major class of device/service as per the Bluetooth specification.
Minor Device Class	The minor class of device/service as per the Bluetooth specification.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

DJI Log Files

Description	DJI Log Files contains data from the frame times logged during drone flights, which are extracted from the encrypted log files. Frame time states are logged every tenth of a second and include information about the drone at that point in time. The decrypted log files are stored at your AXIOM temporary file location in a folder called DecryptedLogFiles.
Recovery method	Parsing

Attribute	Description
Latitude	The latitude of the drone when the frame time state was logged.
Longitude	The longitude of the drone when the frame time state was logged.
Frame Time Date/Time - UTC (yyyy-mm-dd)	The date and time of the frame time that was captured in the log.

Additional Information

This artifact requires that you allow a decryption option to acquire data. To learn more about this artifact, sign in to the Support Portal to read the article Decrypt DJI Flight Logs.

DJI Media

Description	DJI Media contains the media files that have been found inside the DJI application.

Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file.
Type	The type of the media. It can be Cached, Saved or Edits.
MIME Type	The MIME type of the media.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the media file.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.

Attribute	Description
MD5 Hash	An MD5 hash of the picture content.
SHA1 Hash	A SHA1 hash of the picture content.
PhotoDNA Hash	The hash of the picture content for PhotoDNA.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Exif Data	A searchable field for all raw exif properties.

Additional Information

DJI User Information

Description	DJI User Information contains user information about the last logged in user of a DJI drone application.
Recovery method	Parsing

Attribute	Description
User Email	The email address of the logged in user.
Device Platform	The device platform used by the logged in user.

Additional Information

Fitbit Floors

Description	Fitbit Floors specifies the number of floors a user has traveled up and down within a day.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the associated user profile.
Date	The date that the floor-traveling data was generated.
Floors	The number of floors traveled.

Additional Information

Fitbit Heart Rate

Description	Fitbit Heart Rate specifies the heart rate of the person wearing a Fitbit. Each record displays the average heart rate for a given 5 minute interval and the daily average resting heart rate.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the associated user profile.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the average heart rate calculation.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the average heart rate calculation.
Average Heart Rate (BPM)	The average heart rate.
Type	Indicates whether the average heart rate is a periodic average (every 5 minutes) or a daily average resting heart rate.

Additional Information

Fitbit Profiles

Description	Fitbit Profiles specifies information from the Fitbit profiles that the user has set up on the device.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the associated user profile.
Full Name	The first and last name of the person associated with the profile.
Birthday (yyyy-mm-	The birthday of the person associated with the profile.

Attribute	Description
dd)	
Profile Image URL	The location of the profile image.
Height (cm)	The height of the person in centimeters.
Gender	The gender of the person.
Walking Stride Length (cm)	The walking stride length of the person in centimeters.
Running Stride Length (cm)	The running stride length of the person in centimeters.
Current Timezone Offset (Minutes)	The timezone offset in minutes of the profile.
Country	The country the profile user may be in. For example, if the person is from Canada the value would be en_CA.

Additional Information

Fitbit Sleep

Description	Fitbit Sleep contains information about the user's sleeping patterns.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the associated user profile.

Attribute	Description
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the person went to bed.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the person got out of bed.
Time In Bed (Minutes)	The total time in minutes that the person was in bed (awake and asleep).
Time Awake (Minutes)	The total time in minutes that the person was awake in bed.
Time Asleep (Minutes)	The total time in minutes that the person was asleep.

Additional Information

Fitbit Steps

Description	Fitbit Steps specifies information about the number of steps a person takes while wearing a Fitbit. Steps are aggregated for a 15 minute interval and then stored.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the associated user profile.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the accumulated steps.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the accumulated steps.
Steps Taken	The accumulated steps taken.

Additional Information

Latent Wireless Geolocated Wifi Hotspots

Description	Latent Wireless Geolocated WiFi Hotspots contains information about WiFi hotspots that were discovered using a Latent Wireless device. Latent Wireless stores information about the hotspots in a database that Magnet AXIOM can parse for details about each hotspot.
Recovery method	Parsing

Attribute	Description
MAC Address	The MAC address of the detected WiFi hotspot.
First Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was first discovered.
Last Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was last seen.
Strongest Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was detected at its highest strength.
Network Name (SSID)	The SSID of the WiFi hotspot.
Channel	The WiFi hotspot channel.
RSSI	The received signal strength indicator for the WiFi hotspot.
Latitude	The latitude where the WiFi hotspot was detected.

Attribute	Description
Longitude	The longitude where the WiFi hotspot was detected.
Secure	Indicates whether the WiFi hotspot is secure.

Additional Information

MPT Application Details

Description	MPT Application Details contains information about activities that are triggered by applications and logged in the MPT on LG devices.
Recovery method	Parsing

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	The date and time that the log was entered into MPT.
Package Name	The internal Android package name of this application.
Application Name	The name used to describe this application to users.
Activity Type	A description of the type of activity taking place that is recorded.
Group Name	The application group name (Phone, Multimedia, Utilities, System UI, or Other Apps).
Additional Information	Additional descriptive text about the logged activity.

Additional Information
In the event that the device battery has fully depleted, such as after an extended period of time powered off in an evidence locker, the device system clock will reset to Unix epoch (1970-01-01 00:00). Timestamps for events recovered from the device's database will reflect this clock reset.

MPT Application History

Description	MPT App Usage contains information about application launches, overall usage, and installation/update/deletion timestamps (as recovered from the MPT on LG devices).
Recovery method	Parsing

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	The date and time that this log was entered into MPT.
Package Name	The internal package name belonging to the application.
Version	The version number of the application. This value is not available if the app has been updated or deleted and will report the value "deleted".
Status	An interpreted value for the status of the application package when the log was updated.
Installed Date/Time - UTC (yyyy-mm-dd)	Indicates when the package was installed by either the device or the user.

Attribute	Description
Updated Date/Time - UTC (yyyy-mm-dd)	Indicates when the package was updated by either the device or the user.
Deleted Date/Time - UTC (yyyy-mm-dd)	Indicates when the package was deleted by the user.
Usage Time (milliseconds)	The usage, in seconds, that this application has on record.
Number of Launches	The number of launches that this application has on record.

Additional Information
In the event that the device battery has fully depleted, such as after an extended period of time powered off in an evidence locker, the device system clock will reset to Unix epoch (1970-01-01 00:00). Timestamps for events recovered from the device's database will reflect this clock reset.

MPT Cell Towers

Description	MPT Cell Towers contains records of which cell towers a device connects to at a given time. Records are recovered from the MPT on LG devices, and are defined in the following format: MCC:MNC:LAC:CID.
Recovery method	Parsing

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	The date and time that this log was entered into MPT.
CellID	A GSM Cell ID (CID) is a generally unique number used to identify each base transceiver station (BTS) or sector of a BTS within a location area code (LAC) if not within a GSM network.
Location Area Code	Location Area Code (LAC) is a unique number describing the set of base stations that are grouped together to optimize signalling.
Mobile Country Code	Mobile Country Code (MCC) is used in combination with Mobile Network Code (MNC) to uniquely identify a mobile network operator (carrier).
Mobile Network Code	Mobile Network Code (MNC) is used in combination with Mobile Country Code (MCC) to uniquely identify a mobile network operator (carrier).

Additional Information

In the event that the device battery has fully depleted, such as after an extended period of time powered off in an evidence locker, the device system clock will reset to Unix epoch (1970-01-01 00:00). Timestamps for events recovered from the device's database will reflect this clock reset.

MPT Recent Activity

Description	MPT Recent Activity tracks when applications were launched and terminated (as recovered from the MPT on LG devices).
Recovery method	Parsing

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	The date and time that this log was entered into MPT.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that this application was started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that this application was terminated.
Package Name	The internal package name belonging to the application.

Additional Information

In the event that the device battery has fully depleted, such as after an extended period of time powered off in an evidence locker, the device system clock will reset to Unix epoch (1970-01-01 00:00). Timestamps for events recovered from the device's database will reflect this clock reset.

MPT Wifi Events

Description	MPT Wifi Events includes connection and disconnection events for device wireless networking (as recovered from the MPT on LG devices).
Recovery method	Parsing

Attribute	Description
Date/Time - UTC (yyyy-mm-	The date and time that this log was entered into MPT.

Attribute	Description
dd)	
State	The event state. Values can be decoded as follows: 0 = Disconnecting, 1 = Disconnected, 2 = Connecting, 3 = Connected, 4 = Suspended.
Additional Information	This field is not always populated, but includes (separated by newlines): BSSID, IP Address, Link Speed, RSSI, Supplicant State.

Additional Information
In the event that the device battery has fully depleted, such as after an extended period of time powered off in an evidence locker, the device system clock will reset to Unix epoch (1970-01-01 00:00). Timestamps for events recovered from the device's database will reflect this clock reset.

Pebble Activity Information

Description	Pebble Activity Information specifies the physical activities that were tracked by the Pebble watch.
Recovery method	Parsing

Attribute	Description
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the activity.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the activity.

Attribute	Description
Duration (Seconds)	The duration of the activity.
Steps Taken	The total number of steps taken during the activity.
Active Calories (Cal)	The number of calories being burned during the activity.
Serial Number	The serial number of the Pebble watch used to track the activity.

Additional Information
The Active Calories column is always empty for Android.

Pebble Applications

Description	Pebble Applications specifies the Pebble applications that are installed.
Recovery method	Parsing

Attribute	Description
Title	The title of the Pebble Application.
Installed Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was installed.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was updated.
Created By	The creator of the application.
Type	The type of application in the Pebble application

Attribute	Description
	store.
Version	The version of the application.
Download URL	The URL where the application can be downloaded from.
Website URL	The URL of the application website.
Creator Email Address	The email of the creator for the application.
Companion Application	A companion application to the current application.
Companion Website	The website to the companion application.

Additional Information

Pebble Calendar Events

Description	Pebble Calendar Events contains calendar events that are displayed on the Pebble Watch Timeline.
Recovery method	Parsing

Attribute	Description
Title	The title of the calendar event.
Description	A short description of the calendar event.

Attribute	Description
Locale	The location of the event.
Calendar Display Name	The display name of the calendar to which the event belongs.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the event.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the event.
Organizer Name	The organizer of the event.
Calendar Account	The calendar to which the event belongs.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was created on the Pebble application.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was updated.
User Account	The user account observing the event.
Attendees	The number of attendees to the event.
Is Recurring	Indicates whether the event is recurring.
Organizer	Indicates whether the user is the organizer of the event.

Additional Information

Pebble Contacts

Description	Pebble Contacts contains contact information that's accessible from the Pebble watch.
Recovery method	Parsing

Attribute	Description
Display Name	The display name of the contact.
Phone Number	The phone number of the contact.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message from the contact.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact was created.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact was updated.

Additional Information

Pebble Detected Android Applications

Description	Pebble Detected Android Applications indicates the applications that were detected by the Pebble Android application.
Recovery method	Parsing

Attribute	Description
Application Name	The name of the detected application.
Last Message Received Date/Time - UTC (yyyy-mm-dd)	The date and time when a message or notification was last received from the application.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the application was detected by the Pebble application.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the detection was updated.
Application Version	The current version of the application.
Package Name	The package name of the application.

Additional Information

Pebble Device Information

Description	Pebble Device Information specifies the hardware information of the Pebble watch.
Recovery method	Parsing

Attribute	Description
Friendly Name	The display name of the contact.
Last Connected Date/Time - UTC (yyyy-mm-dd)	The start date and time when the Pebble watch was last connected to the Android application.

Attribute	Description
MAC Address	The MAC address of the Pebble watch.
Serial Number	The serial number of the Pebble watch.
Revision Number	The revision number of the Pebble watch.
Language	The user selected language of the Pebble watch.

Additional Information

Pebble Notifications

Description	Pebble Notifications specifies the notification that was sent to the Pebble watch.
Recovery method	Parsing

Attribute	Description
Text	The content of the notification.
Title	The title of the notification.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the notification.
Original Date/Time - UTC (yyyy-mm-dd)	The original date and time of the notification.
Removed Date/Time - UTC (yyyy-mm-dd)	The date and time when the notification was removed.

Attribute	Description
Message Source	The source application of the notification.
Sent to Wearable	Indicates whether the notification was sent to the Pebble watch.
Dismissed	Indicates whether a notification was dismissed on the Pebble watch.

Additional Information

Pebble Physical Characteristics

Description	Pebble Physical Characteristics specifies the user's activity profile information.
Recovery method	Parsing

Attribute	Description
Gender	The gender of the user.
Age	The age of the user.
Height (cm)	The height of the user in centimeters.
Weight (kg)	The weight of the user in kilograms.

Additional Information

Pebble Weather Locations

Description	Pebble Weather Locations contains location information that's tracked by the Pebble Watch.
Recovery method	Parsing

Attribute	Description
Location Name	The name of the tracked location.
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time of the location data.
Updated Date/Time - UTC (yyyy-mm-dd)	The updated date and time of the location data.

Additional Information

The latitude and longitude are not a precise values, but they can place the Pebble Watch in a specific city.

Ring Cached Media

Description	Ring Cached Media contains the cached media files that have been found inside the Ring application.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
MIME Type	The MIME type of the media.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the media file.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
MD5 Hash	An MD5 hash of the picture content.
SHA1 Hash	A SHA1 hash of the picture content.
PhotoDNA Hash	The hash of the picture content for PhotoDNA.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been

Attribute	Description
	recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Exif Data	A searchable field for all raw Exif properties.

Additional Information

Ring Device Information

Description	Ring Device Information contains information about Ring home security devices. Please note that latitude and longitude values are based on the address location entered by the user, and do not necessarily reflect GPS reported device locations.
Recovery method	Parsing

Attribute	Description
Device ID	The unique number identifying the device.
Device Name	The name that the user assigned to the device.
Device Type	The type of the device.
User ID	The unique number identifying the device user.
Owner ID	The unique number identifying the owner of the security system.

Attribute	Description
Address	The full address of the camera location set by the user.
Timezone	The timezone set for the device.
Latitude	The latitude of the camera's address set by the user.
Longitude	The longitude of the camera's address set by the user.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the device was set up.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the device was modified by the software, not by the user.

Additional Information

Ring User Information

Description	Ring User Information contains information about the Ring user of the home security device.
Recovery method	Parsing

Attribute	Description
User ID	The unique number identifying the device user.
First Name	The first name of the user.
Last Name	The last name of the user.

Attribute	Description
Email Address	The email address associated with the user account.
Phone Number	The phone number associated with the user account.
Two-Factor Authentication Phone Number	The two-factor authentication (2FA) phone number associated with the user account.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the device was set up.

Additional Information

Samsung Health Steps (Device)

Description	Samsung Health Steps (Device) shows the number of steps taken during the activities tracked by the Samsung Health application on a non-wearable device. The information about the steps taken is particularly useful because it gives a sense of the user's activity level at any given time.
Recovery method	Parsing

Attribute	Description
Steps Taken	The number of steps taken in the given time interval.
Date/Time - Local Time (yyyy-mm-dd)	The end date and time of the interval.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Samsung Health Steps (Wearable)

Description	Samsung Health Steps (Wearable) shows the number of steps taken during the activities tracked by the Samsung Health application on a wearable device. The information about the steps taken is particularly useful because it gives a sense of the user's activity level over any given period of time.
Recovery method	Parsing

Attribute	Description
Steps Taken	The cumulative number of steps taken in the given time interval.
Date/Time - UTC (yyyy-mm-dd)	The end date and time of the interval.
Cycle Count	The cycle count is an incrementing number that resets when a new session of steps has been started.

Additional Information

Samsung Health User Profiles

Description	Samsung Health User Profiles contains information from the Samsung Health profile on the device.
Recovery method	Parsing

Attribute	Description
User ID	The Samsung account identifier of the user.
Email Address	The email address of the user.
Weight (kg)	The weight of the user in kilograms.
Gender	The gender of the user.
Last Known Location Latitude	The latitude of the last known activity of the user from the Samsung Health app.
Last Known Location Longitude	The longitude of the last known activity of the user from the Samsung Health app.
Accuracy	The accuracy of the last known activity location data (assumed to be in meters).

Additional Information

Samsung Keyboard Clipboard History

Description	Samsung Keyboard Clipboard History recovers text, attachments, and

	HTML that the user copied while using the Samsung Keyboard application. A user's clipboard can contain sensitive data that the user interacted with, but may not be recoverable from their device otherwise.
Recovery method	Parsing

Attribute	Description
ID	The identifier of the clipboard item that was copied by the user.
Copied Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was copied.
Type	The type of content that was copied. Values can be Text, attachment and HTML. The attachment value will be represented by its MIME type. Any other numerical values are unknown.
Text	The text that was copied, if applicable.
HTML Body	The HTML body of the URL that was copied, if applicable.
Application UID	The unique identifier of the application. You can match the UID to the package name, found in the Installed Applications Artifact.
Attachment	The attachment that was copied to the clipboard, if applicable. The MIME type will be provided in the Type column, if an attachment is recovered.

Additional Information

SIM Card ICCID

Description	SIM Card ICCID contains the ICCID number that identifies the device's SIM card.
Recovery method	Parsing

Attribute	Description
ICCID	The integrated circuit card identifier.

Additional Information

SIM Card IMSI

Description	SIM Card IMSI contains IMSI numbers used to identify the mobile subscriber, as recovered from the SIM card.
Recovery method	Parsing

Attribute	Description
IMSI	The international mobile subscriber identity.

Additional Information

SIM Card Phone Numbers

Description	SIM Card Phone Numbers contains records of all the phone numbers saved to the device SIM card. The type of number is indicated by the record type.
Recovery method	Parsing

Attribute	Description
Phone Number	The phone number for the specific record type.
Label	The optional contact description/name of the phone number stored on the SIM card.
Record Type	Identifies the type of record that the phone number is. The Record Type value can be Abbreviated dialing numbers (ADN), Emergency call codes (ECC), Last number dialed (LND), MSISDN, Service dialing numbers (SDN), or Fixed dialing numbers (FDN).

Additional Information

SIM Card Service Providers

Description	SIM Card Service Providers contains the names of mobile service providers that the device has connected with, and which are recovered from the SIM card.
Recovery method	Parsing

Attribute	Description
Service Provider Name	The identity of the mobile phone service provider.

Additional Information

SIM Card SMS Messages

Description	SIM Card SMS Messages contains messages sent or received by the local user which were saved to the SIM card.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the SMS message.
Recipient	The recipient of the SMS message.
Message Date/Time	For incoming messages, this timestamp indicates when the message was received by the mobile service center. For outgoing messages, there is no data available for this field.
Message	The message body of the SMS message.
Deleted	Identifies whether the message has been deleted (Yes or No).
Message Status	Identifies whether the message has been read, unread, draft or sent.
SMSC	The short message service center number.

Additional Information

Your Phone Companion Info

Description	Your Phone Companion Info contains information about the computers that are synced to the local device using Your Phone, and information about the types of data are synced from device to computer.
Recovery method	Parsing

Attribute	Description
Application Version	The version of the Your Phone Companion application running on the device.
Registered Date/Time - UTC (yyyy-mm-dd)	The date and time that the application was registered with Your Phone (this value should correspond to the install date).
Remote IDs	GUID identifiers generated within Your Phone to uniquely identify the remote computers this device synchronizes with.
Remote Computer Names	The names of the remote computers that this device synchronizes with.
Photo Sync Enabled	Indicates whether photos are synchronized between the device and the remote computer.
MMS Messages Enabled	Indicates whether MMS messages are synchronized between the device and the remote computer.
MMS Media	Indicates whether media sent via MMS are synchronized between the

Attribute	Description
Enabled	device and the remote computer.
SMS Messages Enabled	Indicates whether SMS messages are synchronized between the device and the remote computer.
Messaging Enabled	Indicates whether sending SMS/MMS messages using Your Phone on the remote computer is enabled.
Last Login Date/Time - UTC (yyyy-mm-dd)	The last time that the application signed in to the Your Phone servers (this value may not correspond to a user-initiated event).
Application Run Count	The number of times that the application has run.
Remote User Display Name	The display name of the user account on the remote system, which is typically the user's Windows account.
Remote Username	The username on the remote system, which is typically the user's Windows account.
Remote User ID	The user ID on the remote system, which is typically the user's Windows live account ID.
User First Seen Date/Time - UTC (yyyy-mm-dd)	The first time that the user entered the Your Phone ecosystem. This value may not correspond to the registered date if Your Phone was previously installed on other devices.

Additional Information

Custom

File Signature Mismatch (Audio)

Description	File Signature Mismatch (Audio) contains identified mismatches between a known file signature header and the extension (or lack thereof) for an audio file. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.
Attachment	The mismatched file.

Additional Information

File Signature Mismatch (Container)

Description	File Signature Mismatch (Container) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a container. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mis-match.
File Path	The path to the mismatched file.
Attachment	The mismatched file.

Additional Information

File Signature Mismatch (Document)

Description	File Signature Mismatch (Document) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a document. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type, we return a mis-match.
File Path	The path to the mismatched file.
Attachment	The mismatched file.

Additional Information

File Signature Mismatch (Picture)

Description	File Signature Mismatch (Picture) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a picture. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file. If the mime type is unknown, this defaults to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file. If the mime type is unknown, this defaults to application/octet-stream. If there is no file extension, but the mime type is known, a mismatch is is returned.
File Path	The path to the mismatched file.
Attachment	The mismatched file.

Additional Information

File Signature Mismatch (Video)

Description	File Signature Mismatch (Video) contains identified mismatches between a

	known file signature header and the extension (or lack thereof) for a video. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.
Attachment	The mismatched file.

Additional Information

Documents

CSV Documents

Description	CSV Documents contains CSV documents (.csv) that are located on the system.
Recovery method	Parsing

Attribute	Description
File Name	The name of the CSV document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last modified.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was created.
File Content	The content of the CSV document.
Size (Bytes)	The size of the CSV document in bytes.
SHA1 Hash	The SHA1 hash of the contents of the document.
MD5 Hash	he MD5 hash of the contents of the document.

Additional Information
For information about supported formats, see Supported media and file types.

Evernote Accounts

Description	Evernote Accounts contains information about the user accounts that have been used to log in on the device.
Recovery method	Parsing

Attribute	Description
User Name	The display name of the user's account
User ID	The user ID of the account.
Email	The email address associated with the account.
Full Name	The full name associated with the account.
Active Account	Indicates which account was active at the time of acquisition.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the account was created.
Login Date/Time - UTC (yyyy-mm-dd)	The date and time that the account was initially logged in on the device.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the account was last updated.

Additional Information

Evernote Contacts

Description	Evernote Contacts contains information about users that have communicated with the local user account.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the contact.
Contact ID	The contact ID of the contact.
Account Name	The account name of the contact.

Additional Information

Evernote Notes

Description	Evernote Notes contains any notes associated with the local user, including notes shared from other users to the local user.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the note.
Content	The content of the note.

Attribute	Description
Type	The type of note.
File Name	The name of the attachment that was included with the note.
File	The attachment that was included in the note.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was created.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was updated.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was deleted.
Owner	The owner of the note. If a note is shared from one user to another, the owner is the user that shared the note.
Shared With	The accounts that the note was shared with.
Last Modifier Name	The username of the last modifier of the note.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time of the starting time for the reminder of the note.
End Date/Time - UTC (yyyy-mm-dd)	The date and time of the end time for the reminder of the note.
Locale	The location where the note was taken.
Latitude	The latitude of the location where the note was taken.
Longitude	The longitude of the location where the note was taken.
Notebook Name	The name of the notebook where the note was saved.

Additional Information

Evernote Work Chat

Description	Evernote Work Chat contains messages sent and received by the local user.
Recovery method	Parsing and carving

Attribute	Description
Sender ID	The unique ID of the sender.
Sender Name	The name of the sender.
Sent Date/Time	The date and time when the message was sent.
Message Body	The body of the message.
Participants	The participants of the chat.
Participant IDs	The IDs of the participants of the chat.

Additional Information

Google Keep Notes

Description	Google Keep Notes contains information about the notes that have been accessed using Google Keep on the device.

Recovery method	Parsing

Attribute	Description
Title	The title of the note.
Owner	The email of the user who created the note.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was last edited by a user.
Content	The text content of the note.
Pinned	Indicates if the note is pinned (Yes if pinned, no otherwise).
Deleted	Indicates if the note has been deleted (Yes if deleted, no otherwise).
Archived	Indicates if the note is archived (Yes if archived, no otherwise).
Labels	The labels on the note.
Attachments	The file names of any attachments for the note.

Additional Information

Hangul Word Processor

Description	Hangul Word Processor specifies information about files that were created using Hangul Word Processor.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the found file.
Password Required	Indicates whether the file requires a password to be opened.
Application Version	The version of the software used to create the file.
Preview Text	A preview of the file content that contains the first 1024 symbols.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was modified on the filesytem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was accessed on the filesytem.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was created on the filesytem.
Title	The title field of the document.

Attribute	Description
Subject	The subject field of the document.
Author	The author field of the document.
Date String	The date field of the document.
Keyword	The keyword field of the document.
Additional Information	Any additional information that the author provided for the document. Appears as 'Other' field in the software.
Last Saved By	The username of the last user that saved the file.
Document Created Date/Time - Local Time (yyyy-mm-dd)	The date and time when the file was originally created.
Preview Image	An image preview of the title page of the file.
File	The contents of the Hangul Word document.
MD5 Hash	A MD5 hash of the Hangul Word document.
SHA1 Hash	A SHA1 hash of the Hangul Word document.

Additional Information

For information about supported formats, see Supported media and file types.
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Microsoft Excel Documents

Description	Microsoft Excel is a spreadsheet processor developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File	The actual file.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
Size (Bytes)	The size of the document.
Title	The title metadata.
Saved Size (Bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
Subject	The subject metadata.
Authors	The authors of the document.
Keywords	The keywords in the metadata of the document.
Comment	The comments metadata.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information
For information about supported formats, see Supported media and file types.

Microsoft PowerPoint Documents

Description	Microsoft PowerPoint is a presentation creator developed by Microsoft. This table captures documents created with PowerPoint, extracted from the filesystem and carved from unallocated space.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File	The actual file.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
File System Last Accessed	The date and time when the file was last accessed on the

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	filesystem.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
Size (Bytes)	The size of the document.
Title	The title of the file.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Comment	The comments in the metadata of the file.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

Microsoft Word Documents

Description	Microsoft Word is a word processor developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File	The actual file.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
Size (Bytes)	The size of the document.
Title	The title of the file.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Subject	The subject of the file.
Authors	The authors of the file.

Attribute	Description
Keywords	The keywords in the metadata of the file.
Comment	The comments in the metadata of the file.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

PDF Documents

Description	Portable Document Format (PDF) is a file format used to present documents in a manner independent of application software, hardware, and operating systems. This table captures documents in this file format, extracted from the filesystem and carved from unallocated space.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
Title	The title of the file.
Authors	The authors of the file.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Subject	The subject of the file.
Keywords	The keywords in the metadata of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
MD5 Hash	An MD5 hash of the PDF content.
SHA1 Hash	A SHA1 hash of the PDF content.
File	The PDF file.

Additional Information
For information about supported formats, see Supported media and file types.

RTF Documents

Description	RTF Documents contains information for each RTF document that was recovered from the search.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the RTF document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was created.
File Content	The contents of the RTF document.
File Size (Bytes)	The size of the RTF document.
MD5 Hash	A MD5 hash of the RTF content.
SHA1 Hash	A SHA1 hash of the RTF content.

Additional Information
For information about supported formats, see Supported media and file types.

Samsung Notes

Description	Samsung Notes contains information about the notes that a user has created on their Samsung device.
Recovery method	Parsing

Attribute	Description
Title	The title of the note.
Content	The contents within the note.
Folder	The folder that the note is stored in.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the note was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the note was last modified.
Encrypted	Indicates whether or not the note has been encrypted.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time that the note was deleted.
Favorite	Indicates whether or not the note was favorited.
Note ID	The note's unique identifier.
First Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the note was first accessed.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the note was last accessed.

Additional Information

Text Documents

Description	Text documents (.txt) that are located on the system.
Recovery method	Parsing

Attribute	Description
Filename	The name of the text document.
Size (Bytes)	The size of the text document in bytes.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was created.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.
File Content	The content of the text document.

Additional Information

For information about supported formats, see Supported media and file types.

Thinkfree Office Viewer Files

Description	Thinkfree Office Viewer Files contains information about the files that the user has opened using Thinkfree Office Viewer. Even if the user has deleted the file from the device, this artifact can still recover information about the file if they opened it in the viewer.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file that was opened in Thinkfree Office Viewer.
File Size (Bytes)	The size of the file.
File System Created Date/Time	The date and time when the file was created on the filesystem.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last viewed.
Favorited	Indicates whether the file has been made a favorite.
File Path	The path to the local file.

Additional Information

Email and Calendar

Android Emails

Description	Android Emails contains the email fragments that were recovered from an Android device.
Recovery method	Parsing and carving

Attribute	Description
Sender	Who sent the email.
Recipients	Who the email was sent to.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the email.
Subject	The subject of the email.
Email Body	The body of the email
BCC	Who was BCC'd on the email.
CC	Who was CC'd on the email.
Sync Server Date/Time - UTC (yyyy-mm-dd)	The date and time that the server synchronized the email.
Status	Identifies if the email was read or unread.
Attachments	The attachments in the email.

Additional Information

Android Gmail Conversations

Description	Android Gmail Conversations contains information about email conversations between the local user and others, as recovered from an Android device.
Recovery method	Parsing and carving

Attribute	Description
Conversation Date/Time - UTC (yyyy-mm-dd)	The date and time when the first message in the conversation was sent.
Subject	The subject of the conversation.
Snippet	A snippet of text from the first message in the conversation.
Attachments	Any attachments that were sent during the conversation.
Permanent Link	A URL to the conversation.

Additional Information

Android Yahoo Mail Attachments

Description	Android Yahoo Mail Attachments contains attachments from emails stored by the Android Yahoo Mail application.
Recovery method	Parsing and carving

Attribute	Description
Message ID	The database key for the message. This key can be used to match up an attachment with an email found in Android Yahoo Mail Emails.
Attachment Name	The file name of the attachment.
Download URL	The URL of the original image attachment, if applicable.
Thumbnail URL	The URL of the thumbnail of the image attachment, if applicable.
Original Saved Location	The path at which this attachment was first saved, if any.
Attachment Size (bytes)	The size of the attached file.
Download State	The displayed value is either 'Complete' or 'Incomplete'.
MIME Type	The file type in MIME format.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the attachment was received or sent. The date and time should match the corresponding entry in Android Yahoo Mail Emails.
Sender	The name of the sender
Attachment Type	The location specified when the attachment is recovered. Downloaded: Recovered from the Download folder indicating it was downloaded by the local user. Sent Locally: Recovered from the autosaved_attachment folder indicating it was sent locally. Cached/Thumbnail: The original or thumbnail

Attribute	Description
	of an image recovered from the cache folder.
Attachment	The attachment.

Additional Information

Android Yahoo Mail Emails

Description	Android Yahoo Mail Emails contains carved and non-carved emails stored by the Android Yahoo Mail application.
Recovery method	Parsing and carving

Attribute	Description
Message ID	The database key for the message. This key can be used to match up an email with attachments found in Android Yahoo Mail Attachments.
From	The email address of the sender.
Recipients	A list of email addresses and labels for the intended recipients in the 'To' field of the email.
Subject	The subject line of the email.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was received or sent.
Sent Date/Time -	The date and time that the email was sent.

Attribute	Description
UTC (yyyy-mm-dd)	
Received Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was received.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was last viewed on the local device.
Body	The body of the email in plain text.
Folder ID	The name of the folder that the email was stored in.
Reply To	The email address to which replies to this email will be sent.
Cc	A list of email addresses and labels for the intended recipients in the 'Cc' field of the email.
Bcc	A list of email addresses and labels for the intended recipients in the 'Bcc' field of the email.
Snippet	A short preview of the text of the email body.
Favorited	Whether the email has been favorited locally. The displayed value is either 'Yes' or 'No'.
Replied	Whether the local user has replied to the email. The displayed value is either 'Yes' or 'No'.
Read Status	Whether the email has been opened locally. The displayed value is either 'Read' or 'Unread'.
Has Attachment	Whether the email has an attachment. The displayed value is either 'Yes' or 'No'.

Additional Information

Android Yahoo Mail User Accounts

Description	Android Yahoo Mail User Accounts contains local user accounts from the Android Yahoo Mail application.
Recovery method	Parsing and carving

Attribute	Description
User Name	The user ID of the account.
First Name	The first name of the person associated with the account.
Last Name	The last name of the person associated with the account.
Preferred Name	The user's custom preferred name.
Email Address	The account's email address.

Additional Information

Calendar Events

Description	The Android Calendar application is a default application on Android.
Recovery method	Parsing and carving

Attribute	Description
Summary	A summary of the calendar appointment.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the appointment starts.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the appointment ends.
Event Location	The location of the calendar appointment.
Notes	Notes about the calendar appointment.
Calendar	The name of the calendar from which the event was generated.
Attendees	The attendees of the event.
Timezone	The timezone the appointment is in.
URL	A URL associated with the event.

Additional Information

Calendar Events (UFED Agent)

Description	Calendar Events (UFED Agent) contains details about a user's calendar events on Android. These messages are recovered from <calendar> tag found in a UFED Report.xml
Recovery method	Parsing

Attribute	Description
Subject	The subject of the scheduled event. This data is retrieved from the <subject> tag within the calendar element in a UFED Report.xml.
Event Location	The location of the scheduled event. This data is retrieved from the <location> tag within the calendar element in a UFED Report.xml.
Notes	Notes about the scheduled event. This attribute is referred to as the <Description> in the evidence acquired from the UFED and is retrieved from the <description> tag within the calendar element in a UFED Report.xml.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the scheduled event. This data is retrieved from the <start> tag wihin the calendar element in a UFED Report.xml.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the scheduled event. This data is retrieved from the <end> tag within the calendar element in a UFED Report.xml.
Repeat Until Date/Time - UTC (yyyy-mm-dd)	The date and time when this recurring scheduled event expires. This data is retrieved from the <repeat_until> tag within the calendar element in a UFED Report.xml.
Repeat Interval	Describes the type of recurring event. This data is retrieved from the <repeat_type> tag within the calendar element in a UFED Report.xml.
Repeat Every	Describes the frequency of the recurring event. This data is retrieved from the <repeat_every> tag within the calendar element in a UFED Report.xml.
Repeat On	Indicates the specific day of occurrence of the recurring event. This data is retrieved from the <repeat_position> tag within the calendar element in a UFED Report.xml.

Additional Information

Gmail Emails

Description	Gmail Emails contains the Gmail email fragments that were recovered from an Android device.
Recovery method	Parsing and carving

Attribute	Description
To Address(es)	The recipient(s) of the email.
From Address	The sender of the email.
Thread ID	The ID of the conversation the email is from. Emails with the same Thread ID belong to the same conversation.
Subject	The subject of the email.
Sent Date/Time - UTC (yyyy-mm-dd)	The date that the email was sent.
Received Date/Time - UTC (yyyy-mm-dd)	The time that the email was received.
Email Body	The body of the email.
Email Snippet	A snippet of the email.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.

Attribute	Description
Reply Address(es)	The reply-to address for the email.
Attachment Data Recovered	Indicates whether attachments for the email were recovered.
Attachments	The file names of any attachments for the email.
Saved Attachments	The file paths of any attachments for the email which were saved locally.
Date/Time - UTC (yyyy-mm-dd)	The date and time when message was either sent or received.

Additional Information

Google Calendar Calendars

Description	Google Calendar Calendars contains a list of all the calendars the user has synced to their Google account.
Recovery method	Parsing

Attribute	Description
Account ID	The account ID assigned by Google
Calendar Display Name	The name of the calendar.
Description	The description of the calendar.

Attribute	Description
Timezone	The timezone of the calendar.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the calendar was created.
Visibility	Indicates if the calendar is visible or hidden on the phone.
Access	The level of permissions the user has for the calendar (Owner Access or Read Only).
Calendar ID	A unique ID for the calendar.

Additional Information

Google Calendar Events

Description	Google Calendar Events contains information about a user's calendar events on the Google Calendar application.
Recovery method	Parsing

Attribute	Description
Event Name	The name of the event.
Description	The description of the event.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time of the event.

Attribute	Description
Event End Date/Time - UTC (yyyy-mm-dd)	The date and time of the end of the event.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time of when the event was created.
Invitees	The email addresses of those invited to the event.
Event ID	The unique ID of the event.
Account ID	The unique identifier of the owner of the account.
Owner Email	The email address of the owner of the event.
Owner Name	The name of the owner of the event.
Calendar ID	The unique ID of this calendar.
Calendar Display Name	The display name of the calendar to which the event belongs.
Event Location	The location of the event.
Latitude	The latitude of the event.
Longitude	The longitude of the event.
Location URL	The unique location URL for the event's location.
Recurrence	The recurrence of the event.
Event URL	The unique URL of the event.

Additional Information

Outlook Accounts

Description	Outlook Accounts contains information about the user accounts that have been logged in to on the device.
Recovery method	Parsing

Attribute	Description
Email Address	The email address associated with the account.
Description	A description of the account, as set by the user.
Display Name	The display name for the user.
User ID	The ID number associated with the account.
Password/Token	The refresh token of the account.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time that the password/token expires.
Birthday (yyyy-mm-dd)	The user's birthday in yyyy-mm-dd format.
Package Name	The package name of the application.

Additional Information

Outlook Appointments

Description	Microsoft Outlook is a personal information manager and email client. Outlook Appointments captures information related to appointments sched-

	uled in Outlook.
Recovery method	Parsing

Attribute	Description
Sender Name	The person who requested the appointment.
Sender Exchange Account	The sender's Exchange account name.
Recipients	The recipients of the appointment invitation.
Subject	The subject of the appointment.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the appointment starts.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the appointment ends.
Body	The body of the appointment description.
CC	The CC'd recipients of the appointment invitation.
BCC	The BCC'd recipients of the appointment invitation.
Companies	The companies involved in the appointment.
Attachments	The attachments for the appointment.
Locale	The location of the appointment.
Is All-day Event	Indicates if the appointment is an all-day event.
Is Recurring	Indicates if the appointment is recurring.
Recurrence Pattern Description	Describes the recurrence pattern of the appointment, if

Attribute	Description
	applicable.
Sensitivity	Indicates if the appointment is sensitive.
Is Hidden	Indicates if the appointment is hidden.
Is Private	Indicates if the appointment is private.
Priority	The priority of the appointment.
Importance	The appointment importance setting.
MD5 Hash	The MD5 hash of the appointment.
SHA1 Hash	The SHA1 hash of the appointment.

Additional Information

Outlook Contacts

Description	Microsoft Outlook is a personal information manager and email client. Outlook Contacts captures information related to contacts stored in Outlook.
Recovery method	Parsing

Attribute	Description
Display Name	The contact's display name.

Attribute	Description
Customer ID	The customer ID of the contact.
Email Address 1	The contact's primary email address.
Email Display As 1	The display string of the contact's primary email address.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact details were last modified.
Company Name	The contact's company name.
Department Name	The contact's department name.
Title	The contact's job title.
Profession	The contact's profession.
Manager Name	The name of the contact's manager.
Office Location	The contact's office location.
Business Address	The physical address of the business.
Business Phone	The contact's business phone number.
Business Phone 2	The contact's secondary business phone number.
Business Fax	The contact's business fax number.
Business Homepage	The website of the contact's business.
Email Display Name 1	The display name of the contact's primary email address.
Email Address 2	The contact's secondary email address.

Attribute	Description
Email Display As 2	The display string of the contact's secondary email address.
Email Display Name 2	The display name of the contact's secondary email address.
Email Address 3	The contact's tertiary email address.
Email Display As 3	The display string of the contact's tertiary email address.
Email Display Name 3	The display name of the contact's tertiary email address.
Cellular Phone	The contact's mobile phone number.
Home Address	The contact's home address.
Home Phone	The contact's home phone number.
Home Phone 2	The contact's secondary home phone number.
Home Fax	The contact's home fax number.
FTP Site	The contact's FTP site.
Body	More information about the contact.
Attachments	Any attachments to the contact entry.
Last Modifier Name	The name of the person who last modified the contact details.
MD5 Hash	The MD5 hash of the contact.
SHA1 Hash	The SHA1 hash of the contact.

Additional Information

Outlook Emails

Description	Microsoft Outlook is a personal information manager and email client. Outlook Messages captures information related to emails sent and received in Microsoft Outlook.
Recovery method	Parsing

Attribute	Description
Sender Name	The sender of the email.
Sender Email	The email address of the sender.
Recipients	The recipients of the email.
Subject	The subject of the email.
Sender Exchange Account	The sender's Exchange account name.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was created.
Sync Date/Time - UTC (yyyy-mm-	The date and time when the email synced with the HxStore platform.

Attribute	Description
dd)	
Submitted Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was submitted.
Delivered Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was delivered.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was last modified.
Body	The body of the email. For HxStore data sources that include email bodies deleted when an account was removed, the displayed value is the path where the email body was located on the file system.
Folder Name	The name of the folder where the email is stored.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Attachments	The list of attachments on the email.
Headers	The raw email headers.
Priority	The priority of the email.
Importance	The importance of the email.

Attribute	Description
Sensitivity	The sensitivity of the email.
Read	Indicates whether the email was opened and therefore marked as Read. Note that Outlook users can also manually mark emails as either Read or Unread.
MD5 Hash	The MD5 hash of the email.
SHA1 Hash	The SHA1 hash of the email.

Additional Information

ProtonMail Contacts

Description	ProtonMail is a free end-to-end encrypted email service. ProtonMail Contacts contains information about contacts messaged through the email application ProtonMail.
Recovery method	Parsing

Attribute	Description
Name	The name of the contact.
Email	The email address of the contact.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact was added.
Modified Date/Time - UTC (yyyy-mm-	The date and time when the contact was last mod-

Attribute	Description
dd)	ified.
Metadata	The vCard associated with the contact.
Avatar	The avatar of the contact.

Additional Information

ProtonMail Emails

Description	ProtonMail is a free end-to-end encrypted email service. ProtonMail Emails contains information about emails sent and received with ProtonMail.
Recovery method	Parsing

Attribute	Description
From	The email address that sent the email.
To	The recipient(s) of the email.
Subject	The subject of the email.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the email.
Type	The type of the email, including if the email was incoming, outgoing, or a draft.
Body	The body of the email.

Attribute	Description
Folder	The name of the folder where the email is stored.
Read	Whether or not the email was read.
Deleted	Whether or not the email was deleted.
Starred	Whether or not the email was starred.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Has Attachments	Whether or not the email had attachments or embedded attachments. The attachments may not be recoverable by Axiom.
Attachment Name(s)	The name(s) of the file(s) attached to the email or embedded in the email body.
Headers	The raw email headers.
Size	The size of the email.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the email will expire.

Additional Information

Samsung Email Logs

Description	Samsung Email Logs contains the email logs that were recovered from a Samsung device.
Recovery method	Parsing

Attribute	Description
Name	The name of the person/business the email is with.
Email Address	The email address of person/business the email is with.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the email.
Message Content	The email message content.
Subject	The subject of the email.

Additional Information

Encryption and Credentials

Android KeyStore

Description	Android KeyStore contains passwords and tokens for websites and other internet services that are recovered from Android KeyStore.
Recovery method	Parsing

Attribute	Description
Account	The user account that the keystore entry applies to.
File Name	The name of the keystore data file.
Type	The type of the keystore data.
Key	The private key found in the keystore data.

Attribute	Description
Value	The blob value.
Flags	The flags byte.
Blob Info	The info byte.
Initialization Vector	The initialization vector.
AEAD Authentic-ation Tag	The tag used for authentication encryption with associated data (used by KeyStore 3).
MD5 Hash	The MD5 hash used for encryption (used by KeyStore 2).

Additional Information

Android KeyStore - GrayKey

Description	Android KeyStore - GrayKey contains passwords and tokens from the Android GrayKey image, reading the 'android_keystore' file generated by the GrayKey tool.
Recovery method	Parsing

Attribute	Description
Package Name	The package name of the application.
Description	The description of the data provided by the application for the keystore.
Encrypted Data	The encrypted hexidecimal bytes of the keystore data.
Decrypted Data	The decrypted hexidecimal bytes of the keystore data.

Additional Information

Location and Travel

Android Google Maps

Description	Android Google Maps contains information about the locations that a user searches for using Google Maps.
Recovery method	Parsing and carving

Attribute	Description
Search Query	The location that the user searched for
Latitude	The latitude associated with the search.
Longitude	The longitude associated with the search.
URL	The URL that contains the search query.
CID	A unique ID - also known as ludocid - that Google assigns to a specific business location in order to identify it within its systems.
FID	A unique ID that relates to reviews that Google holds about a specific business.

Additional Information

Android Wi-Fi Profiles

Description	Wi-Fi Profiles contains a list of the saved Wi-Fi Profiles on a mobile device.
Recovery method	Parsing and carving

Attribute	Description
Network Name (SSID)	The name of the network.
Security Mode	The security mode of the network.
Network Password	The password used to log onto the network.
User Name	The username that was used to log onto the network.
WEP Key	The WEP key used to log onto the network
MAC Address	The MAC Address of the network.
Network ID	An integer used to identify the network. As networks are added to the device, this value gets incremented (the first network added has an ID of 0, the second has an ID of 1, and so on). If a network is deleted and re-added at a later date, it receives the next new ID available instead of reassuming its original ID.
Profile Created Date/Time - Local Time	The date and time that the Wi-Fi profile was created.

Attribute	Description
(yyyy-mm-dd)	
Last Connected Date/Time - Local Time (yyyy-mm-dd)	The date and time of the last network connection.
Connection Count	The number of times that the network was connected to by the device.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Google Maps Directions

Description	Google Maps Directions contains information about directions queries requested by the user using Google Maps.
Recovery method	Carving

Attribute	Description
Origin Address	The address where the direction starts from. This value can be an address, a business description or latitude/longitude coordinates.
Origin Lat-	The latitude associated with the origin address.

Attribute	Description
itude	
Origin Longitude	The longitude associated with the origin address.
Destination Address	The destination address where the direction goes to. Several destinations can be added to a direction but only the last one is displayed.
Destination Latitude	The latitude associated with the destination address.
Destination Longitude	The longitude associated with the destination address.
Number of Stops	The number of stops (if any) between origin and destination addresses.
URL	The URL associated with the direction query. Directions can be viewed in a browser by appending the URL to the end of 'www.google.com/maps'.

Additional Information

Google Maps Saved Locations

Description	Google Maps Saved Locations contains information about locations that the user may have saved as places of interests, such as their home and work locations, places they've starred, and places they want to go to. Users can also create their own custom location lists to add locations to. These locations will synchronize between different devices on Google Maps when signed into the same account.

Recovery method	Parsing

Attribute	Description
Location Name	The name of the location the user saved.
Address	The address or locale of the location the user saved.
URL	The Google Maps URL to the business or location.
Latitude	The latitude of the location saved.
Longitude	The longitude of the location saved.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the location was added to a list.

Additional Information

Last Known Locations

Description	Last Known Locations contains a list of the last known locations of the Android device, as tracked by the GPS receiver and recovered using dumpsys.
Recovery method	Parsing

Attribute	Description
Serial Number	The serial number of the Android device.
Type	The type of receiver.
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Altitude (meters)	The altitude of the location.

Additional Information

OnStar RemoteLink Accounts

Description	Contains information about all the OnStar RemoteLink accounts found on the device.
Recovery method	Parsing

Attribute	Description
Account Number	The OnStar account number of the suspect.
Account Key	A secondary identifier for the account on the device.
Created Date/Time	The date and time the account was created on the device.
Updated Date/Time	The date and time the account was updated on the device.

Attribute	Description
Country Code	The country code associated with the user account.
First Name	The first name of the account holder.
Last Name	The last name of the account holder.
Selected VIN	The VIN of the vehicle that was selected by the app at the time of extraction.

Additional Information

OnStar RemoteLink Hotspot Info

Description	Information about the vehicle Wi-Fi hotspots associated with an OnStar account.
Recovery method	Parsing

Attribute	Description
Network Name (SSID)	The name of the vehicle's hotspot.
Network Password	The password of the vehicle's hotspot.
Created Date/Time	The date and time the hotspot was created.
Updated Date/Time	The date and time the hotspot was updated.
VIN	The Vehicle Identification Number that the hotspot is associated with.

Additional Information

OnStar RemoteLink Recent Location Searches

Description	OnStar RemoteLink Recent Location Searches contains the location searches and commands performed on the results of the searches.
Recovery method	Parsing

Attribute	Description
Destination Address	The addresses searched for by the suspect.
Timestamp Date/Time	The date and time that the search was completed.
Created Date/Time	The date and time the entry was created on the device.
Updated Date/Time	The date and time the entry was updated on the device.
Command	The command used to send the address to the vehicle.
Command Status	The status of the command.
Destination Name	The name of the destination address if one was assigned.
VIN	The Vehicle Identification Number of the vehicle to which the command was sent.

Additional Information

OnStar RemoteLink Remote Commands

Description	OnStar RemoteLink Remote Commands contains information about commands sent from the device.
Recovery method	Parsing

Attribute	Description
Requested Command	The command requested by the user.
Request State	The state of the request.
Sent Date/Time	The date and time that the command was sent to the vehicle.
Completion Date/Time	The date and time that the command was completed.
Command Description	The description of the command that was sent, if one is available.
VIN	The Vehicle Identification Number of the vehicle that the command was sent to.
Request ID	The ID of the request that was sent, if available.

Additional Information

OnStar RemoteLink Saved Places Of Interest

Description	OnStar RemoteLink Saved Places Of Interest contains addresses for places of interest saved in the OnStar RemoteLink application.
Recovery method	Parsing and carving

Attribute	Description
Address	The full address stored in the application.
State/Province	The state/province of the address.
Country	The country of the address.
Latitude	The latitude of the address to map on the world map.
Longitude	The longitude of the address to map on the world map.
Address URL	The URL of the address as stored by OnStar.
Created Date/Time	The date and time that the saved entry was created on the device.
Updated Date/Time	The date and time that the saved entry was updated on the device.
Name	The name of the saved address.

Additional Information

OnStar RemoteLink Saved Wireless Carrier

Description	OnStar RemoteLink Saved Wireless Carrier contains information about the

	wireless accounts associated with a vehicle.
Recovery method	Parsing

Attribute	Description
Carrier Account ID	The account identifier of the carrier account.
Carrier Type Code	The code that represents the account type.
Carrier Type Description	The carrier associated with the account.
Created Date/Time	The date and time that the account entry was created on the device.
Updated Date/Time	The date and time that the account entry was updated on the device.
Account Type	The type of wireless account.
Account Description	The description of the account type.
VIN	The Vehicle Identification Number of the vehicle that the wireless account is associated with.

Additional Information

OnStar RemoteLink Vehicle Diagnostics

Description	OnStar RemoteLink Vehicle Diagnostics contains information about the dia-

	gnostic values that were retrieved from the vehicle.
Recovery method	Parsing

Attribute	Description
Diagnostic Name	The name of the diagnostic test that was retrieved.
Unit	The unit of measurement associated with the diagnostic test.
Value	The value associated with the diagnostic test.
Created Date/Time	The date and time that the diagnostic value was retrieved.
Updated Date/Time	The date and time that the diagnostic value was updated.
Completion Date/Time	The date and time that the server retrieved the diagnostic value from the vehicle.
VIN	The Vehicle Identification Number of the vehicle that the diagnostic value was retrieved from.

Additional Information

OnStar RemoteLink Vehicle Info

Description	OnStar RemoteLink Vehicle Info contains information about the vehicle associated with the account.
Recovery method	Parsing

Attribute	Description
VIN	The Vehicle Identification Number of the vehicle associated with the account.
Vehicle Make	The make of the vehicle.
Vehicle Model	The model of the vehicle.
Year	The year of production of the vehicle.
Created Date/Time	The date and time that the vehicle information was added to the device.
Updated Date/Time	The date and time that the vehicle information was updated on the device.
Phone Number	The phone number associated with the vehicle.
Account Number	The OnStar account number that the vehicle is associated with.

Additional Information

Samsung Positioning Path History

Description	Samsung Positioning Path History shows the locations that the user has been to with a certain level of accuracy.
Recovery method	Parsing and carving

Attribute	Description
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the user was at the location.
Accuracy	The horizontal accuracy of the location in meters. The confidence of this accuracy is 68%, meaning there is 68% probability that the actual location is within the circle defined by the point and the radius accuracy.

Additional Information
The KeyStore key is required to decrypt the Samsung Positioning databases, which can be retrieved from the Android KeyStore Artifact. In that artifact, locate the item with Package Name com.samsung.android.samsungpositioning, and copy the key from the Decrypted Data column.

Uber Accounts

Description	Uber Accounts contains account information for riders, as recovered from the Uber application (passenger only).
Recovery method	Parsing

Attribute	Description
First Name	The first name of the account holder.

Attribute	Description
Last Name	The last name of the account holder.
Mobile Phone	The mobile phone number associated with the acount.
Email	The email associated with the account.
Share Code	A unique share code associated with the rider.
User ID	The user ID uniquely identifying the account.
Password/Token	The unique token associated with the account.
Latitude (On App Startup)	The latitude of the user when the application was last opened.
Longitude (On App Startup)	The longitude of the user when the application was last opened.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the user last opened the application.
Last Payment Profile ID	The ID of the payment profile that was last used by the user.
Profile Image URL	The URL of the profile image for the account.
Downloaded Profile Image	The profile picture of the account.
Service	The Android package ID or Apple bundle ID of the service that the account was used for.

Additional Information

Uber Cached Locations

Description	Uber Cached Locations contains information about locations that Uber caches, such as the initial location on the application's startup, or locations from a trip (passenger only).
Recovery method	Parsing

Attribute	Description
Address	The address of the cached location.
Name	The name of the cached location.
Latitude	The GPS latitude of the cached location.
Longitude	The GPS longitude of the cached location.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the location was cached.
Tag	The tags assigned to the location by the user. These tags are user generated.
Categories	The categories assigned to the location by Uber.

Additional Information

Uber Payments

Description	Uber Payments contains payment information associated with a user's

	rides, as recovered from the Uber application (passenger only).
Recovery method	Parsing and carving

Attribute	Description
Rider Name	The name of the passenger/rider.
Share Code	A unique share code associated with the rider.
Cost	The cost of the trip.
Currency	The currency used to measure the cost of the trip.
Duration (Seconds)	The duration of the trip.
Distance (Kilometers)	The distance of the trip.
Payment Method	The method of payment.
Card Display Name	The payment card display name.

Additional Information

Uber Profiles

Description	Uber Profiles contains information about a user's Uber profiles, as recovered from the Uber application (passenger only).
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the profile.
Profile Email	The email associated with the profile.
Profile User ID	The unique user ID (UUID) associated with the profile.
Profile Payment User ID	The unique user ID that is the payment method for this profile.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the profile was created.

Additional Information

Uber Trips

Description	Uber Trips contains information about a user's Uber rides, as recovered from the Uber application (passenger only).
Recovery method	Parsing

Attribute	Description
Booking Date/Time UTC (yyyy-mm-dd)	The date and time when the trip was booked.
Origin Address	The address of the original start location.
Destination Address	The address of the final destination.

Attribute	Description
Arrival Date/Time UTC (yyyy-mm-dd)	The date and time when the vehicle arrived at the destination address.
Duration (Seconds)	The duration of the trip.
Distance	The distance of the trip, units unknown.
Driver Name	The first name of the driver.
Vehicle Make	The make of the driver's vehicle.
Vehicle Model	The model of the driver's vehicle.
Vehicle Type	The type of Uber car service.
Driver Rating	The driver's rating.
Driver Picture URL	The URL to the driver's profile picture.
Cost	The cost of the trip.
Currency	The currency used to measure the cost of the trip.
Status	The status of the trip.
Route Map URL	The URL to the route taken in the trip.

Additional Information

Waze Events

Description	Waze Events can contain information about upcoming trips that a user has planned.

Recovery method	Parsing

Attribute	Description
Name	The name of the place.
Address	The house number and street name of the place.
City	The city of the address.
State	The state/province of the address.
Country	The country of the address.
Start Date/Time	The start date and time that was recommended for the planned drive.
End Date/Time	The date and time that the user planned to arrive at the destination.
Created Date/Time	The date and time when the event was created.
Is All-day Event	Indicates if the planned drive is an all-day event.
Latitude	The GPS latitude coordinates of the place.
Longitude	The GPS longitude coordinates of the place.

Additional Information

Waze Favorites

Description	Waze Favorites contains information about locations that a user has bookmarked as a favorite.

Recovery method	Parsing

Attribute	Description
Name	The name of the place bookmarked as a favorite
Address	The house number and street name of the place.
City	The city of the address.
State	The state/province of the address.
Country	The country of the address.
Created Date/Time	The date and time that the address was added as a favorite.
Modified Date/Time	The date and time that the favorite location was last modified by the user.
Accessed Date/Time	The date and time that the favorite location was last accessed in Waze.
Latitude	The GPS latitude coordinates of the place.
Longitude	The GPS longitude coordinates of the place.

Additional Information

Waze Places

Description	Waze Places contains all of the places that the user has searched using Waze.

Recovery method	Parsing

Attribute	Description
Name	The name of the place.
Address	The house number and street name of the place.
City	The city of the address.
State	The state/province of the address.
Country	The country of the address.
Created Date/Time	The date and time when the address was entered in Waze.
Accessed Date/Time	The last date and time when the address was accessed in Waze.
Latitude	The GPS latitude coordinates of the place.
Longitude	The GPS longitude coordinates of the place.

Additional Information

Media

AMR Files

Description	AMR Files contains voicemail messages or memos for both iOS and Android.
Recovery method	Carving

Attribute	Description
File Name	The name of the file the AMR was recovered from.
Size (Bytes)	The size of the AMR content.
MD5 Hash	An MD5 hash of the AMR content.
SHA1 Hash	A SHA1 hash of the AMR content.
Audio	The contents of an AMR file.
Media Duration (Seconds)	The duration of the audio clip in seconds.

Additional Information

For information about supported formats, see Supported media and file types. Media duration is calculated from the number of speech frames carved from the AMR data, where each speech frame has a duration of 20ms, as AMR files do not contain metadata for duration.

Audio

Description	Audio contains Audio files that are recovered and use .mp3 or .wav formats.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file.
File Extension	The extension of the file.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was created.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was last modified.
File Size (Bytes)	The size of the audio file.
MD5 Hash	An MD5 hash of the audio content.
SHA1 Hash	A SHA1 hash of the audio content.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the audio clip in seconds (extracted from Exif data).
Exif Created	The date and time when the audio clip was first recorded (extracted from Exif

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	data).
Exif Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio clip was edited (extracted from Exif data).
Timezone	The timezone setting on the recorder at the time when the audio clip was recorded (extracted from Exif data).
Software	The software used to record or modify the audio clip. This could either be the OS version of the phone used to record the audio clip or the name of the software used to edit the audio clip in post-production (extracted from Exif data).
Latitude	The GPS latitude coordinates of where the audio clip was recorded (extracted from Exif data).
Longitude	The GPS longitude coordinates of where the audio clip was recorded (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of where the audio clip was recorded (extracted from Exif data).
Exif Data	A searchable field for all raw Exif properties.

Additional Information

For information about supported formats, see Supported media and file types.
To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Calc Vault Browser Bookmarks

Description	Calc Vault Browser Bookmarks contains the webpages a user has saved while using Calc Vault.
Recovery method	Parsing

Attribute	Description
Name	The name of the bookmark.
URL	The URL of the bookmark.
User Added	Indicates whether the user added the bookmark (Yes if the user added the bookmark, or No if it is a default bookmark).

Additional Information

Calc Vault Browser History

Description	Calc Vault Browser History contains information about the webpages a user has visited using Calc Vault.
Recovery method	Parsing

Attribute	Description
Name	The name of the webpage visited.
URL	The URL of the webpage visited.

Additional Information

Camera History

Description	Camera History contains a list of the instances where applications have accessed the camera functionality on a device. This artifact can show when an application package accesses camera functionality, which can help the investigator determine when a suspect may have been using their device's camera.
Recovery method	Parsing

Attribute	Description
Date/Time - Local Time (yyyy-mm-dd)	The local date and time of the event.
Action	The action that describes the event.
Camera ID	An ID that can indicate the location of the camera on the phone. The location of the camera can be front, rear, or other.
Package Name	The package name for the application that's accessing the camera.
Process ID	The ID of the process accessing the camera.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Carved Video

Description	Carved Video contains videos that are recovered using carving. Supported formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. Other container formats can also be recovered provided that their underlying packets are the same as one of the supported formats.
Recovery method	Parsing

Attribute	Description
Content Format	The format of the video.
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
File Size (Bytes)	The size of the container and file.
Container Format	The format of the video container.
Saved Video Size (Bytes)	The size of the video that was saved to the database.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Additional Information

As of February 20 2020, this artifact will no longer be included under Videos. Carved Video functionality will be included in the 'Videos' artifact instead.

Google Photos Albums

Description	Google Photos Albums contains information about the albums recovered from the device.
Recovery method	Parsing

Attribute	Description
Title	The name of the album.
Owner	The owner of the album.
User ID	The unique user ID of the owner of the album.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the album was created.
Shared With	A list of the user IDs the album is shared with.
Shared	Indicates if the album is shared with another user.
Album Cover URL	The url of the cover photo for the album.
Album URL	The url of the album.

Additional Information

Google Photos Comments

Description	Google Photos Comments contains information about comments left on an album or individual media by users.
Recovery method	Parsing

Attribute	Description
Author	The author of the album comment.
User ID	The unique user ID of the author of the album comment.
Comment	The content of the comment. Comments include likes when the user clicks a heart-shaped like button.
Item Name	The name of the item that the comment belongs to. The user can comment on albums or individual media.
Type	The type of the item that the comment belongs to. The type can be Album or Media.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the comment was created.

Additional Information

Google Photos Media

Description	Google Photos Media contains information about media items added to Google Photos.

Recovery method	Parsing

Attribute	Description
File Name	The file name of the media item.
Album	The album that the media item belongs to.
Owner	The owner of the media item.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the media item was created.
Size	The size of the media item in bytes.
Duration	The duration of the media item if it is a video.
Caption	The caption of the media item.
Latitude	The latitude of the media item.
Longitude	The longitude of the media item.
Deleted	Indicates whether or not the media item has been deleted. This data is unavailable in Android.
Picture URL	The url of the media item.
Profile Picture URL	The profile picture url of the owner of the media item.

Additional Information

Motion Photos

Description	Motion Photos contains an image and embedded mp4 that has been carved.
Recovery method	Parsing

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.

Attribute	Description
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture, or the name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Latitude	The latitude coordinate in decimal degrees.

Attribute	Description
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS latitude (extracted from Exif data).
Longitude	The longitude coordinate in decimal degrees.
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the picture was taken (extracted from Exif data).
Exif Data	A searchable field for all raw exif properties.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.

Additional Information

If you're having issues previewing this artifact in your cases or exports, see Videos for Motion Photos and Live Photos do not play correctly.

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Pictures

Description	Pictures contains pictures that were retrieved using either carving or parsing techniques. The supported picture formats are JPEG (.jpeg, .jpg, .jpe), PNG (.png), Bitmaps (.bmp), Graphics Interchange Format (.gif), Icons (.ico), and Tagged Image File Format (.tif, .tiff).
Recovery method	Parsing and carving

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the that file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-	The last modified date and time of the picture in the file system.

Attribute	Description
mm-dd)	
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).

Attribute	Description
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The latitude coordinate in decimal degrees.
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS latitude (extracted from Exif data).
Longitude	The longitude coordinate in decimal degrees.
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Exif Data	A searchable field for all raw exif properties.

Attribute	Description
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicates whether the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

For information about supported formats, see Supported media and file types.
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.
To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Private Photo Vault Albums

Description	Private Photo Vault Albums contains information about the albums a user creates to organize their media in the Private Photo Vault application. The album information can be useful intelligence for how a user might have organized encrypted media.
Recovery method	Parsing

Attribute	Description
Album Title	The name of the album.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the album was created on the device.
Last Modified Date/Time - UTC (yyyy-mm-dd)	Not available on Android.
Decoy	Indicates whether the album is hidden (accessible with a different passcode) or not.
Password	The password protecting the album, if any. Does not affect encryption.
PIN	The value used to generate the encryption key. It can be either a numeric PIN (4 digits) or a sequence of values (2 to 9) of an unlock pattern.

Additional Information

Private Photo Vault Media

Description	Private Photo Vault Media contains information about encrypted media files that the user stores in the Private Photo Vault application. If decryption is successful, the decrypted media content is made available in this artifact. Metadata about the encrypted media files, such as timestamps, are always available. Users will often resort to encrypted media applications for storing illicit material. Being able to decrypt this media can be crucial to a case.
Recovery method	Parsing

Attribute	Description
File Path	The path to the encrypted media file.
Media Type	The type of media (photo or video).
Album Title	The associated album title.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the media was created on the device.
Last Modified Date/Time - UTC (yyyy-mm-dd)	Not available on Android.
Thumbnail Path	Not utilized on Android - see the 'Private Photo Vault Thumbnails - Android' artifact instead.
Picture	The encrypted media.
Thumbnail File	The thumbnail of the encrypted media.

Additional Information

Private Photo Vault Thumbnails - Android

Description	On Android, Private Photo Vault does not explicitly reference thumbnails in the database. Further, multiple resolutions can exist. This artifact will decrypt all of the thumbnails found in the thumbnails directory.
Recovery method	Parsing

Attribute	Description
File Name	The path to the encrypted thumbnail.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the media was created or imported into Private Photo Vault.
Thumbnail File	The thumbnail of the encrypted media.

Additional Information
This artifact may be useful in situations where the original media or database rows have been deleted but thumbnail files remain. It is possible for the same encrypted media to have multiple thumbnails (different resolutions).

Samsung Story Service

Description	Samsung Story Service is a Samsung exclusive application that generates location and AI recognition data for media files on the device. The AI generated data is generated by the application.
Recovery method	Parsing

Attribute	Description
File Path	The file path of the media attachment on the device.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the media file in the file system.
Latitude	The latitude associated with the media file.

Attribute	Description
Longitude	The longitude associated with the media file.
Country	The country associated with the media file.
Locale	The locale associated with the media file's location data. This can be a municipality or settlement depending on the location.
Face Count	The number of faces recognized by AI in the media file.
Image Recognition Objects	AI generated object names for objects in the media file.
Image Recognition Metadata	The AI generated percentages by which people in the media file belong to age group and gender categories.
Media	The media file, if recovered successfully.

Additional Information

Videos

Description	Videos contains videos that are recovered using parsing or carving. Supported formats for parsing include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. Supported carving formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. For more information about supported video formats, see Supported media and file types.
Recovery method	Parsing

Attribute	Description
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
File Name	The name of the file.
File Extension	The extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was last modified.
File Size (Bytes)	The size of the video.
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed, including potential metadata located at the end of the video. "Partial" indicates that only Exif information in the header section of the video file was recovered, which should only occur with very large videos (in excess of the limit set in the options screen). "Failed" indicates that the information may

Attribute	Description
	have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The resolution of the video (extracted from Exif data).
Original Height	The resolution of the video (extracted from Exif data).
Exif Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was first recorded (extracted from Exif data).
Exif Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the video being recored (extracted from Exif data).
Software	The software used to record or modify the video. This could either be the OS version of the phone used to record the video or name of the software used to edit the video in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to record the video (extracted from Exif data).
Model	The model of the camera used to record the video (extracted from Exif

Attribute	Description
	data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to record the video (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS latitude coordinates of the camera where the video was recorded (extracted from Exif data).
Longitude	The GPS longitude coordinates of the camera where the video was recorded (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the video was recorded (extracted from Exif data).
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.
Content Format	The format of the carved video.
Container Format	The format of the carved video container.
Saved Video Size (Bytes)	The size of the carved video that was saved to the database.
Exif Data	A searchable field for all raw exif properties.

Additional Information
If AXIOM Process is configured to save a set amount of data from carved videos, any generated MD5 and SHA1 hashes are based on the saved data, not the full video. This behavior might cause issues when searching for known video hashes, as the hash for a carved video will differ from the actual video if it exceeds the size limit set in AXIOM Process. To learn more about Exif data for videos, see Extracting Exif data from videos.

Operating System

.DS_Store Records

Description	.DS_Store Records contains all the records extracted from .DS_Store files found on the computer. Each record represents a property of a file or a folder. The significance of this artifact is an indicator of high likelihood that the user of the computer was aware of these files and folders with a possibility of attributing a date to that awareness.
Recovery method	Parsing

Attribute	Description
Record Name	The name of the file or folder as stored in the .DS_Store file.
Record Type	The type of the record, or property, that is being logged in the .DS_Store file for a particular file or folder.
Record Value	The value of the property for the given file or folder.
Record Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was modified.

Attribute	Description
Record Path	The full path to the file or folder
.DS_Store Created Date/Time - UTC (yyyy-mm-dd)	The created date of the .DS_Store file from which the record was extracted.
.DS_Store Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date of the .DS_Store file from which the record was extracted.
.DS_Store Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date of the .DS_Store file from which the record was extracted.

Additional Information

In the Apple macOS operating system, .DS_Store (Desktop Services Store) is a hidden file that stores the display information of its containing folder, similar to the file desktop.ini in Microsoft Windows. The file tracks information such as icon positions, view settings, cached file size, cached last modified date, and even the choice of a background image. The .DS_Store is created and maintained by the Finder application in any folder that it accesses, even on remote file systems mounted from servers that share files (for example, via Server Message Block (SMB) protocol or the Apple Filing Protocol (AFP)). .DS_Store files are also included in archives created by macOS users, such as ZIP files, and they are backed up by some cloud file backup services. This means that the presence of .DS_Store Records artifacts on non-Mac evidence such as Windows, Mobile, or Cloud indicates that some of the data may have originated or have been accessed from a macOS computer at some point. For more information on .DS_Store files and their forensic significance see: .DS_Stores: Like Shellbags but for Macs.

Accounts Information

Description	Contains the login information and tokens for accounts on the Android device.
Recovery method	Parsing

Attribute	Description
User Name	The user name associated with the account.
Account Type	The type of account.
Service Name	The name of the application as the device sees it.
Password/Token	The password/token stored on the device to connect to the account.
Last Login Date/Time - UTC (yyyy-mm-dd)	The date and time of the last successful login.
Additional Information	Additional information on the service used by the account, such as the SHA-1 hash of the service.

Additional Information

Android Downloads

Description	Android Downloads contains file download information from a recovered Android device.

Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified.
Save Location	The absolute path on the device to the file downloaded.
Notification Package	The Android package name that the download was initiated in.
Bytes Downloaded	The bytes that were downloaded.
Total Bytes	The total bytes of the file.

Additional Information

File System Information

Description	File System Information contains all of the relevant information about the hard drives in use by the operating system.
Recovery method	Parsing

Attribute	Description
ID	The identifier of the hard drive.
Volume Serial Number	This field only applies to FAT and NTFS file systems. This is a 32-bit unsigned int value that is stored in Bios Paramter Block (BPB) and is showed in a special hex format â€“ XXXX-XXXX e.g. EABB-6573. For other file systems, the value of this field should show "n/a".
Full Volume Serial Number	This field is a 64-bit volume serial number that is only present in BPB of NTFS file system, for example AABBCCDDEEFF0011. For non-NTFS file systems, "n/a" is displayed for this field.
File System	The type of the file system (e.g "Microsoft NTFS").
Sectors per cluster	The number of sectors in a file system cluster.
Bytes per sector	The number of bytes per sector.
Starting Sector	The starting sector for this partition.
Ending Sector	The ending sector for this partition.
Total Sectors	Encase shows different values for this field based on how a volume is added to the case. For example, if you add just a volume (e.g. your local C:\ drive), it shows 123410271 for the number of sectors, but if you add your local physical drive 0 to the case and then select your C:\ volume in the "Entries" tree (note: your C drive would most likely have another letter in this tree, e.g. E:), then total number of sectors would be one more that the other value, i.e. 123410272. the value show for this field is taken from BPB, which matches the first value. The other value is shown when the parent physical drive is present probably comes from the partition table, and it counts VBR as well.

Attribute	Description
Total Clusters	The number of clusters comprising the file system.
Free Clusters	The number of unallocated clusters in the file system.
Total Capacity (Bytes)	This value is calculated by (Total Clusters) x (Cluster Size), which shows the capacity of the file system and not the volume containing it. The size of the volume would be higher than this value.
Unallocated Area (Bytes)	The number of unallocated bytes on the file system, which is calculated by (Number of free clusters) x (cluster size).
Allocated Area (Bytes)	This value is calculated by (Number of allocated clusters) x (cluster size).
Volume Name	The volume label stored in Volume Boot Record (VBR).
Volume Offset (Bytes)	The offset (in bytes) of the volume containing this file system from beginning of the disk. "0" is displayed if the image and/or drive being searched is the image of one volume. Encase shows the number of sectors for this field instead of the number of bytes.
Drive Type	The type of the hard drive.

Additional Information

Google Accounts

Description	Google Accounts contains the Google accounts that are currently signed in on any Google application on the device.
Recovery method	Parsing

Attribute	Description
Account Name	The account name of the user.
Display Name	The display name of the user.
Profile ID	The GAIA ID.
Profile Image URL	The URL for the user's profile image.

Additional Information

Wi-Fi Logs - Android

Description	Wi-Fi Logs - Android contains information about the Wi-Fi networks that a device has connected to.
Recovery method	Parsing

Attribute	Description
Network Name (SSID)	The name of the saved network.
BSSID	A unique identifier for the specific access point, which is often represented as the MAC address for the access point's wireless adapter.
Date/Time - Local Time (yyyy-mm-dd)	The date and time of the network connection. In instances where the year is missing from the source data, this value is represented as a string instead of a date/time.

Attribute	Description
First Connected Date/Time - Local Time (yyyy-mm-dd)	The date and time of the connection event.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Peer to Peer

Beam Transactions

Description	Beam Transactions provides information about any logged transactions that have been sent by the user on the app.
Recovery method	Parsing

Attribute	Description
Transaction ID	The unique identifier associated with the transaction.
Event Type	The type of transaction that occurred.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time when the cryptocurrency event took place.
Address	The cryptocurrency address the transaction was sent to.

Attribute	Description
Crypto Amount	The amount of cryptocurrency that was sent. The currency types are BEAM and GROTH.
Cost	The fee that was charged for the transaction.
Kernel ID	The unique identifier of the kernel associated with the transaction.
Note	The note that was sent with the transaction.

Additional Information

BRD Events

Description	BRD Events provides information about events triggered by the user while using the Breadwallet BRD app.
Recovery method	Parsing

Attribute	Description
Event Name	The name of the event that occurred.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time when the event took place.

Additional Information

BRD Transactions

Description	BRD Transactions provides information about any logged transactions that have been sent by the user on the app.
Recovery method	Parsing

Attribute	Description
Transaction ID	The unique identifier associated with the transaction.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time when the cryptocurrency transaction took place.
Address	The cryptocurrency address where the cryptocurrency transfer was deposited. Note: The address is currently only recovered for Bitcoin and Doge.
Crypto Amount	The amount and type of cryptocurrency that was transferred.

Additional Information

Coinbase Purchases

Description	Coinbase Purchases provides information about any cached crypto-currency purchases that have happened on the app. Cached purchase information may not exist in all cases.
Recovery method	Parsing

Attribute	Description
Crypto Amount	The amount of cryptocurrency that was purchased.
Cost	The total cost of the purchase.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the purchase action was created.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the purchase action was updated.
Payout Date/Time - UTC (yyyy-mm-dd)	The date and time when the purchase was paid out.
Unit Price	The price of the cryptocurrency unit at the time of the purchase.
Type	The type of purchase action that occurred.

Additional Information

Coinbase Transactions

Description	Coinbase Transactions provides information about any cached cryptocurrency transactions that have been sent by the user on the app. Cached transaction information may not exist in all cases.
Recovery method	Parsing

Attribute	Description
Address	The cryptocurrency address the transaction was sent to.
Crypto Amount	The amount of cryptocurrency that was sent.
Value	The total value of the cryptocurrency that was sent at the time of the transaction.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time when the cryptocurrency event took place.
Note	The note that was sent with the transaction.

Additional Information

Coinbase Users

Description	Coinbase Users provides information about the cached local user.
Recovery method	Parsing

Attribute	Description
Name	The name of the user.
ID	The user ID.
User Name	The username associated with the user.
Email	The email of the user.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the user was created.

Attribute	Description
Avatar URL	The URL targeting the user's avatar image.
Biography	The user biography.
State	The state/province the user resides in.
Country	The country the user resides in.
Address	The address of the user.

Additional Information

Coinomi Transactions

Description	Coinomi Transactions provides information about any logged transactions that have been sent/received by the user of the application. These records are carved and should be verified as they may include compressed or truncated data.
Recovery method	Carving

Attribute	Description
Transaction ID	The unique identifier associated with the transaction.
Event Type	The type of transaction that occurred. E.g. BitCoin, Doge, LiteCoin, etc.
Address	The cryptocurrency address the transaction was sent to.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time when the cryptocurrency event took place.

Additional Information

Exodus Transactions

Description	Exodus Transactions provides information about any cached crypto-currency transactions that have been sent or received by the user on the app. Cached transaction information may not exist in all cases.
Recovery method	Parsing

Attribute	Description
Transaction ID	The ID of the transaction.
Address	The cryptocurrency address the transaction was sent to or received from.
Crypto Amount	The amount of cryptocurrency in the transaction.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time when the transaction took place.
Type	The type of transaction that occurred, either Sent or Received.

Additional Information

Peer-to-Peer

Torrent Active Transfers

Description	Torrent Active Transfers contains information about the torrents that are active on the user's system.
Recovery method	Parsing

Attribute	Description
Torrent Name	The name of the torrent file.
Potential App Name	The name of the application that the torrent was potentially downloaded with.
Download Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file download was started.
Download Completed Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file download was completed.
Download URL	The URL to download the torrent.
Downloaded Bytes	The total number of bytes that has been downloaded.
Download Location	The location on the disk to where the torrent was downloaded.
Bytes Uploaded	The total number of bytes that the system has uploaded for this torrent.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the active transfer was last modified.

Additional Information

Torrent Feeds

Description	Torrent Feeds contains information about RSS feeds that a user subscribes to that contains torrents available for download.
Recovery method	Parsing

Attribute	Description
Feed Name	The name of RSS subscription feed.
Feed URL	The URL of the RSS subscription feed.
Torrent Name	The name of the torrent available for download from the feed.
Download URL	The URL to download the torrent.
Description	A description of the contents of the torrent.
Published Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent feed item was published.
Status	The status of the feed item, either 'Downloaded' or 'Not Downloaded'.

Additional Information

Torrent File Fragments

Description	Torrent File Fragments contains data that is carved or parsed from .torrent files that are used to download torrents from various networks on the Internet.
Recovery method	Carving

Attribute	Description
Name	The name of the torrent file
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file was modified.
Torrent Creation Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file was originally created.
Torrent Files	The files that are listed in the torrent to be downloaded.

Additional Information

Social Networking

Android Instagram Following

Description	Android Instagram Following contains information about the users that are being followed by the local user.
Recovery method	Parsing

Attribute	Description
ID	The unique identification number of a user.
User Name	The username of the user account.
Full Name	The full name of the user.
Biography	The biography written by the user.
External Access	A URL to an external website, provided by the user.
Blocked	Indicates whether the user being followed is blocked by the local user.
Status	Indicates the follow status of the local user (Following, Requested, and Not following).
Profile Picture URL	The URL to the profile picture of the user.
Account Type	The account status of the user (Private or Public).

Additional Information

Android Instagram Posts

Description	Android Instagram Posts contains the posts that a user has put onto Instagram.
Recovery method	Parsing

Attribute	Description
Post ID	The post ID.
ID	The ID of the user who made the post.
User Name	The username on Instagram.
Full Name	The full name of the user.
Comment Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the comment was created.
Text	The text for the given image.
Profile Picture URL	The URL to the profile picture of the user.
Downloaded Profile Picture	The downloaded profile picture.
Posted Image URL	The URL to the image that was posted.
Type	The type of the post.
Posted Date/Time - UTC (yyyy-mm-dd)	The date that the post was made.
Device Date/Time - UTC (yyyy-mm-dd)	The date that the user viewed the post.

Additional Information

Android Instagram Users

Description	Android Instagram Users contains information on users of Instagram.
Recovery method	Parsing

Attribute	Description
ID	The ID of the user.
User Name	The username of the user on Instagram.
Full Name	The full name of the user.
Profile Picture URL	The URL to the profile picture of the user.
Downloaded Profile Picture	The downloaded profile picture.

Additional Information

Android Meet24 Cache Records

Description	Android Meet24 Cache Records contains items cached by Meet24 to improve performance.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached item.

Attribute	Description
First Visited Date/Time - UTC (yyyy-mm-dd)	The first date and time that the URL was visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL was visited.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL cache was synced.
File Type	The type of file that was cached, if a file was cached.
Content Size	The size of the file that was cached, if a file was cached.
Picture	The bytes of a picture file, if a picture file was cached.
Content	The bytes of a non-picture file that was cached.

Additional Information

Android Meet24 Cookies

Description	Android Meet24 Cookies contains cookies that Meet24 uses for persistent data.
Recovery method	Parsing

Attribute	Description
Host	The host of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie is supposed to expire.
Path	The path of the cookie.

Additional Information

Android Tinder Accounts

Description	Android Tinder Accounts contains all of the recovered Android Tinder Accounts.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of current account owner.

Attribute	Description
Name	The name of the account user.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The last date and time that the account user was active.
Biography	A brief written biography about the users account.
Birthday (yyyy-mm-dd)	The birthday of the account user.
Profile Picture URL	The URL of the user's profile picture. A user might have more than one profile picture.
Distance (Miles)	The distance that the user is searching for matches.
Gender	The gender of the account user.

Additional Information

Android Tinder Matches

Description	Android Tinder Matches contains all of the recovered Android Tinder Matches.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the user whom you are matched with.
User Name	The name of the user whom you are matched with.

Attribute	Description
Created Date/Time	The creation date of the match entry in UTC.
Last Activity Date/Time	The last time that there was activity with the match in UTC.
Created Date/Time - Local Time (yyyy-mm-dd)	The creation date of the match entry.
Last Activity Date/Time - Local Time (yyyy-mm-dd)	The last time that there was activity with the match.
Gender	The gender of the matched user.
Message Count	The number of messages that were exchanged with the matched profile.
Viewed Profile	Whether or not the user has viewed the profile.
Draft Message	The contents of a pending draft message.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Android Tinder Messages

Description	Android Tinder Messages contains all of the recovered Android Tinder Messages.
Recovery method	Parsing and carving

Attribute	Description
Sender ID	The user ID of the user whom is part of this conversation and is sending.
Recipient ID	The user ID of the user whom is part of this conversation and is receiving.
Match ID	The ID of the match who the message is received from.
Message Sent Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the message was sent.
Message Sent Date/Time	The date and time when the message was sent in UTC.
Message Body	The body of the message.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Android Tinder Photos

Description	Android Tinder Photos contains all of the recovered Android Tinder Photos.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the user whom the picture belongs to.
User Name	The name of the user whom this picture belongs to.
Image URL	The URL to the Tinder photo.
Downloaded Image	The downloaded image.

Additional Information

Android Whisper Posts

Description	Android Whisper Posts contains the posts stored by the Whisper application.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username of the person at the time when the post was posted.
Text	The content of the post.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time that the post was posted.
Image URL	The URL to the image of the post.
Downloaded Image	The downloaded image from the post, if the option is turned

Attribute	Description
	on in Report Viewer.
Locale	The location of the user when the post was posted.
Latitude	The latitude of the user when the post was posted.
Longitude	The longitude of the user when the post was posted.
Hearts	The number of hearts the post has received.
Replies	The number of replies to the post.

Additional Information

To learn more about Whisper, see Artifact profile: Whisper.

Facebook

Facebook, being one of the most popular social networking sites in the world, presents numerous opportunities for gathering evidence. You can recover messages that are sent and received, status updates and wall posts, and pages and pictures that the user views. On mobile devices, you can also recover user profiles and contacts.

Facebook can provide background information about a user, as well as evidence of who they are communicating with or associated with. Status and location updates can provide details about where a user has been and what they've been doing.

Forensic notes

The Facebook Pictures artifact represents cached pictures found on the system that originated from Facebook. When caching pictures, Facebook names the pictures using a particular format which allows forensic tools to know that they come from Facebook. These pictures can be user profile pictures, friends' pictures, or any other picture that gets cached while browsing Facebook.

Artifacts

Related resources

How important are Facebook artifacts?

Recovering Facebook artifacts

Android Facebook Messages

Description	Android Facebook Messages contains Facebook messages recovered from the Android device.
Recovery method	Parsing and carving

Attribute	Description
Text	The content of the message.
Email	The email of the user sending a message.
Name	The display name of the user sending a message.
User Key	The facebook ID for the user sending a message.
Delivery Timestamp Date/Time	The delivery time of the message.
Send Timestamp Date/Time	The time when the message was sent.
Message ID	The unique ID of the message that was sent.

Attribute	Description
Message Source	Indicates if the message was sent from the web, messenger, chat, or mobile.
Latitude	The latitude coordinate in decimal degrees associated with the message.
Longitude	The longitude coordinate in decimal degrees associated with the message.

Additional Information

Android Facebook Pictures

Description	Android Facebook Pictures contains Facebook pictures that are recovered from the Android device.
Recovery method	Parsing

Attribute	Description
URL	The URL of the Facebook picture.
Filename	The file's absolute path on the device.
Image	The picture that was recovered.

Additional Information

Facebook Comments

Description	Facebook Comments contains information about comments that have been cached on the device. A cached comment does not necessarily imply that the local account interacted with the comment, just that it was cached on the device. Further investigation should be performed to confirm the user's activity.
Recovery method	Parsing

Attribute	Description
Author ID	The comment author's Facebook profile ID.
Comment	The message content of the comment.
Comment Created Date/Time - UTC (yyyy-mm-dd)	When the comment was created.
Post ID	The ID of the post on which the comment was made.

Additional Information

Facebook Contacts

Description	Facebook Contacts contains contact information stored by the Facebook application.
Recovery method	Parsing and carving

Attribute	Description
Profile ID	The Facebook profile ID of the contact.
First Name	The Facebook contact's first name.
Last Name	The Facebook contact's last name.
Display Name	The Facebook contact's display name.
Picture URL	The URL to the picture.
Phone Numbers	The contact's phone numbers.

Additional Information

Facebook Events

Description	Facebook Events contains information for events created on Facebook that have been cached onto the device. A cached event does not necessarily imply that the user interacted with the event, just that it has been cached on the device. Further investigation should be performed to confirm the user's activity.
Recovery method	Parsing

Attribute	Description
Event	Name of the event.
Host	The host of the event.

Attribute	Description
Host User ID	The user ID of the host.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time of the event.
Event End Date/Time - UTC (yyyy-mm-dd)	The date and time of the end of the event.
Time Range - Local Time (yyyy-mm-dd)	The local time range of the event relative to the user.
Timezone	The time zone of the event.
User Response	The user's attendance response to the event. This response includes Going if the user plans to attend, Invited if the user was invited but has not yet responded, and Maybe if the user is interested in attending.
Notifications	Indicates if the user has notifications turned on for the event. This indication includes Unwatched if the user is not following the event, Watched if the user is following the event, and Going if the user is planning to attend in which case notifications are turned on by default.
Event Type	The type of the event including if the event is private or public.
Location Type	The location type of the event.
Event Location	The location of the event.
Latitude	The latitude associated with the event.

Attribute	Description
Longitude	The longitude associated with the event.
Event URL	The Facebook URL of the event.
Event ID	The ID of the event.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Facebook Posts

Description	Facebook Posts contains information about posts that have been cached on the device. A cached post does not necessarily imply that the local account interacted with the post, just that it was cached on the device. Further investigation should be performed to confirm the user's activity.
Recovery method	Parsing

Attribute	Description
Author	The author of the post. The author could be a user, a page, or a group.
Author ID	The author ID of the post.
Post	The body of the post.
Title	The title of the post.

Attribute	Description
Posted Date/Time - UTC (yyyy-mm-dd)	When the post was created.
Type	The type of the post.
Visibility	The visibility of the post.
Latitude	The latitude associated with the post.
Longitude	The longitude associated with the post.
Page ID	The page ID that the post was posted to.
Parent ID	The parent post ID of the post.
Attachment Type	The type of the content that was shared in the post.

Additional Information

Facebook User/Friends

Description	Facebook User/Friends contains profile information for the Facebook users and friends recovered from the Android device.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the user/friend.
Friend/User	Indicates if the information is for the user or a friend.

Attribute	Description
Display Name	The display name of the user/friend.
First Name	The first name of the user/friend.
Last Name	The last name of the user/friend.
Email(s)	The user/friends email address(es).
User Image URL	The URL to the user/friends profile picture.
Image	The profile picture.
Phone Number	The user/friends phone number.
Other	Additional information about user/friend.
Birthday (yyyy-mm-dd)	The user/friends birthday.

Additional Information

Foursquare Check-ins

Description	Foursquare Check-ins contains information about the user's check-ins.
Recovery method	Parsing and carving

Attribute	Description
User ID	The user ID
User First Name	The user's first name.

Attribute	Description
User Last Name	The user's last name.
User Email	The email address of the account used to check in.
Check-In Date/Time - UTC (yyyy-mm-dd)	The date and time when the user checked-in to the specified locaiton.
Location Name	The name of the location that the user checked into.
Comment	The comment a user left about their check-in for the location.
Address	The address of the check-in location.
Latitude	The latitude of the check-in location.
Longitude	The longitude of the check-in location.
City	The city of the check-in location.
State	The state of the check-in location.
Country	The country of the check-in location.
Been Here Count	The number of times that the user has checked into this location.
User Gender	The user's gender.

Additional Information

Foursquare Locations

Description	Foursquare Locations contains the location information viewed in Foursquare.
Recovery method	Parsing and carving

Attribute	Description
Location Name	The name of the location.
Address	The address of the location.
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Distance (meters)	The distance the user is from the location.
City	The city of the location.
State	The state of the location.
Country	The country of the location.

Additional Information

Foursquare Searches

Description	Foursquare Searches contains the search terms used in Foursquare.
Recovery method	Parsing and carving

Attribute	Description
Search Term	The search term used within Foursquare.

Additional Information

Grindr Buddies

Description	Grindr Buddies contains the buddies and their details that were extracted from the current user's Android data.
Recovery method	Parsing and carving

Attribute	Description
Public ID	The ID of the user in the buddy list.
Display Name	The display name of the buddy.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The date and time when the buddy was last seen.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message that was sent or received from this buddy.
Description	The description of the buddy.
Age	The age of the buddy.
Height (cm)	The height of the buddy.
Weight (kg)	The weight of the buddy.

Attribute	Description
Ethnicity	The ethnicity of the buddy.
Type of User	The type of user.
Distance	The distance of the buddy from the current user.
Favorited	Indicates whether the buddy is a favorite buddy of the current user.
Facebook Account	The name of the user's linked Facebook account.
Instagram Account	The name of the user's linked Instagram account.
Twitter Account	The name of the user's linked Twitter account.

Additional Information

Grindr Messages

Description	Grindr Messages contains the messages (and their details) that were extracted from a user's Android data.
Recovery method	Parsing and carving

Attribute	Description
Sender ID	The ID of the sender of the message.
Receiver ID	The ID of the receiver of the message.

Attribute	Description
Conversation Partner	The buddy's display name the message was with.
Group ID	The ID of the group the message was sent in.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received.
Message Body	The body of the message.
Has Attachment	Whether or not the message has an attachment.
Read Status	The status of the message (Read or Unread).
Message Direction	Indicates whether the message was incoming to the device, or outgoing from the device.

Additional Information

GROWLr Chat Messages

Description	GROWLr Chat Messages contains the messages on the device that were sent or received through Growlr.
Recovery method	Parsing

Attribute	Description
Account ID	The ID of the other person that the message is with.

Attribute	Description
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent or received.
Message	The body of the message.
Message Type	Indicates whether the message was incoming or outgoing.
Message Status	The status of the message (Read or Unread).
Image Filename	The path to the image that is associated with the message.
Image	The attached image.
Voice Filename	The filename of the attached voice message.
Voice	The attached voice data.

Additional Information

GROWLr Notes

Description	GROWLr Notes contains the notes on Growlr that the user has made, and when they were last modified.
Recovery method	Parsing

Attribute	Description
Text	The body of the note.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the note was modified.

Additional Information

Instagram Direct Messages

Description	Instagram Direct Messages contains Instagram direct messages that are sent or received by the local user.
Recovery method	Parsing

Attribute	Description
Sender	The username of the sender of the message.
Recipient	The username of the recipient of the message.
Message	The message that was sent.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Direction	The direction of the message, relative to the source of the hit.
Picture	The picture attribute is empty for Android as recovered pictures are located in the Attachment attribute instead.

Attribute	Description
Attachment	The attachment that was sent.
Attachment Path	The path to the attachment that was sent.
Media URL	The URL to the media of the message.
Type	The message type.
Status	The status of the message.
Latitude	The latitude of the message.
Longitude	The longitude of the message.
Caption	The original message of a forwarded post.
Original Author	The original author of a forwarded post.
Original Date/Time - UTC (yyyy-mm-dd)	The original date and time of a forwarded post.
Chat ID	The ID of the chat.

Additional Information

Attachments can only be retrieved when searching a full physical extraction of a device.

Instagram Group Members

Description	Instagram Group Members contains information about the Instagram groups that the local user is a member of.
Recovery method	Parsing

Attribute	Description
Group Member	The username of the group member.
Group Name	The name of the group.

Additional Information

Instagram Media

Description	Instagram Media contains the media files that have been found inside the Insatgram application.
Recovery method	Parsing

Attribute	Description
Picture	The picture of the media, or a storyboard if the media is a video.
MIME Type	The MIME type of the media.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.

Attribute	Description
Size (Bytes)	The size of the media file.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
URL	The URL to the media.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

Instagram Profiles

Description	Instagram Profiles contains profile information for the users that the local user has had communications with, or has been referred to through direct message communications.
Recovery method	Parsing

Attribute	Description
User Name	The username of the profile.
Name	The name that is associated with the profile.
User ID	The user ID associated with the profile.
Profile Picture URL	The profile picture of the user's profile.
Local User	Indicates whether the profile belongs to a user logged into the device.
Is Private	Indicates whether the profile is private or not.
Biography	The biography of the user associated with the account.
Following	Indicates whether the user of the profile is following the local user.
Is Followed By	Indicates whether the local user is following the user profile.
Post Notifications	Indicates whether the local user has turned on post notifications for the user profile. This attribute is only populated if the local user is following this user profile.
Email	The public email address associated with this user profile.
Phone Number	The public phone number associated with the user profile.
Address	The public address associated with the user profile.
City	The city associated with the user profile.
ZIP/Postal Code	The ZIP/postal code associated with the user profile.
Latitude	The latitude of the location associated with the user profile.
Longitude	The longitude of the location associated with the user profile.

Additional Information

For Android devices, the Following attribute will always be empty.

Life360 Circle Members

Description	Life30 Circle Members contains information about the members of a circle. A circle is comprised of a group of individuals, such as a family, that the local user has created or has been added to by another circle member.
Recovery method	Parsing

Attribute	Description
Member ID	The unique member ID of the circle member.
First Name	The first name of the member.
Last Name	The last name of the member.
Email Address	The email address of the member.
Phone Number	The phone number of the member.
Circle Name	The name the circle.
Circle ID	The ID of the circle.

Additional Information

Life360 Local User Account

Description	Life360 Local User Account contains information about local user accounts.
Recovery method	Parsing

Attribute	Description
User ID	The unique ID of the local user.
First Name	The first name of the local user.
Last Name	The last name of the local user.
Email Address	The email address of the local user.
Phone Number	The phone number of the local user.

Additional Information

Life360 Messages

Description	Life360 Messages contains messages sent and received by the local user within a circle that they're a member of.
Recovery method	Parsing

Attribute	Description
Sender ID	The unique ID of the sender.
Sender Name	The name of the sender.
Recipient ID(s)	The ID(s) of the recipient(s).
Recipient Name(s)	The name(s) of the recipient(s).
Message Type	The type of the message.
Message	The message content.
Created Date/Time	The date and time when the message was created.
Picture URL	The URL of the picture on the Life360 server, if a picture is included in the message.
Read	The read status of the message.
Latitude	The latitude of the location, if the message is a map location.
Longitude	The longitude of the location, if the message is a map location.
Location Name	The name of the location if the message is a map location.
Location Acquired Date/Time	The date and time when the location was acquired if the message is a map location.

Additional Information

Life360 Places

Description	Life360 Places indicates favorite locations that are saved by the user or

	the application.
Recovery method	Parsing

Attribute	Description
Place Name	The name of the place. The name can be either user-defined or a default name defined by the application.
Place Address	The address of the place.
Circle ID	The ID of the circle where the place was found.
Owner ID	The owner ID of the place, if the place was created by user.
Latitude	The latitude of the place.
Longitude	The longitude of the place.

Additional Information

Life360 Trip Locations

Description	Life360 Trip Locations indicates the locations that the user visits (or passes by on the way to a destination). During a trip, the application will log locations at regular intervals along the way.
Recovery method	Parsing

Attribute	Description
Updated Date/Time	The date and time that the trip details were last updated. Updates to the trip can be triggered by the user or the application.
Circle ID	The circle ID of the user who created this trip.
User ID	The unique ID of the user who created this trip.
Start Date	The date that the trip happened (days begin at 12:00 AM local time).
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Start Date/Time	The date and time when the user arrived at the location.
End Date/Time	The date and time when the user left the location.
Location Name	The name of the location if it is a user created place.
Location Address	The address of the location.

Additional Information

LinkedIn Connections

Description	LinkedIn Connections contains information about LinkedIn users that have communicated with the local user account.
Recovery method	Parsing

Attribute	Description
Public ID	The public ID of the LinkedIn connection.
First Name	The first name of the LinkedIn connection.
Last Name	The last name of the LinkedIn connection.
Occupation	The occupation of the LinkedIn connection.

Additional Information

LinkedIn Messages

Description	LinkedIn Messages contains messages sent and received by the local user.
Recovery method	Parsing

Attribute	Description
Sender Name	The name of the sender.
Recipient Name(s)	The name(s) of the recipient(s).
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The body of the message.
Attachment Name	The name of attachment to the message.
Attachment URL	The URL of attachment to the message.

Attribute	Description
Attachment Type	The type of the attachment to the message.
File	The attachment file to the message.

Additional Information

LinkedIn Profile

Description	LinkedIn Profile contains information about the user accounts that the local user has used to log in on the device.
Recovery method	Parsing

Attribute	Description
UserName	The username of local user.
First Name	The first name of the local user.
Last Name	The last name of the local user.
Full Name	The full name of the local user.
Summary	A summary of the local user. This information is provided by the user and can indicate a number of different things, including the user's position or status.

Additional Information

LinkedIn Searches

Description	LinkedIn Searches contains information about the searches that a LinkedIn user has made on the local device.
Recovery method	Parsing

Attribute	Description
Search Keyword	The keyword used by the user as a search term.
Date/Time	The date and time when the search occurred.
Search Type	The type of the search. This fragment is only populated if the user has specified the type of search to execute.

Additional Information

Musical.ly Local Users

Description	Musical.ly Local Users contains all of the users that have logged in to Musical.ly on the local device.
Recovery method	Parsing

Attribute	Description
User Name	The user's login name.
User Nick-name	The user's chosen nickname.
User ID	The ID of the user in Musical.ly systems.
Account Description	The description that the user has given themself.
Image URL	The URL of the user's profile picture.
Instagram Account	The user's Instagram account.
Google Account	The user's Google account.
YouTube Chan-nel	The user's YouTube Channel.
IP Address	The public IP address of the device that the user logged in with.
Is Private	Indicates whether the user prevents others from discovering their profile (Yes or No).
Hide Location	Indicates whether the user keeps their geolocation inforomation hidden on their profile page (Yes or No).
Messaging Availability	Indicates who is able to message the user, as specified by the user (Public or Friends Only).
Country Code	The country code of the country that the user has set for themself.
Language	The language code of the language that the user has set for themself.

Additional Information
The country code and language of the local user cannot be retrieved on Android devices.

Musical.ly Messages

Description	Musical.ly Messages contains messages sent or received in Musical.ly.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message.
Recipient	The recipient of the message.
Message	The body of the message. This value is empty if a picture message was sent.
Direction	The direction of the message, relative to the source database.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was either received or sent on the local device.
Picture	The picture that was sent or received. This value is empty if a text message has been sent.
Read	Indicates whether or not the message has been read by the local device (Yes or No).
Message Status	The status of the message (Delivered or Pending Internet Connection).

Additional Information
The read status for messages cannot be retrieved from Android devices.

Musical.ly Posts

Description	Musical.ly Posts contains posts that Musical.ly has retrieved from the web.
Recovery method	Parsing

Attribute	Description
User Name	The username of the poster.
User Nickname	The nickname of the poster.
User ID	The ID of the poster.
Caption	The caption the user wrote for their post.
Picture	The locally cached post's preview picture.
Cached Video Size (Bytes)	The size of the locally cached post's video.
Video URL	The URL of the post's video.
Picture URL	The URL of the post's preview picture.

Additional Information
The picture and cached video of posts cannot be retrieved on Android devices.

Musical.ly Users

Description	Musical.ly Users contains all of the users that the local user has viewed in Musical.ly.
Recovery method	Parsing

Attribute	Description
User Name	The user's login name.
User Nickname	The user's chosen nickname.
User ID	The ID of the user in Musical.ly systems.
Account Description	The description that the user has given themself.
Profile Picture URL	The URL of the user's profile picture.
Instagram Account	The user's Instagram account.
Google Account	The user's Google account.
YouTube Chan-nel	The user's YouTube Channel.
Is Private	Indicates whether the user prevents others from discovering their profile (Yes or No).
Is Friend	Indicates whether the user is a friend of the local user in the source data-

Attribute	Description
	base (Yes or No).
Following	Indicates whether the local user in the source database is following this user (Yes or No).
Post Notifications	Indicates whether the local user wants to receive notifications when this user makes a post (Yes or No).
Hide Location	Indicates whether the user keeps their geolocation information hidden on their profile page (Yes or No).
Messaging Availability	Indicates who is able to message the user, as specified by the user (Public or Friends Only).
Country Code	The country code of the country that the user has set for themself.
Language	The language code of the language that the user has set for themself.

Additional Information
The country code and language of the user cannot be retrieved on Android devices.

Parler Activity - Android

Description	Parler Activity contains information about the posts and comments that the local user makes.
Recovery method	Parsing

Attribute	Description
Type	The type of activity (Post, Comment or Echo).
Post ID	The unique identifier associated with the post.
Comment ID	The unique identifier associated with the comment.
Creator ID	The unique identifier associated with the user who did the activity.
Body	The body of the post or comment.
Content Link	The URL of the post or comment.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the post or comment was created.
Parent ID	The unique identifier for the post or comment that this activity is a response to.
Comments Count	The number of comments on the post.
Deleted	Indicates whether the activity was deleted
Reposts Count	The number of times the activity has been reposted
Upvotes	The number of upvotes the activity has
Downvotes	The number of downvotes the activity has

Additional Information

Parler Users - Android

Description	Parler Users contains information about the local user account and any other users they've interacted with.
Recovery method	Parsing

Attribute	Description
ID	The unique identifier associated with the user.
User Name	The user name of the user.
Name	The name of the user.
Biography	The biography of the user.
Local Account	Indicates whether or not the user is the local user.
Joined Date/Time - UTC (yyyy-mm-dd)	The date and time the user joined Parler.
Verified	Indicates whether or not the user is verified on Parler.
Private	Indicates whether or not the user's account is private.
Followers	The number of followers the user has.
Following	The number of accounts the user is following.
Blocked	Indicates whether or not this user was blocked by the local user.
Posts Count	The number of posts the user has.
Likes Count	The number of likes the user has.

Additional Information

Pinterest Accounts

Description	Pinterest Accounts contains information about the accounts that the local user has logged in with on the device.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the local user.
Full Name	The full name of the local user.
Email	The email address of the local user.
Created Date/Time	The created date and time of the local user.
Gender	The gender of the local user.
Country	The country of the local user.
Locale	The location of the local user.
Profile Image URL	The profile image URL of the local user.
Active	The current status of the local user indicates whether the account is coming from an active database.

Additional Information

Pinterest Boards

Description	Pinterest Boards contains information about the boards that were created by local user.
Recovery method	Parsing

Attribute	Description
ID	The ID of the board.
Name	The name of the board.
Type	The category type of the board.
Description	The description of the board.
Created Date/Time	The created date and time of the board.
Website URL	The URL of the board.
Owner ID	The owner ID of the board.
Active Account	Active Account indicates whether the board is from the account that's currently logged in on the device.

Additional Information

Pinterest Following

Description	Pinterest Following contains information about the people or boards that

	local user follows.
Recovery method	Parsing

Attribute	Description
Type	Type indicates what is being followed (People or Board).
ID	The ID of the following.
Name	The name of the following.
Description	The description of the following.
Email	The email address of the following.
Created Date/Time	The created date and time of the following.
Country	The country of the following.
Locale	The location of the following.
Profile Image URL	The profile image URL of the following.
Website URL	The website URL of the following.
Active Account	Active Account indicates whether the following user is of the account that's currently logged in on the device.

Additional Information

Pinterest Messages

Description	Pinterest Messages contains messages or pins sent and received by the local user.
Recovery method	Parsing

Attribute	Description
Sender ID	The ID of the sender.
Sender Name	The name of the sender.
Recipient ID(s)	The user ID(s) of the recipient(s).
Recipient Name(s)	The name(s) of the recipient(s).
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The content of the message.
Pin Title	The title of the pin.
Pin Picture URL	The picture URL associated with the pin.
Attachment Name	The file name of the picture cache associated with the pin.
Attachment	The attachment associated with the pin.
Active Account	Active Account indicates whether the following user is of the account that's currently logged in on the device.

Additional Information

Pinterest Pins

Description	Pinterest Pins contains information about the items that the local user has pinned to their own board.
Recovery method	Parsing

Attribute	Description
Title	The title of the pin.
Description	The description of the pin.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the pin.
Website URL	The URL of the website associated with the pin.
Posted Image URL	The posted image URL associated with the pin.
Attachment Name	The name of the attachment associated with the pin.
Attachment	The attachment associated with the pin.
Pinner ID	The pinner ID of the pin.
Active Account	Active Account indicates whether the following user is of the account that's currently logged in on the device.

Additional Information

Reddit Accounts

Description	Reddit Accounts contains information about the user accounts that are used to log in to the Reddit application on the device.
Recovery method	Parsing

Attribute	Description
User ID	The Reddit user ID.
Account ID	The unique account ID for the user.
Email Address	The email address of the user.
Icon URL	The URL to the user's account icon.
Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time of the Reddit account.

Additional Information

Reddit Posts

Description	Reddit Posts contains information about the posts recovered from the device. These posts might be ones the user has read or created on their device.
Recovery method	Parsing

Attribute	Description
Title	The title of the Reddit post.
Subreddit Name	The subreddit name where the post was posted.
Author	The author of the post.
Over 18	Indicates whether or not the post was flagged as mature content.
Content Link	The URL to content from the post if applicable, or the URL to the post if there is no external content.
URL	The URL of the post.
Saved	Indicates whether or not the post was saved by the user.
Read Date/Time - UTC (yyyy-mm-dd)	The date and time that the user read the post.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the post was created.

Additional Information

Reddit Recently Visited Subreddits

Description	Reddit Recently Visited Subreddits contains information about the subreddits that a user has recently visited while on their device.
Recovery method	Parsing

Attribute	Description
Subreddit Name	The name of the subreddit.
Sort Order	The order in which posts were sorted within the subreddit (e.g. New, Hot, Top, Controversial).
Sort Time Frame	The time frame in which posts were sorted within the subreddit (e.g. Day, Week, Month, Year).
Description	The public facing description of the subreddit.
User Name	The user who visited the subreddit.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the user last visited the subreddit.
Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time of the subreddit.

Additional Information

Sina Weibo Posts

Description	Sina Weibo Posts contains Sina Weibo posts that are recovered from a device.
Recovery method	Parsing and carving

Attribute	Description
User ID	The unique identifier for the user posting.
User Nickname	The user's nickname.
Post Date/Time - UTC (yyyy-mm-dd)	The date and time that the content was posted.
Post	The content of the post.
Profile Image URL	The URL for the profile image of the user.
Downloaded Profile Image	The raw content of the user's profile image, downloaded from the URL shown in the Profile Image URL column.
Post Image URL	The URL of the image in the post, if applicable.
Downloaded Post Image	The raw content of the image in the post, if applicable, and is downloaded from the URL shown in the Post Image URL column.
Posted Source	Information that describes the device from where the post was made.
Latitude	The latitude of the post's source device when the post was made.
Longitude	The longitude of the post's source device when the post was made.

Additional Information

Sina Weibo Private Messages

Description	Sina Weibo Private Messages contains Sina Weibo messages that are recovered from a device.
Recovery method	Parsing

Attribute	Description
Conversation Partner ID	The unique ID of the conversation partner.
Conversation Partner	The name of the conversation partner.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent/received.
Message	The actual private message content.
Profile Image URL	The URL for the profile image of the user.
Downloaded Profile Image	The raw content of the user's profile image, downloaded from the URL shown in the Profile Image URL column.
Attachment Type	The type of attachment associated with the message.
Attachment Local File Path	The local path to the file attachment.

Additional Information

TikTok Contacts

Description	TikTok Contacts contains information about a user's contacts in TikTok.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username of the contact.

Attribute	Description
Nickname	The nickname of the contact.
ID	The unique ID of the contact.
Profile Picture URL	The URL of the profile picture of the contact.

Additional Information

TikTok Media

Description	TikTok Media contains media that were either viewed or created by the user.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
File Extension	The extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the media file was created.
Last Accessed Date/Time - UTC (yyyy-	The date and time when the media file was last accessed.

Attribute	Description
mm-dd)	
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the media was last written to.
Type	The type of the media (Video or Photo).
Status	The status of the media (Cached, Draft, Published, Watched). Media that are reported as a Cached may not imply that the media was watched by the local user but that it was swiped on their Home feed. Further investigation should be performed to confirm which videos were watched by the local user.
Skin Tone Percentage	The amount of skin tone found in the video.
File Size (Bytes)	The size of the video.
MD5 Hash	An MD5 hash of the video content. If frames are not generated properly for the video, then the file was truncated due to the entire video not being cached on the device. The MD5 hash reported is generated using the available portion of the video.
SHA1 Hash	A SHA1 hash of the video content. If frames are not generated properly for the video, then the file was truncated due to the entire video not being cached on the device. The SHA1 hash reported is generated using the available portion of the video.
Category	An integer that indicates the Project VIC category for the video.

Attribute	Description
Attachment	The media.
Recorded Audio	The audio track recorded with the media.
Sound	The sound file added to the media.
Duration	The duration of the video in seconds, taken from the file metadata.
Caption	The text for any captions that the media had.
Recorded From Camera	Indicates if the video was recorded from the camera of the device in iOS draft videos.
Muted	Indicates if the microphone of the device was muted in iOS draft videos.

Additional Information

For cached videos recovered from the cachev2 directory, AXIOM Process repairs the file header to enable video previewing in AXIOM Examine. If you create a report with attachments from the Artifacts explorer, the exported video attachment will contain the modified header. To export the original file, find the original source in the File System explorer in AXIOM Examine and export from this location. The MD5 hash and SHA1 hash are generated using the repaired video file.

Draft videos may come in the form of separate files for the video, audio, and added sound. In these cases, the hit will include a complete video made from the combined video, audio, and sound, as well as each component file.

TikTok Messages

Description	TikTok Messages contains information about the messages that a user

	sends or receives using TikTok.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the message.
Recipient	The recipient of the message.
Message	The content of the message.
Message Type	The type of the message.
Media URL	The URL of any media attached to the message.
Created Date/Time	The time that the message was sent.
Read	Whether the recipient has read the message.
Deleted	Whether the message has been deleted.

Additional Information

Tumblr Blogs

Description	Tumblr Blogs contains information about the blogs that the user has interacted with. These blogs can include both followed and blocked blogs, though it's not currently possible to distinguish between the two.
Recovery method	Parsing

Attribute	Description
Blog Title	The title of the blog.
Description	The description of the blog.
Creator Name	The name of the blog's creator.
URL	The URL to the blog.

Additional Information

Tumblr Chat Messages

Description	Tumblr Chat Messages contains messages that were sent and received using Tumblr.
Recovery method	Parsing

Attribute	Description
Sender	The display name of the user who sent the message.
Recipient	The display name of the user who received the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The body of the message.
Media URL	The URL of any media attached to the message.

Attribute	Description
Entry ID	The database ID of the request or response from the Tumblr application.

Additional Information

Tumblr Tags

Description	Tumblr Tags contains information about the subject tags that the local user has selected. Selecting a tags expresses the user's interest in a subject so they can see more content of that type.
Recovery method	Parsing

Attribute	Description
Tag	The tag that the local user selected.

Additional Information

Twitter Direct Messages

Description	Twitter Direct Messages contains carved and noncarved direct messages from the Twitter application. Note: Carving will not retrieve the names and screen names of the sender and receiver. Also, carving may be unable to retrieve the message direction on newer versions of Twitter.

Recovery method	Parsing and carving

Attribute	Description
Text	The text of the direct message.
Sender ID	The Twitter ID of the sender.
Recipient ID(s)	The Twitter ID for the recipient(s).
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time that the direct message was sent or received.
Direction	Whether the message was sent or received.
Sender Name	The name of the person sending the direct message.
Sender Screen Name	The screen name or Twitter handle of the person sending the direct message.
Recipient Name(s)	The name(s) of the person(s) receiving the direct message.
Recipient Screen Name(s)	The screen name(s) or Twitter handle(s) of the person(s) receiving the direct message.
Attachments	The attachments associated with the direct message.

Additional Information

Twitter Tweets

Description	Twitter Tweets contains carved and noncarved tweets from the Twitter application.
Recovery method	Parsing and carving

Attribute	Description
Author ID	The numeric ID of the account that posted the tweet.
Status ID	The unique ID of the tweet.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the tweet was created.
Tweet	The text content of the tweet.
Favorited	Whether the tweet has been favorited.
Latitude	The latitude of the location from which the tweet was posted.
Longitude	The longitude of the location from which the tweet was posted.
Retweet Count	The number of times that the tweet has been retweeted.
Tweet Source	The interface that was used to post the tweet.

Additional Information

Twitter Users

Description	Twitter Users contains information about users that were cached on the local user's device.
Recovery method	Parsing and carving

Attribute	Description
User ID	The user's Twitter user ID.
User Name	The user's Twitter username.
Full Name	The user's full name.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the user's Twitter profile was created.
Description	The short profile description that the user writes for themself.
Web URL	The user's website URL.
Following	'Yes' if the local user is following this account, 'No' otherwise. If this attribute is empty, it's undetermined whether the local user is following this account.
Locale	The location the user is from.
Protected	Whether or not the user's account was protected.
Followers	The number of followers that the user has.
Friends	The number of friends that the user has.

Attribute	Description
Statuses	The number of different statuses that the user has had.
Image URL	The URL to the user's profile picture.
Friend Metadata Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the user's meta information was last updated.
Header URL	The URL to the user's profile banner picture.

Additional Information

VK Messages

Description	VK Messages contains VK messages (either private or group messages) as well as the details about pictures, video, and audio that may have been sent.
Recovery method	Parsing and carving

Attribute	Description
Sender ID	The user ID of the message sender.
Receiver ID(s)	The user ID of the message recipient. This column can contain multiple user IDs if the message is from a group conversation.
Message Date/Time -	The date and time that the message was sent/received.

Attribute	Description
UTC (yyyy-mm-dd)	
Message Text	The message text that was sent/received.
Type	The type of message sent. The possible types are 'Private Message' for one-to-one conversations or 'Group Message' for one-to-many conversations.
Message Deleted	The deletion state of the message is unsupported in VK Android and will therefore be empty.
Read State	The read state of the message is unsupported in VK Android and will therefore be empty.
Forwarded Message Content	This column contains the original time that a message was sent, the user ID that originally sent the message, and the content (for example, text, video, or audio).
VK Attachment	This column contains details of the attachment that was sent. For picture attachments, a URL to a scaled picture is provided for downloading. When a video is sent, a thumbnail is provided with details of the video (title, date/-time, duration and description). When audio is sent, a URL to the audio is provided as well as the title, artist, and duration.
Latitude	The latitude in VK Android will be contained within VK Attachment or Forwarded Message Content and this column will be empty.
Longitude	The longitude in VK Android will be contained within VK Attachment or Forwarded Message Content and this column will be empty.
Attachment	The attachment that was sent.

Additional Information

The latitude and longitude attributes of this artifact typically only include data if the message has a Geo Location attachment. VK for Android stores location data as an attachment within a BLOB column, and if there are multiple attachments, one VK Messages item could include more than one latitude and longitude. To avoid confusion or displaying incorrect information, the location information typically appears in the attachment or forwarded message content.

VK Users

Description	VK Users contains the various users the data owner has been in communication with, as well as the users own profile.
Recovery method	Parsing and carving

Attribute	Description
User ID	The user ID of the user.
Gender	Identifies whether the user is a male or female.
Birthdate (yyyy-mm-dd)	The birthdate of the user.
First Name	The first name/given name of the user.
Last Name	The last name/surname of the user.
Profile Image	The URL to the users profile image.
Downloaded Profile Image	

Additional Information

Whisper Messages

Description	Whisper Messages contains the messages that were sent and received between the local user and others.
Recovery method	Parsing and carving

Attribute	Description
Partner Name	The username of the person the chat was with.
Message Text	The content of the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Status	The status of the message (Received or Sent).
Read	Whether or not the message was read by its recipient.
Image	The image that was sent or received.

Additional Information
To learn more about Whisper, see Artifact profile: Whisper.

Web Related

Aloha Browser Autofill

Description	Aloha Autofill contains records of the autofill values that Aloha saves for dif-

	ferent types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill was last used.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Aloha Browser Bookmarks

Description	Aloha Bookmarks contains the webpages that a user has bookmarked.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.

Attribute	Description
Title	The name of the bookmark.
Parent	The name of the parent folder of the bookmark
Is Folder	Indicates whether the bookmark entry is a folder.

Additional Information

Aloha Browser Downloads

Description	Aloha Browser Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download URL	The URL of the file that was downloaded.
File Path	The absolute path on the device to the file downloaded.
URL	The URL of the site in which the file was downloaded.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was downloaded.

Additional Information

Aloha Browser History

Description	Aloha Browser History contains information about the websites that the user visits.
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the user first visited the webpage.
Title	The title of the webpage.
Visit Count	The number of times the user has visited that webpage.

Additional Information

Android Browser Bookmarks

Description	Android Browser Bookmarks contians the webpages that a user has book-marked.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Name	The name of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date/time when the bookmark was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date/time when the bookmark was last modified.
Is Folder	Indicates whether the bookmark entry is a folder.

Additional Information

Android Browser Search Terms

Description	Android Browser Search Terms contains information about the keyword search terms a user has provided in the browser.
Recovery method	Parsing

Attribute	Description
Search Term	The search term that the user entered.
Search Date/Time - UTC (yyyy-mm-dd)	The date/time when the search was entered.

Additional Information

Android Browser Web History

Description	Android Browser Web History contains information about the websites that the user has visited.
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Title	The title of the webpage that was visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date/time when the webpage was last visited.
Visit Count	The number of times the webpage was visited.

Additional Information

Android Firefox Bookmarks

Description	Android Firefox Bookmarks contains bookmarks from the Firefox web browser on an Android device.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the bookmark.
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was last modified.
Keyword	Any keywords that have been associated with the bookmark. These keywords are user generated.
Description	A description of the bookmark.
Bookmark Data	Any tags that have been associated with the bookmarks. These tags are user generated.
Deleted	Indicates whether the bookmark was deleted (Yes or No).

Additional Information

Android Firefox Web History

Description	Android Firefox Web History contains the webpage history from the Firefox web browser on an Android device.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the webpage.
URL	The URL of the webpage.
First Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the person first visited the webpage.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage history was last modified.
Visit Count	The number of times that the user has visited that webpage.
Deleted	Indicates whether the webpage history was deleted (Yes or No).

Additional Information

Baidu Searches

Description	Baidu Searches Contains information about the search history using the Baidu application.
Recovery method	Parsing

Attribute	Description
Search Term	The term that was searched.

Attribute	Description
Picture Path	The path to the picture that was searched.
Picture URL	The URL of the picture that was searched.
Search Type	The type of search. The options are Text or Picture.
Search Date/Time	The date/time of the search.
File	The file associated with the search.

Additional Information

Baidu Web Visits

Description	Baidu Web Visits contains a history of the websites that the user visited using the Baidu application.
Recovery method	Parsing

Attribute	Description
URL	The URL of the website.
Web Page Title	The title of the webpage.
Visited Date/Time	The date/time when the URL was visited

Additional Information

Brave Autofill

Description	Brave Autofill contains records of the autofill values that Brave saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The autofill count.

Additional Information

Brave Bookmarks

Description	Brave Bookmarks contain bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was

Attribute	Description
	added.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was last visited.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Brave Cookies

Description	Brave Cookies contain cookies that Brave downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	The domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Brave Downloads

Description	Brave Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Saved To	The absolute path on the device to the downloaded

Attribute	Description
	file.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Brave FavIcons

Description	Brave Favicons contains the favicons that Brave displays in the address bar when visiting a website. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Brave Keyword Search Terms

Description	Information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Brave Tab History - Android

Description	A history of websites the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the web page (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Search Term	The value the user entered into a search.

Additional Information

Brave Top Sites

Description	A list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Additional Information

Brave Web History

Description	A history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Brave Web Visits

Description	A history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

Chrome

Google Chrome is free web browser developed by Google and is available on all major operating systems, for both mobile and desktop. As of 2016, Chrome usage represents over 70% of the world's total browser traffic.

Analyzing the websites a user visits and the time the visits occur can provide valuable insights about a user. One notable feature that Google Chrome has is that it allows users to sync their bookmarks, browsing history, and more across multiple platforms and devices by using cloud sync accounts.

Forensic notes

Web Visits vs Web History

Chrome has two distinct artifacts that are very similar nature: Chrome Web Visits and Chrome Web History. Both of these artifacts are recovered from the History database. Chrome Web History is parsed from the URLS table and only contains information for the last visited date of a particular website. Chrome Web Visits can contain multiple entries for the same website, giving the examiner a more complete look at browser usage if the user visited a website multiple times. For example, if a user visits www.magnetforensics.com six times, the Chrome Web History artifact displays only the last time the site is visited, while the Chrome Web Visits artifact potentially displays records for all six instances. Chrome Web Visits was added in a later version of Chrome than Chrome Web History.

Carved web history

The Chrome / 360 Safe Browser / Opera Carved Web History is essentially the same as Chrome Web History except that it's recovered using carving and you may find additional deleted hits with it. The 360 Safe and Opera browsers are included in this artifact because when the data is carved, it's not possible to tell which browser the hit comes from as they're all formatted the same way.

Autofill and profile data

Chrome stores field data that the user has previously input as autofill and profile settings. For example, if you visit magnetforensics.com and login to the customer portal, browsers automatically save your username (and other details) so that you don't have to type it in each time you visit the site. This data is helpful for recovering usernames and other information that your user has filled out on various sites.

Sessions and tabs

When the system has an active session available, Chrome stores the browsing activity as the Chrome Current Session and any tabs that are open as Chrome Current tabs. The previous session and tabs are maintained in Chrome Last Session and Chrome Last Tabs so that the user can restore the last session and tabs if Chrome is closed.

Artifacts

Related resources

Artifact profile: Google Chrome

How does Chrome's 'incognito' mode affect digital forensics?

Forensic email analysis: browser artifacts you may find on a PC or laptop

Chrome Affiliations

Description	Chrome Affiliations contains information about visited pages and the domains their affiliated domains. Typical examples are; login page, advertiser, or CDN affiliated with a larger domain.
Recovery method	Parsing

Attribute	Description
Name	The name of the website visited.
URL	The url of the page visited.
Domain	The domain the visited page is affiliated with.

Attribute	Description
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time of the last visit to the affiliated url.

Additional Information

Chrome Archived Keyword Search Terms

Description	Chrome Archived Keyword Search Terms contains keyword search terms that were archived by the browser.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Chrome Archived Web History

Description	Android Archived Web History contains an archived history of old

	webpage visits.
Recovery method	Parsing

Attribute	Description
URL	The URL where the archived web history is located.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.
Title	The title of the archived web history.
Visit Count	The total number of visits to the URL.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
ID	The ID for the web history archive.

Additional Information

Chrome Autofill Profiles

Description	Android Chrome Autofill Profiles contains profiles that Chrome uses to fill in forms with saved values.
Recovery method	Parsing

Attribute	Description
Name	The name for the autofill profile.
Email	The email used in the the autofill profile.
Number	The phone number used in the autofill profile.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the profile was last modified.
Company	The company name used in the autofill profile.
Address Line 1	The address Line 1 used in the autofill profile.
Address Line 2	The address Line 2 used in the autofill profile.
City	The city used in the autofill profile.
State	The state used in the autofill profile.
Zipcode	The ZIP code used in the autofill profile.
Country	The country used in the autofill profile.

Additional Information

Chrome Autofill

Description	Chrome Autofill contains records of the autofill values that Chrome saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was last used.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Chrome Bookmarks

Description	Chrome Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Chrome Cache Records

Description	Chrome Cache Records contains content that Chrome downloads and caches to speed up rendering times. Cached content can include pictures, text, HTML, JavaScript, and more.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached item.
Website	The website visted. This fragment will be empty for Android.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was first visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the record was last modified.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the cache was last synced with the server. This fragment will be emtpy for Android.

Attribute	Description
State	The state of the record. This may be Normal (Live), Doomed (Marked for Deletion), or Evicted (Deleted). This fragment will be emtpy for Android.
File Type	The type of file that was cached.
Content Size (Bytes)	The size of the cached file.
Picture	The cached picture if the file type is a picture. Otherwise, this column is empty.
Content	The cached file contents if the file type is not a picture. Otherwise, this column is empty.
File Name	The file name of the cached item.
MD5 Hash	An MD5 hash of the cached item if it is a picture. Otherwise, this column is empty.
SHA1 Hash	A SHA1 hash of the cached item if it is a picture. Otherwise, this column is empty.
PhotoDNA Hash	The hash of the cached item for PhotoDNA if it is a picture. Otherwise, this column is empty.

Additional Information

Chrome Cookies

Description	Chrome Cookies contains cookies that Chrome downloads from the Internet. These cookies contain information about the websites that a user vis-

	its.
Recovery method	Parsing

Attribute	Description
Host	The domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Chrome Current Session

Description	Chrome Current Session contains information about the browser session that's currently underway.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Title	The title of the webpage.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Current Tabs

Description	Chrome Current Tabs contains information about the tabs that are open in the current browser session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Title	The title of the webpage.

Attribute	Description
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Downloads

Description	Android Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the file that was downloaded.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the download began.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the download ended.
Saved To	The local path where the file was downloaded.
State	The state of the downloaded file.
Opened	Whether or not the download was opened by the

Attribute	Description
	user.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Chrome FavIcons

Description	Android Chrome Favicons contains the favicons that Chrome displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Chrome Keyword Search Terms

Description	Chrome Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Chrome Last Session

Description	Chrome Last Session contains information about the previous browser session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.

Attribute	Description
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Title	The title of the webpage.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Last Tabs

Description	Chrome Last Tabs contains information about the tabs that were open during the previous session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Title	The title of the webpage.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Logins

Description	Android Chrome Logins contains login information that a user provides in Chrome. Passwords are often encrypted, so you might not be able to recover them unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username of the login.
Password	The password of the login.
GUID	The GUID of the login found in the keychain.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the login was created.
Last Login Date/Time - UTC (yyyy-mm-dd)	The date and time when the login was last used successfully. If the login is unsuccessful for the page or account, this date and time will not be updated.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the login was last modified.
URL	The URL of the login page.

Additional Information

Chrome Saved Credit Cards

Description	Android Chrome Saved Credit Cards contains the credit card information saved by the user.
Recovery method	Parsing

Attribute	Description
Name On Card	The name of the person on the credit card.
Card Number	The number on the credit card.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the information was last modified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the card was last used.
GUID	The GUID of the user.
Expiry Date	The date the credit card is supposed to expire in month-year format.

Additional Information

Chrome Sync Accounts

Description	Chrome Sync Accounts contains information about the Chrome accounts that a user has logged in with. Chrome syncs data to the cloud so that a user can log in on multiple devices.
Recovery method	Parsing

Attribute	Description
Sync Id	The unique ID for the account that's used to sync data to the cloud.
Account Name	The name of the sync account.
Google Account	The GAIA ID of the sync account.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the sync account was synced.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the sync account was created.
Profile Picture URL	The profile picture URL of the sync account.
Active	Indicates whether or not the sync account is active.

Additional Information

Chrome Sync Data

Description	Chrome Sync Data contains information about the data that Chrome has synced to a user's account in the cloud.
Recovery method	Parsing and carving

Attribute	Description
Name	The name of the sync key.
Local Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the local system.
Server Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the server.
Local Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the local system.
Server Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the server.
Type	The type of data that is synced (bookmark, favicon, type URL, and so on).
Parsed Content	The type of parsed data.
Favicon Image	The actual favicon image.

Additional Information

Chrome Tab History

Description	Chrome Tab History contains a history of websites that the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
Entry ID	The unique ID of a webpage entry in a tab. iOS only.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request open the webpage. For example, the referrer source might be from Google or another third-party application.
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Search Term	The value that the user entered into a search.

Additional Information

Chrome Top Sites

Description	Android Chrome Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the site.
Rank	The rank of the website, where the rank is based on how frequently the website was visited. A value of 1 indicates the most frequent and values increment to 8 as frequency decreases. A value of -1 indicates a site that the user manually added to the list of top sites.
Thumbnail	The thumbnail of the site.

Additional Information

Chrome Web History

Description	Chrome Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Chrome Web Visits

Description	Android Chrome Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is link.
Visit Source	The source of the visit.

Additional Information
To learn more about the Transition Type fragment, sign in to the Support Portal to read the article Google Chrome transition types.

Dolphin Browser Bookmarks

Description	Dolphin Browser Bookmarks contains bookmarks from the Dolphin web browser on an Android device.
Recovery method	Parsing

Attribute	Description
Title	The title of the bookmark.

Attribute	Description
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was modified.
Visits	The number of times that the user visited this bookmark.

Additional Information
The Modified Date/Time field is always empty for Android.

Dolphin Browser History

Description	Dolphin Browser History contains the webpage history from the Dolphin web browser on an Android device.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the webpage.
URL	The URL of the webpage.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the user first visited the webpage.

Attribute	Description
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the user last visited the webpage.
Visits	The number of times that the user has visited the webpage.

Additional Information

DuckDuckGo Bookmarks

Description	DuckDuckGo Bookmarks contains information about the webpages that a user has bookmarked.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Name	The name of the bookmark.
Favorite	Indicates whether the link was added as a favorite. This value is not currently populated for Android.

Additional Information

DuckDuckGo Cookies

Description	DuckDuckGo Cookies contains cookies that DuckDuckGo downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

DuckDuckGo Current Tabs

Description	DuckDuckGo Current Tabs contains information about the tabs that are open in the current browser session.
Recovery method	Parsing

Attribute	Description
URL	The URL of the webpage.
Title	The title of the webpage.
Was Viewed	Whether the tab was viewed on the local device or not.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that URL was accessed.
Attachment Path	If a snapshot was saved for that tab, this fragment stores the path of the snapshot image file.
Attachment	If a snapshot was saved for that tab, this is the attachment.

Additional Information

DuckDuckGo Whitelisted Websites

Description	DuckDuckGo Whitelisted Websites contains information about domains that are trusted or protected from deletion by the user.
Recovery method	Parsing

Attribute	Description
Domain	The domain of the website.
Status	Whether the domain was whitelisted or fire proofed. Whitelisted indicates to DuckDuckGo that the domain should always be trusted. Fire proofed domains will keep the navigation data even if the user clicks the option 'Clear All Tabs and Data'.

Additional Information

Ecosia Autofill

Description	Ecosia Autofill contains records of the autofill values that Ecosia saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The count of the autofill.

Additional Information

Ecosia Bookmarks

Description	Ecosia Bookmarks contain browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Ecosia Cookies

Description	Ecosia Cookies contains cookies that Ecosia downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	The domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Ecosia Downloads

Description	Ecosia Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.

Attribute	Description
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Saved To	The absolute path on the device to the downloaded file.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Ecosia FavIcons

Description	Ecosia Favicons contains the favicons that Ecosia displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time when the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Ecosia Keyword Search Terms

Description	Ecosia Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Additional Information

Ecosia Logins

Description	Ecosia Logins contains login information that a user provides in Ecosia. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the data was created.
URL	The URL of the login page.

Additional Information

Ecosia Tab History

Description	Ecosia Tab History contains a history of websites that the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the webpage (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Search Term	The value that the user entered into a search.

Additional Information

Ecosia Top Sites

Description	Ecosia Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the site.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Additional Information

Ecosia Web History

Description	Ecosia Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Ecosia Web Visits

Description	Ecosia Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

Edge Chromium Bookmarks

Description	Browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Edge Chromium FavIcons

Description	Contains the favicons that Chrome displays in the address bar for the web-site that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Updated Date/Time - UTC (yyyy-mm-dd)	The last time the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Edge Chromium Keyword Search Terms

Description	Information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Edge Chromium Tab History

Description	A history of websites the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the web page (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Search Term	The value the user entered into a search.

Additional Information

Edge Chromium Web History

Description	A history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Edge Chromium Web Visits

Description	A history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

Firefox Add-ons

Description	Firefox Add-ons contains the add-ons from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
Name	The name of the add-on.

Attribute	Description
Version	The version the add-on.
Install Date/Time - UTC (yyyy-mm-dd)	The date and time when the add-on was installed.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the add-on was updated.
Extension Enabled	Indicates whether the add-on is enabled by the user.
Description	The description of the add-on.

Additional Information

Firefox Cache Records

Description	Firefox Cache Records contains the files that the Firefox web browser has cached on a device.
Recovery method	Parsing

Attribute	Description
URL	The URL of file that was cached.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cache file was created.
MIME Type	The MIME type of the file.

Attribute	Description
Content Size (Bytes)	The size of the cached file.
Image	A preview of the cached file, if the cached file is anything but a picture.
Content	The content of the cached file.

Additional Information

Firefox Cookies

Description	Firefox Cookies contains the cookies from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
Host	The host domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.

Attribute	Description
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie will expire, if it is set to expire.
Path	The path to the cookie.

Additional Information

Firefox FormHistory

Description	Firefox FormHistory contains the form history from the Firefox web browser on a device.
Recovery method	Parsing and carving

Attribute	Description
Field Name	The name of the field.
Value	The value of the field.
First Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the field was first used.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the field was last used.
Times Used	The number of times that the field was used.
ID	The unique ID of the field.

Additional Information

Firefox Web History

Description	Firefox Web History contains the webpages from the last active session from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
URL	The URL of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage.
Visit Count	The number of times that the webpage has been visited.
Typed	Indicates whether the user typed the URL (Yes or No).

Additional Information

Firefox Web Visits

Description	Firefox Web Visits contains all of the non-archived URL visits for Firefox.
Recovery method	Parsing

Attribute	Description
URL	The URL that was visited.
Title	The title of the page that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the page was visited.
Typed	Indicates whether the user typed the URL (Yes or No).
Transition Type	Identifies how the transition to the page happened.

Additional Information

Google Analytics First Visit Cookies

Description	Google Analytics First Visit Cookies contains information about Google Analytics first-visit cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Host	Contains the domain of the URL.
Creation DateTime	The date and time when the site was first visited.
Most Recent Visit Date/Time	The date and time of most recent session.

Attribute	Description
2nd Most Recent Visit Date/Time	The date and time of previous session.
Hits	The number of visits.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics First Visit Cookies Carved

Description	Google Analytics First Visit Cookies Carved contains information about Google Analytics first-visit cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	Contains the domain of the URL.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Most Recent Visit Date/Time - UTC (yyyy-mm-dd)	The date and time of the most recent session.
2nd Most Recent Visit Date/Time - UTC (yyyy-mm-dd)	The date and time of the second most recent session.
Hits	The number of visits.

Additional Information

Google Analytics Referral Cookies

Description	Google Analytics Referral Cookies contains information about Google Analytics referral cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Cookie Source	The source URL used to reach the site.
Host	Contains the domain of the URL.
Update Date/Time	The last time the cookie was updated.
Campaign	The method of referral.
Access Method	Indicates whether the site was accessed organically or was referred.
Keyword	The keywords used to arrive at the site.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics Referral Cookies Carved

Description	Google Analytics Referral Cookies Carved contains information about Google Analytics referral cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	Contains the domain of the URL.
Last Update Date/Time - UTC (yyyy-mm-dd)	The last time the cookie was updated.
Cookie Source	The source URL used to reach the site.
Access Method	Indicates whether the site was accessed organically or was referred.
Campaign	The method of referral.
Keyword	The keywords used to arrive at the site.
Path to Page	

Additional Information

Google Analytics Session Cookies

Description	Google Analytics Session Cookies contains information about Google Analytics session cookies that are discovered in other artifacts.

Recovery method	Carving

Attribute	Description
Host	Contains the domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start time of the current sesion.
Outbound Link Events Left	
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics Session Cookies Carved

Description	Google Analytics Session Cookies Carved contains information about Google Analytics session cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	Contains the domain of the URL.
Start Current Session Date/Time	The start date and time of the current sesion.

Attribute	Description
Page Views	The number of visits to this page from the user.
Outbound Link Events Left	

Additional Information

Google Analytics URLs

Description	Google Analytics URLs contains URLs that are discovered in other artifacts that are related to Google Analytics.
Recovery method	Carving

Attribute	Description
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	Contains the domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.

Attribute	Description
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics URLs Carved

Description	Google Analytics URLs Carved contains information about Google Analytics URLs that are recovered using carving.
Recovery method	Carving

Attribute	Description
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all of the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	Contains the domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.

Additional Information

Iron Browser Autofill

Description	Iron Browser Autofill contains records of the autofill values that Iron Browser saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Iron Browser Bookmarks

Description	Iron Browser Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Iron Browser Cookies

Description	Iron Browser Cookies contains cookies that Iron Browser downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Iron Browser Downloads

Description	Iron Browser Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the downloaded was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the downloaded finished.
Saved To	The absolute path on the device to the file down-

Attribute	Description
	loaded.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Iron Browser FavIcons

Description	Iron Browser Favicons contains the favicons that Iron Browser displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Iron Browser Keyword Search Terms

Description	Iron Browser Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Additional Information

Iron Browser Logins

Description	Iron Browser Logins contains login information that a user provides in Iron Browser. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the data was created.
URL	The URL of the login page.

Additional Information

Iron Browser Tab History

Description	Iron Browser Tab History contains a history of websites that the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the webpage (for example, the referrer source might be from Google or

Attribute	Description
	another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Search Term	The value that the user entered into a search.

Additional Information

Iron Browser Top Sites

Description	Iron Browser Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Additional Information

Iron Browser Web History

Description	Iron Browser Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Iron Browser Web Visits

Description	Iron Browser Web Visits contains a history of the websites that the user visits (includes all visits).

Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

Kiwi Browser Autofill

Description	Kiwi Browser Autofill contains records of the autofill values that Kiwi Browser saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Kiwi Browser Bookmarks

Description	Kiwi Browser Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Kiwi Browser Cookies

Description	Kiwi Browser Cookies contains cookies that Kiwi Browser downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Kiwi Browser Downloads

Description	Kiwi Browser Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the downloaded was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the downloaded finished.
Saved To	The absolute path on the device to the file downloaded.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Kiwi Browser FavIcons

Description	Kiwi Browser Favicons contains the favicons that the Kiwi Browser displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Kiwi Browser Keyword Search Terms

Description	Kiwi Browser Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Additional Information

Kiwi Browser Tab History

Description	Kiwi Browser Tab History a history of websites the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the web page (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.

Attribute	Description
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Search Term	The value the user entered into a search.

Additional Information

Kiwi Browser Top Sites

Description	Kiwi Browser Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Additional Information

Kiwi Browser Web History

Description	Kiwi Browser Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Kiwi Browser Web Visits

Description	Kiwi Browser Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

Lunascape Autofill

Description	Lunascape Autofill contains records of the autofill values that Lunascape saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was last used.
Value	The saved autofill value for this type of field.
Count	The number of times that the autofill has been applied.

Additional Information

Lunascape Bookmarks

Description	Lunascape Bookmarks contains the webpages that a user has bookmarked.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Title	The name of the bookmark.

Additional Information

Lunascape Cookies

Description	Lunascape Cookies contains information about the cookies that the browser downloaded from the websites that the user has visited.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Lunascape History

Description	Lunascape History contains information about the websites that the user

	visits.
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.

Additional Information

Malware/Phishing URLs

Description	Malware/Phishing URLs contains records that are believed to be either malware or phishing related URLs.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the website.
URL	The URL of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time this is associated with the artifact.

Attribute	Description
Artifact	The name of the artifact that the URL belongs to.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Mi Browser Autofill

Description	Mi Browser Autofill contains records of the autofill values that Mi Browser saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Mi Browser Bookmarks

Description	Mi Browser Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was created.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Mi Browser Cookies

Description	Mi Browser Cookies contains cookies that Mi Browser downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	The domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Mi Browser Downloads

Description	Mi Browser Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.

Attribute	Description
File Name	The name of the file that was downloaded.
Downloaded Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was downloaded.
Saved To	The absolute path on the device to the downloaded file.
File Size (Bytes)	The file size of the download.

Additional Information

Mi Browser History

Description	Mi Browser History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.

Additional Information

Mint Browser Bookmarks

Description	Mint Browser Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was created.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Mint Browser Cookies

Description	Mint Browser Cookies contains cookies that Mint Browser downloads from the Internet. These cookies contain information about the websites that a user visits.

Recovery method	Parsing

Attribute	Description
Host	The domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Mint Browser Downloads

Description	Mint Browser Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the file that was downloaded.
Downloaded Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was downloaded.
Saved To	The absolute path on the device to the downloaded file.
File Size (Bytes)	The file size of the download.

Additional Information

Mint Browser History

Description	Mint Browser History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.

Additional Information

Naver Web History

Description	Naver Web History contains a record of all the websites a user has visited using the Naver browser. This artifact tracks the first instance and last instance that a user has visited a site.
Recovery method	Parsing

Attribute	Description
Title	The title of the website that the user visited.
URL	The URL of the website that the user visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the user last visited the website.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the user first visited the website.

Additional Information

Opera Autofill

Description	Opera Autofill contains records of the autofill values that Opera saves for different types of text fields.

Recovery method	Parsing and carving

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Opera Bookmarks

Description	Opera Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was added.
Name	The name of the bookmark.

Attribute	Description
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Opera Cookies

Description	Opera Cookies contain cookies that Opera downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing and carving

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie expires.
Path	The path of the cookie value.

Additional Information

Opera Downloads

Description	Opera Downloads includes information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the downloaded was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the downloaded finished.
Saved To	The absolute path on the device to the file downloaded.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Opera FavIcons

Description	Opera Favicons contains the favicons that Opera displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing and carving

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Opera Keyword Search Terms

Description	Opera Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing and carving

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Opera Top Sites

Description	Opera Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Additional Information

Opera Web History

Description	Opera Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Opera Web Visits

Description	Opera Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Indicates how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is link.
Visit Source	The source of the visit.

Additional Information

Pornography URLs

Description	Pornography URLs contains records of what are believed to be pornography related URLs.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the website.

Attribute	Description
URL	The URL of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact that the URL belongs to.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information
You can find a list of the domains that are supported by this refined result at Pornography URLs.

Potential Browser Activity

Description	The Browser Activity artifact will recover browser-related URLs. This includes Chrome Incognito and Firefox Private Browsing URLs, HTTP request artifacts from multiple browsers, and regular web browsing artifacts. This does not include metadata such as the Windows username, dates/times, and so on. Note that some recovered URLs can be from background browser processes related to certificate authorities, etc.
Recovery method	Carving

Attribute	Description
URL	The URL that the request was sent to.
User Agent	The string that represents the browser that sent the request.

Additional Information

Puffin Browser Bookmarks

Description	Contains bookmarks from the Puffin Browser for Android.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the bookmark.
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the user last visited the web page.
Visits	The number of times the user visited this bookmark.

Additional Information

Puffin Browser History

Description	Contains the web history for the Puffin Browser for Android.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the web page.
URL	The URL of the web page.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the user last visited the web page.
Last Accessed Date/Time - Local Time (yyyy-mm-dd)	The date and time the user last visited the web page.
Visits	The number of times the user has visited that web page.

Additional Information
Last Accessed Date/Time - Local Time is always empty for Android Puffin Browser History Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Rebuilt Webpages

Description	Rebuilt Webpages contains the data that allows for the reconstruction of webpages.
Recovery method	Not applicable

Attribute	Description
Page Title	The title.

Attribute	Description
URL	The URL.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the original record was created.
Domain	The domain.
Cache Table	The table that the data to re-construct the page came from.
Cache RowID	The row ID in the table that constructed the rebuilt webpage.

Additional Information

Samsung Browser Archived Keyword Search Terms

Description	Keyword search terms that were archived by the browser.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Samsung Browser Archived Web History

Description	Samsung Browser Archived Web History contains an archived history of old webpage visits.
Recovery method	Parsing

Attribute	Description
URL	The URL where the archived web history is located.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was visited.
Title	The title of the archived web history.
Visit Count	Total visits to this URL.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
ID	The ID for the web history archive.

Additional Information

Samsung Browser Autofill

Description	Samsung Browser Autofill contains a collection of saved values that were used to fill in forms and fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Value	The value.
Count	The count of the autofill.

Additional Information

Samsung Browser Autofill Profiles

Description	Samsung Browser Autofill Profiles contains the profiles that Samsung Browser uses to fill in forms with saved values.
Recovery method	Parsing

Attribute	Description
Name	The name for the autofill profile.
Email	The email used in the the autofill profile.
Number	The phone number used in the autofill profile.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the profile was last modified.
Company	The company name used in the autofill profile.

Attribute	Description
Address Line 1	The address Line 1 used in the autofill profile.
Address Line 2	The address Line 2 used in the autofill profile.
City	The city used in the autofill profile.
State	The state used in the autofill profile.
Zipcode	The Zip Code used in the autofill profile.
Country	The country used in the autofill profile.

Additional Information

Samsung Browser Bookmarks

Description	Samsung Browser Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Name	The title of the bookmarked page.
Account Name	The user account that created the bookmark.
Device ID	The ID of the device the bookmark was created on.

Attribute	Description
Device Name	The name of the device the bookmark was created on.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time whne the bookmark was last modified.
Deleted	Whether the bookmark has been deleted.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark (URL or Folder).

Additional Information

Samsung Browser Cache Records

Description	Content that Samsung Browser downloads and caches to speed up rendering times. Cached content can include pictures, text, html, javascript, and more.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached item.
First Visited Date/Time - UTC	The date and time the URL was first visited.

Attribute	Description
(yyyy-mm-dd)	
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time the cache was last synced with the cloud.
File Type	The type of file that was cached.
Content Size (Bytes)	The size of the cached file.
Picture	The cached picture if the file type is a picture. Otherwise, this column is empty.
Content	The cached file contents if the file type is not a picture. Otherwise, this column is empty.

Additional Information

Samsung Browser Cached Thumbnails

Description	Samsung Browser Cached Thumbnails contains thumbnail previews of the web pages that a user visits while using the browser.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached item.
Thumbnail	A partial screenshot of the web page which is used as a thumbnail.
Preview Image	A full screenshot of the cached web page.

Additional Information

Samsung Browser Cookies

Description	Samsung Browser Cookies contains cookies that Samsung Browser downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.

Attribute	Description
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Samsung Browser Current Session

Description	Information about the browser session that's currently underway.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Title	The title of the web page.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Samsung Browser Current Tabs

Description	Information about the tabs that are open in the current browser session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Title	The title of the web page.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Samsung Browser Downloads

Description	Information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.

Attribute	Description
File Name	The file name of the download.
Start Time Date/Time - UTC (yyyy-mm-dd)	The download start time.
End Time Date/Time - UTC (yyyy-mm-dd)	The download end time.
Saved To	The location that the download was saved to.
State	The state of the download.
Opened By User	Whether the download is opened by the user.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	File size of the download.

Additional Information

Samsung Browser FavIcons

Description	Contains the favicons that Samsung Browser displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	Page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	Last time the favicon was updated.

Attribute	Description
Icon URL	Icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Samsung Browser History Index

Description	An index of the webpages the user has visited in the past.
Recovery method	Parsing

Attribute	Description
Page URL	The URL of the webpage.
Visited On Date/Time - UTC (yyyy-mm-dd)	When the webpage was visited.
Title	The title of the webpage.
Body	A snippet of the webpage.

Additional Information

Samsung Browser Keyword Search Terms

Description	Information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Samsung Browser Last Session

Description	Information about the previous browser session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Title	The title of the web page.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Samsung Browser Last Tabs

Description	Information about the tabs that were open during the previous session.
Recovery method	Parsing

Attribute	Description
URL	The web page URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Title	The title of the web page.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Samsung Browser Logins

Description	Login information that a user provides in Samsung Browser. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the data was created.
URL	The URL of the login page.

Additional Information

Samsung Browser Media History

Description	Samsung Browser Media History contains information about the media files (audio and video) that the user views in the browser.
Recovery method	Parsing

Attribute	Description
Page URL	The URL of the page that contains the media file.
Video URL	The URL of the media file.
Title	The media title.
Thumbnail	The media thumbnail.
Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the user visited the page containing the media file.
Played (Seconds)	The duration of the media file that has been played, in

Attribute	Description
	seconds.
Duration (Seconds)	The full duration of the media file, in seconds.

Additional Information

Samsung Browser Saved Credit Cards

Description	Samsung Browser Saved Credit Cards contains information about the credit cards that a user has saved to their device.
Recovery method	Parsing

Attribute	Description
Name On Card	The name of the person on the credit card.
Card Number	The number on the credit card.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the information was last modified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time the credit card autofill information was last used.
GUID	An ID for the credit card.
Expiry Date	The date the credit card is supposed to expire in format 'month-year'.

Additional Information

Samsung Browser Saved Pages

Description	Samsung Browser Saved Pages contains information about web pages that were saved for offline viewing by the user. This includes basic page data, preview icon, user and device info. In addition, an .mhtml backup of the page is recovered, if it wasn't deleted.
Recovery method	Parsing

Attribute	Description
URL	The URL of the saved webpage.
Title	The title of the saved webpage.
Description	The brief description of the saved webpage.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the page was saved.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when saved page was last modified.
Icon	The preview icon for the saved page.
Deleted	Indicates whether saved page backup was deleted.
Account Name	The email account of the user that saved the page.
Device ID	The device ID.

Attribute	Description
Device Name	The device name.
Page Saved	The HTML content of the saved page. Uses .mhtml format instead of .html, which can affect display in various browsers.

Additional Information

Samsung Browser Shortcuts

Description	Contains all of the shortcuts used by Google Samsung Browser for user entered URLs.
Recovery method	Parsing

Attribute	Description
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - UTC (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the web page.
Times Used	The number of times the shortcut has been used.

Attribute	Description
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

Additional Information

Samsung Browser Tab History

Description	A history of websites the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the web page (for example, the referrer source might be from Google or another third-party application).

Attribute	Description
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Search Term	The value the user entered into a search.

Additional Information

Samsung Browser Tabs

Description	Samsung Browser Tabs contains information about the tabs that the user has opened in the browser (not including private browsing). This artifact can also recover tabs that were opened but deleted.
Recovery method	Parsing

Attribute	Description
Tab ID	The ID of the tab. This value can be used to identify specific tab files.
Tab URL	The URL of the website open in the tab.
Tab Title	The title of the website that's open in the tab.
Deleted	Indicates whether the tab has been deleted in the browser.

Attribute	Description
Account Name	The email account of the user that opened the tab.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was last modified.
Sync Date/Time - UTC (yyyy-mm-dd)	Indicates the date and time that the tab was last synced, if the browser on the local device is synced with another device.
Device Name	The device name.
Device ID	The device ID.

Additional Information

Samsung Browser Top Sites

Description	A list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the site was last updated.
Title	Title of the site.
Thumbnail	Thumbnail of the site

Additional Information

Samsung Browser Web History

Description	A history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Samsung Browser Web Visits

Description	A history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

Sleipnir Autofill

Description	Sleipnir Autofill contains records of the autofill values that Sleipnir saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was last used.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Sleipnir Bookmarks

Description	Sleipnir Bookmarks contains the webpages that a user has bookmarked.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was added.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was last updated.
Name	The name of the bookmark.

Attribute	Description
Type	The type of bookmark.
Parent Folder	The name of the parent folder of the bookmark.

Additional Information

Sleipnir Cookies

Description	Sleipnir Cookies contains information about the cookies that the browser downloaded from the websites that were visted by the user.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie expires.
Path	The path of the cookie value.

Additional Information

Sleipnir Search Terms

Description	Sleipnir Search Terms contains information about the keyword search terms that a user has provided in the browser.
Recovery method	Parsing

Attribute	Description
Search Term	The search term that the user entered.
URL	The URL of the keyword search.
Search Date/Time - UTC (yyyy-mm-dd)	The date and time when the keyword search took place.
Count	The number of times that the search occured.

Additional Information

Sleipnir Web History

Description	Sleipnir Web History contains information about the websites that the user visited.
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.

Additional Information

UC Browser Bookmarks

Description	UC Browser Bookmarks contains the webpages that a user has bookmarked.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Title	The title of the bookmark.
Is Folder	Indicates if the bookmark entry is a folder.

Additional Information

UC Browser Cookies

Description	UC Browser Cookies contains information about the cookies that the browser downloaded from the website that the user has visited.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

UC Browser Downloads

Description	UC Browser Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
File Name	The name of the downloaded file.
Saved To	The absolute path on the device to the file downloaded.
Download URL	The URL of the file that was downloaded.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the downloaded finished.
File Size (Bytes)	The file size of the download.

Additional Information

UC Browser History

Description	UC Browser History contains information about the websites that the user visits.
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.

Additional Information

WebKit Browser Session/Tabs (Carved)

Description	WebKit Browser Sessions/Tabs contains information about the browser sessions and tabs that the user has open, while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers, such as Firefox and Safari, aren't likely to appear under this artifact.
Recovery method	Carving

Attribute	Description
URL	The URL of the webpage.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

WebKit Browser Web History (Carved)

Description	WebKit Browser Web History contains information about the websites that a user visits while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers aren't likely to appear under this artifact, however, some URLs found by other browsers may also be found by this artifact.
Recovery method	Carving

Attribute	Description
URL	The URL of the visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited
Title	The title of the visited webpage.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the webpage was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Whale Autofill

Description	Whale Autofill contains records of the autofill values that Whale saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Whale Bookmarks

Description	Whale Bookmarks contans browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Whale Cookies

Description	Whale Cookies contains cookies that Whale downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-	The date and time when the cookie was created.

Attribute	Description
dd)	
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Whale Downloads

Description	Whale Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was finished.
Saved To	The absolute path on the device to the downloaded file.

Attribute	Description
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Whale FavIcons

Description	Whale Favicons contains the favicons that Whale displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Whale Keyword Search Terms

Description	Whale Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Additional Information

Whale Logins

Description	Whale Logins contains login information that a user provides in Whale. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username entered.
Password	The password entered.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the data was created.
URL	The URL of the login page.

Additional Information

Whale Tab History

Description	Whale Tab History contains a history of websites that the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the webpage (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.

Attribute	Description
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Search Term	The value that the user entered into a search.

Additional Information

Whale Top Sites

Description	Whale Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the site.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Additional Information

Whale Web History

Description	Whale Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Whale Web Visits

Description	Whale Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

Yandex Autofill

Description	Yandex Autofill contains records of the autofill values that Yandex saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.

Attribute	Description
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Yandex Bookmarks

Description	Yandex Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time whne the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Yandex Cookies

Description	Yandex Cookies contains the cookies that Yandex downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Yandex Downloads

Description	Yandex Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Saved To	The absolute path on the device to the downloaded file.
State	The completion state of the download.
Opened By User	Indicates whether the user opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Yandex FavIcons

Description	Yandex Favicons contains the favicons that Yandex displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time when the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Yandex Keyword Search Terms

Description	Yandex Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Yandex Logins

Description	Yandex Logins contains login information that a user provides in Yandex. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the data was created.
URL	The URL of the login page.

Additional Information

Yandex Shortcuts

Description	Yandex Shortcuts contains all of the shortcuts used by Yandex for user entered URLs.
Recovery method	Parsing

Attribute	Description
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - UTC (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the webpage.
Times Used	The number of times that the shortcut was used.
Transition Type	Describes how the browser navigated to the URL of the shortcut. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

Additional Information

Yandex Sync Data

Description	Yandex Sync Data contains information about the data that Yandex has synced to a user's account in the cloud.
Recovery method	Parsing

Attribute	Description
Name	The name of the sync key.
Local Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the local system.
Server Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the server.
Local Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the local system.
Server Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the server.
Type	The type of data that is synced (bookmark, favicon, type URL, and more).
Parsed Content	The type of parsed data.
Favicon Image	The actual favicon image.

Additional Information

Yandex Top Sites

Description	Yandex Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Additional Information

Yandex Web History

Description	Yandex Web History a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Yandex Web Visits

Description	Yandex Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.

Attribute	Description
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

YARA Rules

YARA Rule Matches

Description	The YARA artifact contains information about files and processes that matched with conditions specified in a YARA rule.
Recovery method	Parsing

Attribute	Description
File Name	The name and extension of the file whose content matched with the condition(s) from the YARA rule. The value is blank if the match came from a process (executable/application that was loaded into memory at the time of the memory dump) during memory analysis using the Comae plugin option.

Attribute	Description
File size (bytes)	The size of the file in bytes. The value is blank if the match came from a Process.
Process Name	The name of the process that matched with the condition(s) from the YARA rule. The value is blank if the match came from a file.
Process ID	The ID of the process (PID). The value is blank if the match came from a File.
Matched rule set(s)	List of the paths and respective YARA rule sets that had a match.
Matched rule	The YARA rule name that a match was found for.
Matching conditions	List of conditions for the YARA rule that had a match.

Additional Information

iOS

Advanced Search Tools

Dynamic Application Finder

Description	Artifacts found using the Dynamic Application Finder vary depending on your case's evidence. To learn more, see Processing details > Find more artifacts in the AXIOM User Guide.
Recovery method	Parsing

Attribute	Description

Additional Information

Application Usage

Apple Maps - Biome App Intents

Description	Apple Maps - Biome App Intents contains information about application intents from the Apple Maps app related to locations and navigation.
Recovery method	Parsing

Attribute	Description
Type	The type of app intent, such as Navigation, PlaceCardTap, etc.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the app intent was created.
Action	The intended action of the app intent, such as START_NAV, GET_DIRECTIONS, etc.
Status	The status of the app intent action, such as New Request, Continue, etc.
Location Name	The name of the location.
Address	The street address of the location.
City	The city of the location.
State/Province	The state or province of the location.
ZIP/Postal Code	The ZIP or postal code of the location.
Country	The country of the location.
ID	The ID of the app intent action.

Additional Information

Application Install States

Description	Application Install States contains a list of state changes that occur while an application installs or is uninstalled on an iOS device.
Recovery method	Parsing

Attribute	Description
Action	The type of change that occurred to the application.
Package Name	The internal name of the application.
Date/Time	The date and time that the event occurred.
Path	The file path to the package of the application.

Additional Information

Application Permissions - MacOS, iOS

Description	Application Permissions contains information about the application permissions that a user is prompted to accept or decline while using iOS applications.
Recovery method	Parsing

Attribute	Description
Application	The application that requests the permission.
Service Name	The permission service name.
Allowed	Indicates whether the application is allowed to use the service/permission.
Prompt Count	The number of times that the user was prompted to give the permission to the application.

Additional Information

Biome Application Focus

Description	Biome Application Focus provides information about the applications that were in focus on the device screen, within a recorded interval.
Recovery method	Parsing

Attribute	Description
Bundle ID	The bundle name of the application, used to uniquely identify it in the application store.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time of when the application was brought into focus.
End Date/Time - UTC (yyyy-mm-dd)	The date and time of when the application was removed from focus.
Metadata	Metadata relating to the application in focus.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time of when the Biome record was created.
GUID	The GUID of the Biome record.

Additional Information

Biome Application Install States

Description	Biome Application Install States provides information about when applications were installed on the device.

Recovery method	Parsing

Attribute	Description
Application Name	The name of the application.
Bundle ID	The bundle name of the application, used to uniquely identify it in the application store.
Type	The type of the application.
Install State	The install state of the application (Installed or Uninstalled).
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time when the Biome record was logged.
GUID	The GUID of the Biome record.

Additional Information

Biome Application Intents

Description	Biome Application Intents provides additional context and details about user interactions with the device. Application Intents are recorded by the system and are not always initiated by user interaction. For example, an intent is recorded when the user initiates a call and also when a call is received but isn't answered.
Recovery method	Parsing

Attribute	Description
Bundle ID	The bundle name of the application, used to uniquely identify it in the application store.
Type	The type of interaction intent as recorded by the device (e.g., SendMessage, StartCall).
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time when the Biome record was created.
GUID	The GUID of the Biome record.

Additional Information

Biome Application Launch

Description	Biome Application Launch provides information about when applications were launched on the device.
Recovery method	Parsing

Attribute	Description
Bundle ID	The bundle name of the application, used to uniquely identify it in the application store.
Transition Type	The type of transition used to launch the application.
Type	Indicates where the application was launched (Local or Remote).

Attribute	Description
Device ID	The ID of the remote device presented as a GUID.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time of when the Biome record was created.
Display Version	The display version of the application.
Internal Version	The internal version of the application.

Additional Information

Biome CarPlay Connections

Description	Biome CarPlay provides information about when the device was connected with a vehicle using CarPlay.
Recovery method	Parsing

Attribute	Description
Status	The status of the CarPlay connection (connected or disconnected).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the CarPlay period began.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the CarPlay period ended.
Recorded Date/Time - UTC (yyyy-	The date and time when the Biome record was logged.

Attribute	Description
mm-dd)	
GUID	The GUID of the Biome record.

Additional Information

Biome Device Orientation States

Description	Biome Device Orientation States provides information about the orientation of the device within recorded intervals.
Recovery method	Parsing

Attribute	Description
State	The orientation of the device (Portrait or Landscape).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the orientation period began.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the orientation period ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time when the Biome record was logged.
GUID	The GUID of the Biome record.

Additional Information

Biome Device Plugged-in States

Description	Biome Device Plugged-in States provides information about when the device was plugged in.
Recovery method	Parsing

Attribute	Description
GUID	The GUID of the Biome record.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the device was plugged in.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the device was unplugged.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time when the Biome record was logged.

Additional Information

Biome Device Screen Backlight States

Description	Biome Screen Backlight States provides information about the device back-light within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time. This information can help identify whether a device was in active use within a specific interval.
Recovery method	Parsing

Attribute	Description
State	The screen backlight state of the device. This value indicates whether the screen backlight is on or off.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started for First Backlight After Wakeup records.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended for First Backlight After Wakeup records.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.
Type	The type of record for the screen backlight state, which might have been retrieved from the public Backlight folder, or from the restricted _ DKEvent.User.IsFirstBacklightOnAfterWakeup folder.
GUID	The GUID of the Biome record.

Additional Information

Biome Do Not Disturb Status

Description	Biome Do Not Disturb Status provides information about when the device was put into the Do Not Disturb state.
Recovery method	Parsing

Attribute	Description
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the Do Not Disturb period began.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the Do Not Disturb period ended.
Status	The status of Do Not Disturb (On or Off).
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time when the Biome record was logged.
GUID	The GUID of the Biome record.

Additional Information

Biome Keybag Lock States

Description	Biome Keybag Lock States provides information about when the device was locked and unlocked. An absence of a recorded interval might mean that device was turned off during that time.
Recovery method	Parsing

Attribute	Description
State	The lock state of the device (locked or unlocked).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the device changed lock state.

Attribute	Description
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the current lock state ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time when the Biome record was logged.
GUID	The GUID of the Biome record.

Additional Information

Biome Safari History

Description	Biome Safari History provides information about webpages that were accessed using the Safari browser, as recovered from iOS Biome
Recovery method	Parsing

Attribute	Description
URL	The URL of the webpage that was accessed with Safari browser.
Title	The title of the webpage that was accessed with Safari browser.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was accessed with Safari browser.
Recorded Date/Time - UTC	The date and time that the Biome record was logged.

Attribute	Description
(yyyy-mm-dd)	
GUID	The GUID of the Biome record.

Additional Information

Biome Safari Page View

Description	Biome Safari Page View provides information about websites visited in the Safari application.
Recovery method	Parsing

Attribute	Description
Title	The title of the website.
URL	The URL of the website.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time when the Biome record was logged.
Content	The contents of the website in plain text.

Additional Information

Biome Siri Execution

Description	Biome Siri Execution provides information about the use of Siri.
Recovery method	Parsing

Attribute	Description
Intent Type	The intended function type executed by SiriKit (e.g., SendMessageIntent, StartCallIntent).
Bundle ID	The bundle name of the application executed, used to uniquely identify it in the application store.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time when the Biome record was logged.
GUID	The GUID of the Biome record.

Additional Information

Biome Siri UI Usage

Description	Biome Siri UI Usage provides information about the use of Siri.
Recovery method	Parsing

Attribute	Description
Value	Indicates either the start or the end of a Siri UI session.
Action Type	The type of interaction with Siri (e.g. VIEWMODE, dis-

Attribute	Description
	missalReason).
Triggers	The type of trigger for the action (e.g. User, HardwareButton, OutgoingPhoneCall, AppLaunch, Timeout).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the usage started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the usage ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time when the Biome record was logged.
GUID	The GUID of the Biome record.

Additional Information

Biome User Activity

Description	Biome User Activity provides information about various actions user performed on a device.
Recovery method	Parsing

Attribute	Description
Title	The title of the activity
Action Type	The activity type.

Attribute	Description
Service	The service associated with the activity.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time when the Biome record was logged.
Content Link	The content link associated with the activity.
Metadata	Includes extra details about the activity, such as draft messages, cached media, or email address, depending on the application.
GUID	The GUID of the Biome record.

Additional Information

Facebook Messenger - Biome App Intents

Description	Facebook Messenger - Biome App Intents contains information about application intents from the Facebook Messenger app related to sent and received messages and calls.
Recovery method	Parsing

Attribute	Description
Partner	The name of the conversation partner.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the app intent was created.
Type	The type of app intent, such as send message, call,

Attribute	Description
	etc.
Direction	Indicates whether the message was sent or received by the device.
Picture	The profile picture of the conversation partner.
Chat ID	The ID of the Facebook Messenger chat.

Additional Information

Instagram - Biome App Intents

Description	Instagram - Biome App Intents contains information about application intents from the Instagram app related to sent and received messages.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message.
Recipient	The recipient of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the sent message app intent was created.
Direction	Indicates whether the message was sent or received by the device.
Chat ID	The ID of the Instagram chat.

Additional Information

Installed Applications

Description	Installed Applications contains a list of all of the applications on an Android device, including their versions.
Recovery method	Parsing

Attribute	Description
Package Name	The internal name of the application.
Display Name	The display name of the application.
AXIOM Supported	The application that the data was recovered from, as defined by AXIOM artifact processing.
Icon	The icon for the application. Some icons may be converted from a propertiary Apple CgBI PNG image format to a standard PNG image format to display correctly.
Platform	The platform of the application.
Type	The type of application (either System or User).
Installed Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was installed.

Attribute	Description
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the application was last updated.
Display Version	The display version of the application.
Internal Version	The internal version of the application.
Secondary Package Names	If known by AXIOM, other internal names of the application, which are not the primary Package Name.
Application UID	The unique identifier of the application. Some applications reference a UID in their data instead of a package name. You can cross-reference this value with an application package name. Note that this attribute applies to Android only.
AppSource	The path of where the .app file application is located for the installed application.
Application Data	The path, or paths of where the user data is stored for the installed application
User Accessible Application	Whether it is a third party application, or a native application that can be executed by the user.

Additional Information

Note that different file paths from the Application Data attribute could contain similar content. This may occur when one file path is a symbolic link to another on the same device, linking between the original file and a copy created by a backup image.

InteractionC

The InteractionC artifacts reveal a high-level view of communications between users, across multiple applications based on identifiers (such as a phone number or email address). These artifacts can be recovered from both native and third-party applications on an iOS device.

Information about a user's contacts can be recovered, including identifiers and display names. The date and time, as well as the quantity and direction of a user's interactions can also be recovered. In an investigation, this data can be used to determine the extent of a user's interaction with a contact and any patterns in their interactions. This can be helpful when verifying a suspect's claim about their interactions (not including the content of messages).

Within the CoreDuet folder, InteractionC data is contained in the InteractionC database, which can only be recovered through file system extractions. There are different ways to extract the file system, including acquisition by GrayKey and jailbreaking.

Artifacts

InteractionC Interactions

InteractionC Contacts

InteractionC Contacts

Description	InteractionC Contacts contains information about the contacts that have been recorded as having interacted with the local user. This artifact can reveal a high-level view of how the local user communicates with a contact

	across multiple applications, provided that the contact uses the same identifier (for example, a phone number or email address).
Recovery method	Parsing

Attribute	Description
Identifier	The identifier of the contact being communicated with. This value can be an email, a phone number, or another unique identifier for the contact.
Display Name	The display name of the contact.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact was first recorded in the database. This value can coincide with the date and time of the first interaction, but in some cases, it appears that this value gets recorded without an interaction having occurred.
First Incoming Interaction Date/Time - UTC (yyyy-mm-dd)	The first recorded date and time of an incoming interaction.
Last Incoming Interaction Date/Time - UTC (yyyy-mm-dd)	The last recorded date and time of an incoming interaction.
First Outgoing Interaction Date/Time -	The first recorded date and time of an outgoing interaction.

Attribute	Description
UTC (yyyy-mm-dd)	
Last Outgoing Interaction Date/Time - UTC (yyyy-mm-dd)	The last recorded date and time of an outgoing interaction.
Incoming Interaction Count	The number of incoming interactions recorded between the local user and the contact.
Outgoing Interaction Count	The number of outgoing interactions recorded between the local user and the contact.

Additional Information

To learn more about InteractionC, see Artifact profile: InteractionC.

InteractionC Interactions

Description	InteractionC Interactions contains information about the individual interactions that occurred with a contact, and were tracked in the InteractionC database. Interactions can be phone calls, emails, or messages from one of many different applications (native and third-party).
Recovery method	Parsing

Attribute	Description
Bundle ID	The application bundle through which the interaction was initiated.
Display Name	The display name of the contact that was interacted with.
Sender	The sender of the interaction.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that an interaction was first recorded.
Start Date/Time - UTC (yyyy-mm-dd)	The first recorded date and time of an interaction.
End Date/Time - UTC (yyyy-mm-dd)	The last recorded date and time of an interaction.

Additional Information
To learn more about InteractionC, see Artifact profile: InteractionC.

iOS App Cache

Description	iOS App Cache contains a cache of web content from various applications on an iOS device.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached content.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date that the cached content was created on the local device.
Content	The raw cached content. If the content is an image, this field is blank and the Image column is populated instead.
File Type	The type of the cached file, such as HTML, JS, CSS, or JPEG.
Content Size (Bytes)	The size of the cached content in bytes.
Image	The raw content of the cached image. This field is blank if the content is not an image, as in the case of HTML, JavaScript, or CSS for example.

Additional Information

iOS Call Logs - Biome App Intents

Description	iOS Call Logs - Biome App Intents contains information about application intents from the iOS phone application.
Recovery method	Parsing

Attribute	Description
Partner	The phone number or email address of the conversation

Attribute	Description
	partner.
Partner Name	The name of the conversation partner.
Direction	Indicates whether the call was incoming or outgoing.
Call Date/Time - UTC (yyyy-mm-dd)	The date and time that the app intent was created.

Additional Information

iOS Device Information

Description	iOS Device Information contains information about the physical device, such as model information, the software version, timezone information, and the IMEI.
Recovery method	Parsing

Attribute	Description
IMEI(s)	The IMEI(s) associated with the device.
Unique Device Identifier	A SHA1 hash that represents a unique identifier for the device.
Serial Number	The serial number of the device.

Attribute	Description
Device Name	The name of the device.
Display Name	The display name of the device.
Model	The device model.
Model ID	The ID of the model.
Build Version	The version of the build.
ICCID	The ID of the integrated circuit card.
IMSI	The IMSI associated with the device.
Advertising ID	The advertising ID associated with the device.
Is Encrypted	Indicates whether the phone is encrypted. This value is True if the phone is encrypted, and is False otherwise.
Location Services Enabled	Indicates whether location services are enabled. This value is True if the location services have been enabled on this device, and is False otherwise.
Backup File Creation Date/Time	The date and time that the most recent backup file was created (this might represent an iTunes backup or iCloud backup).
Last iTunes Backup Date/Time	The date and time that the most recent iTunes backup file was created.
Last Cloud Backup Date/Time	The date and time that the most recent cloud backup file was created.
Backup Com-	The name of the computer that the device is backed up to.

Attribute	Description
puter Name	
Backup Computer Type	The type of the backup computer (for example, PC or MAC).
OS Version	The iOS version number.
iCloud Account Present	Indicates whether an iCloud account is present on the device.
iTunes Version	The iTunes version number.
Was Passcode Set	Indicates whether a password was set on the device.
Find My iPhone Enabled	Indicates whether Find My iPhone is enabled.
Bluetooth Address	The Bluetooth address of the device.
AirDrop ID	The AirDrop ID of the device.
Device Class	The class of device (iPhone).
MEID	The MEID associated with the device.
Service Provider Country Code	The country code given by the service provider.
Mobile Net-	The network code for the device.

Attribute	Description
work Code	
Model Number	The model number of the device hardware.
Device Date/Time - UTC (yyyy-mm-dd)	The time of the device's clock.
Timezone	The timezone for the device.
Timezone Setting	The timezone setting for the device. Can be 'Automatic' when the timezone is determined by the device, or 'Manual' when the timezone is set by the user.
Language	The language of the device.
Locale	The locale of the device.
UTC Offset	The timezone offset from UTC for the device.
MAC Addresses	The MAC addresses of the device.
Home Screen Wallpaper	The wallpaper used on the home screen for the primary user or account on the device. If this field is empty, then the home screen is the same picture as the lock screen.
Lock Screen Wallpaper	The wallpaper used on the lock screen for the primary user or account on the device. In some rare cases, there may be multiple lock screen directories found, which will be reported as sources in the hit and in the artifact log.

Additional Information

iOS iMessage/SMS/MMS - Biome App Intents

Description	iMessage/SMS/MMS - Biome App Intents contains information about application intents from the iOS Messages app related to sent and received messages.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message.
Recipient(s)	The recipient of the message.
Message	The message that was sent for the app intent. This fragment might contain the Object Replacement Character (U+FFFC), which indicates a non-text message is present, such as a picture, video, etc.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the sent message app intent was created.
Direction	Indicates whether the message was sent or received by the device.
Type	The type of message the app intent represents, such as iMessage, SMS, etc.

Additional Information

iOS Spotlight

Description	iOS Spotlight contains the iMessage/SMS/MMS messages that have been saved by the Spotlight application.
Recovery method	Parsing and carving

Attribute	Description
Partner	The partner of the iMessage/SMS/MMS.
Message	The content of the iMessage/SMS/MMS.
Summary	A summary of the content of the iMessage/SMS/MMS.

Additional Information

iOS User Shortcut Dictionary

Description	iOS User Shortcut Dictionary contains the shortcuts and phrases that a user has on their device.
Recovery method	Parsing and carving

Attribute	Description
Shortcut	The sequence of characters that indicate when a phrase should be written.

Attribute	Description
Phrase	The phrase that the user wants typed when a sequence of characters are typed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the shortcut and phrase were created.

Additional Information

iOS User Word Dictionary

Description	iOS User Word Dictionary contains the words that a user has typed on the device.
Recovery method	Parsing

Attribute	Description
Word	The word that the user has typed.

Additional Information

KnowledgeC Activity Level

Description	KnowledgeC Activity Level provides information about the KnowledgeC stream type of activity level.
Recovery method	Parsing

Attribute	Description
Activity Type	The activity level.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Application Activities

Description	KnowledgeC Application Activities contains information about activities associated with specific applications.
Recovery method	Parsing

Attribute	Description
Application Name	The bundle name of the application associated with activity.
Activity	The description associated with the activity.
Activity Type	The type of activity that occurred. This value displays the package where the activity orginates from.
URL	The URL associated with the activity, if one exists.

Attribute	Description
Event Date/Time - UTC (yyyy-mm-dd)	The date and time when the activity occurred.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Application Focus

Description	KnowledgeC Application Focus provides information about the applications that were in focus on the device screen, within a recorded interval.
Recovery method	Parsing

Attribute	Description
Application Name	The bundle name of the application in focus.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Application Install States

Description	KnowledgeC Application Install States provides information about when applications were installed or uninstalled on the device.
Recovery method	Parsing

Attribute	Description
Application Name	The bundle name of the application that was installed or deleted.
Install State	The install state of the application (Installed or Uninstalled).
State Changed Date/Time - UTC (yyyy-mm-dd)	The date and time that install state last changed.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Application Intents

Description	KnowledgeC Application Intents bring additional context and detail to user interactions with the device. Application Intents are recorded by the system and are not always initiated by user interaction. For example, an intent is recorded when the user initiates a call and also when a call is received but isn't answered.

Recovery method	Parsing

Attribute	Description
Intent Type	The type of interaction intent as recorded by the device.
Intent Class	The class of the intent.
Intent Action	The action that the user intended.
Bundle ID	The application bundle through which the action was initiated.
Metadata	Additional details about the intent. This can include items such as alarm times and details spoken to Siri.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time of the intent as recorded by the device.

Additional Information

KnowledgeC Application Usage

Description	KnowledgeC Application Usage provides information about the applications that were used on the device, within a recorded interval.
Recovery method	Parsing

Attribute	Description
Application Name	The bundle name of the application used.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Application Web Usage

Description	KnowledgeC Application Web Usage provides information about the applications that were used to access webpages on a iOS device, within a recorded interval.
Recovery method	Parsing

Attribute	Description
Application Name	The bundle name of the application that accessed the webpage.
Domain	The domain name of the webpage.
URL	The URL of the webpage.
Start Date/Time - UTC (yyyy-mm-	The date and time that the time interval started.

Attribute	Description
dd)	
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Device Lock States

Description	KnowledgeC Device Lock States provides information about whether the device is locked or unlocked within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time.
Recovery method	Parsing

Attribute	Description
State	The lock state of the device (Locked or Unlocked).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Device Orientation States

Description	KnowledgeC Device Orientation States provides information about the orientation of the device within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time.
Recovery method	Parsing

Attribute	Description
State	The orientation state of the device (Portrait or Landscape).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Device Plugged-in States

Description	KnowledgeC Device Plugged-in States provides information about the plugged-in state of a device within recorded intervals. An absence of a

	recorded interval might mean that device was turned off during that time. Knowing when a device is connected to a charger or a computer using a USB can help to identify how the device is used.
Recovery method	Parsing

Attribute	Description
State	The plugged-in state of the device. This value shows whether a device is plugged in and/or connected via USB (Plugged in or Unplugged).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Do Not Disturb Usage

Description	KnowledgeC Do Not Disturb Usage contains system activity information for the Do Not Disturb setting on the device.
Recovery method	Parsing

Attribute	Description
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Keybag Lock States

Description	KnowledgeC Keybag Lock States provides information about whether the device's keybag is locked or unlocked within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time.
Recovery method	Parsing

Attribute	Description
State	The lock state of the keybag (Locked or Unlocked).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Media History

Description	KnowledgeC Media History provides information about what type of audio or video media that the user was engaging with at what time, as recovered from knowledgeC.db
Recovery method	Parsing

Attribute	Description
Application Name	The bundle name of the application that was used to play the specified media.
Album	The album name of the specified media.
Title	The title of the specified media.
Artist	The artist of the specified media.
Duration (Seconds)	The duration of the specified media in seconds.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the media started playing.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the media stopped playing.

Additional Information

KnowledgeC Notification Usage

Description	KnowledgeC Activity Level provides information about the KnowledgeC stream type of activity level.
Recovery method	Parsing

Attribute	Description
Bundle ID	The bundle ID.
Type	The type of notification.
Device ID	The device ID.
Process ID	The process ID.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Safari History

Description	KnowledgeC Safari History provides information about webpages that were accessed using the Safari browser, as recovered from know-

	ledgeC.db
Recovery method	Parsing

Attribute	Description
URL	The URL of the webpage that was accessed with Safari browser.
Title	The title of the webpage that was accessed with Safari browser.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was accessed with Safari browser.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Screen Backlight States

Description	KnowledgeC Screen Backlight States provides information about the device backlight within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time. This information can help identify whether a device was in active use within a specific interval.
Recovery method	Parsing

Attribute	Description
State	The screen backlight state of the device. This value indicates whether the screen backlight is on or off.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Siri Intents

Description	KnowledgeC Siri Intents contains information about Siri interactions with the user's device.
Recovery method	Parsing

Attribute	Description
Event Type	The event type that triggered the Siri Intent.
Intent Type	The type of the Siri Intent.
Details	Additional details about the Siri Intent. This can include items such as message text and contact information.

Attribute	Description
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.
Metadata	The binary plist blob data parsed from the KnowledgeC database.
Additional Data	The protobuf data parsed from the KnowledgeC database blob data.

Additional Information

KnowledgeC Siri UI Usage

Description	KnowledgeC Siri UI Usage contains logs of the time windows that the Siri UI is in use.
Recovery method	Parsing

Attribute	Description
Value	Indicates either the start or the end of a Siri UI session.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

Screen Time Application Usage

Description	Screen Time Application Usage contains usage and notification information for all applications tracked by Screen Time. The application (and this artifact) tracks data in 60 minute intervals, so any usage and notification data applies only to that segment of time. This artifact can help identify when an application was in use and for how long, both on the local device and other devices that are synced under the same Apple ID/Family Account.
Recovery method	Parsing

Attribute	Description
Application Name	The bundle name of the application that's being tracked using Screen Time.
Domain	The name of the domain associated to the webpage that the user was visiting.
Interval Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the 60 minute interval. Screen time tracks usage in these hour-long blocks.
Total Time (Seconds)	The total time that was spent using the application within the time interval.
Notifications	The number of notifications received by the application within the time interval.

Attribute	Description
Pickups	The number of times that the application receives focus, such as when the application starts, or if the user switches contexts within the time interval.
Device Name	The name of the device where the application was used. It can be empty for cloud-synched data or all devices data.
Given Name	The given name of the user associated with the device.
Family Name	The last name of the user associated with the device.

Additional Information

Screen Time Synced Applications

Description	Screen Time Synced Applications contains list of all the applications that are being tracked using Screen Time. This list includes applications that are installed on the local user's device, or are installed on other devices connected to the same family account or use the same Apple ID.
Recovery method	Parsing

Attribute	Description
Application Name	The bundle name of the application that's being tracked using Screen Time.
Unique Device Identifier	The ID of the device where the application is installed.

Attribute	Description
Device Name	The name of the device where the application was installed.
Given Name	The given name of the user associated with the device.
Family Name	The last name of the user associated with the device.
Account Type	The family account type of the user associated with the device. The value is Unknown if a family account wasn't set.

Additional Information

Signal - Biome App Intents

Description	Signal - Biome App Intents contains information about application intents from the Signal app related to sent and received messages and calls.
Recovery method	Parsing

Attribute	Description
Partner	The name of the conversation partner.
Partner Phone Number	The phone number of the conversation partner.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the app intent was created.
Type	The type of app intent, such as send message, call, etc.
Direction	Indicates whether the call or message was sent or

Attribute	Description
	received by the device.
Chat ID	The ID of the Signal chat.

Additional Information

Siri - Biome App Intents

Description	Siri - Biome App Intents contains information about application intents from Siri related to the use of Siri and interactions with other applications.
Recovery method	Parsing

Attribute	Description
Application	The name of the application executed by the Siri app intent.
Type	The type of app intent, such as Show, Engagement, etc.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the app intent was created.
Metadata	The details of the intended action executed by the Siri app intent.

Additional Information

Snapchat - Biome App Intents

Description	Snapchat - Biome App Intents contains information about application intents from the Snapchat app related to sent and received messages.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message.
Recipient	The recipient of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the sent message app intent was created.
Direction	Indicates whether the message was sent or received by the device.
Chat ID	The ID of the Snapchat chat.

Additional Information

Spotlight Searches

Description	Spotlight Searches contains the keyword search terms that a user has entered in the Spotlight feature on iOS.
Recovery method	Parsing and carving

Attribute	Description
Search Term	The value that the user searched in Spotlight.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date/time when the protobuf was recorded in the Segb file.

Additional Information

Wallet Passes

Description	Wallet Passes contains information on passes (boarding passes, coupons, event tickets, store cards, and others) that have been saved to the user's Apple Wallet application.
Recovery method	Parsing

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Organization	The organization that issued this pass.
Description	A description of the pass.
Serial Number	The serial number of the pass. This is vendor-specific, so cannot be assumed to be unique across passes.
Type	The type of the pass, e.g. Boarding Pass.
Effective Date/Time - UTC	The date and time that the pass becomes relevant (e.g. a start date or boarding time).

Attribute	Description
(yyyy-mm-dd)	
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time that the pass is no longer relevant.
Header Fields	The content of the dynamic header fields structure in the file, which are supplied by the vendor. These are presented as (key) label : value and delimited with a newline.
Primary Fields	The content of the dynamic primary fields structure in the file, which are supplied by the vendor. These are presented as (key) label : value and delimited with a newline.
Secondary Fields	The content of the dynamic secondary fields structure in the file, which are supplied by the vendor. These are presented as (key) label : value and delimited with a newline.
Auxiliary Fields	The content of the dynamic auxiliary fields structure in the file, which are supplied by the vendor. These are presented as (key) label : value and delimited with a newline.
Back Fields	The content of the dynamic back fields structure in the file, which are supplied by the vendor. These are presented as (key) label : value and delimited with a newline.

Additional Information

Wallet Payment Cards

Description	Wallet Payment Cards contains information on payment cards that have been saved to the user's Apple Wallet application.
Recovery method	Parsing

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Issuer	The organization that issued this payment card (typically a bank).
Payment Method	The payment method (i.e. credit or debit).
Last Four Digits	The card's last four digits.
Expiry Date	The expiry month and year as indicated on the card.
Account Description	A description of the account that backs this payment card.
DPAN	The Device Primary Account Number that links the device and bank account/credit card.
Country Code	The two-character country code in which this card was issued.

Additional Information

Wallet Transactions

Description	Wallet Transactions contains information about transactions that have been completed with the Apple Wallet application. This artifact can also recover transactions with cards that are associated with the wallet but aren't made through the Apple Wallet application.
Recovery method	Parsing

Attribute	Description
Transaction Date/Time - UTC (yyyy-mm-dd)	The date and time that the transaction was initiated.
Name	The merchant's name.
Cost	The amount of the transaction converted to represent the expected format. Due to multiple currencies worldwide, refer to the Cost (Raw) value if the Cost value does not represent the current currency as expected.
Cost (Raw)	The raw amount of the transaction from the database without any conversion. Depending on the currency, this value might need to be converted manually to a value representative of the currency in use.
Currency	The currency of the transaction.
Latitude	The latitude of the first location acquisition after the transaction was conducted (may be inaccurate if there's a large time gap between the two).
Longitude	The longitude of the first location acquisition after the transaction was conducted (may be inaccurate if there's a large time gap between the

Attribute	Description
	two).
Accuracy	The distance from the original geographic coordinate that could yield the user's actual location. The unit of measurement is presumed to be meters.
Altitude (meters)	The altitude in meters of the first location acquisition after the transaction was conducted (may be inaccurate if there's a large time gap between the two).
Location Acquired Date/Time - UTC (yyyy-mm-dd)	The date and time that the location was acquired.
Status	The transaction status (raw data - uninterpreted).
Type	The transaction type (raw data - uninterpreted).
DPAN	The Device Primary Account Number linking the device and bank account/credit card.
Categories	The merchant's primary business category (e.g. restaurant).
Street	The merchant's street address.
City	The merchant's city.
State/Province	The merchant's state/province.
Country	The merchant's country.
ZIP/Postal Code	The merchant's ZIP or postal code.
Business Phone	The merchant's phone number.

Additional Information

Weather - Biome App Intents

Description	Weather - Biome App Intents contains information about application intents from the Weather app related to location.
Recovery method	Parsing

Attribute	Description
City	The city where the device checked the weather.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the app intent was created.
Latitude	The latitude coordinate of the location.
Longitude	The longitude coordinate of the location.

Additional Information

WhatsApp Biome App Intents - iOS

Description	WhatsApp Biome App Intents - iOS contains information about application intents from the WhatsApp app related to sent and received messages and calls.
Recovery method	Parsing

Attribute	Description
Partner	The ID of the conversation partner.
Partner Name	The name of the conversation partner.
Partner Phone Number	The phone number of the conversation partner.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the app intent was created.
Type	The type of app intent, such as send message, call, etc.
Direction	Indicates whether the message was sent or received by the device.
Chat ID	The ID of the WhatsApp chat.

Additional Information

Cloud Storage

Google Drive Items

Description	Google Drive Items contains information about the documents, folders and media that have been accessed using Google Drive on the device.
Recovery method	Parsing

Attribute	Description
Account ID	The unique account identifier of the local user.
Title	The title of the item.
File ID	The unique identifier of the item.
Local File Name	The local file name of the item.
File Type	The mime type of the item.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was modified.
Shared With Me Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was shared with the local user.
Last Viewed By Me Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was last viewed by the local user.
Deleted	Indicates whether the item was deleted.
Starred	Indicates whether the item was starred.
Folder	Indicates whether the item is a folder.
Owner	Indicates whether the local user is the owner of the item.
Attachment	The recovered file, if it was locally available on the device.

Additional Information

Google Drive Thumbnails

Description	Google Drive Thumbnails contains information about thumbnail pictures of the Google Drive items found on the device.
Recovery method	Parsing

Attribute	Description
File ID	The unique identifier of the item.
Account ID	The unique account identifier of the local user.
Attachment	The generated thumbnail of the document
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was modified.

Additional Information

iCloud Devices

Description	iCloud Devices show a list of devices that have access to the iCloud.
Recovery method	Parsing

Attribute	Description
Device Name	The name of the device.

Additional Information

iCloud Downloads

Description	iCloud Downloads show a list of files that have been either recently downloaded or are pending download.
Recovery method	Parsing

Attribute	Description
File Name	The name of the iCloud file.
Download State	Indicates whether the file is available on the local drive or is pending download.
File Size (Bytes)	The size of the file in bytes.
Download Request Date/Time - UTC (yyyy-mm-dd)	The date and time that the download was requested.

Additional Information

iCloud Local Files

Description	iCloud Local Files are files that have been imported from the local computer or synced remotely from the iCloud Drive folder on a iOS machine.
Recovery method	Parsing

Attribute	Description
File/Folder Name	The name of the iCloud file or folder.
iCloud Drive Path	The iCloud drive path to the file or folder.
Original File Name	The name of the file when it was first loaded to the iCloud Drive.
Package Name	The package ID of the application used to interact with the file.
File Size (Bytes)	The size of the file in bytes.
Item Type	Indicates whether an item is a file, a folder, or a hidden iCloud File. Hidden iCloud files are used as markers for upload and download sync states and are .iCloud files.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file or folder was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file or folder was modified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when that the file was last accessed on the iCloud Drive.
Device Name	The name of the device.

Additional Information

iCloud Server Files

Description	iCloud Server Files are files that exist on the iCloud server, and may not exist on the local iOS machine.
Recovery method	Parsing

Attribute	Description
File/Folder Name	The name of the iCloud file or folder.
iCloud Drive Path	The iCloud drive path to the file or folder.
Original File Name	The name of the file when it was first loaded to the iCloud Drive.
File Size (Bytes)	The size of the file in bytes.
Item Type	Indicates whether an item is a file, a folder, or a hidden iCloud File. Hidden iCloud files are used as markers for upload and download sync states and are .iCloud files.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file or folder was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file or folder was modified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when that the file was last accessed on the iCloud Drive.

Attribute	Description
Device Name	The name of the device.
Shared	Indicates whether the file was shared or not.

Additional Information

iCloud Uploads

Description	iCloud Uploads show a list of files that have been either recently uploaded or are pending upload.
Recovery method	Parsing

Attribute	Description
File Name	The name of the iCloud file.
Upload State	Indicates whether the file is available on the local drive or is pending upload.
File Size (Bytes)	The size of the file in bytes.
Upload Request Date/Time - UTC (yyyy-mm-dd)	The date and time that the upload was requested.

Additional Information

iOS Dropbox

Description	iOS Dropbox contains information from the iOS Dropbox Database regarding the cached files.
Recovery method	Parsing and carving

Attribute	Description
Account ID	The ID number associated with the account.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last modified.
Client Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last modified on the client.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last viewed.
Dropbox File Path	The relative path to the file in the Dropbox application.
Size (Bytes)	The size of the file in bytes.
View Count	The number of times that the file has been viewed.
Favorite	Indicates whether or not the file has been favorited (Yes or No).
Revision Number	The revision number for the file.
Local File Path	The local path on the disk where the cached file was found.
Image	The image data for the file.

Additional Information

iOS Dropbox Carved

Description	iOS Dropbox Carved contains file information from the iOS Dropbox application.
Recovery method	Parsing and carving

Attribute	Description
File Path	The path to the location where the file was stored, relative to the Dropbox folder.
Size (Bytes)	The size of the file in bytes.
View Count	The number of times that the file was viewed.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last viewed.
Client Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the local client last modified the file.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified.
Favourite	Indicates whether the file is marked as a favourite.
Revision Number	The revision number of the file.
Image	The raw image content of the file.

Additional Information

MEGA Accounts

Description	MEGA Accounts contains information about the accounts that the local user has logged in with on the device.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the local user.
Email Address	The email address of the local user.
First Name	The first name of the local user.
Last Name	The last name of the local user.

Additional Information

MEGA Chat

Description	MEGA Chat contains messages sent and received by the local user.
Recovery method	Parsing

Attribute	Description
Sender ID	The ID of the sender.
Sender Email	The email address of the sender.
Recipient ID(s)	The user ID(s) of the recipient(s).
Recipient Email(s)	The email address of the recipient of the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message Body	The body of the message.
Message Type	The type of the message.
Attachment Name	The file name of the attachment in a message.
File	The attachment in the message. For video files, the preview might only be a thumbnail of the original video.

Additional Information

MEGA Contacts

Description	MEGA Contacts contains information about MEGA users that have communicated with the local user account.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the contact.
Email Address	The email address of the contact.
First Name	The first name of the contact.
Last Name	The last name of the contact.

Additional Information

Communication

AIM Buddies

Description	AIM Buddies contains information about the local user's buddies in the iOS AIM application.
Recovery method	Parsing

Attribute	Description
User AIM ID	The AIM ID of the local user.
Buddy Name	The name of the buddy.
Buddy Display ID	The display ID of the buddy.
Buddy AIM ID	The AIM ID of the buddy.
Buddy Icon URL	The URL of the buddy's icon.

Attribute	Description
Downloaded Buddy Icon	The dowloaded icon of the buddy.
Buddy Group	Identifies if the row is a buddy or group chat. The possible values are Buddies or groupcht.
Group Chat ID	The ID of the group chat, if applicable.

Additional Information

AIM Messages

Description	AIM Messages contains messages that were sent and received from the iOS AIM application.
Recovery method	Parsing and carving

Attribute	Description
Sender	The email address of the sender of the message.
Receiver	The email address of the receiver of the message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that is associated with the message.
Message	The message content in HTML or plaintext format.
Latitude	The latitude of the location from where the message was sent.

Attribute	Description
Longitude	The longitude of the location from where the message was sent.

Additional Information

Apple Contacts - iOS

Description	Apple Contacts contains information about the contacts that a user has saved to their device.
Recovery method	Parsing and carving

Attribute	Description
First Name	The first name of the contact.
Last Name	The last name of the contact.
Picture	The profile picture of the contact, in its full size.
Phone Number (s)	The phone numbers associated with the contact.
Email(s)	The email addresses associated with the contact.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact's information was created.

Attribute	Description
Address	The physical address associated with the contact.
Website	The website associated with the contact.
Middle Name	The middle name of the contact.
Organization	The organization or business associated with the contact.
Organization Phonetic	The phonetic spelling of the organization.
Department	The department associated with the contact.
Note	The notes associated with the contact.
Favorited	Indicates whether a contact has been set as a favorite by the user.
Favorite Contact Entry	An entry for the contact (such as a phone number) that the user has set as the preferred contact method. This attribute also indicates the default action used by the device when the entry is used.
Birthday (yyyy-mm-dd)	The birthday of the contact.
Alternate Birth-day	The alternate birthday of the contact.
Job Title	The job title associated with the contact.
Nickname	The nickname associated with the contact.
Thumbnail	The profile picture of the contact, in thumbnail size.
Prefix	The prefix of the contact's name (e.g. Mr., Mrs., Dr.).
Suffix	The suffix of the contact's name (e.g. PH.D, Ed.D, LL.D).

Attribute	Description
User Accounts	A comma separated list that includes all of the social media accounts associated with this contact.
First Name Phonetic	The phonetic spelling of the contact's first name.
First Name Pronunciation	The pronunciation of the contact's first name.
Middle Name Phonetic	The phonetic spelling of the contact's middle name.
Middle Name Pronunciation	The pronunciation of the contact's middle name.
Last Name Phonetic	The phonetic spelling of the contact's last name.
Last Name Pronunciation	The pronunciation of the contact's last name.
Previous Last Name	The previous last name of the contact.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact's information was last modified.

Additional Information

BlackBerry Messenger Contacts

Description	BlackBerry Messenger Contacts contains the BBM Contacts recovered from an iOS device.
Recovery method	Parsing

Attribute	Description
BlackBerry PIN	Contains the contacts BlackBerry PIN.
Display Name	Contains the contacts display name.
Personal Message	Contains the contacts personal message.
Personal Message Last Update Date/Time - UTC (yyyy-mm-dd)	The data and time the contacts personal message was updated.
Avatar	The contacts avatar.
Avatar Content Type	The avatar content type. An example is 'image/jpeg'
Locale	The contacts location.
Timezone	The contacts timezone.

Additional Information

BlackBerry Messenger File Transfers

Description	BlackBerry Messenger File Transfers contains the BBM File Transfers

	recovered from an iOS device.
Recovery method	Parsing

Attribute	Description
BlackBerry PIN	BlackBerry PIN of the contact who the transfer is with.
Display Name	Display name of the contact who the transfer is with.
Transfer Date/Time - UTC (yyyy-mm-dd)	The date and time the transfer took place.
Transfer Direction	Indicates whether a file was sent or received.
Transfer State	Indicates whether a file transfer is 'Pending Approval' or 'Complete'.
Local File Path	The path on the device to the data transferred.
Content Type	The type of data that was transferred.
Transfer Description	Description of what is being transferred.
Attachment	The file that was transferred.
Total Transfer Size (Bytes)	The number of bytes the transferred file is.
Bytes Transferred	The number of bytes that were transferred.

Additional Information

BlackBerry Messenger Invitations

Description	BlackBerry Messenger Invitations contains the BBM invite requests recovered from an iOS device.
Recovery method	Parsing

Attribute	Description
BlackBerry PIN	The BlackBerry PIN of the user sending the invite request.
Display Name	The display name of the user sending the invite request.
Local Email Address	The local email address of the user.
Remote Email Address	The remote email address of the user.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date/time when the invite was sent/received.
Direction	This column states if the invite is a received invite or a sent invite.
Invitation Status	Contains the status of the invite request. The value can be Pending Approval or Unknown.
Invite Method	The method used for sending the invite request. The value can be Via PIN or Unknown.
Subject	The subject used for the invite request.
Greeting	The message sent with the invite request.

Additional Information

BlackBerry Messenger Locations

Description	BlackBerry Messenger Locations contains the BBM locations recovered from an iOS device.
Recovery method	Parsing

Attribute	Description
BlackBerry PIN	The BlackBerry PIN of the location sender.
Display Name	The display name of the location sender.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date/time when the location was sent/received.
Message Type	Indicates whether the message was sent or received.
Location Name	The name of the location
Latitude	The latitude of the location
Longitude	The longitude of the location
Altitude (meters)	The altitude of the location.
Accuracy (meters)	The accuracy in meters.
Street	The street address of the location.
City	The city of the location.
State/Province	The state/province of the location.
Country	The country of the location.
ZIP/Postal Code	The postal code/ZIP of the location.

Additional Information

BlackBerry Messenger Messages

Description	BlackBerry Messenger Messages contains the BBM messages recovered from an iOS device.
Recovery method	Parsing and carving

Attribute	Description
Conversation ID	The conversation identifier.
BlackBerry PIN	The BlackBerry PIN of who sent the message to the device or who's receiving a message from the device.
Display Name	The display name of who sent the message to the device or who's receiving a message from the device.
Participants	The display names of the people in the conversation.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent/received.
Message Content	The message sent/received.
Message Type	Contains the type of message that was sent. This can be one of the following: Message, Ping, File, Picture, Notification, Location.
Message Status	The status of the message (received or sent).
Message State	Contains the state of the message. This can be one of the fol-

Attribute	Description
	lowing: 'Sent', 'Undelivered', 'Delivered, Unread', 'Read'.
Attachment	The attachment that was sent/received.

Additional Information

BlackBerry Messenger Profile

Description	BlackBerry Messenger Profile contains the BBM Profiles recovered from an iOS device.
Recovery method	Parsing

Attribute	Description
BlackBerry PIN	The BlackBerry PIN associated with the profile.
Display Name	The display name associated with the profile.
Personal Message	The profiles personal message.
Personal Message Last Update Date/Time - UTC (yyyy-mm-dd)	The date and time the profile message was last updated.
Avatar	The profiles avatar.
Avatar Content Type	The avatar content type. An example is 'image/jpeg'.

Attribute	Description
Locale	The location of the profile.
Timezone	The timezone of the profile.
Keeps Chat History	Indicates whether or not the user keeps chat history.

Additional Information

Burner Contacts

Description	Burner Contacts contains information about a subject's Burner Contacts, as recovered from their iOS device.
Recovery method	Parsing

Attribute	Description
Contact ID	The ID of the contact.
Contact Name	The name of the contact.
Phone Number	The phone number of the contact.
Burner ID	The ID of the Burner application associated with the contact.
Date/Time Created - UTC (yyyy-mm-dd)	Indicates when the contact was created.

Additional Information

Burner Messages

Description	Burner Messages contains information about messages and calls that are sent and received using Burner.
Recovery method	Parsing

Attribute	Description
Sender	The phone number of the sender.
Recipient	The phone number of the recipient.
Message	The body of the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Direction	Indicates whether the message was incoming or out-going.
Message Type	The type of message.
Media URL	The URL to the media file attached to the message.
Voicemail URL	The URL of the voicemail.

Additional Information

Burner Numbers

Description	Burner Numbers contains information about the burner numbers that the local user created.
Recovery method	Parsing

Attribute	Description
Burner ID	The ID of the Burner number.
Burner Number	The Burner phone number.
Display Name	The display name associated with the Burner number.
Created Date/Time	Indicates when the Burner number was created.
Expiration Date/Time	Indicates when the number will expire.
Mobile Phone	The phone number used to sign in to the Burner Application.
User ID	The user ID of the user who is signed in.

Additional Information

Chatous Chat Messages

Description	Chatous Chat Messages contains messages sent and received using Chatous.
Recovery method	Parsing

Attribute	Description
Sender	The display name of the user who sent the message. This value is Local User if the sender was the local user.
Recipient	The display name of the user who received the message. This value is Local User the sender was the local user.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The body of the message.
Attachment Name	The name of the attachment that was sent.
Attachment Data Recovered	Indicates whether attachment data was recovered (Yes or No).

Additional Information

Chatous Chat Partners

Description	Chatous Chat Partners contains information about the users that the local user has communicated with.
Recovery method	Parsing

Attribute	Description
Screen Name	The name of the chat partner.
Last Message Date/Time -	The date and time of the last message in the chat.

Attribute	Description
UTC (yyyy-mm-dd)	
Age	The age of the chat partner.
Gender	The gender of the chat partner. A blank value indicates that the chat partner is the Team Chatous account.
Locale	The location of the chat partner.
About	A summary of the chat partner.
Tag	The tag that matched the local user and the chat partner for a chat.
Profile Tags	The hashtags that the chat partner uses to describe themselves.

Additional Information

Discord Messages

Description	Discord Messages contains information about messages and calls that are sent and received using Discord. Messages from some channels might be missing if they haven't been cached by the application. This artifact uses both parsing and carving techniques to recover messages.
Recovery method	Parsing

Attribute	Description
Sender	The username of the message sender.
Sender ID	The ID of the message sender.
Message	The message content. If the message sent is a sticker, the message will display 'Sticker(sticker name)'.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Last Edited Date/Time - UTC (yyyy-mm-dd)	If the message has been edited then this indicates the date and time when the last edit has occurred.
Message Type	The type of the message (Message or Call).
Channel ID	The ID of the channel that the message was sent in.
Attachment URL	If the message includes an attachment, then this value indicates the saved URL of the attachment.
Attachment Name	If the message includes an attachment, then this value indicates the file name of the attachment.
Embedded Content Title	If the message contains a link, then this then this value indicates the title that's displayed in the link preview.
Embedded Content Description	If the message contains a link, then this value indicates the description that's displayed in the link preview.
Call End Date/Time - UTC (yyyy-mm-dd)	If the message was a call, this indicates the date and time that the call ended.
Pinned	Indicates whether a message is pinned (True or False).

Attribute	Description
Message ID	The Message ID of the message that this message is replying to.
Mentions	The user mentioned in the message, if present.
In Reply To	The Message ID of the message that this message is replying to.
Reactors	The users who reacted to this message, if any. The order of reactors does not correspond to the reactions used.
Reaction	The emojis that were used to react to the message, if any. If a custom emoji is used, the name of that emoji will be listed instead of the emoji itself.

Additional Information

Facebook Messenger Calls

Description	Facebook Messenger Calls contains call data recovered from Facebook Messenger. Provides useful background information on a suspect, including who he or she is communicating or associated with. Status and location updates in social media can also provide location information about the suspect.
Recovery method	Parsing

Attribute	Description
User Key	The user key of the call partner. If the call was made in a group chat, this field will be empty.

Attribute	Description
Thread Key	The thread key of the group where the call was made. If the call was made in a chat with only one other person, this field will be empty.
Partner Name	The name of the call partner. If the call was made in a group chat, this field will be empty.
Group Name	The name of the group where the call was made. If the call was made in a chat with only one other person, this field will be empty.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the call.
Call Duration	The duration of the call in a friendly text format. This field is left empty if the call wasn't answered.
Call Duration (Seconds)	The duration of the call in seconds. This field is left empty if the call wasn't answered.
Call Type	The type of the call. The call type is either a voice call or a group voice call.
Answered	Indicates whether the call was answered or not.
Direction	The direction of the call.
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).

Additional Information

Facebook Messenger End-to-End Encrypted Chats

Description	Facebook Messenger End-to-End Encrypted (E2EE) Chats contains messages recovered from Facebook Messenger E2EE chats on the device.
Recovery method	Parsing

Attribute	Description
Sender Name	The display name of the person sending the message.
Recipient Name	The display name of the person receiving the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message	The text of the end-to-end encrypted message.
Direction	The direction of the message (Incoming or Outgoing) relative to the local user's device.

Additional Information

Facebook Messenger Groups

Description	Facebook Messenger Groups contains data about group chats on Facebook Messenger. Provides useful background information on a suspect, including who he or she is communicating or associated with. Status and location updates in social media can also provide location information about the suspect.

Recovery method	Parsing and carving

Attribute	Description
Group Name	The display name of the group.
Participants User Names	The user names of the users that are a part of the group.
Participants	The user names of the group members.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The date and time of the last activity recorded in the group.
Senders User Names	The user names of the users that recently participated in the group.
Sender(s)	The IDs of the users that recently participated in the group (for example, by sending a message).
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
Message Count	The approximate number of messages in the group.
Thread Key	The thread key of the group.

Additional Information

Facebook Messenger Messages

Description	Facebook Messenger Messages contains messages recovered from Facebook Messenger. Provides useful background information on a suspect,

	including who he or she is communicating or associated with. Status and location updates in social media can also provide location information about the suspect.
Recovery method	Parsing and carving

Attribute	Description
Sender Name	The display name of the person sending the message.
Sender ID	The user ID of the person sending the message.
Receiver Name	The display name of the person receiving the message.
Group Name	The display name of the group receiving the message.
Receiver ID	The user ID of the person receiving the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time when message was sent.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time the message was deleted from the application.
Text	The text of the message.
Message Type	The type of message that was sent. If multiple attachments were sent together, this fragment indicates the number of attachments.
Send State	Represents whether the message was sent, received or queued.

Attribute	Description
Media Info	The information about the media that is found. This value can be a URL to the media, a file name, or a sticker ID.
Latitude	The latitude portion of the location data that is sent with the message.
Longitude	The longitude portion of the location data that is sent with the message.
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
Thread ID	The thread ID of the message. This is also the Facebook ID of the remote party.
Message ID	The internal unique message ID.
Message Source	The source of the message creation platform.
Attachment	The recovered attachment. If the attachment is a video, the video gets segmented into multiple files. Each segment gets collected for playback in Magnet AXIOM, but the actual file size might differ from the size that AXIOM reports due to the segmentation.

Additional Information

Facebook Messenger Users Contacted

Description	Facebook Messenger Users Contacted contains information about users contacted from the device using Facebook Messenger. Status and location updates in social media can provide detail on where the suspect has been. In addition, this artifact provides background information on a sus-

	pect,including who he or she is communicating or associated with.
Recovery method	Parsing and carving

Attribute	Description
User Key	The user key of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
Name	The display name of the user.
Username	The unique identifier of the user.
Profile Image	The profile image of the user.
Profile Picture URL	The URL of the user's profile picture.
Is App User	Identifies whether the user is using Facebook Messenger or not.
Is Friend	Identifies whenever the user is a friend of the local user.
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
Rank	The user's rank within the application.

Additional Information

Glide Messages

Description	Glide Messages contains messages sent and received by the local user.
Recovery method	Parsing

Attribute	Description
Sender ID	The unique user ID of the sender.
Sender Name	The name of the sender.
Recipient ID (s)	The identifier(s) of the recipient(s).
Recipient Name(s)	The name(s) of the recipient(s).
Message	The body of the message. Forwarded messages have had a 'Fwd:' prefix added to help differentiate them from the original message.
Message Type	The type of the message.
Created Date/Time	The date and time when the message was created.
Read	The read status of the message.
Media URL	The URL to the media of the message.
Chat Type	The type of the chat.

Additional Information

Glide Users

Description	Glide Users contains information about the various users that the suspect has encountered using Glide.
Recovery method	Parsing

Attribute	Description
User ID	The unique ID of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
Email Address	The email address of the user.
Gender	The gender of the user.
Account Type	The type of the user.
Last Seen Date/Time	The last time the user was seen online.

Additional Information

Google Duo Accounts

Description	Google Duo contains information about the first time a user logged into Google Duo.
Recovery method	Parsing

Attribute	Description
User ID	A phone number that the user can receive a verification code through SMS from.
Created Date/Time	The date and time that the local user entered the verification code.

Additional Information

Google Duo Activity

Description	Google Duo Activity contains details about audio calls, video calls, and messages sent and received by the user.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message or call.
Recipient(s)	The recipient(s) of the message or call.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the message or call.
Activity Type	The type of activity. Possible values include Audio Call, Video Call, and Message.
Direction	The direction of the activity.

Attribute	Description
Call Status	The status of the call. Possible values include Answered, Not Answered, and Rejected.
Call Duration (Seconds)	The duration of the call.
Message ID	The ID of the message (if the Activity Type is Message).
Message	The content of the message.
Attachment Name	The name of the attachment from the message.
Reaction	The reaction to a message. You can associate the reaction to the message through the Message ID. In the Google Duo app, the reaction is overlaid on the message, but in AXIOM Examine, the reaction is presented on its own.
Attachment	The attachment from the message.

Additional Information

Google Duo Group Calls

Description	Google Duo Group Calls contains details about the video calls made and received by the user.
Recovery method	Parsing

Attribute	Description
Session ID	The session ID of the group call.
Call Status	The status of the call. Incoming Initiated indicates an incoming call request, Incoming Cancelled indicates that the caller cancelled the request before connecting, and Call indicates an incoming call that was connected or an out-going call that is unknown if any participants joined the call.
Caller	The phone number of the caller.
Recipient(s)	The recipients of the call.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the call.
Call Duration (Seconds)	The duration of the call.
Call Type	The type of call.

Additional Information

Google Duo Groups

Description	Google Duo Groups contains membership information of Google Duo Groups.
Recovery method	Parsing

Attribute	Description
Group Chat ID	The ID of the group.
Group Name	The display name of the group.
Group Member Name(s)	The display names of the group members.
Group Member ID(s)	The IDs of the group members.

Additional Information

Google Duo Users

Description	Google Duo Users contains details about the user's contacts. Google Duo stores both contacts that are already signed up with Duo as well as contacts from the user's address book that can be invited to Duo.
Recovery method	Parsing

Attribute	Description
Contact Name	The name of the contact.
Contact ID	The ID of the contact.
Device Type	The ID type of the contact (e.g. home, mobile, main).
Sync Date/Time - UTC (yyyy-mm-dd)	The date the contacts were synced with the phone.
Blocked	Indicates if the contact is blocked.

Attribute	Description
Avatar	The avatar of the contact.
Contact Type	Indicates if the contact can be communicated with over Duo or if they are in the local user's address book.
Local User	Indicates if the contact is the local user.

Additional Information

Google Hangouts Voice Calls

Description	Google Hangouts Voice Calls contains a history of voice calls between the local user and other users.
Recovery method	Parsing

Attribute	Description
Phone Number	The phone number of the call participant.
Call Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the call started.

Additional Information

Google Meet Meeting History - iOS

Description	Google Meet Meeting History contains the meetings that any local user on

	the device has joined.
Recovery method	Parsing

Attribute	Description
User ID	The ID of the user who is signed into Google Meets on the local device.
User Email	The email associated with the user ID.
User Name	The name associated with the user ID.
Joined Date/Time - Local Time	The local date and time that the local user joined the meeting.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

GroupMe Accounts

Description	GroupMe Accounts contains information about the accounts that the local user has logged in with on the device.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the local user.
Display Name	The display name of the local user.
Email Address	The email address of the local user.
Phone Number	The phone number of the local user.
Created Date/Time	The date and time that the account was created (specific to iOS).
Login Date/Time	The date and time that the account was logged in on this device (specific to Android).
Profile Picture URL	The URL of the profile picture of the local user.
Password/Token	The local user password or token.
Platform	The cloud platform name.

Additional Information

GroupMe Contacts

Description	GroupMe Contacts contains information about a user's contacts.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the contact.
Display Name	The display name of the contact.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact was added.

Additional Information

GroupMe Groups

Description	GroupMe Groups contains information about the groups that the logged-in user is a member of.
Recovery method	Parsing

Attribute	Description
Group	The group number.
Group Name	The name of the group.
Topic	The topic of the group.
Creator ID	The creator identifier of the group.
Created Date/Time	The date and time that the group was created.
Group Member ID(s)	The IDs of all group participants.
Group Member Name(s)	The names of all group participants.

Additional Information

GroupMe Messages

Description	GroupMe Messages contains messages sent and received using

	GroupMe.
Recovery method	Parsing

Attribute	Description
Sender Name	The name of the message sender.
Sender ID	The user ID of the message sender.
Recipient Name(s)	The user name(s) of the message recipient(s).
Recipient ID(s)	The user ID(s) of the message recipient(s).
Sent Date/Time	The date and time that the message was sent.
Message	The message text.
Photo URL	The URL to the photo associated with the message.
Video URL	The URL to the video associated with the message.
Locale	The name of the location in the location data sent with the message.
Latitude	The latitude part of location data sent with the message.
Longitude	The longitude part of location data sent with the message.
Event	The event sent with the message.
Document Title	The document details sent with the message.
Poll	The poll details sent with the message.

Additional Information

Houseparty Messages

Description	Houseparty Messages contains messages recovered from Houseparty.
Recovery method	Parsing

Attribute	Description
Sender	The username of the person sending the message.
Recipient	The username of the person receiving the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The content of the sent message.
Read Status	Indicates whether or not the message has been read.

Additional Information

Houseparty Users

Description	Houseparty Users contains information about the users contacted from the device using Houseparty.
Recovery method	Parsing

Attribute	Description
User Name	The username of the user.

Attribute	Description
Full Name	The full name of the user.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the user account was created.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the user account was last updated.

Additional Information

imo Contacts

Description	imo Contacts contains information about a user's contacts.
Recovery method	Parsing

Attribute	Description
User ID	The unique user ID of the contact.
Display Name	The display name of the contact.
Name	The full name of the contact.
Phone Number	The phone number of the contact.
Number of Times Contacted	The number of times that the local user initiates contact (by message or call) with the contact.

Additional Information

imo Messages

Description	imo Messages contains information about sent and received messages and calls made using the imo application.
Recovery method	Parsing

Attribute	Description
Local User	Indicates the local user identifier of the account.
Remote User ID	The user ID of the remote conversation partner.
Remote User Display Name	The display name of the remote conversation partner.
Direction	The direction of the message.
Message	The message content.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message Type	The type of the message (either call or message).
Attachment Path	The path to locate any attachments on the device.
Attachment	The attachment on the device.

Additional Information

iOS Burner Conversations

Description	iOS Burner Conversations contains the Burner conversations that were recovered from an iOS device.
Recovery method	Parsing

Attribute	Description
Message Body	The body of the last message in the conversation.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message in the conversation.
Burner Number	The Burner number on the device that is a part of the conversation.
Conversation Partner	The phone number of the other person in the conversation.
Conversation Name	The name of the conversation.
Duration (Seconds)	The duration of the conversation in seconds.
Status	The status of the message (Read, Unread, Sent, or Not Sent).
Type	The type of the last interaction in the conversation. This values can be any of the following: Outgoing Text Message, Incoming Text Message, Incoming Phone Call, Missed Incoming Phone Call, Outgoing Phone Call, Incoming Voice Mail.
Voicemail URI	The URL to the voice mail, if applicable.

Additional Information

iOS Burner Numbers

Description	iOS Burner Numbers contains the Burner numbers that were recovered from an iOS device.
Recovery method	Parsing

Attribute	Description
Account Number	The phone number of the user's Burner account.
Burner Number	The phone number that was generated by Burner.
Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the Burner number was updated.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the Burner number was generated.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the Burner number will expire.
About	Information about the Burner number.

Additional Information

iOS Call Logs

Description	iOS Call Logs contains iOS Call Logs from the iOS native phone application.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Partners	The phone number of the conversation partner.
Partner Name	The name of the conversation partner.
Direction	The direction of the call, which is either incoming or outgoing.
Call Type	The type of iOS call. The call is either FaceTime (Audio or Video) or a regular phone call.
Call Status	The status of the call, which is either answered or unanswered.
Call Date/Time - UTC (yyyy-mm-dd)	The date and time when the call was placed.
Call End Date/Time - UTC (yyyy-mm-dd)	The date and time when the call ended. This value is calculated by adding the Call Duration to the Call Date/Time.
Call Duration	The duration of the call in one of the following formats: HH:MM:SS (hours, minutes, seconds) or DD:HH:MM:SS (days, hours, minutes, seconds).

Attribute	Description
Application Name	The package name of the application that made the call.
Partner Location	The location of the other participant of the call, which is either a full address or a Mobile Country Code (MCC).
Service Provider	The service provider that handled the call.

Additional Information

iOS Google Hangouts Cached Images

Description	iOS Google Hangouts Cached Images contains the cached images from Google Hangouts from an iOS device.
Recovery method	Parsing

Attribute	Description
Image URL	The URL of the cached image.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last date and time that the image was accessed.
Local File Path	The location to the image on the user's device.
File Size (Bytes)	The size of the image in bytes.
Image	The cached image.

Additional Information

iOS Google Hangouts Contacts

Description	iOS Google Hangouts Contacts contains the contacts of a person from Google Hangouts from an iOS device.
Recovery method	Parsing

Attribute	Description
Display Name	The display name of the contact.
Google Hangouts ID	The ID of the user in Google Hangouts.
Avatar URL Suffix	The suffix of the user's avatar URL.
Is Blocked	Indicates whether the person is blocked
Is Favorite	Indicates whether the person is favourited.

Additional Information

iOS Google Hangouts Messages

Description	iOS Google Hangouts Messages contains the messages from Google Hangouts from an iOS device.
Recovery method	Parsing

Attribute	Description
Sender / Event Initiator	The sender or event initiator of the message.
Recipient(s)	The recipients of the message.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time of the message or event.
Message	The body of the message.
Event	The event that is the message. This value can be Message, User Joined Group Conversation, User Left Group Conversation, Video Call Started, Video Call Ended, or User Toggled History.
Event Expiry Date/Time - UTC (yyyy-mm-dd)	The date and time when the message or event expires.
Conversation Is Deleted	Indicates whether the conversation was deleted.
Image URL	The URL to the image of the conversation.
Downloaded Image	
Locale	The location of the message.
Address	The address of the message.
Latitude	The latitude of the message.
Longitude	The longitude of the message.

Additional Information

iOS iMessage/SMS/MMS

Description	iOS iMessage/SMS/MMS contains all of the iMessages, SMSs and MMSs sent by the user.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the message.
Recipient(s)	The recipient of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The message that was sent. This fragment may contain the Object Replacement Character (U+FFFC) which indicates a non-text message is presented such as a picture, video, etc. If the non-text message is found, it will be presented as an attachment.
Message GUID	A unique identifying GUID for the message. This fragment is used to connect edited versions of the same message
Type	The direction of the message.
Status	The status of the message indicates whether the message was sent or received, if it was read, or if the message is an edit of an existing message.

Attribute	Description
Message Delivered Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was delivered.
Message Read Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was read.
Edit Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the edited version of the original message was sent
Message Unsent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was unsent.
Recently Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was recently deleted by the user. Recently deleted messages will stay on the device for 30 days or until they are permanently deleted by the user.
Mentions	Any individuals that are tagged in the message.
Reaction	Indicates the type of reaction or 'tapback' to a message (heart, like, etc.), if

Attribute	Description
	applicable.
Attachment Path	The file location where the attachment is stored.
Attachment Data Recovered	The data of any files attached to the message.
Sent By Siri	Indicates whether the message was sent by the user through Siri.
Transcript	A text transcript of the audio message. The audio message itself is automatically deleted a few minutes after being sent.
Chat ID	The identifier of the chat that the message is in.
Latitude	The latitude of the vCard attachment, if provided.
Longitude	The longitude of the vCard attachment, if provided.

Additional Information

iOS iMessage/SMS/MMS - App Intents

Description	iOS iMessage/SMS/MMS - App Intents contains information about application intents from the iOS Messages app related to sent and received messages.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message.
Recipient(s)	The recipient of the message.
Message	The message that was sent for the app intent. This fragment might contain the Object Replacement Character (U+FFFC), which indicates a non-text message is presented, such as a picture, video, etc.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the sent message app intent was created.
Type	The type of message the app intent represents, such as iMessage, SMS, etc.

Additional Information

iOS Kik Messenger Attachments

Description	iOS Kik Messenger Attachments contains the attachments of messages from Kik Messenger from an iOS device.
Recovery method	Parsing

Attribute	Description
Attachment Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.

Attribute	Description
Attachment	The attachment.
Attachment (Plain Text)	The attachment, if its format is plain text (for example, a URL).

Additional Information

iOS Kik Messenger Messages

Description	iOS Kik Messenger Messages contains Kik Messenger messages that were sent or received by the local user.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Partner	The person the local user sent a message to or received a message from.
Partner Display Name	The partner's display name.
Received (Device Time) Date/Time - UTC (yyyy-mm-dd)	The date and time that message was received.
Sent (Device Time)	The date and time that message was sent from the device.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Sent (Server Time) Date/Time - UTC (yyyy-mm-dd)	The date and time that message was sent from the server.
Message Body	The body of the message.
Message Type	The type of message. The pssible values are Message Received, Message Sent, User Joined, and Unknown Message Type.
Anonymous Chat	Indicates whether the message was part of an anonymous chat.
Anonymous Chat Expiry Date/Time - UTC (yyyy-mm-dd)	If the message was part of an anonymous chat, this indicates whether the anonymous chat has expired.
Attachment	The attachment that was sent with the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time when message was either sent or received.

Additional Information

iOS Kik Messenger Users

Description	iOS Kik Messenger Users contains information about a user's Kik Messenger contacts.

Recovery method	Parsing

Attribute	Description
User ID	The identifier of the user.
Kik ID	The Kik identifier of the user.
Chat User ID	The chat user identifier of the user.
Username	The username of the user.
Email	The email address of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
Display Name	The display name of the user.
Image URL	The URL to the profile picture of the user.
Last Message	The last sent message by the user.
Last Sent Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the last sent message.

Additional Information

iOS Messages Preferences

Description	iOS Messages Preferences contains information about important settings

	of the Messages application.
Recovery method	Parsing

Attribute	Description
Synced To iCloud	Indicates if the Messages application is synced to iCloud.
All Aliases	All aliases of the Messages application used to receive and reply to iMessages.
Selected Aliases	Aliases of the Messages application that are used to start new conversations.
Pinned Contacts	Contacts pinned to the top of the Messages application.
Message Kept Days	How long the messages are kept on the phone.
Blocked Users	The list of callers that are currently blocked from calling or sending SMS texts / iMessages.
SMS Forwarding Enabled	Indicates if the user has enabled SMS forwarding to other iOS or macOS devices without cellular service.

Additional Information

iOS Textfree Cache Records

Description	iOS Textfree Cache Records contains the web cache for the iOS Textfree

	application.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached content.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date that the cached content was created on the local device.
Content	The raw cached content. This field is blank if the content is an image, in which case, the Image column is populated instead.
File Type	The type of the cached file, such as HMTL, JS, CSS, or JPEG.
Content Size (Bytes)	The size of the cached content in bytes.
Image	The raw content of the cached image. This is blank if the content is not an image (i.e. HTML, JS, CSS, etc.).

Additional Information

iOS TextNow Contacts

Description	TextNow Contacts contains the application, phone, email, and group contacts that a user has in the TextNow application.
Recovery method	Parsing

Attribute	Description
Contact ID	The name of the contact.
Contact Type	The contact's type.
Local Contact Key	The numeric key for the contact.
Contact Display Name	The display name contact.
Contact Label	The descriptive label of the contact.

Additional Information

iOS TextNow Groups

Description	TextNow Groups contains membership information for TextNow group chats.
Recovery method	Parsing and carving

Attribute	Description
Group Chat ID	The ID for the group.
Group Name	The name of the group.
Contact ID	The name of the group member.
Contact Type	The contact's type.
Local Contact Key	The numeric key for the group member.
Contact Display Name	The display name of the group member.

Additional Information

iOS TigerText Messages

Description	iOS TigerText Messages contains sent and received messages with attachments from iOS TigerText application.
Recovery method	Parsing

Attribute	Description
Sender Display Name	The display name of the sender.
Sender Username	The user ID of the sender.
Sender First Name	The first name of the sender.
Sender Last Name	The last name of the sender.
Sender Email	The email address of the sender.
Sender Phone Number	The phone number of the sender.
Recipient Display Name	The display name of the recipient.
Recipient Username	The user ID of the recipient.
Recipient First Name	The first name of the recipient.
Recipient Last Name	The last name of the recipient.
Recipient Email	The email address of the recipient.
Recipient Phone Number	The phone number of the recipient.

Attribute	Description
Message Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message Expiry Date/Time - UTC (yyyy-mm-dd)	The date and time that the message will expire.
Message Recalled	Indicates whether the message was recalled (Yes or No).
Message Deleted	Indicates whether the message was deleted (Yes or No).
Attachment Type	The type of the attached file, in MIME format.
Attachment	The content of the attachment file.
Message Status	The status of the message (New, Delivered, or Read).
Sender Organization Name	The name of the sender's organization, or Personal if the user has none.
Recipient Organization Name	The name of the recipient's organization, or Personal if the user has none.

Additional Information

iOS Voice Mail

Description	iOS Voice Mail contains messages left on the voicemail for the iOS device, along with any greetings messages recorded by the local user. This includes audio or video voicemail messages left using FaceTime.

Recovery method	Parsing

Attribute	Description
Media	The raw audio or video content of the voicemail.
Sender	The sender of the voicemail.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the voicemail was sent.
Transcript	A text transcript of the voicemail message.
Type	The type of voicemail. Message type indicates a voicemail message left by a caller, and Greeting type indicates the greeting recorded by the local user.
Duration (Seconds)	The duration of the voicemail in seconds.

Additional Information

IP Addresses - Audio/Video Calls

Description	IP Addresses of web audio/video calls show who a user was communicating with. Each instance of this artifact represents a single hop in the communication chain. By showing the relationship between multiple hops, you can determine where a call originated from and what the final destination was.

Recovery method	Carving

Attribute	Description
Call ID	The ID of the call.
Message ID	The ID of the message.
Domain	The domain used for the call.
Connection Type	The type of connection.
Origin IP Address	The originating IP address for this hop in the call.
Origin Port	The originating port for this hop in the call.
Destination IP Address	The destination IP address for this hop in the call.
Destination Port	The destination port address for this hop in the call.
Date/Time - UTC (yyyy-mm-dd)	The timestamp associated with this hop in the call.
Remote User ID	The unique ID of the remote user.
Communication Protocol	The communication protocol for this call (either UDP or TCP).
Metadata	Any additional details about the call.

Additional Information

KakaoTalk Messages - iOS

Description	KakaoTalk Messages contains messages that are sent or received by the user.
Recovery method	Parsing

Attribute	Description
Sender ID	The KakaoTalk ID of the sender.
Sender Name	The name of the sender if available, or the nickname otherwise.
Recipient ID	The KakaoTalk ID of the recipient.
Recipient Name	The name of the recipient if available, the nickname otherwise.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was created.
Message Read Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was deleted from the application.
Message Direction	Indicates whether the message was sent or received.
Message	The message content.
Metadata	JSON data that contains additional information for message types other than text.
Attachment	The attachment sent.

Additional Information
Message and sender information are not available for deleted messages.

LINE Contacts

Description	LINE Contacts contains the user's LINE contacts.
Recovery method	Parsing

Attribute	Description
Line ID	The LINE ID of the contact.
Name	The name of the LINE contact.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the user contact was added.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact was last updated.
Status Message	The status of the contact.
Hidden	Indicates whether the contact has been marked as hidden.
Favorite	Indicates whether the contact has been marked as favorite.

Additional Information

LINE Local Users

Description	LINE Local Users contains the local user accounts for LINE on the device.
Recovery method	Parsing

Attribute	Description
Line ID	The LINE specific, unique identifier of the user.
User Name	The user's account name.
User Nickname	The user's nick name.
Status Message	The status that the user has set for themselves.
Unread Message Count	The number of unread messages the user has.
Missed Call Count	The number of missed calls the user has.

Additional Information

LINE Messages

Description	LINE Messages contains the LINE messages that were recovered from an iOS device.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the message. The sender value can be the sender's name or Local User.
Recipient(s)	The recipient(s) of the message.
Message Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was created, or the date and time that the call was started if the message is a call or video call.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent, or the date and time that the call was ended if the message is a call or video call.
Message	The body of the message.
Message Type	The type of the message. The Message Type value can be Audio, Call, Contact Card, File, Location, Note, Picture, Sticker, or Text.
Contact Card Name	The first and last name of the contact.
Read Count	The number of times that the message has been read.
Location Address	The address of the location.
Latitude	The latitude of the location when message type is Location.
Longitude	The longitude of the location when the message type is Location.
Audio Length (Seconds)	The length of the audio in seconds when the message type column is Audio.
Call Duration (Seconds)	The duration of the call in seconds when the message type is Call.
File Attachment	The name of the file that's sent when the message type is File.
File Size (Bytes)	The size of the file sent in bytes.

Attribute	Description
Attachment	The attachment sent with the message.
Thumbnail	A thumbnail of the image (if available).

Additional Information

LINE Pictures

Description	LINE Pictures contains the LINE pictures that were recovered from an iOS device.
Recovery method	Parsing

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed	The last accessed date and time of the picture in the file system.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time when the picture being

Attribute	Description
	taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture, or the name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS latitude coordinates of the camera where the picture was taken (extracted from Exif data).
Longitude	The GPS longitude coordinates of the camera where the picture was taken (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the pciture was taken (extracted from Exif data).
Exif Data	A searchable field for all raw exif properties.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA	The hash of the image content for PhotoDNA.

Attribute	Description
Hash	
Category	An integer that indicates the Project VIC category for the picture.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Mail.Ru Agent Contacts

Description	Mail.Ru Agent Contacts contains contact info for the Agent application on iOS.
Recovery method	Parsing

Attribute	Description
Contact ID	The user ID of the contact.
Display Name	The display name of the contact.
Account Type	The type of the contact. This value can be Agent ID or Agent Channel.
Local User ID	The unique ID of the local user.

Additional Information

Mail.Ru Agent Messages

Description	Mail.Ru Agent Messages contains messages sent or received by the Agent user on iOS.
Recovery method	Parsing

Attribute	Description
Local User ID	The unique ID of the local user.
Remote User ID	The user ID of the remote participant of the chat.
Remote Participant Display Name	The display name of remote participant.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was created.
Message	The content of the message.
Type	The type of the message. The value can be Text Message, Voice Call, Video Call or File Transfer.
Duration (Seconds)	The duration of voice or video call.
Direction	The direction of the message.
File Name	The file name of the attachment.
File	The attachment associated with the message.

Additional Information

Mail.Ru Agent User Accounts

Description	Mail.Ru Agent User Accounts contains information about the Agent user accounts that are saved locally on the iOS device.
Recovery method	Parsing

Attribute	Description
User ID	The unique ID of the local user.
Active	Indicates whether or not the account is currently logged in.
First Name	The first name of the account.
Last Name	The last name of the account.
Display Name	The display name of the account.
Birthday	The birthday of the account.
Phone Number	The phone number of the account.
Gender	The gender of the account.
Home Address	The home address of the account.

Additional Information

ooVoo Chat History

Description	ooVoo Chat History contains the chat history between the data owner and

	their contacts.
Recovery method	Parsing

Attribute	Description
Message ID	The ooVoo unique message identifier.
Sender User ID	The ooVoo identifier of the sender.
Receiver User ID(s)	The ooVoo identifier of the recipient(s).
Chat Date/Time - UTC (yyyy-mm-dd)	The date and time of the conversation.
Message	The actual message content.
Message Type	The type of message that was sent. Some examples of message type are chat, video, and image.
Message Direction	Indicates whether the message was sent (Outgoing) or received (Incoming).
Group Name	The name that is associated with a group conversation. If the chat is between two people the name will be empty.
Video URL	The address of the video that was sent in the message.
Image URL	The address of the image that was sent in the message.
Source	The location where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

ooVoo Contact List

Description	ooVoo Contact List contains the list of contacts that the data owner has on ooVoo.
Recovery method	Parsing

Attribute	Description
Display Name	The contact display name.
User ID	The contact's unique ooVoo identifier.
Status Message	A message set by the contact. This message can contain insight into how the person is feeling, as well as their ideas and thoughts.
Birthday (yyyy-mm-dd)	The contact's birthday.
Phone Number	The contact's phone number.
Password	The contact's password stored as plain text.
Platform	The cloud platform name.

Additional Information

ooVoo Phone Book

Description	ooVoo Phone Book contains the name and phone number of contacts from the data owner's iOS device.
Recovery method	Parsing

Attribute	Description
Contact Name	The name of the contact.
Phone Number	The contact's phone number.
Source	The location where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

QQ File Transfers

Description	QQ File Transfers contains QQ file transfers recovered from the iOS QQ International application.
Recovery method	Parsing

Attribute	Description
Local User ID	The local user ID who the file was transferred with.
Chat Partner / Group Chat ID	The unique ID of the chat partner or group the file was transferred with.
Partner Display Name	The name displayed for the partner the file was transferred with.
Server Date/Time - UTC (yyyy-mm-dd)	The server date and time that the file was transferred.
Direction	Sent/Received: Indicates the direction of the file transfer relative to the local user.
File Name	The file name of the file transferred.
File Path	The file path of the file transferred.
File Size (bytes)	The size of the file transferred.
MD5 Hash	The MD5 hash of the file.
SHA1 Hash	The SHA1 hash of the file.

Additional Information

QQ Local Users

Description	QQ Local Users contains QQ local users recovered from the iOS QQ International application.
Recovery method	Parsing

Attribute	Description
Local User ID	The user ID of the local user.
Local User Display Name	The name displayed for the local user.
Country	The country of the user.
City	The city of the user.
Age	The user's age in years.
Birthday (yyyy-mm-dd)	The user's birthday in YYYY-MM-DD format.
Email	The user's email address.

Additional Information

QQ Messages

Description	QQ Messages contains messages stored by the iOS QQ International application.
Recovery method	Parsing and carving

Attribute	Description
Local User ID	The unique ID of the local user.
Local User Display Name	The name displayed for the local user.
Chat Partner / Group Chat ID	The unique ID of the chat partner or group.

Attribute	Description
Sender User ID	The unique ID of the sender.
Sender Display Name	The name displayed for the sender.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the message.
Message	The text of the message.
Type	The type of content in the message.
Sent/Received	Indicates whether the message is incoming or outgoing (Sent or Recieved).
Read	Indicates whether the message has been read (Read or Unread).

Additional Information

QQ Messages Carved

Description	QQ Messages Carved contains carved messages stored by the iOS QQ International application.
Recovery method	Parsing

Attribute	Description
Local User ID	The unique ID of the local user.

Attribute	Description
Local User Display Name	The name displayed for the local user.
Chat Partner / Group Chat ID	The unique ID of the chat partner or group.
Sender User ID	The unique ID of the sender.
Sender Display Name	The name displayed for the sender.
Message	The text of the message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the message.
Type	The type of content in the message.
Sent/Received	Indicates whether the message was incoming or outgoing.
Read	Indicates whether the message was read.

Additional Information

Session Communities

Description	Session Communities contains information about the open session groups that the local user has joined.
Recovery method	Parsing

Attribute	Description
Group Name	The name of the session community.
URL	The URL for the community.
Description	The description of the session community.
User Count	The number of users in the session community.

Additional Information

Session Groups

Description	Session Groups specifies each of the Session groups that the local user is a member of.
Recovery method	Parsing

Attribute	Description
Group Name	The name of the group.
Group ID	The ID of the group.
Group Member(s)	The member name(s) of the group.
Group Member ID(s)	The member ID(s) of the group.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the group was created.

Additional Information

Session Messages

Description	Session Messages contains information about the messages and calls that are exchanged between the local user and other users on an iOS device.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message.
Sender ID	The ID of the message sender.
Recipient	The message recipient.
Recipient ID	The ID of message recipient.
Message	The content of the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received.
Type	The type of the message.
Direction	The direction of the message (Incoming or Outgoing).
Attachment Name	The name of the message attachment if one was sent.
Attachment	The content of the attachment if one was sent.
Expiration (dd hh:mm:ss)	The expiration policy that was set on the conversation at the time of sending the message.

Attribute	Description
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the message is set to expire.

Additional Information

Session Users

Description	Session Users contains information about the users the local user has associated with through communities, group chats, or direct messages.
Recovery method	Parsing

Attribute	Description
User ID	The user ID.
Display Name	The display name of the user.
Local User	Indicates with 'Yes' if the user is the local user. Otherwise, the field is empty.
Display Name Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the display name was last modified by the user.

Additional Information

Signal

Signal is an encrypted messaging and voice calling application that's available for Android and iOS. The application enables a user to send content (messages, pictures, and videos) to other users and to groups of users. Signal also includes the capability for users to set a password on the application to protect their data.

The content shared between a user and their contacts can be valuable information, as well as the phone numbers of group members and the names of local users. In an investigation, this information can offer insight into the purpose of a suspect's interactions and can be used to identify users who have been in contact with a suspect. Other information can also be recovered, such as message timestamps and shared location messages. This information can be used in piecing together a timeline of a suspect's activity, or for determining their previous whereabouts.

Signal for iOS

Even though Signal uses encryption to protect its data, it's still possible to recover useful artifacts from Android and iOS devices. In cases where the user doesn't set a password, application data can often be recovered and decrypted. Even if decryption is not possible, group and user information, and information about messages can still be recovered (excluding the actual message and attachment content). In addition, latitude and longitude from location messages are also recoverable (these are messages that a user sends that includes their current location).

For instances when the user does set a password, you can provide a list of potential Signal account passwords in AXIOM Process or IEF to use as the key for decrypting the data. Once decrypted, message content and attachments are made available.

On iOS devices, you can also decrypt data by providing a key form the target device's keychain. A common way of obtaining this key is by recovering it from the keychain.plist file that GrayKey generates during an acquisition. To decrypt the application data, add the key to AXIOM Process when you set up your search. Once decrypted, message content and attachments are made available.

Artifacts

Signal Group Members

Signal Local User

Signal Messages

Signal Stories

Signal Users

Resources

Decrypt app data using the iOS Keychain and Graykey

Signal Group Members

Description	Signal Group Members specifies the members from each of the Signal groups that the local user is a member of.
Recovery method	Parsing

Attribute	Description
Group Member	The phone number of the group member.
UUID	The UUID associated with the group member.
Group Name	The name of the group.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the group was created.
Group Avatar	The avatar of the group.

Additional Information

Signal Local User

Description	Signal Local User contains information about the local user account.
Recovery method	Parsing

Attribute	Description
Local User	The full name of the local user.
Avatar	The avatar used by the local user account.

Additional Information

Signal Messages - iOS

Description	Signal Messages contains information about the messages and calls that are exchanged between the local user and other users on an iOS device.
Recovery method	Parsing

Attribute	Description
Sender	The full name of the sender of the message.
Recipient(s)	The full name(s) of the message recipient(s)

Attribute	Description
Group Name	The name of the group that the message was set in.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received.
Message	The content of the message.
Attachment Name	The name of the message attachment if one was sent.
Attachment	The content of the attachment if one was sent.
Type	The type of the message.
Direction	The direction of the message (incoming or outgoing).
Call Status	The status of the call (connected or missed).
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the message is set to expire.
Expiration (dd hh:mm:ss)	The expiration policy that was set on the conversation at the time of sending the message.

Additional Information

Signal Stories

Description	Signal Stories contains information about stories that are posted, viewed, or exchanged between the local user and other users on an iOS device.

Recovery method	Parsing

Attribute	Description
Sender	The sender of the story.
Recipient(s)	The story recipient(s)
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the story was created.
Story ID	The record ID of the story hit.
Uploaded Date/Time - UTC (yyyy-mm-dd)	The date and time when the story attachment was uploaded if one was added.
Recipient Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the recipient received the story.
Read Date/Time - UTC (yyyy-mm-dd)	The earliest date and time when the story was read.
Direction	The direction of the story (incoming or outgoing).
Content Type	The content type of the story, such as 'text/html', 'image/jpeg', 'video/mp4', etc.
Story Name	The name of the story.
Text	The text content of the story if the content type was text.
Caption	The caption of the story.
Attachment Name	The name of the story attachment if one was added.
Attachment	The content of the attachment if one was sent.

Additional Information

Signal Users

Description	Signal Users lists all the users and profiles present in the application. This artifact usually recovers user information for the local user, although it is not possible to indicate with certainty which user is the local user.
Recovery method	Parsing

Attribute	Description
Phone Number	The phone number associated with the user.
UUID	The unique user ID (UUID) associated with the user.
Full Name	The full name of the user, as stored by the Signal application. For version 3.2 and later, it stores the concatenation of the profile name and the family name columns.
Profile Name	The profile name of the user. This is usually a nickname.
Family Name	The last name of the user.
Type of User	The type of the user.
Local User	Indicates whether the user is logged into the device.
Avatar	The user's avatar.

Additional Information

Skype Accounts

Description	Skype Accounts contains information about the Skype accounts that are recovered, such as user information and when the account was created.
Recovery method	Parsing

Attribute	Description
Skype Name	The Skype name of the account.
Display Name	The display name of the account.
Full Name	The full name of the account.
Email(s)	The email of this account.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date when the profile was created.
Last Online Date/Time - UTC (yyyy-mm-dd)	The last time that the account was online.
Birthday (yyyy-mm-dd)	The birthday of the account.
Gender	The gender of the account.
City	The city where the account is located.
State/Province	The state/province where the account is located.
Country	The country where the account is located.

Attribute	Description
Home Phone	The home phone of this contact.
Office Phone	The office phone of this account.
Mobile Phone	The mobile phone of this account.
Homepage	The homepage of this contact.
About Info	The about info of this contact.
Profile Last Modified On Date/Time - UTC (yyyy-mm-dd)	The date when the profile was last modified.
Mood Text	The text used to express mood.
Last Used On Date/Time - UTC (yyyy-mm-dd)	The last time that the account was used.
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	The time that the avatar was created.
Picture	The avatar for this contact.

Additional Information

Skype Activity

Description	Skype Activity contains interactions that occurred between users on Skype. These interactions include messages, message drafts, group interactions, calls, sent and recieved files, and SMS.
Recovery method	Parsing and carving

Attribute	Description
Conversation ID	The ID of this conversation.
Profile Name	The local user's profile name.
Sender	The username of the sender/initiator of the interaction.
Sender Email	The sender's email as given in the message (if available).
Recipient(s)	The recipients or targets of the interaction.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the interaction was initiated.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the interaction was last updated (for example, when a call ends).
Message Type	The type of the interaction.
Message	The content of the message or a summary of the interaction. Drafted messages will begin with [Draft].
Emotion Count	The number of reactions to the interaction. Reactions include likes, dislikes, emojis and more.
File Name	The name of any attached files associated with the interaction.
File Size (Bytes)	The size in bytes of any attached files.
Attachment	The attachment associated with the activity.
Attachment Data Recovered	Indicates whether the attached file was recovered from the local filesystem.
Thumbnail URL	A URL that directs to the thumbnail picture (if applicable).
Call Duration (Seconds)	The length of the call in seconds (if applicable).

Attribute	Description
Metadata	The content of the message, if it consisted of interpreted data (XML or JSON data, rather than plain text).

Additional Information
This artifact only applies to Skype 8.1 and later.

Skype Calls

Description	Skype Calls contains information about Skype calls that occured between users.
Recovery method	Parsing and carving

Attribute	Description
Local Username	The user logged into Skype at the time of the call.
Call Initiator	The user who started the call.
Initiator Display Name	The display name of the user. This might be different from the user-name.
Recipient Name(s)	The users who accepted a call from the call initiator and participated in the call for a period of time.
Call Participants	The users who accepted and participated in the call from the call ini-tiator for some duration.
Started Date/Time	The start time of the call.

Attribute	Description
- UTC (yyyy-mm-dd)	
Duration	The total duration of the Skype call.
Metadata	Additional details about the call extracted in XML format. This includes information on the amount of time that each participant was in the call.

Additional Information

Skype Chat Messages

Description	Skype Chat messages contains Skype chat messages sent from one user to another.
Recovery method	Parsing and carving

Attribute	Description
Chat ID	The ID of the chat.
Profile Name	The profile name of the caller.
Author	The author of the message.
Recipient(s)	The recipient(s) of the chat.
From Display Name	The display name of the message sender.

Attribute	Description
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The body of the message or a description of the action taken. For example, adding another participant to a group chat or sharing a file or picture.
Attachment Name	The name of the attachment that was sent. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Attachment Size (bytes)	The size of the attached file, in bytes. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Metadata	Additional details about the action, extracted in its original XML format.
Message Status	The status of the message.
Message Type	The type of message.

Additional Information

Skype Chatsync Messages

Description	Skype Chatsync Messages contains Skype messages sent from one user to another that are parsed from the chatsync directory.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of this message.
Chat Partner / Group Chat ID	The other part of this message.
Chat Initiator	The initiator of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The content or body of the message.
Message Type	The type of the message.

Additional Information

Skype Contacts

Description	Skype Contacts contains information about Skype contacts that are recovered, which may or may not be added contacts.
Recovery method	Parsing

Attribute	Description
Profile Name	The profile name of the user.
Skype Name	The Skype name of the contact.
Full Name	The full Name of this account

Attribute	Description
Display Name	The display name of this account.
Email(s)	The email of this account.
Last Online Date/Time - UTC (yyyy-mm-dd)	The last time that the account was online.
Is Blocked	Indicates whether the contact is blocked.
Contact Added	Specifies whether the contact is an added contact or just cached into the database (1 if the contact was added, 0 otherwise). Contacts can be cached into the database for a variety of reasons (for example, as a suggested contact).
Birthday (yyyy-mm-dd)	The birthday of this account.
Gender	The gender of this account.
City	The city where this account is located.
State / Province	The state/province where this account is located.
Country	The country where this account is located.
Home Phone	The home phone of this contact.
Office Phone	The office phone of this account.
Mobile Phone	The mobile phone of this account.
PSTN Num-	The PSTN number of this contact.

Attribute	Description
ber	
Homepage	The homepage of this contact.
About Info	The about info of this contact.
Profile Loaded Date/Time - UTC (yyyy-mm-dd)	Previously called Profile Created On Date/Time, this attribute represents the date and time when a contact's profile is first created on the user's device. When the profile information is updated by the contact, the date in the database is also updated.
Mood Text	The text used to express mood.
Last Used On Date/Time - UTC (yyyy-mm-dd)	The last time that the account was used.
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	The time that the avatar was created.
Image	The image for this contact.

Additional Information

Skype Emotions

Description	Skype Emotions contains reactions from users on Skype messages.
Recovery method	Parsing and carving

Attribute	Description
Emotion	The type of emotion that the user reacted to the message with. The emotion is displayed using the shortcut from Skype (for example, "cwl" represents the emotion "Crying With Laughter").
Message Content	The content of the message that the user reacted to. If the content of the message is plain text, this attribute matches the "Message" attribute from the "Skype Activity" artifact. Otherwise, this attribute matches the "Metadata" attribute.
Skype Name	The Skype name of the user who reacted to the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the user reacted to the message.

Additional Information

Skype File Transfers

Description	Skype File Transfers contains files that are transferred from one user to another using Skype.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Partner Handle	The username of the file transfer partner.
Partner Display Name	The display name of the file transfer partner.
File Name	The name of the file that was being transferred.
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the file transfer was started.
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date and time when the file transfer was completed.
File Path	The path to the local file.
Transferred File	The file that was transferred.
Type	The type of file that was being transferred.
File Size (Bytes)	The size of the file being transferred.
Bytes Transferred	The number of bytes that were transferred.
Status	The status of the file (for example, transfer, transferring or cancelled).

Additional Information

Skype Group Chat

Description	Skype Group Chat contains information about the Skype group chats that a user is a part of.

Recovery method	Parsing

Attribute	Description
Chat ID	The group chat's unique identifier.
Profile Name	The name of the user.
Participants	The participants of the chat.
Posters	The users that have posted to the chat.
Active Members	The currently active user's of the group.
Started Date/Time - UTC (yyyy-mm-dd)	The date and time that the chat started.
Chat Name	The name of the chat.
Last Changed Date/Time - UTC (yyyy-mm-dd)	The date and time that the chat was modified.

Additional Information

Skype IP Addresses

Description	Skype IP Addresses contains IP addresses that are associated with a Skype user account.
Recovery method	Parsing and carving

Attribute	Description
Username	The username of Skype accounts.
IP Address	The IP address for the Skype user.
Date/Time - UTC (yyyy-mm-dd)	The date and time.
IP Address Type	The type of IP address (Local or Public).

Additional Information

Skype Notifications

Description	Skype Notifications contains notifications shown to users on Skype.
Recovery method	Parsing and carving

Attribute	Description
Read	Indiactes whether the user has read the notification.
Conversation ID	The ID of this conversation.
Profile Name	The local user's profile name.
Sender	The username of the sender/initiator of the interaction.
Recipient(s)	The recipients or targets of the interaction.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the interaction was initiated.
Last Modified Date/Time -	The date and time that the interaction was last updated (for

Attribute	Description
UTC (yyyy-mm-dd)	example, when a call ends).
Message Type	The type of the interaction.
Message	The content of the message or summary of the interaction.
Emotion Count	The number of reactions to the interaction. Reactions include likes, dislikes, emojis, and more.
File Name	The name of any attached files associated with the interaction.
File Size (Bytes)	The size in bytes of any attached files.
Attachment	The attachment file (if applicable).
Attachment Data Recovered	Indicates whether the attached file was recovered from the local filesystem.
Thumbnail URL	A URL that directs to the thumbnail picture (if applicable).
Metadata	The content of the message, if it consisted of interpreted data (XML or JSON data, rather than plain text).

Additional Information

Skype SMS

Description	Skype SMS contains SMS messages that a user sends or recieves using Skype.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Message Sent Date/Time - (UTC) (yyyy-mm-dd)	The date and time that the message was sent.
Author	The author of the message.
Message	The message content.
Target Number(s)	The phone numbers of the recipients.
Status	The status of the message.
Reply-to Number	A phone number that the recipients can reply to.

Additional Information

Skype Voicemails

Description	Skype Voicemails contains voicemails that a user sends or recieves using Skype.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Partner Handle	The username of the conversation partner.

Attribute	Description
Partner Display Name	The display name of the conversation partner.
Subject	Identifies the subject of the voicemail.
Message Sent Date/Time - (UTC) (yyyy-mm-dd)	The date and time when the message was sent.
Duration	The length of the voicemail.
Allowed Duration	The maximum length allowed for the voicemail.
Size	The size of the recording.
Path	The file path of the voicemail.
Type	Identifies whether the voicemail was received or sent.
Status	The status of the voicemail, recording or played for example.

Additional Information

Slack Accounts

Description	Slack Accounts contains account information on accounts signed onto the local device.
Recovery method	Parsing

Attribute	Description
User	The local user account that is signed onto the device.
Display Name	The local user display name of the account that is signed onto the device.
Email Address	The local user email address of the account that is signed onto the device.
User ID	The Slack local user ID of the account that is signed onto the device. This unique identifier is tied to the Slack workspace that the account is a member of. If an account is signed into multiple Slack workspaces, then there will be a Slack ID generated per workspace.
Account Creation Date/Time (yyyy-mm-dd)	The account creation date/time.
Last Accessed Date/Time	The date/time that the account was last accessed on the device.
Password/Token	The password/token of the account that is signed onto the device.
Group ID	The group ID of the Slack workspace that the account is a member of.
Group Name	The group name of the Slack workspace that the account is a member of.
Domain	The domain of the Slack workspace that the account is a member of.
Service	The Android package ID or Apple bundle ID of the service that the account was used for.

Additional Information

Slack Channel Messages

Description	Slack Channel Messages contains messages sent or received in channels in the user's Slack workspace.
Recovery method	Parsing

Attribute	Description
Workspace ID	The unique identifier for the Slack workspace.
Sender	The name or user ID of whoever sent the message.
Channel Name	The name of the channel that the message was sent to.
Message	The message text.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message Status	The delivered status of the message.

Additional Information

Slack Channels

Description	Slack Channels contains information about each of the channels and conversations that exist in a user's Slack workspace.
Recovery method	Parsing

Attribute	Description
Channel Name	The name of a channel or message group.
Channel ID	The ID of a channel or message group.
Workspace ID	The unique identifier for the Slack workspace.
Created By	The name or user ID of whoever created the channel.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the channel was created.
Topic	The topic text for the channel.
Topic Author	The name or user ID of whoever last wrote the topic text.
Channel Type	The type of channel (Public, Private, General, Single User DM, or Multi User DM.)
Last Read Date/Time - UTC (yyyy-mm-dd)	The date and time when the channel was last read.
Member	Represents whether or not the local user is a member of the channel.
Starred	Represents whether or not the local user has starred the channel.

Additional Information

Slack Direct Messages

Description	Slack Direct Messages contains information about direct messages sent or

	received in 1:1 chats or group chats.
Recovery method	Parsing

Attribute	Description
Workspace ID	The unique identifier for the Slack workspace.
Sender	The name or user ID of whoever sent the message.
Recipient(s)	The name(s) or user ID(s) of the message recipient (s).
Message	The message text.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message Status	The delivered status of the message.

Additional Information

Slack Files

Description	Slack Files contains information about any files that have been saved to the Slack workspace. Files may or may not have been shared with other users.
Recovery method	Parsing

Attribute	Description
Workspace ID	The unique identifier for the Slack workspace
Title	The title given to the file.
File Name	The name of the file.
Created By	The name or user ID of whoever created the file.
Permanent Link	A permalink to the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was uploaded.
FileSize	The size of the file.
Deleted	Represents whether or not the file has been deleted.

Additional Information

Slack Users

Description	Slack Users contains information about each user in the Slack workspace.
Recovery method	Parsing

Attribute	Description
Workspace ID	The unique identifier for the Slack workspace.

Attribute	Description
Full Name	The full name of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
User Name	The unique username of the user.
Display Name	The Slack display name of the user.
Email	The user's email.
Phone Number	The user's phone number.
Member ID	The user's ID.
Title	The user's title.
Status Message	The status message for the user.
Account Type	The type of account that the user has.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the user was last updated.
Timezone	The timezone that the user is in.

Additional Information

Snapchat Cached Videos

Description	Snapchat Cached Videos contains videos stored by the Snapchat application on iOS

Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file.
File Extension	The extension of the file.
Image	A generated thumbnail of the video.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the video file was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the video file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the video was last written to.
Skin Tone Percentage	The amount of skin tone found in the video.
File Size (Bytes)	The size of the video in bytes.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Additional Information

Snapchat Chat Messages

Description	Snapchat Chat Messages contains the chat messages sent between users.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the message.
Recipient(s)	The recipients of the message.
Message ID	The unique ID for the message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the chat message.
Message	The content of the message.
Type	The type of the message. This value can be one of the following: Snap, Text, Media, Voice, Emoji, Call/Deleted message/Mini/Game (Snapchat removed Mini/Game feature in early 2023), Screenshot, Unsuccessful voice call, Unsuccessful video call, or Spotlight.
Saved By Sender	Indicates whether the message was saved by the sender (Yes or No).
Saved By Recipient	Indicates whether the message was saved by the recipient (Yes or No).
Released By	Indicates whether the recipient let the chat message be deleted (Yes or

Attribute	Description
Recipient	No).
Message Status	The status of the message.
Skin Tone Percentage	The calculated percentage of skin tone in the attachment.
MD5 Hash	An MD5 hash of the attachment content.
SHA1 Hash	A SHA1 hash of the attachment content.
Attachment	The attachment content that was decrypted.
Chat ID	The ID of the Snapchat conversation.

Additional Information

Snapchat Contacts

Description	Snapchat Contacts contains information about the user's Snapchat friends as well as contact information from the user's device that was requested by the Snapchat application.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username of the contact.

Attribute	Description
Display Name	The display name of the contact on the local device.
Phone Number	The contact's phone number.
User ID	The unique user identifier of the contact, useful for identifying who may own an account across devices.
Local User	Indicates whether the listed user account is the local account on the device. This is empty if the local user could not be determined.
Legacy User Name	The username that the contact previously used.
Added Them Date/Time - UTC (yyyy-mm-dd)	The date and time that the local user on the device added the contact.
Added Me Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact added the local user on the device.
Contact Type	Indicates the type of contact. App Native indicates that the contact is a Snapchat user, while Device Native indicates that the contact is from the user's device.

Additional Information

Snapchat Conversations - iOS

Description	Snapchat Conversations - iOS contain information about all the chats recovered from the local device.

Recovery method	Parsing and carving

Attribute	Description
Local User	The unique ID for the local user.
Chat ID	A unique ID for the conversation.
Group Name	The group name associated with the conversation.
Creator ID	The unique ID of the creator of the conversation.
Participants	A list of participants that belong to the conversation.
Group Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the group was created.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The date and time in which a message was last sent.

Additional Information

Snapchat Group Members

Description	Snapchat Group Members contains information about participants of the groups that the local user is a member of.
Recovery method	Parsing and carving

Attribute	Description
Group Chat ID	The ID of the group.
Group Name	The name of the group.
Group Member	The user name of the group participant.
User ID	The ID of the group participant.
Added Date/Time - UTC	The date and time that the participant joined the group.
Deleted	Whether the participant left the group (Yes or No)

Additional Information

Snapchat Memories

Description	Snapchat Memories contains pictures and videos that the Snapchat user saves as a memory.
Recovery method	Parsing

Attribute	Description
Entry ID	The ID of the memory.
User ID	The ID of the user.
Created Date/Time - UTC (yyyy-mm-	The date and time when the snap was originally taken.

Attribute	Description
dd)	
Timezone	The time zone of the device when the original snap was taken, or when the media was moved from the device's gallery to the My Eyes Only section of the application.
Type	Indicates whether the memory is saved as a regular snap or My Eyes Only, the latter being password protected.
Media Type	The media type, either Picture, Video, or Video (First Frame). Video (First Frame) indicates that the full video was not recovered.
Duration (Seconds)	The duration of time before the snap expires.
Attachment URL	The url of the memory.
Attachment	The attachment for the memory, if it's not a picture.
Latitude	The latitude of the location where the snap was originally taken.
Longitude	The longitude of the location where the snap was originally taken.
Size (Bytes)	The encrypted size of the snap media. Any overlay that was added to the snap is not included when determining the size of the snap media.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Attachment Path	The file path of the media attachment on the device.
Skin Tone Percentage	The percentage of the picture that appears to be skin tone. Any overlay that was added to the snap is not included when calculating the skin tone.
MD5 Hash	The MD5 hash of the decrypted media. Any overlay that was added to the

Attribute	Description
	snap is not included when creating the hash signature.
SHA1 Hash	The SHA1 hash of the decrypted media. Any overlay that was added to the snap is not included when creating the hash signature.
PhotoDNA Hash	The PhotoDNA hash of the image.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information
To learn how to extract encrypted data from this artifact, see Decrypt app data using the iOS Keychain and GrayKey.

Snapchat My Story - iOS

Description	Snapchat My Story - iOS contains information about a collection of Snaps which can exist for a 24 hour period.
Recovery method	Parsing and carving

Attribute	Description
Local User	The unique ID for the local user.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time when the Snapchat Story was originally created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the Snapchat Story expires and will be automatically deleted.
URL	The URL for the local user's Snapchat Story.

Additional Information

Snapchat Stories - iOS

Description	Snapchat Stories contains information about a collection of snaps, which can exist for a 24 hour period.
Recovery method	Parsing and carving

Attribute	Description
Title	The name of the story.
Creator ID	The unique ID of the user that created the story.
Creator Name	The username of the user that created the story.
Participant IDs	The unique IDs of members of this story.
Participants	The display names or usernames of members of this story.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the story was originally created.
Last Posted Date/Time - UTC (yyyy-mm-dd)	The date and time that content was last posted to the story.
Type	Indicates the type of story (Group, My Story, Private, Shared). All invited

Attribute	Description
	users can contribute to Group and Shared stories. Only the account owner can contribute to My Story and Private stories.
Shared	Indicates whether others can add snaps to this story.
Geofenced	Indicates whether the story is geofenced, meaning only users within a fixed radius of a certain latitude or longitude coordinate can post to and view the story.
Latitude	For geofenced stories, the latitude of the center of the geofence.
Longitude	For geofenced stories, the longitude of the center of the geofence.

Additional Information

Snapchat Story Snaps - iOS

Description	Snapchat Story Snaps contains information about snaps that have been posted to a story.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username of the user that posted the snap.
Display Name	The display name of the user that posted the snap.
Story Name	The name of the story the snap was posted to.

Attribute	Description
Caption	A caption that was added to the snap.
Attachment URL	The URL of any additional attachment linked to the snap.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time when the snap was recorded.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time when the snap was posted to the story.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the snap will expire.
Screenshot Taken	Indicates whether a screenshot of the snap was taken (Yes or No).
Saved By User	Indicates whether the local user saved the snap (Yes or No).
Private	Indicates whether the snap has been posted to a private story.
Attachment Name	The name of the attachment file associated with the snap.
Attachment Path	The path to the attachment file.
Skin Tone Percentage	The calculated percentage of skin tone in the attachment.
MD5 Hash	An MD5 hash of the attachment content.
SHA1 Hash	A SHA1 hash of the attachment content.
Attachment	The attachment content that was decrypted.

Additional Information

TamTam Messenger Channels - iOS

Description	TamTam Messenger Channels contains messages that belong to channel conversations recovered from the local device. The user must be subscribed to the channel in order to receive the messages.
Recovery method	Parsing

Attribute	Description
Sender	The name of the channel in which the message originated.
Sender ID	The TamTam ID of the channel in which the message originated.
Recipient	The display name of the owner contact that received the message.
Recipient ID	The TamTam ID of the owner contact that received the message
Message	The content of the message. If the messages is a contact share, this attribute displays the text from the VCard.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the message.
Latitude	The latitude coordinate, if the message type is Geo location.
Longitude	The longitude coordinate, if the message type is Geo location.
Attachment URL	A URL for any attachments that are sent or received. Attachments can

Attribute	Description
	be downloaded from this URL. However, to recover pictures properly, you must append '&fn=w_1440' manually to the end of the URL.
Attachment	The locally stored attachment, if the attachment was sent by the local user.

Additional Information
In TamTam Messenger 3.0.0, video attachments aren't always available. To learn more, see Reviewing video files from TamTam Messenger v3.0.0.

TamTam Messenger Contacts - iOS

Description	TamTam Messenger Contacts displays information about the TamTam contacts associated with the local user's account (including the local user).
Recovery method	Parsing

Attribute	Description
Contact ID	A unique ID for the contact.
Profile Name	The profile name of the contact.
Website URL	The contact's TamTam website URL, if one exists.
About Info	Information that the user has provided about themself.
Avatar URL	A URL to the user's profile picture. A termination '&fn=w_1440' should be manually added to the URL to properly display the picture.

Attribute	Description
Updated Date/Time - UTC (yyyy-mm-dd)	The last time the contact was updated on the local device. If the contact was not added by the local user, this does not display a value. Some contacts might be stored on the local user's device and may have not been added to their contact list. For example, this might occur when the local user belongs to a group but does not have all of the group participants as contacts. In these cases, TamTam adds the group contacts to the app database but they won't automatically be updated.

Additional Information

TamTam Messenger Conversations - iOS

Description	TamTam Messenger Conversations contains information about all chats recovered from the local device, including individual, group, channel and draft messages.
Recovery method	Parsing

Attribute	Description
Chat ID	A unique ID for the conversation.
Chat Type	The type of conversation (Individual, Group, User Channel, or Default Channel). Individual indicates one-to-one conversations, while Group indicates many-to-many conversations. User Channel indicates a one-to-many conversation created by a TamTam user. Default Channels are one-to-many conversations created and managed by TamTam.

Attribute	Description
Participants	A list of participants that belong to that conversation. User Channels only display the local user as a participant, whereas Default Channels do not display any participants.
Chat Name	The name of the conversation (only available in Groups and Channels).
Description	A description of the conversation (only available in Groups and Channels). Channels may have more than one description in the blob data, the second occurrence is used by default. The first occurrence of the description may be used for default seeded channels.
Conversation Status	Indicates the state of the owner's participation in the conversation.
Last Sent Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time in which a message was last sent.
Address URL	The URL for the channel's webpage. Users can sign up to the channel using this page if the channel is public.

Additional Information

TamTam Messenger Groups - iOS

Description	TamTam Messenger Groups contains all messages that belong to group conversations recovered from the local device.
Recovery method	Parsing

Attribute	Description
Sender	The display name of the contact who sent the message. If the sender is not a contact and therefore unknown to the owner, the TamTam Sender ID is displayed.
Sender ID	The TamTam ID of the contact who sent the message.
Recipient	The display name of the owner user who received the message.
Recipient ID	The TamTam ID of the owner user who received the message.
Message	The content of the message. If the messages is a contact share, this attribute displays the text from the VCard.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the message.
Status	Indicates whether the original message had been edited or deleted by the sender.
Latitude	The latitude coordinate, if the message type is Geo location.
Longitude	The longitude coordinate, if the message type is Geo location.
Attachment URL	A URL for any attachments that are sent or received. Attachments can be downloaded from this URL. However, to recover pictures properly, you must append '&fn=w_1440' manually to the end of the URL.
Attachment	The locally stored attachment.

Additional Information

In TamTam Messenger 3.0.0, video attachments aren't always available. To learn more, see Reviewing video files from TamTam Messenger v3.0.0.

TamTam Messenger Messages - iOS

Description	TamTam Messenger Messages contains all individual messages (one-to-one) recovered from the local device.
Recovery method	Parsing

Attribute	Description
Sender	The display name of the contact who sent the message.
Sender ID	The TamTam ID of the contact who sent the message.
Recipient	The display name of the contact that received the message.
Recipient ID	The TamTam ID of the contact that received the message.
Message	The content of the message. If the messages is a contact share, this attribute displays the text from the VCard.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the message.
Status	Indicates whether the original message had been edited or deleted by the sender.
Latitude	The latitude coordinate, if the message type is Geo location.
Longitude	The longitude coordinate, if the message type is Geo location.
Attachment URL	A URL for any attachments that are sent or received. Attachments can be downloaded from this URL. However, to recover pictures properly,

Attribute	Description
	you must append '&fn=w_1440' manually to the end of the URL.
Attachment	The locally stored attachment.

Additional Information
In TamTam Messenger 3.0.0, video attachments aren't always available. To learn more, see Reviewing video files from TamTam Messenger v3.0.0.

Telegram Channel Chats - iOS

Description	iOS Telegram Channel Chats contains information about the channel chats that the suspect participates in using the Telegram application.
Recovery method	Parsing

Attribute	Description
Chat ID	The ID number for the channel chat.
Title	The title of the channel chat.
Channel Type	The type of channel that the chat happened in (Persistent or Temporary.)
Last Sender	The full name of the user that sent the last message in the chat.
Last Sender Id	The user ID of the user that sent the last message in the chat.

Attribute	Description
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message in the chat.
Last Message	The last message that was sent in the channel chat.
Read Only (Yes/No)	Indicates whether this channel chat is read only to the local user.
Flags	The status flags associated with the chat.

Additional Information

Telegram Chats - iOS

Description	iOS Telegram Chats contains information about the chats that the suspect participates in using the Telegram application.
Recovery method	Parsing

Attribute	Description
Chat ID	The ID number for the chat.
Title	The title of the chat.
Last Sender	The full name of the user that sent the last message in the chat.
Last Sender Id	The user ID of the user that sent the last message in the chat.
Last Message Date/Time	The date and time of the last message in the chat.

Attribute	Description
- UTC (yyyy-mm-dd)	
Last Message	The last message that was sent in the channel chat.
Flags	The status flags associated with the chat.
Number of Participants	The number of people who have actively participated in the chat.
Participant Information	A list of users who have participated in the chat. This data consists of the full name and user ID of each participant.

Additional Information

Telegram Messages - iOS

Description	iOS Telegram Messages contains individual chat messages that are sent and received using the Telegram application.
Recovery method	Parsing

Attribute	Description
Sender Name	The full name of the person who sent the message.
Sender ID	The user ID of the person who sent the message.
Recipient Name	The full name of the person who received the message.
Recipient ID	The user ID of the person who received the message.

Attribute	Description
Message	The content of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Image	The image that was sent or received.
Message Status	The status of the message (Received or Sent).
Read Status	Indicates whether or not the message has been read when the message was received.
Type	The type of the message that was sent or received. This value can be either a Message, Video Call, or System Message.
Secret Chat	Indicates whether a message is sent as a secret chat. This field says 'Yes' if the message is a secret chat, and is empty if it isn't a secret chat.
Message ID	The ID number of the message.
Chat ID	The ID number for the chat that the message was sent in.
Flags	The status flags associated with the message.
Attachment Name(s)	The name of the attachments that were sent.

Additional Information

Telegram Users - iOS

Description	iOS Telegram Users contains information about the various users that the suspect has encountered using Telegram, either directly or as part of a channel chat.
Recovery method	Parsing

Attribute	Description
User ID	The ID number for the user.
First Name	The first name of the user.
Last Name	The last name of the user.
User Name	The user name of the user.
Phone Number	The phone number of the user.
Deleted	Indicates whether or not the user's account has been deleted.
Local First Name	The localized first name of the user. This attribute is unavailable for versions newer than 3.2.2.
Local Last Name	The localized last name of the user. This attribute is unavailable for versions newer than 3.2.2.
Gender	The gender of the user. This attribute is unavailable for versions newer than 3.2.2.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The last time that the user was seen by the local user.

Additional Information

Textfree Attachments

Description	Textfree Attachments contains attachments from the iOS Textfree application.
Recovery method	Parsing and carving

Attribute	Description
Message ID	The ID for the message.
Media URL	The URL from where the media could originaly be downloaded.
Type	The type of media, such as picture, voicemail, or video.
Preview	The binary data of the attachment. If the attachment is a video, the preview is a frame from the video.
Metadata	Any metadata associated with the attachment, such as Voicemail Duration.
Media ID	The internal ID used by the application. This value may point to other places where the attachment is used and/or contained.

Additional Information

Textfree Contacts

Description	Textfree Contacts contains the contacts from the iOS Textfree application.
Recovery method	Parsing and carving

Attribute	Description
First Name	The first name of the contact.
Last Name	The last name of the contact.
Company Name	The company name of the contact.
Phone Numbers	All phone numbers associated with the contact.
Email(s)	All emails associated with the contact.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the contact was modified.
Contact ID	The internal ID used by the application. This value may point to other places where the attachment is used and/or contained.

Additional Information

Textfree Groups

Description	Textfree Groups contains information about group chats from the iOS Text-free applications.
Recovery method	Parsing and carving

Attribute	Description
Group	The group number.

Attribute	Description
Group Phone Number	The phone number of the group.
Group Member Name(s)	The names of all group participants.
Group Member Phone Number(s)	The phone numbers of all group participants.

Additional Information

Textfree Messages / Calls

Description	Textfree Messages contains messages from the iOS Textfree application.
Recovery method	Parsing and carving

Attribute	Description
Sender	The name of the sender.
Sender ID	The ID of the sender.
Recipient(s)	The name(s) of the recipient(s).
Recipient ID(s)	The ID(s) of the recipient(s). This value may contain the contact's phone number.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that is associated with the message.
Message	The content of the message.

Attribute	Description
Type	The type of the message (e.g., Message, Call).
Chat Type	The type of the chat (e.g., Individual, Group).
Direction	The direction of the message (e.g., Outgoing, Incoming).
Call Duration (Seconds)	The call duration in seconds, if the message is a call.
Message Status	The read status of the message (e.g., Read, Unread).
Attachment Type	The type of media file attached (e.g., jpeg, png, wav).
Attachment	The media attached to the message.
Media URL	The URL where the media might have originally been downloaded from.

Additional Information

TextMe Calls

Description	TextMe Calls contains information about the calls that the suspect participates in using the TextMe application.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the call.
Sender Phone Num-	The phone number of the sender.

Attribute	Description
ber	
Recipient	The recipient of the call.
Recipient Phone Number	The phone number of the recipient.
Display Name	The chosen display name for the call participant.
Call Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the call was initiated.
Call End Date/Time - UTC (yyyy-mm-dd)	The date and time when the call ended.
Direction	The direction of the call, either incoming or outgoing.
Status	Whether the call was unanswered, answered, or if the caller left a voicemail.
Call Type	Indicating if the call was an audio call or video call. In later versions of TextMe, this indicates whether the call was 'in', 'out' or 'missed'.
Voicemail	The associated voicemail message.

Additional Information

For iOS TextMe Calls, we cannot determine Call Type (e.g. Audio or Video) or Status (e.g. Answered or Unanswered). Therefore, the columns will always be empty.

TextMe Conversations

Description	TextMe Conversations contains details about all the conversations the

	local user is a part of.
Recovery method	Parsing

Attribute	Description
Chat Name	The name of the conversation.
Participants	The participants of the conversation.
Conversation ID	The ID of the conversation.

Additional Information

TextMe Messages

Description	TextMe Messages contains individual chat messages that are sent and received using the TextMe application.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the message.
Sender Phone Number	The phone number of the sender.
Recipient(s)	The user name(s) of the recipient(s).
Recipient Phone Number	The phone number(s) of the recipient(s).

Attribute	Description
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent, regardless of whether the message was sent or received.
Message	The body of the message.
Direction	Whether the message was sent or received.
Status	Whether the message was unsent, sent, delivered, or read.
Attachment Name	The name of the attachment, if one exists (can be pictures, videos, or URL links).
Attachment Path	The file path of the attachment, if one exists.
Attachment Type	The file type of the attachment, if one exists.
Attachment	The attachment data.
Group Name	The display name of the group.

Additional Information

For iOS TextMe Messages, the attachments are located at the same folder as the database, so the Attachment Path column will always be empty.

TextNow Calls

Description	TextNow Calls contains information about calls and voicemails that are sent and received through the TextNow applications.
Recovery method	Parsing and carving

Attribute	Description
Call Type	The type of call or voicemail.
Direction	Indicates whether the call was incoming or outgoing.
Server Date/Time - UTC (yyyy-mm-dd)	The date and time that the voicemail was registered by the TextNow server.
Device Date/Time - UTC (yyyy-mm-dd)	The date and time that the call or voicemail was registered by the local device.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the call.
Duration (Seconds)	The duration of the call.
Contact ID	The ID for the other call participant.
Local Contact Key	The numeric key for the other call participant.
Contact Display Name	The display name of the other call participant.
Contact Type	The other participant's contact type.
Conversation Type	The type of conversation.
Conversation Partner	The name of the other call participant.
Voicemail URL	The URL of the voicemail.
Call Status	Indicates whether the voicemail was received by the user.
Attachment Path	The voicemail attachment path.
Call ID	The SIP ID of the call.

Additional Information

If the Contact Name cannot be determined, the Local Contact Key may be used to locate the corresponding entry in the iOS TextNow Contacts artifact.

TextNow Chat

Description	TextNow Chat contains chat messages that are sent and received through the TextNow application.
Recovery method	Parsing and carving

Attribute	Description
Message	The body of the message.
Server Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was registered by the TextNow server.
Device Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was registered by the local device.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Contact ID	The ID for the other message participant.
Local Contact Key	The numeric key for the other message participant.
Contact Display Name	The display name of the other message participant.
Contact Type	The other participant's contact type.

Attribute	Description
Message Type	The type of message.
Message Direction	Indicates whether the message was incoming or outgoing.
Conversation Type	The type of conversation.
Author Name	The author of the message.
Message Status	The status of the message (read or unread).
Group Name	The group name, if the message was sent to a group chat.
Signature	The user's appended signature.
Attachment Path	The attachment path.
File Name	The file name of the attachment.
Attachment	The video or picture attachment file that was sent.

Additional Information

If the Contact Name cannot be determined, the Local Contact Key may be used to locate the corresponding entry in the iOS TextNow Contacts artifact.

TextNow Profile

Description	TextNow Profile contains the TextNow user's profile and application preference settings.
Recovery method	Parsing and carving

Attribute	Description
First Name	The first name of the TextNow user.
Last Name	The last name of the TextNow user.
Email	The email of the TextNow user.
User Name	The username of the TextNow user.
Phone Number	The phone number of the TextNow user.
Last Number Called	The last number called using the TextNow application by the user.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the profile information was last updated.
Gender	The gender of the TextNow user.
Birthday (yyyy-mm-dd)	The birthday of the TextNow user.
Forwarding Number	The forwarding number in use by the TextNow user.
Forwarding Expiry UTC (yyyy-mm-dd)	The date and time at which forwarding expires.
Signature	The signature automatically appended to the end of each TextNow message sent by the user.
TextNow Credit	The TextNow credit held by the user.
Balance	The TextNow cash balance held by the user.

Additional Information

TextPlus Calls

Description	TextPlus Calls contains call information from TextPlus data on an iOS device.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username of the TextPlus account.
User	The identifier for the recipient of the call. This could be a GUID or phone number depending on the TextPlus version.
Display Name	The display name of the TextPlus account.
Conversation Name	The name of the conversation.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the call was made.
Call Duration (Seconds)	The duration of the call.
Call Type	The type of the call. This value can be missed, outgoing, or incoming.
Answered	Indicates whether the call was answered or not.
Attachment URL	The URL associated with the voicemail attached to the call.

Additional Information

Group messages are not supported at this time, instead messages sent simultaneously to more than one recipient are displayed as separate hits.

TextPlus Messages

Description	TextPlus Messages contains message information from TextPlus data on an iOS device.
Recovery method	Parsing and carving

Attribute	Description
Sender Name	The sender of the message.
Sender	The identifier for the sender of the message. This could be a GUID or phone number depending on the TextPlus version.
Recipient Name	The recipient of the message.
Recipient	The identifier for the recipient of the message. This could be a GUID or phone number depending on the TextPlus version.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent or received.
Message Body	The text contents of the message.
Message Type	Indicates if the message is an incoming message, outgoing message, or an unknown message type.
Status	Indicates if the message was read ('Read'), unread ('Unread') or has an unknown status.

Additional Information

Threema

Threema is an instant messaging application for iOS and Android, which provides end-to-end encryption of all user communications, including texts, voice calls, media files and more. In addition to providing end-to-end encryption, Threema allows you to create an account without requiring personal information such as your phone number or email address.

The content of a suspect's sent and received messages can be valuable to an investigation, as well as their name and the names of their recipients. Other information can also be recovered, such as the shared location of a suspect, as well as when a message was sent, delivered, and read. This information can help to identify users who have been working with a suspect, the possible whereabouts of a suspect, and can offer insight into the purpose of a suspect's interactions.

Cryptography Details

Threema uses the NaCL Networking and Cryptography Library to provide end-to-end encryption and to secure the transport of incoming and outgoing messages.

Local Data encryption

All messages sent and received using Threema are encrypted and stored on a user's mobile device. On iOS devices, Threema stores a user's local data in a Core Data database, which is backed up by the files found in the application's private data directory. This data includes message history, contacts, and more, and is protected with an encryption key that is created from the device's UID key and passcode. To decrypt the data on an iOS device, the device must be jailbroken or you will need to acquire the device image using GrayKey.

Artifacts

Threema Messages

Threema Users

Threema Messages

Description	Threema Messages contains messages sent and received by the local Threema user.
Recovery method	Parsing

Attribute	Description
Sender	The display name of the sender.
Recipient(s)	The display names of the recipients.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The content of the message.
Read Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was read.
Delivered Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was delivered.
Message Type	The type of message that was sent. This can include Audio, File, Image, Location, Text, or Video.
Message Direction	The direction of the message.
Duration	The duration in seconds of the Audio or Video.
Latitude	The latitude extracted from the location data that is sent with the message.
Longitude	The longitude extracted from the location data that is sent with

Attribute	Description
	the message.
File Name	The name of the file that was sent.
Attachment	The file that was sent.

Additional Information
To learn more about Threema, see Artifact profile: Threema.

Threema Users

Description	Threema Users contains information about the various users that the suspect has encountered using Threema.
Recovery method	Parsing

Attribute	Description
Display Name	The display name of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
Avatar	The avatar of the user.

Additional Information
To learn more about Threema, see Artifact profile: Threema.

Viber Messages

Description	Viber Messages contains details about sent or received Viber messages on an iOS device.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the message.
Sender Name	The name of the person who sent the message.
Recipient(s)	The recipient(s) of the message. In a group chat, the recipients will be shown as a comma-delimited list.
Recipient Screen Name (s)	The screen name(s) of the person(s) who received the message.
Participant	The contact name of one of the participants of the record. It is up to the investigator to determine if this is the local user, or that of the chat partner.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message that was sent. If the message type was a call this will identify if the call was outgoing, incoming or a missed call. For locations the message is a google maps link to the sent location. For images the message can be empty or a blurb of text.

Attribute	Description
Chat Type	The type of conversation where the message originates from (Group chat or One-to-one).
Type	The type of message that was sent. Possible values include Text, Sticker, Call, Video, Location, Notification, and Image.
Message Status	The status of the message. This can be one of the following: 'Sent / Failed', 'Sent / Not Delivered', 'Sent / Delivered', or 'Received'.
Attachment Name	The attachment file name, as stored in the application.
File Attach-ment	The attachment file name, as named by the user.
File Size (Bytes)	The size of the file.
State	The state of the attachment. This can be one of the following: Complete / Pending, Downloading, or Incomplete Upload / Incomplete Download.
Secret Chat	Indicates whether a message is sent in a secret chat (Yes if true).
Expiration (dd hh:mm:ss)	If the message is a secret chat message, this value represents the time limit that the message can be visible for before it disappears. The value is con-verted from seconds and reported as a timestamp in dd:hh:mm:ss format.
Repeat Count	If the message was a call, the number of times that the call was repeated.
File Path	If the message included an attachment, the path to the attachment on the local phone, in the form of a URL.
Location Address	The address for the location that was sent.

Attribute	Description
Latitude	The map latitude location information.
Longitude	The map longitude location information.
Nearby Locations	The locations that are geographically close to the user when they use the Share Location feature within the application (these locations are cached even if a location is not actually shared).
Attachment	The attachment, as stored in the application.

Additional Information

WeChat Friends

Description	WeChat Friends contains stored contact information for the WeChat application on iOS.
Recovery method	Parsing and carving

Attribute	Description
Username	The unique username of the local user's friend. Usernames ending with @chatroom are chat rooms.
Nickname	The nickname of the friend.
Gender	The friend's gender.
Phone Number	The friend's phone number.

Attribute	Description
Email	The friend's email address.
Full Name	The friend's full name.
Participants	A list of the participants that belong to the chat room.
Original Location	The geolocation that is configured from a list of countries and cities when the user creates their account. This is not a real-time location.
Profile Picture URL	The profile picture URL of the friend.

Additional Information

WeChat Messages

Description	WeChat Messages contains stored messages for the WeChat application on iOS.
Recovery method	Parsing and carving

Attribute	Description
Sender User Name	The user name or ID of the sender, as assigned by the application.
Sender Nickname	The display name of the sender, as defined by the user.
Recipient	The user name of the person receiving the message.

Attribute	Description
User Name	
Recipient Nickname	The nickname of the person receiving the message.
Group Chat Name	The name of the group chat, if the message is sent in a group chat.
Group Chat ID	The unique ID of the group chat, if the message is sent in a group chat.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was created on the device.
Message	The content of the message. For Shared Information, Picture, and Location messages, this content will be extracted from XML data. Contact Card messages will display the XML data for the contact.
XML Data	The raw XML data for Shared Information, Picture, and Location messages.
Call Duration (Seconds)	The duration of voice and/or video call in seconds.
Type	The type of the message (Text, Picture, Audio, Friend Request, Contact Card, Video, Animated Emoticon, Location Data, Shared Information, Voice/Video Call, Sight Video, Group Voice/Video Call, Notice, Pay Message, or Location Sharing).
Account	The user name of the account that was used to send the message.
Latitude	The latitude of the location data sent within the message.
Longitude	The longitude of the location data sent within the message.

Attribute	Description
Attachment	The attachment (such as audio, video) associated with the message.
Attachment Data Recovered	Indicates whether attachment data was recovered (Yes or Null).
Attachment Path	The absolute path to recovered message attachments.
Content Format	The content format of successfully recovered audio file attachments. AXIOM Process will attempt to decode audio from SILK V3 to WAV. Successfully converted attachments are saved and playable in AXIOM Examine. Unconverted attachments are saved in their original format and can be manually decoded using another tool or method.

Additional Information

WhatsApp

WhatsAppWhatsApp is a cross-platform mobile messaging app that is owned by Facebook and has over a billion registered users as of 2016. Magnet tools support the recovery of messages, contacts, and attachments from WhatsApp conversations on both Android and iOS devices.Information from these artifacts can help investigators identify who a user communicates with, what they talk about, and the possible whereabouts of a user and their contacts.

WhatsApp for iOS

On iOS devices, the ChatStorage.sqlite database stores most of a user's WhatsApp data, including messages, contact information, sender and recipient information, timestamps, geolocation data, and more. Additional information about a user's contacts is stored the Contacts.sqlite database.

To extract these databases, you can back up the device to a computer or iCloud, and then provide the decryption key to access the contents of each database. The alternative method is to jailbreak the device. While a backup is enough to recover the essential files that are needed to restore the device, jailbreaking recovers all files. To back up the device to a computer, you can use an application such as iTunes. If you set a password on the backup, you will need to provide the password in AXIOM Process to be able to continue with this method. To perform a backup of the iOS device to iCloud, you must provide the user's iCloud password and two-factor authentication details or an authentication token (if 2FA is enabled).

Artifacts

WhatsApp Chats

WhatsApp Contacts

WhatsApp Groups

WhatsApp Messages

Resources

Digital Forensics: Artifact Profile – WhatsApp Messenger

WhatsApp Accounts Information - iOS

Description	WhatsApp Accounts Information - iOS contains account information about the local WhatsApp user.
Recovery method	Parsing

Attribute	Description
Picture	The account's profile picture.
WhatsApp Name	The WhatsApp username that is associated with the account.
ID	The Jabber ID associated with the account.
Phone Number	The phone number used to register the account.
Previous Phone Numbers	Past phone numbers used to register the account.
Status	The current status that the user shares.
Number of Launches	The number of times the WhatsApp application has been launched.
Version	The version of the WhatsApp application.

Additional Information

WhatsApp Chats - iOS

Description	WhatsApp Chats - iOS contains information about chat sessions that occur between the local user and another user or group. This artifact indicates the IDs of each participant as well as information about unread messages and the time when the last message was sent.
Recovery method	Parsing and carving

Attribute	Description
Individual Chat Name	If the chat is with an individual, this value indicates the name of the participant.
Group Chat Name	If the chat is a group chat, this value indicates the name of the group.
Chat ID	The ID of the individual or group involved in the chat.
Unread Message Count	The number of unread messages in the chat.
Last Message	The text body of the last message sent in the chat.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the last message in the chat was sent.

Additional Information

WhatsApp Contacts - iOS

Description	WhatsApp Contacts - iOS contains contacts added to WhatsApp by the local user.
Recovery method	Parsing and carving

Attribute	Description
ID	The unique identifier for the contact.
Phone Number	The contact's phone number.

Attribute	Description
Full Name	The contact's full name.
Given Name	The contact's given (i.e. first) name.
About	Description of the contact in WhatsApp.
Is WhatsApp User	Identifies whether the user is using WhatsApp or not. This is determined by checking the user's status and status updated date and time, because a WhatsApp user cannot have a null status.

Additional Information

To learn more about artifacts from WhatsApp Messenger, sign in to the Support Portal to read the article Artifact profile: WhatsApp Messenger.

WhatsApp Groups - iOS

Description	WhatsApp Groups - iOS contains information about the group chats that the user participates in.
Recovery method	Parsing and carving

Attribute	Description
Group Chat ID	The ID of the group chat.
Group Name	A display name of the group chat.
Creator ID	The ID of the group's creator.
Creator Name	The name of the group's creator.

Attribute	Description
Admin IDs	The IDs of the administrators of the group chat.
Admin Names	The names of the administrators of the group chat.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the group chat was created.
Group Member Name(s)	The names of the members in the group.
Group Member ID(s)	The IDs of the members of the group.

Additional Information

WhatsApp Messages - iOS

Description	WhatsApp Messages - iOS contains information about the messages, media, and calls that are sent and received by the user.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the message. When the sender is an individual, this value is a phone number. When the sender is the local user, or if the account has had multiple phone numbers associated to it, this value is replaced with Local User <Evidence Number>. If the message is received from a group chat or a broadcast message, this value is a WhatsApp ID. For messages received from a group chat, to identify the group you can cross reference this value with the Group Chat ID attribute in iOS WhatsApp

Attribute	Description
	Groups.
Sender Nickname	The nickname of the sender.
Recipient	The message recipient. This value can be a phone number or a WhatsApp ID for group or broadcast messages. If the recipient is the local user, the value will be Local User followed by the evidence number.
Recipient Nickname	The nickname of the recipient.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the message. This may be the sent or received time.
Message	The message text body. This field can also contain additional information about the content that is sent or received, such as picture captions, contact card information or calls status.
Message Direction	Indicates whether the message is incoming or outgoing.
Conversation ID	An ID for the conversation that the WhatsApp message is associated with. This value is used to compile messages into chat threads.
Chat Type	The audience for the message or call. Individual indicates one-on-one messages or calls, Group indicates that the message or call involves more than one user, and Broadcast indicates a message with multiple recipients.
Message Status	The status of the message (Sent/Delivered/Read/Unsent).

Attribute	Description
Type	The type of message or call (Text, Picture, Video, Voice record, Document, Geo-location, Contact, Broadcast, Call not answered, GIF, Deleted message for everyone, Audio call, Video call, Unknown).
Duration	If the message type is audio or video, this value indicates the duration in seconds.
Attachment	The raw data for the picture or file attached to the message. The data is loaded from the local media or file path stored in the database, if the path exists.
Location Address	The address of the location attached to the message. This attribute is only populated if the sender shares their location.
Media URL	The URL for media that's included with the message.
Local Media Path	The local media path stored in the database. By default, this is ZMEDIALOCALPATH from the database, but if it's not available, ZTHUMBNAILLOCALPATH is used instead.
Latitude	The latitude of the location from which the message was sent. This attribute is only populated if the message has type Geo-location.
Longitude	The longitude of the location from which the message was sent. This attribute is only populated if the message has type Geo-location.
Starred	Indicates whether the user bookmarked (or 'starred') a message.
Forwarded	Indicates whether the user forwarded a message to another conversation.

Additional Information

To learn more about artifacts from WhatsApp Messenger, sign in to the Support Portal to read the article Artifact profile: WhatsApp Messenger.

Wickr Me

Wickr Me is a private messaging application for iOS and Android, which provides end-to-end encryption of user communications, including texts, audio and video calls, transmitted locations and more. To ensure the security of your messages, Wickr Me encrypts every sent message with a unique key and gives you the option to control how long these messages will remain available to a recipient once read.

The content of a suspect's sent and received messages can be valuable to an investigation, as well as their username and the usernames of their recipients. Other information can also be recovered, such as the date and time of when messages were sent, delivered and read, and a suspect's shared locations. This information can offer insight into the purpose of a suspect's interactions, identify users who have been in contact with a suspect, and can be used to piece together a timeline of a suspect's activity.

Decrypting messages

Some artifact fragments including message type, read status, timestamps and more, can be viewed without decryption. To access encrypted Wickr Me application data, you will need to provide a key from the target device keychain, or the Wickr Me account password. A common way of obtaining the key is by recovering it from the keychain.plist file that GrayKey generates during an acquisition. To decrypt the application data, add the key to AXIOM Process when you set up your search.

Artifacts

Wickr Me Messages

Related Resources

Decrypt app data using the iOS Keychain and GrayKey

Recover the device keychain

Wickr Me Conversations

Description	Wickr Me Conversations contains details about all the Individual, Group, and Room conversations the local user is a part of.
Recovery method	Parsing

Attribute	Description
Conversation ID	The unique identifier for the conversation.
Participants	The names of all participants in the conversation.
Type	The type of conversation. Individual is used for 1-on-1 or group conversations, and Room is used for room conversations.
Name	The name of the Room. Only populated if the conversation is in a room.
Description	The description of the Room. Only populated if the conversation is in a room.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the last message in this conversation was sent.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the conversation was last synced on the device.

Additional Information

To learn more about Wickr Me, see Artifact profile: Wickr Me.

Wickr Me Messages

Description	Wickr Me Messages contains decrypted and decoded messages sent or received by a Wickr Me user on iOS. These messages can include text messages, call logs, transmitted locations, attachments such as pictures and videos, voice messages, and more.
Recovery method	Parsing

Attribute	Description
Sender	The sender's Wickr username.
Recipient(s)	The recipient's Wickr username.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when this message was sent.
Message	The message content.
Message Type	The message type. This value is interpreted from the ZPRIMARYTYPE. This value can be: Text, Call, Attachment, Location, Key Verification, System Message, or Control (Group Conversation Events).
Chat Type	The type of the chat. This value can be Individual, or Room.
Room Name	The name of the chat room.
Direction	Indicates whether the message was incoming or outgoing.
Read	Indicates whether or not the message was read.

Attribute	Description
Call Duration (Seconds)	The duration of the call in seconds.
Call Status	The status of the call, if applicable. This value can be: Started, Completed, Missed, or Cancelled.
Attachment Name	The file name of the attachment included in the message, if applicable.
Attachment Path	The original file path of the encrypted attachment, if applicable.
Attachment	The decrypted attachment file, if applicable (can include photos, video, or voice messages).
Latitude	The latitude of the coordinates (for transmitted locations only).
Longitude	The longitude of the coordinates (for transmitted locations only).

Additional Information

To learn more about Wickr Me, see Artifact profile: Wickr Me.

Wickr Me Users

Description	Wickr Me Users contains details about the users the local user has interacted with in the app.
Recovery method	Parsing

Attribute	Description
User Name	The name of the user.
User ID	The ID of the user.
Starred	Dictates whether the user has been starred or not.
Hidden	Dictates whether the user is hidden or not.
Blocked	Dictates whether the user is blocked or not.
Bot Account	Dictates whether the user is a bot.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The date and time when the user was last active.
Profile Image	The profile image of the user.

Additional Information
To learn more about Wickr Me, see Artifact profile: Wickr Me.

Zalo Contacts

Description	Zalo Contacts contains the user's Zalo contacts.
Recovery method	Parsing

Attribute	Description
User Name	The contact's username.
User ID	The contact's unique user ID.

Attribute	Description
Profile Picture URL	The contact's profile picture URL.
Gender	The contact's gender.
Phone Number	The contact's phone number.
Birthday (yyyy-mm-dd)	The contact's phone number.
Status	The contact's status message.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact was last active.
Is Friend	Indicates whether the contact is friends with the user.
Type	The contact's type of account.

Additional Information
The Last Activity, Is Friend, and Type columns are empty for iOS.

Zalo Groups

Description	Zalo Groups contains Zalo groups that the user participates in.
Recovery method	Parsing

Attribute	Description
Name	The name of the group.
ID	The unique ID of the chat group.

Attribute	Description
Created By	The username of the person who created the chat room.
Group Member(s)	The usernames of all members in the group.
Number of Participants	The number of participants in the group.

Additional Information

Zalo Messages

Description	Zalo Messages contains messages or calls sent or received using Zalo.
Recovery method	Parsing

Attribute	Description
Sender User Name	The username of the person sending the message.
Recipient User Name	The username of the person receiving the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent on the device.
Direction	The direction of the sent message.
Message	The content of the message.
Picture	The picture attachment in the message.
Attachment	Any non-picture attachments in the message, such as audio or video.

Attribute	Description
Duration (Seconds)	The duration of the call.
Status	The status of the call.
Message Type	The type of the message. This can include text, audio, video and more.
Latitude	The latitude data sent within a message.
Longitude	The longitude data sent within a message.
Media URL	The URL of additional media attachments.
Attachment Path	The absolute path to recovered attachments in a message.

Additional Information

Zalo Profiles

Description	Zalo Profiles contains profile information for the local Zalo user.
Recovery method	Parsing

Attribute	Description
User Name	The user's username.
User ID	The user's unique user ID.
Profile Picture URL	The user's profile picture URL.
Gender	The user's gender.

Attribute	Description
Birthday (yyyy-mm-dd)	The user's birthday.
Phone Number	The user's phone number.
Status	The user's status message.

Additional Information
On iOS devices, the value on the Birthday column is 12 hours behind the actual value. Report Viewer displays this as a 12 hour difference, but because Examine doesn't display hours for a birthday, the value appears as the previous day.

Zello Messages

Description	Zello Messages provides information about the various messages the user has sent and received on the app.
Recovery method	Parsing

Attribute	Description
Sender	The display name of the user who sent the message (Local User if it was the local user).
Recipient	The display name of the user who received the message (Local User if it was the local user).
Message	The content of the message.
Sent Date/Time -	The date and time when the message was sent.

Attribute	Description
UTC (yyyy-mm-dd)	
Direction	Indicates whether the message was incoming or outgoing.
Message Type	The type of message. This can include Alert, Audio Message, Location, Message, Picture, or the actual value with "not parsed" indicated in brackets.
Read	Indicates whether or not the message has been read.
Attachment	The recovered picture attachment.
Latitude	The latitude portion of the location data that is sent with the message.
Longitude	The longitude portion of the location data that is sent with the message.

Additional Information

Zello Profiles

Description	Zello Profiles provides information about the various profiles and channels the user has interacted with on the app.
Recovery method	Parsing

Attribute	Description
User Name	The user name for the profile, this will be empty for channel profiles.

Attribute	Description
Name	The display name for the profile, this will be empty for channel profiles.
Created Date/Time - UTC (yyyy-mm-dd)	The data and time when the profile was created.
Channel Name	The name of the channel, this will be empty if the profile is not a channel.
Channel Type	The type of the channel, this will be empty if the profile is not a channel.
Location Name	The name of the profile location.
Website	The website field for the profile.
About	The about field for the profile
Profile Picture URL	A URL corresponding to the profile image for the profile.

Additional Information

Zoom Channels

Description	Zoom Channels contains information about the channels that the local user participates in.
Recovery method	Parsing

Attribute	Description
Channel ID	The ID of the channel.
Channel Name	The display name of the channel.
Owner ID	The ID of the Zoom user that created the channel.
Participant IDs	The IDs of the participants of the channel.
Participants User Names	The names of the participants of the channel.
Description	A description of the channel, as provided by the creator of the channel.

Additional Information

Zoom Chat Messages

Description	Zoom Chat Messages contains details about Zoom chat messages sent outside of a meeting.
Recovery method	Parsing and carving

Attribute	Description
Sender Name	The name of the person who sent the message.
Sender ID	The ID of the person who sent the message.
Buddy ID	The ID of the person or group that the message was sent to.

Attribute	Description
Recipient Name	The name of the person who received the message.
Recipient ID	The ID of the person who received the message.
Group Chat ID	The ID of the group this message was sent in.
Message ID	The GUID of the message.
Message	The body of the message.
Message Date/Time - UTC (yyyy-mm-dd)	A timestamp that indicates when the message is sent or received, depending on whether the local user is the sender or receiver.
Sender	Indicates whether the message was sent by the local user or a remote user. This value can either be Local User or Remote User.
Read	Specifies whether the message has been read (Yes or No).
Message Type	The type of message that was sent. This value can be one of Message, Picture, File, or Notification.
Attachment Name	The name of the attachment that was sent.
Attachment Local File Path	The local path where the attachment was saved. This value is empty if the attachment was not saved.
Attachment	The contents of the attachment if it can be recovered.

Additional Information

The Attachment Name column is always empty on iOS.

Zoom Contacts

Description	Zoom Contacts contains information about a user's Zoom contacts.
Recovery method	Parsing and carving

Attribute	Description
Buddy ID	The user ID of contact.
Email	The email address of contact.
Display Name	The display name of contact.
Description	A description of the contact, as provided by that user.
Personal Meeting ID	An ID that can be used to start up a meeting with the contact.
Region	The default country or region where the contact is located.

Additional Information

Zoom Meeting Messages

Description	Zoom Meeting Messages contains details about Zoom chat messages sent during a meeting.
Recovery method	Parsing and carving

Attribute	Description
Message ID	The GUID of the message.
Sender Name	The name of the person who sent the message.
Sender ID	The ID of the person who sent the message.
Receiver Name	The name of the person who received the message. If blank, the message was sent to everyone in the meeting.
Receiver ID	The ID of the person who received the message. If zero, the message was sent to everyone in the meeting.
Message	The body of the message.
Message Date/Time - UTC (yyyy-mm-dd)	A timestamp that indicates when the message was sent or received, depending on whether the local user was the sender or receiver.
Read	Specifies whether the message has been read. The displayed value is either 'Yes' or 'No'.
Message Type	The type of message that was sent.
Conference ID	The ID for the meeting the message was sent in.

Additional Information

Zoom User Accounts

Description	Zoom User Accounts contains details about the local user's zoom account.
Recovery method	Parsing and carving

Attribute	Description
User ID	The unique identifier for the user.
User Name	The account's username.
Email	The email address associated with the account.
First Name	The user's first name.
Last Name	The user's last name.
Phone Number	The user's phone number.
Profile Image URL	The URL to the user's profile picture.
Downloaded Profile Image	The data for the profile picture.

Additional Information

Connected Devices

Amazon Alexa Audio Activity

Description	Amazon Alexa Audio Activity contains details about audio activity detected by the Amazon Alexa application.
Recovery method	Parsing and carving

Attribute	Description
Text	The spoken audio as interpreted by the Alexa applic-

Attribute	Description
	ation.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the audio was recorded.
Resource URL	The web resource URL for the audio file.

Additional Information
Data is no longer recoverable for this artifact. This behavior was observed in Amazon Alexa 2.2.358771, but might occur in earlier versions as well. In older versions of this application, data is retrieved from the app's cached data and may not represent a complete record of the user's activities. Accessing the web resource URL requires the user's Alexa login credentials.

Amazon Alexa Device Information

Description	Amazon Alexa Device Information contains details about Alexa-enabled devices.
Recovery method	Parsing and carving

Attribute	Description
Device Name	The name of the device.
Customer ID	The Amazon customer identifier.
Device Type	The type of device.
Serial Number	The serial number of the device.

Attribute	Description
MAC Address	The MAC address of the device.
Network Name (SSID)	The network name to which the device is connected.
ZIP/Postal Code	The ZIP or postal code associated with the device.

Additional Information
Data is no longer recoverable for this artifact. This behavior was observed in Amazon Alexa 2.2.358771, but might occur in earlier versions as well. In older versions of this application, data is retrieved from the app's cached data and may not represent a complete record of the user's activities.

Amazon Alexa Tasks

Description	Amazon Alexa Tasks contains details about shopping lists or other tasks tracked by the Amazon Alexa application.
Recovery method	Parsing and carving

Attribute	Description
Text	The spoken task as interpreted by the Alexa application.
Type	The type of task.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the task was last updated.
Created Date/Time - UTC	The date and time that the task was created.

Attribute	Description
(yyyy-mm-dd)	
Customer ID	The customer ID of the task creator.
Completed	Indicates whether the task has been completed.
Deleted	Indicates hether the task has been deleted.
Similar Text	Text that's similar to the text for the task, as determined by the Amazon Alexa application.
Resource URL	The web resource URL for the audio file.

Additional Information
Data is no longer recoverable for this artifact. This behavior was observed in Amazon Alexa 2.2.358771, but might occur in earlier versions as well. Accessing the audio resource URL requires the user's Alexa login credentials.

Amazon Alexa User

Description	Amazon Alexa User contains details about user accounts recognized by the Amazon Alexa application.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username for the account.
Email	The email that is associated with the account.

Attribute	Description
Device Name	The name of the device.
Customer ID	The Amazon customer identifier.

Additional Information
Data is no longer recoverable for this artifact. This behavior was observed in Amazon Alexa 2.2.358771, but might occur in earlier versions as well. In older versions of this application, data is retrieved from the app's cached data and may not represent a complete record of the user's activities.

Amazon Alexa Web Resource

Description	Amazon Alexa Web Resource contains details about Amazon API resources contacted by the Amazon Alexa application.
Recovery method	Carving

Attribute	Description
Resource URL	The URL for the web resource.
Type	The type of data available from the resource.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the resource request was made.

Additional Information
Data is no longer recoverable for this artifact. This behavior was observed in Amazon Alexa 2.2.358771, but might occur in earlier versions as well. In older versions of this application, data is retrieved from the app's cached data and may not represent a complete record of the user's activities. Accessing the web resource URL requires the user's Alexa login credentials.

Apple Health Distance

Description	Apple Health Distance specifies the distances traveled during activities that were tracked by the iOS device. This data could be synced from another device, such as an Apple Watch. Data about the distance, steps, floors, workout, and heart rate of a user can be particularly useful as it provides a look at a user's activity level at any given time.
Recovery method	Parsing

Attribute	Description
Distance (meters)	The distance of walking or running, in meters.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that this activity started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that this activity ended.
Duration (Minutes)	The duration of the activity, in minutes.
Source Type	The name of the device that generated the health data.
Bundle ID	The bundle name of the application that generated the

Attribute	Description
	health data.
Model ID	The model ID of the device where the data synced from.

Additional Information

Apple Health Floors

Description	Apple Health Floors specifies the number of floors climbed during activities that were tracked by the iOS device. This data could be synced from another device, such as an Apple Watch. Data about the distance, steps, floors, workout, and heart rate of a user can be particularly useful as it provides a look at a user's activity level at any given time.
Recovery method	Parsing

Attribute	Description
Floors	The number of floors climbed.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that this activity started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that this activity ended.
Source Type	The name of the device that generated the health data.
Bundle ID	The bundle name of the application that generated the

Attribute	Description
	health data.
Model ID	The model ID of the device where the data synced from.

Additional Information

Apple Health Heart Rate

Description	Apple Health Heart Rate specifies the average heart rate during activities that were tracked by the iOS device, which will be synced from an Apple Watch. Data about the distance, steps, floors, workout, and heart rate of a user can be particularly useful as it provides a look at a user's activity level at any given time.
Recovery method	Parsing

Attribute	Description
Heart Rate	The average heart rate during the activity rounded to the first decimal place.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the activity started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the activity ended.
Unit	The unit used to measure the heart rate.

Attribute	Description
Source Type	The name of the device that generated the health data.
Bundle ID	The bundle name of the application that generated the health data.
Model ID	The model ID of the device where the data synced from. This may not be available since the data is synced from an Apple Watch.

Additional Information

Apple Health Steps

Description	Apple Health Steps specifies the number of steps taken during activities that were tracked by the iOS device. This data could be synced from another device, such as an Apple Watch. Data about the distance, steps, floors, workout, and heart rate of a user can be particularly useful as it provides a look at a user's activity level at any given time.
Recovery method	Parsing

Attribute	Description
Steps Taken	The total number of steps taken during the activity.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that this activity started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that this activity ended.

Attribute	Description
Duration (Minutes)	The duration of the activity, in minutes.
Source Type	The name of the device that generated the health data.
Bundle ID	The bundle name of the application that generated the health data.
Model ID	The model ID of the device where the data synced from.

Additional Information

Apple Health Workout

Description	Apple Health Workout specifies the duration of the activity that was tracked by the iOS device. This data could be synced from another device, such as an Apple Watch. Data about the distance, steps, floors, workout and heart rate of a user can be particularly useful as it provides a look at a user's activity level at any given time.
Recovery method	Parsing

Attribute	Description
Duration (Minutes)	The duration of the activity, in minutes.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that this activity started.
End Date/Time - UTC (yyyy-	The date and time that this activity ended.

Attribute	Description
mm-dd)	
Source Type	The name of the application that generated the health data.
Bundle ID	The bundle name of the application that generated the health data.
Model ID	The model ID of the device where the data synced from.

Additional Information

Arlo Secure Cached Media

Description	Arlo Secure Cached Media contains the cached media files that have been found inside the Arlo Secure application.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
MIME Type	The MIME type of the media.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.

Attribute	Description
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the media file.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
MD5 Hash	An MD5 hash of the picture content.
SHA1 Hash	A SHA1 hash of the picture content.
PhotoDNA Hash	The hash of the picture content for PhotoDNA.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Exif Data	A searchable field for all raw Exif properties.

Additional Information

Arlo Secure Device Information

Description	Arlo Secure Device Information contains information about the Arlo home security device.
Recovery method	Parsing

Attribute	Description
Device ID	The unique number identifying the device.
Device Name	The name that the user assigned to the device.
Device Type	The type of the device.
Serial Number	The serial number of the device.
Device Hardware Version	The hardware version of the device.
Device Software Version	The software version of the device.
Interface Version	The interface version of the device.
Connection State	The connection state of the device.
Permissions	The user permissions on the device.
Timezone	The timezone set for the device.
User ID	The unique number identifying the device user.
Cloud ID	The unique cloud number identifying the device in the file

Attribute	Description
	system.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the device was set up.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the device was modified by the software, not by the user.
Connection Type	The connection type of the device.
Network Name (SSID)	The network name that the device was connected to.
IP Address	The IP Address of the device.

Additional Information

Arlo Secure User Information

Description	Arlo Secure User Information contains information about user accounts linked to the Arlo home security devices. Please note that latitude and longitude values are based on the address location entered by the user, and do not necessarily reflect GPS reported device locations.
Recovery method	Parsing

Attribute	Description
User ID	The unique number identifying the user.
First Name	The first name of the user.

Attribute	Description
Last Name	The last name of the user.
Email Address	The email address associated with the user account.
Address	User provided full address of the camera.
Latitude	User provided latitude address of the camera.
Longitude	User provided longitude address of the camera.
Location Type	The type of location that the user has specified, such as Residential.
Location Name	The user given name of the location.
Device ID	The list of unique numbers identifying the devices of the user.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the user account was created.

Additional Information

Blink Cached Media

Description	Blink Cached Media contains the cached media files that have been found inside the Blink application.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
MIME Type	The MIME type of the media.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the media file.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
MD5 Hash	An MD5 hash of the picture content.
SHA1 Hash	A SHA1 hash of the picture content.
PhotoDNA Hash	The hash of the picture content for PhotoDNA.

Attribute	Description
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Exif Data	A searchable field for all raw Exif properties.

Additional Information

Blink Device Information

Description	Blink Device Information contains information about the Blink home security device.
Recovery method	Parsing

Attribute	Description
Device ID	The unique number identifying the device.
Device Name	The name that the user assigned to the device.
Device Type	The type of the device.
Serial Number	The serial number of the device.
Created Date/Time - UTC (yyyy-	The date and time that the device was set up.

Attribute	Description
mm-dd)	
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the device was modified by the software, not by the user.

Additional Information

Blink User Information

Description	Blink User Information contains information about the Blink user of the home security device.
Recovery method	Parsing

Attribute	Description
User ID	The unique number identifying the device user.
Email Address	The email address associated with the user account.
Phone Number	The masked phone number associated with the user account (for example, +1******1234).

Additional Information

Bluetooth Devices

Description	Bluetooth Devices contains the Bluetooth devices that the iOS device has paired with.
Recovery method	Parsing

Attribute	Description
MAC Address	The MAC address of the device.
Name	The name that has been assigned to the device.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The last date and time when the device was seen in UTC time.
Last Seen Date/Time - Local Time (yyyy-mm-dd)	The last date and time when the device was seen in Local time.
Major Device Class	The major class of device/service as per the Bluetooth specification.
Minor Device Class	The minor class of device/service as per the Bluetooth specification.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

CarPlay Connected Cars

Description	CarPlay Connected Cars provides information about the different cars that have been connected to the device through CarPlay.
Recovery method	Parsing

Attribute	Description
Car Name	The name of the car.
Bluetooth Address	The Bluetooth address of the car.
WiFi UUID	The Universally Unique ID of the WiFi network.
Wireless CarPlay Supported	Indicates whether the car supports CarPlay when the device is in close proximity to the car.
USB CarPlay Supported	Indicates whether the car supports CarPlay when the device is connected via USB.

Additional Information

CarPlay Recently Used Applications

Description	CarPlay Recently Used Applications provides information about applications that have been recently used through CarPlay.
Recovery method	Parsing

Attribute	Description
Bundle ID	The bundle name of the application, used to uniquely identify it in the application store.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was last used through CarPlay.

Additional Information

DJI Connected Devices

Description	DJI Connected Devices contains information on previously connected devices for the last logged in user of the DJI drone application.
Recovery method	Parsing

Attribute	Description
Product Name	The product name of the connected device.
Last Connected Date/Time - UTC (yyyy-mm-dd)	The most recent date and time when the device was connected.
Serial Number	The serial number of the connected device.
Flight Controller Serial Number	The flight controller serial number of the connected device.
Remote Controller Serial Number	The remote controller serial number of the connected device.

Attribute	Description
Remote Controller Chip Serial Number	The remote controller chip serial number of the connected device.
Camera Serial Number	The camera serial number of the connected device.
Firmware Version	The firmware version of the connected device.

Additional Information

DJI Last Flight Session

Description	DJI Last Flight Session contains information about the flights performed by the most recent connected device.
Recovery method	Parsing

Attribute	Description
Last Known Location Latitude	The last known location latitude of the most recent connected device.
Last Known Location Longitude	The last known location longitude of the most recent connected device.
Last Known Location Date/Time - UTC (yyyy-mm-dd)	The last known location date and time of the most recent connected device.
Total Distance (m)	The total distance flown by the most recent connected

Attribute	Description
	device, in meters.
Total Flights	The total number of flights performed by the most recent connected device.
Total Time (s)	The total time flown by the most recent connected device, in seconds.
Heading	The heading that the most recent connected device was pointing, in degrees relative to true north.
Log File Name	The name of the last recorded flight log file.

Additional Information

DJI Log Files

Description	DJI Log Files contains data from the frame times logged during drone flights, which are extracted from the encrypted log files. Frame time states are logged every tenth of a second and include information about the drone at that point in time. The decrypted log files are stored at your AXIOM temporary file location in a folder called DecryptedLogFiles.
Recovery method	Parsing

Attribute	Description
Latitude	The latitude of the drone when the frame time state was logged.

Attribute	Description
Longitude	The longitude of the drone when the frame time state was logged.
Frame Time Date/Time - UTC (yyyy-mm-dd)	The date and time of the frame time that was captured in the log.

Additional Information
This artifact requires that you allow a decryption option to acquire data. To learn more about this artifact, sign in to the Support Portal to read the article Decrypt DJI Flight Logs.

DJI Media

Description	DJI Media contains the media files that have been found inside the DJI application.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file.
Type	The type of the media. It can be Cached, Saved or Edits.
MIME Type	The MIME type of the media.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.

Attribute	Description
Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the media file.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
MD5 Hash	An MD5 hash of the picture content.
SHA1 Hash	A SHA1 hash of the picture content.
PhotoDNA Hash	The hash of the picture content for PhotoDNA.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Exif Data	A searchable field for all raw exif properties.

Additional Information

DJI User Information

Description	DJI User Information contains user information about the last logged in user of a DJI drone application.
Recovery method	Parsing

Attribute	Description
User Email	The email address of the logged in user.
Device Platform	The device platform used by the logged in user.

Additional Information

Find My Devices

Description	A list of the Apple user's device and device info registered within the Find My application.
Recovery method	Parsing

Attribute	Description
Device Name	The name of the device.

Attribute	Description
Device ID	The device identifier.
Device Model	The internal device model.
Device Type	The device type. E.g. Accessory, Apple Watch, iPad, iPhone, MacBook, etc.
Family Shared	Indicates whether the device is shared using Apple Family Sharing.
Location Address	Last known full street address.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp logged for the last known location.
Pending Remote Wipe	Indicates whether a remote device wipe request was issued for this device.
Remote Wipe Request Timestamp - UTC (yyyy-mm-dd)	The timestamp logged for the remote device wipe request.
Remote Wipe Timestamp - UTC (yyyy-mm-dd)	The timestamp logged when a remote device wipe operation was performed.
Accuracy (meters)	GPS horizontal accuracy (in meters).
Latitude	Latitude of the last known location.
Longitude	Longitude of the last known location.

Additional Information

Find My Items

Description	A list of the Apple user's items registered within the Find My application.
Recovery method	Parsing

Attribute	Description
Device Name	The name of the item tracker.
Serial Number	The unique serial number of the tracker.
Device ID	The product identifier.
Owner Email	The email of the owner of the tracker.
Role	The user assigned role for the item being tracked. E.g. Back-back, Keys, Luggage, etc.
Emoji	The user assigned emoji for the item.
Manufacturer	The manufacturer of the device.
Product ID	Product identifier.
Vendor ID	Vendor identifier.
Operating System Version	The firmware version of the tracker item.
Location Address	The last known full street address.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp logged for the last known location.
Accuracy (meters)	GPS horizontal accuracy (in meters).
Latitude	Latitude of the last known location.
Longitude	Longitude of the last known location.

Additional Information

Find My Locations

Description	A list of crowdsourced or safe locations for the Apple user's device/items registered within the Find My application.
Recovery method	Parsing

Attribute	Description
Device ID	The device or product item identifier.
Device Name	The name of the device or item.
Serial Number	The unique serial number.
Location Type	Type of the location for the device/item (crowdsourced or safe location).
Location Address	The last known full street address.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp logged for the last known location.
Accuracy (meters)	GPS horizontal accuracy (in meters).
Latitude	Latitude of the last known location.
Longitude	Longitude of the last known location.

Additional Information

Fitbit Activity Log

Description	Fitbit Activity Log specifies the activities that were tracked by the Fitbit.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the associated user profile.
Type	The type of physical activity.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the average heart rate calculation.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the average heart rate calculation.
Average Heart Rate (BPM)	The average heart rate.
Steps Taken	The total number of steps taken during the activity.
Distance (Kilometers)	The total distance travelled during the activity.
Duration (Seconds)	The duration of the activity.

Additional Information

Fitbit Floors

Description	Analyzing this data can help identify the number of floors a user has traveled within a day.

Recovery method	Parsing

Attribute	Description
User ID	The user ID of the associated user profile.
Date	The date that the floor-traveling data was generated.
Floors	The number of floors traveled.

Additional Information

Fitbit Profiles

Description	Fitbit Profiles specifies information from the Fitbit profiles that the user has set up on the device.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the associated user profile.
Full Name	The first and last name of the person associated with the profile.
Birthday (yyyy-mm-dd)	The birthday of the person associated with the profile.
Profile Image URL	The location of the profile image.

Attribute	Description
Height (cm)	The height of the person in centimeters.
Gender	The gender of the person.
Walking Stride Length (cm)	The walking stride length of the person in centimeters.
Running Stride Length (cm)	The running stride length of the person in centimeters.
Current Timezone Offset (Minutes)	The timezone offset from GMT, in minutes. This value represents the timezone specified in the user's profile, and does not necessarily represent the user's current location.
Country	The country the profile user may be in.

Additional Information
The Birthday (yyyy-mm-dd) column is always null for iOS devices.

Fitbit Sleep

Description	Fitbit Sleep contains information about the user's sleep patterns.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the associated user profile.

Attribute	Description
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the person went to bed.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the person got out of bed.
Time In Bed (Minutes)	The total time in minutes that the person was in bed (awake and asleep).
Time Awake (Minutes)	The total time in minutes that the person was awake in bed.
Time Asleep (Minutes)	The total time in minutes that the person was asleep.

Additional Information

Fitbit Steps

Description	Fitbit Steps specifies information about the number of steps a person takes while wearing the Fitbit. Steps are aggregated for a 60 minute interval and then stored.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the associated user profile.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the accumulated steps.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the accumulated steps.
Steps Taken	The accumulated steps taken.

Additional Information

Latent Wireless Geolocated Wifi Hotspots

Description	Latent Wireless Geolocated WiFi Hotspots contains information about WiFi hotspots that were discovered using a Latent Wireless device. Latent Wireless stores information about the hotspots in a database that Magnet AXIOM can parse for details about each hotspot.
Recovery method	Parsing

Attribute	Description
MAC Address	The MAC address of the detected WiFi hotspot.
First Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was first discovered.
Last Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was last seen.
Strongest Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was detected at its highest strength.
Network Name (SSID)	The SSID of the WiFi hotspot.
Channel	The WiFi hotspot channel.
RSSI	The received signal strength indicator for the WiFi hotspot.
Latitude	The latitude where the WiFi hotspot was detected.

Attribute	Description
Longitude	The longitude where the WiFi hotspot was detected.
Secure	Indicates whether the WiFi hotspot is secure.

Additional Information

Nest Location Configuration

Description	Nest Location Configuration contains configuration and settings related to the structure housing the Nest system.
Recovery method	Parsing and carving

Attribute	Description
Location Name	The name of the location.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the location configuration was created.
City	The local city.
State / Province	The local state or province.
Country Code	The local country code.
ZIP/Postal Code	The local ZIP or postal code.
Latitude	The local latitude.

Attribute	Description
Longitude	The local longitude.
Structure Area (Square Meters)	The floor size of the structure, in square meters.
Emergency Contact Description	The description of the emergency contact.
Emergency Contact Phone	The phone number for the emergency contact.

Additional Information

Nest Temperature Adjustment

Description	Nest Temperature Adjustment contains details about thermostat temperature adjustments made through the Nest application.
Recovery method	Parsing

Attribute	Description
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the adjustment was made.
User ID	The identifier for the user.
Temperature (Celsius)	The temperature setting.
Scheduled Time (Local)	The local time of day at which the temperature adjustment is to take effect.
Scheduled Day	The day of the week at which the temperature adjustment is to take effect.

Additional Information

Nest User

Description	Nest User contains details about Nest user accounts.
Recovery method	Parsing and carving

Attribute	Description
Email	The user's email.
Name	The user's name.
User ID	The user identifier.
Device Location	The location of the primary Nest device.
Profile Image URL	The URL for the user's profile image.

Additional Information

Pebble Activity Information

Description	Pebble Activity Information specifies the physical activities that were tracked by the Pebble watch.
Recovery method	Parsing

Attribute	Description
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the activity.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the activity.
Duration (Seconds)	The duration of the activity.
Steps Taken	The total number of steps taken during the activity.
Active Calories (Cal)	The number of calories burned during the activity.
Serial Number	The serial number of the Pebble watch used to track the activity.

Additional Information

Pebble Calendar Events

Description	Pebble Calendar Events contains calendar events that are displayed on the Pebble Watch Timeline.
Recovery method	Parsing

Attribute	Description
Title	The title of the calendar event.
Description	A short description of the calendar event.

Attribute	Description
Locale	The location of the event.
Calendar Display Name	The display name of the calendar to which the event belongs.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the event.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the event.
Organizer Name	The organizer of the event.
Calendar Account	The calendar to which the event belongs.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was created on the Pebble application.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was updated.
User Account	The user account observing the event.
Attendees	The number of attendees to the event.
Is Recurring	Indicates whether the event is recurring.
Organizer	Indicates whether the user is the organizer of the event.

Additional Information

The following columns are always null for iOS devices: Organizer Name, Owner Account, Created Date/Time, Updated Date/Time, Calendar Account, Attendees, Is Recurring, and Organizer.

Pebble Physical Characteristics

Description	Pebble Physical Characteristics specifies the user's activity profile information.
Recovery method	Parsing

Attribute	Description
Gender	The gender of the user.
Age	The age of the user.
Height (cm)	The height of the user in centimeters.
Weight (kg)	The weight of the user in kilograms.

Additional Information

Pebble Steps

Description	Pebble Steps specifies the steps information tracked by the Pebble smart watch.
Recovery method	Parsing

Attribute	Description
Start Date/Time - UTC (yyyy-	The start date and time of the steps occurance.

Attribute	Description
mm-dd)	
Steps Taken	The number of steps taken during a one minute duration from the start time.
Active Calories (Cal)	The number of active calories burned in the one minute.

Additional Information

Pebble Weather Locations

Description	Pebble Weather Locations contains location information that's tracked by the Pebble Watch.
Recovery method	Parsing

Attribute	Description
Location Name	The name of the tracked location.
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time of the location data.
Updated Date/Time - UTC (yyyy-mm-dd)	The updated date and time of the location data.

Additional Information
The latitude and longitude are not a precise values, but they can place the Pebble Watch in a specific city.

Ring Cached Media

Description	Ring Cached Media contains the cached media files that have been found inside the Ring application.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
MIME Type	The MIME type of the media.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the media file.
Original Width	The original width of the picture, before any applied resizing.
Original	The original height of the picture, before any applied resizing.

Attribute	Description
Height	
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
MD5 Hash	An MD5 hash of the picture content.
SHA1 Hash	A SHA1 hash of the picture content.
PhotoDNA Hash	The hash of the picture content for PhotoDNA.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Exif Data	A searchable field for all raw Exif properties.

Additional Information

Ring Device Information

Description	Ring Device Information contains information about Ring home security devices. Please note that latitude/longitude values are based upon user entered address location and do not necessarily reflect GPS reported device locations.
Recovery method	Parsing

Attribute	Description
Device ID	The unique number identifying the device.
Device Name	The name that the user assigned to the device.
Device Type	The type of the device.
User ID	The unique number identifying the device user.
Owner ID	The unique number identifying the owner of the security system.
Address	The full address of the camera location set by the user.
Timezone	The timezone set for the device.
Latitude	The latitude of the camera's address set by the user.
Longitude	The longitude of the camera's address set by the user.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the device was set up.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the device was modified by the software, not by the user.

Additional Information

Ring User Information

Description	Ring User Information contains information about the Ring user of the home security device.
Recovery method	Parsing

Attribute	Description
User ID	The unique number identifying the device user.
First Name	The first name of the user.
Last Name	The last name of the user.
Email Address	The email address associated with the user account.
Phone Number	The phone number associated with the user account.
Two-Factor Authentication Phone Number	The two-factor authentication (2FA) phone number associated with the user account.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the device was set up.

Additional Information

Seen Bluetooth Devices

Description	Seen Bluetooth Devices keep track of Bluetooth devices that may have been seen by the host device.
Recovery method	Parsing

Attribute	Description
Device Name	The name of the Bluetooth device.
Bluetooth Address	The MAC address of the Bluetooth device.
UUID	The Universially Unique Identifier of the record.

Additional Information

SIM Card Activity

Description	SIM Card Activity contains information about the SIM cards that have been used in an iOS device.
Recovery method	Parsing and carving

Attribute	Description
ICCID	The unique identifier for the SIM card.
Phone Number	The phone number associated with the SIM card.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the SIM card data was updated.
SIM Card Slot	The slot on the phone that the SIM card was inserted in.

Additional Information

SIM Card ICCID

Description	SIM Card ICCID contains the ICCID number that identifies the device's SIM card.
Recovery method	Parsing

Attribute	Description
ICCID	The integrated circuit card identifier.

Additional Information

SIM Card IMSI

Description	SIM Card IMSI contains IMSI numbers used to identify the mobile subscriber, as recovered from the SIM card.
Recovery method	Parsing

Attribute	Description
IMSI	The international mobile subscriber identity.

Additional Information

SIM Card Phone Numbers

Description	SIM Card Phone Numbers contains records of all the phone numbers saved to the device SIM card. The type of number is indicated by the record type.
Recovery method	Parsing

Attribute	Description
Phone Number	The phone number for the specific record type.
Label	The optional contact description/name of the phone number stored on the SIM card.
Record Type	Identifies the type of record that the phone number is. The Record Type value can be Abbreviated dialing numbers (ADN), Emergency call codes (ECC), Last number dialed (LND), MSISDN, Service dialing numbers (SDN), or Fixed dialing numbers (FDN).

Additional Information

SIM Card Service Providers

Description	SIM Card Service Providers contains the names of mobile service providers that the device has connected with, and which are recovered from the SIM card.
Recovery method	Parsing

Attribute	Description
Service Provider Name	The identity of the mobile phone service provider.

Additional Information

SIM Card SMS Messages

Description	SIM Card SMS Messages contains messages sent or received by the local user which were saved to the SIM card.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the SMS message.
Recipient	The recipient of the SMS message.
Message Date/Time	For incoming messages, this timestamp indicates when the message was received by the mobile service center. For outgoing messages, there is no data available for this field.
Message	The message body of the SMS message.
Deleted	Identifies whether the message has been deleted (Yes or No).
Message Status	Identifies whether the message has been read, unread, drafted or sent.
SMSC	The short message service center number.

Additional Information

Your Phone Contacts

Description	Your Phone Contacts contains information about contacts synced from a

	mobile device to a computer using Your Phone. The Your Phone application can sync data from Android and iOS devices to computers running Windows 10.
Recovery method	Parsing

Attribute	Description
Display Name	The contact's display name.
Nickname	The contact's nickname.
Phone Number	The contact's phone number.
Type	The type of phone number associated with the contact, for example Home, Mobile, or Business.
Last Time Contacted Date/Time - UTC (yyyy-mm-dd)	The last time that this contact either sent a message to, or received a message from the synced device or local user since the Your Phone application was installed.
Number of Times Contacted	The number of times the synced device or local user either sent a message to, or received a message from the contact since the Your Phone application was installed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that this contact's details were modified.

Additional Information

Your Phone Devices

Description	Your Phone Devices contains information about the devices that are synced to the user's computer by using the Your Phone application.
Recovery method	Parsing

Attribute	Description
Application Version	The version of Your Phone running on the computer.
Last Run Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was last run on the computer.
Device Application Version	The version of the Your Phone companion application running on the device.
Device ID	A GUID identifier generated to uniquely identify devices within the Your Phone application.
Device Name	The name provided by the device and displayed in the user interface when referring to it.
Device Platform	The device's platform (Android or iOS).
Device Messages Synced Date	The date and time when the device last synchronized its messages data with Your Phone.
Computer Messages Synced Date	The date and time when the computer last synchronized its messages data with Your Phone.
Device Contacts Synced Date	The date and time when the device last synchronized its contacts data with Your Phone.

Attribute	Description
Computer Contacts Synced Date	The date and time when the computer last synchronized its contacts data with Your Phone.
Device Photos Synced Date	The date and time when the device last synchronized its picture data with Your Phone.
Computer Photos Synced Date	The date and time when the computer last synchronized its picture data with Your Phone.

Additional Information

Your Phone Pictures

Description	Your Phone Pictures contains information about pictures synced from a mobile device to a computer using Your Phone. The Your Phone application syncs the 25 most recently taken photos from Android and iOS devices to computers running Windows 10.
Recovery method	Not applicable

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.

Attribute	Description
Device ID	A GUID identifier generated to uniquely identify devices synced using the Your Phone application.
Device Name	The name of the device (as provided by the device) which is displayed in the user interface for Your Phone.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial

Attribute	Description
	indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
GPS Lon-	The GPS longitude coordinates of where the picture was taken (extracted

Attribute	Description
gitude	from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS Latitude (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicates whether the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.
Exif Data	A searchable field for all raw exif properties.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Your Phone SMS/MMS

Description	Your Phone SMS/MMS contains information about messages synced from a mobile device to a computer using Your Phone. The Your Phone application can sync data from Android and iOS devices to computers running Windows 10.
Recovery method	Parsing and carving

Attribute	Description
Sender	The phone number that sent the message.
Recipient(s)	The phone number(s) the message was sent to.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message content.
Message Direction	Indicates whether the message was sent or received by the synced device or local user.
Message Type	Indicates whether the message is SMS or MMS.
Message Status	Indicates whether the message has been read.
Attachment Name	The name of the attached file, if applicable (MMS only).

Additional Information

Custom

File Signature Mismatch (Audio)

Description	File Signature Mismatch (Audio) contains identified mismatches between a known file signature header and the extension (or lack thereof) for an audio file. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file. If we don't know what the MIME type is, we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is, we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type, we return a mismatch.
File Path	The path to the mismatched file.
Attachment	The mismatched file.

Additional Information

File Signature Mismatch (Container)

Description	File Signature Mismatch (Container) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a container. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file. If we don't know what the MIME type is, we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file. If we don't know what the MIME type is, we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type, we return a mis-match.
File Path	The path to the mismatched file.
Attachment	The mismatched file.

Additional Information

File Signature Mismatch (Document)

Description	File Signature Mismatch (Document) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a document. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file. If we don't know what the MIME type is, we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file. If we don't know what the MIME type is, we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type, we return a mis-match.
File Path	The path to the mismatched file.
Attachment	The mismatched file.

Additional Information

File Signature Mismatch (Picture)

Description	File Signature Mismatch (Picture) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a picture. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file. If the mime type is unknown, this defaults to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file. If the mime type is unknown, this defaults to application/octet-stream. If there is no file extension, but the mime type is known, a mismatch is is returned.
File Path	The path to the mismatched file.
Attachment	The mismatched file.

Additional Information

File Signature Mismatch (Video)

Description	File Signature Mismatch (Video) contains identified mismatches between a

	known file signature header and the extension (or lack thereof) for a video. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file. If we don't know what the MIME type is, we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file. If we don't know what the MIME type is, we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type, we return a mismatch.
File Path	The path to the mismatched file.
Attachment	The mismatched file.

Additional Information

Documents

Apple Notes

Description	Apple Notes contains information about the notes that a user has created on their iOS device.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the note.
Folder	The folder that the note is stored in.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the note was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the note was last modified.
Body	The body of the note. This fragment may contain the Object Replacement Character (U+FFFC) which indicates a non-text note is presented such as a picture, video, etc. If the non-text note is found, it will be presented as an attachment.
Summary	The summary of the note.

Attribute	Description
Attachments	A list of attachments contained in the note.
Encrypted	Indicates whether or not the note has been encrypted.
Password Hint	The hint to the encryption password.
Note ID	The notes unique identifier.

Additional Information
To learn how to extract encrypted data from this artifact, see Decrypt app data using the iOS Keychain and GrayKey.

Apple Notes - Voice

Description	Apple Notes Voice contains the recovered voice notes from an iOS device.
Recovery method	Parsing

Attribute	Description
Label	The label of the note.
Audio	The saved voice note.
Saved Date/Time - UTC (yyyy-mm-dd)	The date and time that the voice note was saved.

Attribute	Description
Duration (Seconds)	The duration of the voice note in seconds.
Path	The path to the voice note on the device.
Note ID	The ID of the note.
Version	The version of the note: Original, Duplicate (duplicate copy of the original), Duplicate - Edited (duplicate copy of the original and partly modified), Edited (edited copy of an original note).
Original Path	The path to the original version of an edited note.

Additional Information

CSV Documents

Description	CSV Documents contains CSV documents (.csv) that are located on the system.
Recovery method	Parsing

Attribute	Description
File Name	The name of the CSV document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last modified.
Accessed Date/Time - UTC (yyyy-	The date and time that the CSV document was last

Attribute	Description
mm-dd)	accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was created.
File Content	The content of the CSV document.
Size (Bytes)	The size of the CSV document in bytes.
SHA1 Hash	The SHA1 hash of the contents of the document.
MD5 Hash	he MD5 hash of the contents of the document.

Additional Information
For information about supported formats, see Supported media and file types.

Evernote Accounts

Description	Evernote Accounts contains information about the user accounts that have been used to log in on the device.
Recovery method	Parsing

Attribute	Description
User Name	The display name of the user's account
User ID	The user ID of the account.
Email	The email address associated with the account.

Attribute	Description
Full Name	The full name associated with the account.
Active Account	Indicates which account was active at the time of acquisition.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the account was created.
Login Date/Time - UTC (yyyy-mm-dd)	The date and time that the account was initially logged in on the device.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the account was last updated.

Additional Information

Evernote Contacts

Description	Evernote Contacts contains information about users that have communicated with the local user account.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the contact.
Contact ID	The contact ID of the contact.
Account Name	The account name of the contact.

Additional Information

Evernote Notes

Description	Evernote Notes contains any notes associated with the local user, including notes shared from other users to the local user.
Recovery method	Parsing

Attribute	Description
Title	The title of the note.
Content	The content of the note.
Type	The type of note.
File Name	The name of the attachment that was included with the note.
File	The attachment that was included in the note.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was created.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was updated.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was deleted.
Owner	The owner of the note. If a note is shared from one user to another, the owner is the user that shared the note.

Attribute	Description
Shared With	The accounts that the note was shared with.
Last Modifier Name	The username of the last modifier of the note.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time of the starting time for the reminder of the note.
End Date/Time - UTC (yyyy-mm-dd)	The date and time of the end time for the reminder of the note.
Locale	The location where the note was taken.
Latitude	The latitude of the location where the note was taken.
Longitude	The longitude of the location where the note was taken.
Notebook Name	The name of the notebook where the note was saved.

Additional Information

Evernote Work Chat

Description	Evernote Work Chat contains messages sent and received by the local user.
Recovery method	Parsing

Attribute	Description
Sender ID	The unique ID of the sender.

Attribute	Description
Sender Name	The name of the sender.
Sent Date/Time	The date and time when the message was sent.
Message Body	The body of the message.
Participants	The participants of the chat.
Participant IDs	The participant IDs of the chat.

Additional Information

Google Docs Items

Description	Google Docs Items contains information about the documents and folders that have been accessed using Google Docs on the device.
Recovery method	Parsing

Attribute	Description
Account ID	The unique account identifier of the local user.
Title	The title of the item.
File ID	The unique identifier of the item.
File Type	The mime type of the item.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was created.

Attribute	Description
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was modified.
Shared With Me Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was shared with the local user.
Last Viewed By Me Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was last viewed by the local user.
Deleted	Indicates whether the item was deleted.
Starred	Indicates whether the item was starred.
Folder	Indicates whether the item is a folder.
Owner	Indicates whether the local user is the owner of the item.

Additional Information

Google Docs Thumbnails

Description	Google Docs Thumbnails contains information about thumbnail pictures of the Google Docs documents found on the device.
Recovery method	Parsing

Attribute	Description
File ID	The unique identifier of the item.
Account ID	The unique account identifier of the local user.
Attachment	The generated thumbnail of the document
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was modified.

Additional Information

Google Sheets Items

Description	Google Sheets Items contains information about the spreadsheets and folders that have been accessed using Google Sheets on the device.
Recovery method	Parsing

Attribute	Description
Account ID	The unique account identifier of the local user.
Title	The title of the item.
File ID	The unique identifier of the item.
File Type	The mime type of the item.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was created.
Modified Date/Time - UTC (yyyy-mm-	The date and time when the item was modified.

Attribute	Description
dd)	
Shared With Me Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was shared with the local user.
Last Viewed By Me Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was last viewed by the local user.
Deleted	Indicates whether the item was deleted.
Starred	Indicates whether the item was starred.
Folder	Indicates whether the item is a folder.
Owner	Indicates whether the local user is the owner of the item.

Additional Information

Google Sheets Thumbnails

Description	Google Sheets Thumbnails contains information about the thumbnail pictures of Google Sheets spreadsheets found on the device.
Recovery method	Parsing

Attribute	Description
File ID	The unique identifier of the item.

Attribute	Description
Account ID	The unique account identifier of the local user.
Attachment	The generated thumbnail of the document
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was modified.

Additional Information

Google Slides Items

Description	Google Slides Items contains information about the presentations and folders that have been accessed using Google Slides on the device.
Recovery method	Parsing

Attribute	Description
Account ID	The unique account identifier of the local user.
Title	The title of the item.
File ID	The unique identifier of the item.
File Type	The mime type of the item.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was modified.

Attribute	Description
Shared With Me Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was shared with the local user.
Last Viewed By Me Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was last viewed by the local user.
Deleted	Indicates whether the item was deleted.
Starred	Indicates whether the item was starred.
Folder	Indicates whether the item is a folder.
Owner	Indicates whether the local user is the owner of the item.

Additional Information

Google Slides Thumbnails

Description	Google Slides Thumbnails contains information about thumbnail pictures of the Google Slides presentations found on the device.
Recovery method	Parsing

Attribute	Description
File ID	The unique identifier of the item.
Account ID	The unique account identifier of the local user.

Attribute	Description
Attachment	The generated thumbnail of the document
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the item was modified.

Additional Information

Journals

Description	The Journal artifact contains information about everyday moments and special events of the current user. It may include photos, videos, audio recordings, locations, and more.
Recovery method	Parsing

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the original journal entry was created.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the journal entry was updated.
Title	The title of the journal entry (in raw RTC format).
Text	The text of the journal entry (in raw RTC format).
Attachment Path	The path of the attachment associated with the journal entry.
Attachment Type	The type of the attachment associated with the journal entry.

Attribute	Description
Metadata	The metadata of the attachment associated with the journal entry.
Attachment Data Recovered	Indicates whether the attached file was recovered from the local file system (Yes if recovered).

Additional Information
Journal entries with multiple attachments will display one hit per attachment. The preview card for the journal entry contains the content of both the Title and Text fragments.

Microsoft Excel Documents

Description	Microsoft Excel is a spreadsheet processor developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File	The actual file.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.

Attribute	Description
Size (Bytes)	The size of the document.
Title	The title metadata.
Saved Size (Bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
Subject	The subject metadata.
Authors	The authors of the document.
Keywords	The keywords in the metadata of the document.
Comment	The comments metadata.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

Microsoft PowerPoint Documents

Description	Microsoft PowerPoint is a presentation creator developed by Microsoft. This table captures documents created with PowerPoint, extracted from the filesystem and carved from unallocated space.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File	The actual file.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
Size (Bytes)	The size of the document.
Title	The title of the file.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Subject	The subject of the file.
Authors	The authors of the file.

Attribute	Description
Keywords	The keywords in the metadata of the file.
Comment	The comments in the metadata of the file.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

Microsoft Word Documents

Description	Microsoft Word is a word processor developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File	The actual file.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
Size (Bytes)	The size of the document.
Title	The title of the file.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Comment	The comments in the metadata of the file.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information
For information about supported formats, see Supported media and file types.

PDF Documents

Description	Portable Document Format (PDF) is a file format used to present documents in a manner independent of application software, hardware, and operating systems. This table captures documents in this file format, extracted from the filesystem and carved from unallocated space.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
Title	The title of the file.
Authors	The authors of the file.
Last Modified Date/Time - UTC	The date and time when the document was last modified,

Attribute	Description
(yyyy-mm-dd)	extracted from metadata within the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Subject	The subject of the file.
Keywords	The keywords in the metadata of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
MD5 Hash	An MD5 hash of the PDF content.
SHA1 Hash	A SHA1 hash of the PDF content.
File	The PDF file.

Additional Information

For information about supported formats, see Supported media and file types.

Reminders

Description	iOS Reminders contains information about the reminders, such as due dates and to do lists, that a user has created and accessed in the Reminders app on their device.
Recovery method	Parsing

Attribute	Description
Title	The title of the reminder.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the reminder was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the reminder was last modified.
List Name	The name of the list the reminder belongs to.
Notes	The notes that the user added to the reminder.
Completed	Indicates whether the user has marked the reminder as complete.
Completion Date/Time - UTC (yyyy-mm-dd)	The date and time when the reminder was completed.
Due Date/Time - UTC (yyyy-mm-dd)	The date and time that the user selected as the reminder's due date.
Deleted	Indicates if the reminder was deleted.

Additional Information

RTF Documents

Description	RTF Documents contains information for each RTF document that was recovered from the search.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the RTF document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was created.
File Content	The contents of the RTF document.
File Size (Bytes)	The size of the RTF document.
MD5 Hash	A MD5 hash of the RTF content.
SHA1 Hash	A SHA1 hash of the RTF content.

Additional Information

For information about supported formats, see Supported media and file types.

Text Documents

Description	Text documents (.txt) that are located on the system.
Recovery method	Parsing

Attribute	Description
Filename	The name of the text document.
Size (Bytes)	The size of the text document in bytes.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was created.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.
File Content	The content of the text document.

Additional Information

For information about supported formats, see Supported media and file types.

Email and Calendar

Apple Mail

Description	Apple Mail contains the emails and the fragments of emails that have been extracted from an iOS device.
Recovery method	Parsing and carving

Attribute	Description
To	Who the email was sent to.
From	Who sent the email.
Subject	The subject of the email.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was sent.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was received.
Body	The body of the email. Email bodies formatted in valid html are decoded from quoted-printable.
CC	Who was CC'd on the email.
BCC	Who was BCC'd on the email.
Headers	The headers that are sent with the email.
Summary	The first 512 bytes of the email summary.

Attribute	Description
Size	The size of the email.
Attachment Name(s)	The name(s) of the attachment(s) sent with the email.
Attachment Data Recovered	Indicates if the email attachments were recovered.
Mailbox	The mailbox that the email is in.
Read	States whether or not the email has been read.
Deleted	States whether or not the email has been deleted.
Importance	The importance of the email, set by the sender.

Additional Information

Calendar Events

Description	The iOS calendar application is a default application on iOS.
Recovery method	Parsing and carving

Attribute	Description
Summary	A summary of the calendar appointment.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the appointment starts.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the appointment ends.

Attribute	Description
Event Location	The location of the calendar appointment.
Notes	Notes about the calendar appointment.
Calendar	The name of the calendar from which the event was generated.
Attendees	The attendees of the event.
Timezone	The timezone the appointment is in.
URL	A URL associated with the event.

Additional Information

EML(X) Files

Description	EML(X) Files contains the emails in .eml and .emlx formats that have been found on the device.
Recovery method	Parsing

Attribute	Description
To	The recipients of the email.
From	The sender of the email.
Date/Time	The date and time that the email was sent or received.
Subject	The subject of the email.

Attribute	Description
Body	The body of the email.
CC	The users that received the email by CC.
BCC	The users that received the email by BCC.
Headers	The raw email headers.
Importance	The email importance setting.
Last Read Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was last read, if the data is available.
MD5 Hash	An MD5 hash of the email content.
SHA1 Hash	A SHA1 hash of the email content.
Attachment Name(s)	A list of attachments on the email.

Additional Information

EML(X) files are used by various applications, including the default Mail app and the Airmail app. There might be duplicate results from this artifact and email clients such as Apple Mail, if they originated from the same file. We encourage you to check the source of the hits to determine whether or not they originated from a mail client.

Gmail Emails

Description	Gmail Emails contains the Gmail email fragments that were recovered from an Android device.
Recovery method	Parsing

Attribute	Description
To Address(es)	The recipient(s) of the email.
From Address	The sender of the email.
Thread ID	The ID of the conversation the email is from. Emails with the same Thread ID belong to the same conversation.
Subject	The subject of the email.
Sent Date/Time - UTC (yyyy-mm-dd)	The date that the email was sent.
Received Date/Time - UTC (yyyy-mm-dd)	The time that the email was received.
Email Body	The body of the email.
Email Snippet	A snippet of the email.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Reply Address(es)	The reply-to address for the email.
Attachment Data Recovered	Indicates whether attachments for the email were recovered.
Attachments	The file names of any attachments for the email.
Saved Attachments	The file paths of any attachments for the email which were saved locally.
Date/Time - UTC (yyyy-mm-dd)	The date and time when message was either sent or received.

Additional Information

Google Calendar Calendars

Description	Google Calendar Calendars contains a list of all the calendars the user has synced to their Google account.
Recovery method	Parsing

Attribute	Description
Account ID	The account ID assigned by Google
Calendar Display Name	The name of the calendar.
Description	The description of the calendar.
Timezone	The timezone of the calendar.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the calendar was created.
Visibility	Indicates if the calendar is visible or hidden on the phone.
Access	The level of permissions the user has for the calendar (Owner Access or Read Only).
Calendar ID	A unique ID for the calendar.

Additional Information

Google Calendar Events

Description	Google Calendar Events contains information about a user's calendar events on the Google Calendar application.
Recovery method	Parsing

Attribute	Description
Event Name	The name of the event.
Description	The description of the event.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time of the event.
Event End Date/Time - UTC (yyyy-mm-dd)	The date and time of the end of the event.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time of when the event was created.
Invitees	The email addresses of those invited to the event.
Event ID	The unique ID of the event.
Account ID	The unique identifier of the owner of the account.
Owner Email	The email address of the owner of the event.
Owner Name	The name of the owner of the event.
Calendar ID	The unique ID of this calendar.
Calendar Display Name	The display name of the calendar to which the event

Attribute	Description
	belongs.
Event Location	The location of the event.
Latitude	The latitude of the event.
Longitude	The longitude of the event.
Location URL	The unique location URL for the event's location.
Recurrence	The recurrence of the event.
Event URL	The unique URL of the event.

Additional Information

Google Calendar Reminders

Description	Google Calendar Reminders contains information about the reminders that a user has set in their calendars.
Recovery method	Parsing

Attribute	Description
User Email	The email of the owner of the reminder.
Title	The name of the reminder.
Due Date - UTC (yyyy-mm-dd)	The set due date of the reminder.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the reminder was created.
Snoozed	Indicates if the reminder is snoozed or not.
Recurrence Id	ID assigned by Google to link together recurring reminders.
Recurrence Frequency	The frequency of the recurring reminder (Daily, Weekly, Monthly, or Yearly).
Recurrence Start Date Time	The date and time of when the recurring reminders started.
Recurrence End Date	The date when the reminders stop recurring.
Recurrence Daily Pattern	Indicates the time (HH:mm:ss) or 'All Day' when the daily recurring reminder occurs.
Recurrence Weekly Pattern	Indicates the day of the week (Monday-Sunday) when the weekly recurring reminder occurs.
Recurrence Monthly Pattern	Indicates the date (1-31) when the monthly recurring reminder occurs.
Recurrence Yearly Pattern	Indicates the month and date (January-December, 1-31) when the yearly recurring reminder occurs.

Additional Information

iOS Yahoo Mail Contacts

Description	iOS Yahoo Mail Contacts contains contact details for local user accounts in

	iOS Yahoo Mail application.
Recovery method	Parsing

Attribute	Description
Profile Email	The email address of the local account.
Contact Email	The email address of the contact.
Contact Display Name	The display name of the contact. The Yahoo Mail application may sometimes erroneously store the contact's email address in this column.
Contact Given Name	The given name of the contact.
Contact Family Name	The family name of the contact.
Contact Family Name Sound	The user-specified pronunciation guide for the contact's family name. The Yahoo Mail application may sometimes erroneously store the contact's family name in this column.
Contact Given Name Sound	The user-specified pronunciation guide for the contact's given name. The Yahoo Mail application may sometimes erroneously store the contact's given name in this column.

Attribute	Description
Contact Middle Name	The middle name of the contact.

Additional Information

iOS Yahoo Mail Messages

Description	iOS Yahoo Mail Messages contains emails stored by iOS Yahoo Mail application.
Recovery method	Parsing

Attribute	Description
Account	The email address of the local account.
From	The email address or username of the sender.
To	The email address or username of the recipient(s) in the 'To' field.
Subject	The subject line of the email.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the email was received.
HTML Body	The email body, in HTML format.
CC	The email address or username of the recipient(s) in the

Attribute	Description
	'Cc' field.
BCC	Email address or username of the recipient(s) in the 'Bcc' field.
Snippet	A short preview of the text of the email body.
Content Type	The content type of the email body, in MIME format.
Folder	The name of the folder in which this email is stored.
Read	Indicates whether the email has been read (Yes or No).
Replied	Indicates whether the local account has replied to this email (Yes or No).
Forwarded	Indicates whether the local account has forwarded this email (Yes or No).
Flagged	Indicates whether the email has been flagged (Yes or No).
Erased	Indicates whether the email has been erased (Yes or No).
Draft	Indicates whether the email is a draft (Yes or No).
Attachment Name(s)	The list of file names of the attachments on this email, if any.

Additional Information

iOS Yahoo Mail User Accounts

Description	iOS Yahoo Mail User Accounts contains local user accounts for iOS Yahoo Mail application.
Recovery method	Parsing

Attribute	Description
Email	The email address of the user account.
User	The user ID of the user account.
Name	The full name of the user.
First Name	The first name of the user.
Last Name	The last name of the user.

Additional Information

Outlook Appointments

Description	Microsoft Outlook is a personal information manager and email client. Outlook Appointments captures information related to appointments scheduled in Microsoft Outlook.
Recovery method	Parsing

Attribute	Description
Sender Name	The person who requested the appointment.
Sender Exchange Account	The sender's Exchange account name.
Recipients	The recipients of the appointment invitation.
Subject	The subject of the appointment.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the appointment starts.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the appointment ends.
Body	The body of the appointment description.
CC	The CC'd recipients of the appointment invitation.
BCC	The BCC'd recipients of the appointment invitation.
Companies	The companies involved in the appointment.
Attachments	The attachments for the appointment.
Locale	The location of the appointment.
Is All-day Event	Indicates if the appointment is an all-day event.
Is Recurring	Indicates if the appointment is recurring.
Recurrence Pattern Description	Describes the recurrence pattern of the appointment, if applicable.
Sensitivity	Indicates if the appointment is sensitive.
Is Hidden	Indicates if the appointment is hidden.

Attribute	Description
Is Private	Indicates if the appointment is private.
Priority	The priority of the appointment.
Importance	The appointment importance setting.
MD5 Hash	The MD5 hash of the appointment.
SHA1 Hash	The SHA1 hash of the appointment.

Additional Information

Outlook Contacts

Description	Microsoft Outlook is a personal information manager and email client. Outlook Contacts captures information related to contacts stored in Microsoft Outlook.
Recovery method	Parsing

Attribute	Description
Display Name	The contact's display name.
Customer ID	The customer ID of the contact.
Email Address 1	The contact's primary email address.
Email Display As 1	The display string of the contact's primary email address.

Attribute	Description
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact details were last modified.
Company Name	The contact's company name.
Department Name	The contact's department name.
Title	The contact's job title.
Profession	The contact's profession.
Manager Name	The name of the contact's manager.
Office Location	The contact's office location.
Business Address	The physical address of the business.
Business Phone	The contact's business phone number.
Business Phone 2	The contact's secondary business phone number.
Business Fax	The contact's business fax number.
Business Homepage	The website of the contact's business.
Email Display Name 1	The display name of the contact's primary email address.
Email Address 2	The contact's secondary email address.
Email Display As 2	The display string of the contact's secondary email address.
Email Display Name 2	The display name of the contact's secondary email address.
Email Address 3	The contact's tertiary email address.

Attribute	Description
Email Display As 3	The display string of the contact's tertiary email address.
Email Display Name 3	The display name of the contact's tertiary email address.
Cellular Phone	The contact's mobile phone number.
Home Address	The contact's home address.
Home Phone	The contact's home phone number.
Home Phone 2	The contact's secondary home phone number.
Home Fax	The contact's home fax number.
FTP Site	The contact's FTP site.
Body	More information about the contact.
Attachments	Any attachments to the contact entry.
Last Modifier Name	The name of the person who last modified the contact details.
MD5 Hash	The MD5 hash of the contact.
SHA1 Hash	The SHA1 hash of the contact.

Additional Information

Outlook Emails

Description	Microsoft Outlook is a personal information manager and email client. Outlook Messages captures information related to emails sent and received in Microsoft Outlook.
Recovery method	Parsing

Attribute	Description
Sender Name	The sender of the email.
Sender Email	The email address of the sender.
Recipients	The recipients of the email.
Subject	The subject of the email.
Sender Exchange Account	The sender's Exchange account name.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was created.
Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the email synced with the HxStore platform.
Submitted	The date and time that the email was submitted.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Delivered Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was delivered.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was last modified.
Body	The body of the email. For HxStore data sources that include email bodies deleted when an account was removed, the displayed value is the path where the email body was located on the file system.
Folder Name	The name of the folder where the email is stored.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Attachments	The list of attachments on the email.
Headers	The raw email headers.
Priority	The priority of the email.
Importance	The importance of the email.
Sensitivity	The sensitivity of the email.
Read	Indicates whether the email was opened and therefore marked as Read.

Attribute	Description
	Note that Outlook users can also manually mark emails as either Read or Unread.
MD5 Hash	The MD5 hash of the email.
SHA1 Hash	The SHA1 hash of the email.

Additional Information

Encryption and Credentials

Apple Keychain Generic Passwords

Description	Apple Keychain Generic Passwords contains passwords for applications and services that are saved to the Keychain application. Analyzing results from this artifact can reveal valuable passwords and tokens that are associated with the user's accounts.
Recovery method	Parsing

Attribute	Description
Keychain Property	The keychain property of the keychain item.
Value	The secret value that's associated with the account. The values that have non-printable characters are converted to hex strings. To see what the raw data looks like before conversion, export the hit with attachments.

Attribute	Description
Service Name	The name of the service that has stored data in the keychain.
Account	The account identifier of the keychain item parsed from the 'Keychain Property'.
Password/Token	The password or token of the keychain item parsed from the 'Value'.
Access Group	The access group that the keychain item belongs to.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was last modified.
Original Location	The offset of the keychain item in the keychain database.

Additional Information

Apple Keychain Internet Passwords

Description	Apple Keychain Internet Passwords contains passwords for websites and internet services that are saved to the Keychain application. Analyzing results from this artifact can reveal valuable passwords and tokens that are associated with the user's accounts.
Recovery method	Parsing

Attribute	Description
Label	The label of the keychain item.
Description	The description of the keychain item.
Account	The account identifier of the keychain item.
Value	The secret value that's associated with the account. Values that have non-printable characters are converted to hex strings. To see what the raw data looks like before conversion, export the hit with attachments.
Access Group	The access group that the keychain item belongs to.
DSID	The Destination Signaling Identifier is a unique identifier assigned to a user when they register an iCloud account.
Server	The server address for an internet password item.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was last modified.
Original Location	The associated location of the keychain item in the original SQLite database on the original iOS device.

Additional Information

Apple Keychain Saved Credit Cards

Description	Apple Keychain Saved Credit Cards contain credit card entries saved to the Keychain application.
Recovery method	Parsing

Attribute	Description
Name On Card	The name of the credit card owner as displayed in the card.
Card Number	The credit card number (if available).
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the credit card entry was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the credit card entry was last modified.
Expiry Date	The expiry date of the credit card in month-year format.
Original Location	The associated location of the keychain item in the original SQLite database on the original iOS device.

Additional Information

Location and Travel

Apple Maps Favorites

Description	Apple Maps Favorites contains information about a user's favorited locations.
Recovery method	Parsing

Attribute	Description
Name	The name of the favorited location.
Address	The full address of the favorited location.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the favorited location was added.
Latitude	The latitude coordinate of the favorited location.
Longitude	The longitude coordinate of the favorited location.

Additional Information

Apple Maps Searches

Description	Apple Maps Searches contains searches generated by the user using Apple Maps.
Recovery method	Parsing

Attribute	Description
Search Term	The string of the query used to search for the address.
Address	The full address of the location searched.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the search was created on the device.
Latitude	The latitude portion of the location searched.
Longitude	The longitude portion of the location searched.

Additional Information

Apple Maps Trips

Description	Apple Maps Trips contains trips generated by Apple Maps. Instances of this artifact can be suggested routes as well as trips that the user actually takes.
Recovery method	Parsing

Attribute	Description
Origin Address	The full address of the origin point.
Destination Address	The full address of the destination point.
Origin Lat-	The latitude portion of the origin coordinate.

Attribute	Description
itude	
Origin Longitude	The longitude portion of the origin coordinate.
Destination Latitude	The latitude portion of the destination coordinate.
Destination Longitude	The longitude portion of the destination coordinate.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the user left the origin location of interest
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the user arrived the destination location of interest.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the trip was created on the device or synced on the device. This value does not reflect the time that the user took the trip. This value can also represent the time that the application suggested a route.
Search Term	The string of the query used to search for the destination.

Additional Information

Cached Locations

Description	Cached Locations stores a sample of locations that the iOS device has cached. Each instance contains the location, speed, and direction of travel at that particular point in time. The frequency that location samples are cached can vary depending on device usage, where some applications (such as Maps) can result in samples being cached very frequently.
Recovery method	Parsing and carving

Attribute	Description
Latitude	The latitude of the stored location.
Longitude	The longitude of the stored location.
Accuracy (m)	The radius of horizontal accuracy of the latitude and longitude values.
Altitude (m)	The altitude of the stored location.
Altitude Accuracy (m)	The accuracy of the altitude value.
Direction	The direction of travel of the stored location, measured in degrees and relative to due north.
Speed (m/s)	The instantaneous speed captured for the stored location sample.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the location was recorded.

Additional Information

iOS Google Map Coordinates

Description	iOS Google Map Coordinates contains Google map tile coordinates viewed on an iOS device.
Recovery method	Parsing

Attribute	Description
Image	The map image for the location specified by the X, Y coordinates of a map tile.
Last Touched Date/Time - UTC (yyyy-mm-dd)	The last date and time that the user searched or navigated to the coordinates in Google Maps.
Latitude	The latitude coordinate in decimal degrees.
Longitude	The longitude coordinate in decimal degrees.
X Coordinate	The map tile X coordinate.
Y Coordinate	The map tile Y coordinate.
Zoom Level	The zoom level within the map for the map tile.

Additional Information

When a user searches an address/place, or when the user navigates an area by dragging and zooming the map, Google Maps will display the searched address/place and the surrounding area in the map view. Google Maps might also zoom or adjust the map to give the user a better view of the area. These actions can trigger a change in the Google Map Tiles database, which often results in multiple hits (sometimes hundreds) that represent the areas in tiles that the user viewed. Due to the latency of downloading the data, the last touched

Additional Information
date/time for these hits can vary by several seconds from each other. Taking this behavior into account, you can typically consider hits within a similar time frame to be part of one user action. For more information on iOS Google Map Coordinates, see: Tile coordinates section.

iOS Maps

Description	iOS Maps contains images from iOS maps that were recovered from the device.
Recovery method	Parsing

Attribute	Description
Image	The map tile image.
Labels	Text description of places in the map tile.
Accessed Date/Time	The time the map was searched on the device.
Size (Bytes)	The size of the map image.

Additional Information

iOS Wi-Fi Profiles

Description	Wi-Fi Profiles contains a list of the saved Wi-Fi Profiles on a mobile device.

Recovery method	Parsing

Attribute	Description
Network Name (SSID)	The name of the network.
MAC Address	The MAC Address of the network.
Last Auto Joined Date/Time - UTC (yyyy-mm-dd)	The last date and time that the wireless network was automatically joined by the device.
Last Joined Date/Time - UTC (yyyy-mm-dd)	The last date and time that the wireless network was manually joined by the device.
Security Mode	The security mode of the network.

Additional Information

Lyft Account Information

Description	Lyft Account Information stores information associated with the user's account.
Recovery method	Parsing

Attribute	Description
First Name	The first name of the account holder.

Attribute	Description
Last Name	The last name of the account holder.
Email	The email associated with the account.
Phone Number	The phone number associated with the acount.
Share Code	A unique share code associated with the rider.
Photo URL	The URL of the account's current profile picture.

Additional Information

Lyft Last Known Location

Description	Lyft Last Known Location contains the application user's last known location as recorded by Lyft.
Recovery method	Parsing

Attribute	Description
Latitude	The GPS latitude of the last known location.
Longitude	The GPS longitude of the last known location.
Altitude (m)	The altitude in meters of the last known location.
Date/Time	The date and time when the location was recorded.

Additional Information

Lyft Location Shortcuts

Description	Lyft Location Shortcuts contains information about the locations for which the user has created shortcuts.
Recovery method	Parsing

Attribute	Description
Shortcut Name	The user-defined name of the shortcut.
Tag	The tag that defines the type of shortcut (home, work, or custom).
Location Name	The name of the location based on Lyft's map API.
Address	The address of the shortcut's location.
Latitude	The latitude of the shortcut's location.
Longitude	The longitude of the shortcut's location.
Date/Time - UTC (yyyy-mm-dd)	The date and time the shortcut was cached.

Additional Information

Lyft Rider Payment Details

Description	Lyft Rider Payment Details contains information about the user's payment profile.

Recovery method	Parsing

Attribute	Description
Payment Method	The method of payment made, such as Apple Pay.
Payment Type	The type of payment made, such as Visa or MasterCard.
Payment Profile ID	The ID of the payment profile.
Card Display Name	The payment card display name.

Additional Information

OnStar RemoteLink Hotspot Info

Description	OnStar RemoteLink Hotspot Info contains information about the vehicle WiFi hotspots associated with an OnStar account.
Recovery method	Parsing

Attribute	Description
Network Name (SSID)	The name of the vehicle's hotspot.
Network Password	The password of the vehicle's hotspot.
Created Date/Time	The date and time that the hotspot was created.

Attribute	Description
Updated Date/Time	The date and time that the hotspot was updated.
VIN	The Vehicle Identification Number that the hotspot is associated with.

Additional Information

OnStar RemoteLink Remote Commands

Description	OnStar RemoteLink Remote Commands contains information about commands sent from the device.
Recovery method	Parsing

Attribute	Description
Requested Command	The command requested by the user.
Request State	The state of the request.
Sent Date/Time	The date and time that the command was sent to the vehicle.
Completion Date/Time	The date and time that the command was completed.
Command Description	The description of the command that was sent, if available.
VIN	The Vehicle Identification Number of the vehicle that the command

Attribute	Description
	was sent to.
Request ID	The ID of the request that was sent, if available.

Additional Information

OnStar RemoteLink Saved Wireless Carrier

Description	OnStar RemoteLink Saved Wireless Carrier contains information about the wireless accounts associated with a vehicle.
Recovery method	Parsing

Attribute	Description
Carrier Account ID	The account identifier of the carrier account.
Carrier Type Code	The code that represents the account type.
Carrier Type Description	The carrier that is associated with the account.
Created Date/Time	The date and time when the account entry was created on the device.
Updated Date/Time	The date and time when the account entry was updated on the device.
Account Type	The type of wireless account.

Attribute	Description
Account Description	The description of the account type.
VIN	The Vehicle Identification Number of the vehicle that the wireless account is associated with.

Additional Information

OnStar RemoteLink Searches

Description	OnStar RemoteLink Searches contains possible searched locations.
Recovery method	Parsing

Attribute	Description
Original Search Query	The original search query requested by the user.
Search Date/Time	The date and time of the search.
GPS Latitude	The GPS latitude where the search was performed.
GPS Longitude	The GPS longitude where the search was performed.
Type	The type of returned search results.
Location Name	The name or address of the result destination.
Distance (meters)	The distance, in meters, to the result destination.
Destination Latitude	The latitude of the result destination.
Destination Longitude	The longitude of the result destination.

Additional Information

OnStar RemoteLink Vehicle Diagnostics

Description	OnStar RemoteLink Vehicle Diagnostics contains information about the diagnostic values retrieved from the vehicle.
Recovery method	Parsing

Attribute	Description
Diagnostic Name	The name of the diagnostic test that was retrieved.
Unit	The unit of measurement associated with the diagnostic test.
Value	The value associated with the diagnostic test.
Created Date/Time	The date and time that the diagnostic value was retrieved.
Updated Date/Time	The date and time that the diagnostic value was updated.
Completion Date/Time	The date and time that the server retrieved the diagnostic value from the vehicle.
VIN	The Vehicle Identification Number of the vehicle that the diagnostic value was retrieved from.

Additional Information

OnStar RemoteLink Vehicle Info

Description	OnStar RemoteLink Vehicle Info contains information about the vehicle associated with the account.
Recovery method	Parsing

Attribute	Description
VIN	The Vehicle Identification Number of the vehicle associated with the account.
Vehicle Make	The make of the vehicle.
Vehicle Model	The model of the vehicle.
Year	The year of production of the vehicle.
Created Date/Time	The date and time when the vehicle information was added to the device.
Updated Date/Time	The date and time when the vehicle information was updated on the device.
Phone Number	The phone number associated with the vehicle.
Account Number	The OnStar account number that the vehicle is associated with.

Additional Information

Parked Car Locations

Description	Parked Car Locations contains the locations of a user's vehicle that they've saved and which are tracked by the iOS device.
Recovery method	Parsing

Attribute	Description
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that this log was entered into the cache.
Latitude	The latitude of the Parked Car Location.
Longitude	The longitude of the Parked Car Location.

Additional Information

Significant Locations

Description	Significant Locations contains information about places that are deemed to be significant in some way to the user. These locations can be manually added by the user (such as a home or work address) or are automatically added by Apple. This data is used to help make more personalized predictions.
Recovery method	Parsing

Attribute	Description
Location Name	The name of location.
Address	The address of the location.
City	The city of the location.
Country	The country of the location.
State/Province	The state or province of the location.
ZIP/Postal Code	The ZIP or postal code of the location.
Location Type	The type of location set by the user.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the location was saved.
Latitude	The latitude of the location.
Longitude	The longitude of the location.

Additional Information

Significant Locations Visits

Description	Significant Locations Visits contains information about the saved significant locations that the user visits. These location visits are automatically tracked by the device when the user is in the vicinity.
Recovery method	Parsing and carving

Attribute	Description
Address	The address of the location visited.
City	The city of the location.
Country	The country of the location.
State/Province	The state or province of the location.
ZIP/Postal Code	The ZIP or postal code of the location.
Vicinity Entry Date/Time	The date and time that the user entered the vicinity of the location.
Vicinity Exit Date/Time	The date and time that the user exited the vicinity of the location.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the visit entry was saved.
Latitude	The latitude of the location visited.
Longitude	The longitude of the location visited.
Accuracy	The distance from the original geographic coordinate that could yield the user's actual location. The unit of measurement is presumed to be meters.

Additional Information

Uber Accounts

Description	Uber Accounts contains account information about riders, as recovered from the Uber application (passenger only).
Recovery method	Parsing

Attribute	Description
First Name	The first name of the account holder.
Last Name	The last name of the account holder.
Mobile Phone	The mobile phone number associated with the acount.
Email	The email associated with the account.
Share Code	A unique share code associated with the rider.
User ID	The user ID uniquely identifying the account.
Password/Token	The unique token associated with the account.
Latitude (On App Startup)	The latitude of the user when the application was last opened.
Longitude (On App Startup)	The longitude of the user when the application was last opened.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the user last opened the application.
Last Payment Profile ID	The ID of the payment profile that was last used by the user.
Profile Image URL	The URL of the profile image for the account.

Attribute	Description
Downloaded Profile Image	The profile picture of the account.
Service	The Android package ID or Apple bundle ID of the service that the account was used for.

Additional Information

Uber Cached Locations

Description	Uber Cached Locations contains information about locations that Uber caches, such as the initial location at the time of application startup or locations from a trip (passenger only).
Recovery method	Parsing

Attribute	Description
Address	The address of the cached location.
Name	The name of the cached location.
Latitude	The GPS latitude of the cached location.
Longitude	The GPS longitude of the cached location.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the location was cached.
Tag	The tags assigned to the location by the user. These tags are user generated.
Categories	The categories assigned to the location by Uber.

Additional Information

Uber Locations

Description	Uber Locations contains the latitude and longitude of various locations, as recovered from the Uber application (passenger only).
Recovery method	Parsing

Attribute	Description
Latitude	The recorded GPS latitude.
Longitude	The recorded GPS longitude.
Altitude (meters)	The altitude recorded for the current location.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the current location was saved.

Additional Information

Uber Payments

Description	Uber Payments contains payment information associated with a user's Uber rides, as recovered from the Uber application (passenger only).
Recovery method	Parsing and carving

Attribute	Description
Rider Name	The name of the passenger or rider.
Share Code	The unique share code associated with the rider.
Cost	The cost of the trip.
Currency	The currency used to measure the cost of the trip.
Duration (Seconds)	The duration of the trip in seconds.
Distance (Kilometers)	The distance of the trip in Kilometers.
Payment Method	The method of payment.
Card Display Name	The payment card display name.

Additional Information

Uber Profiles

Description	Uber Profiles contains information about a user's Uber profiles, as recovered from the Uber application (passenger only).
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the profile.
Profile Email	The email associated with the profile.

Attribute	Description
Profile User ID	The unique user ID (UUID) associated with the profile.
Profile Payment User ID	The unique user ID that is the payment method for this profile.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the profile was created.

Additional Information

Uber Rider Payment Details

Description	Uber Rider Payment Details contains information about the user's payment profile, such as their payment method and fare-splitting info (passenger only).
Recovery method	Parsing

Attribute	Description
Card Display Name	The payment card display name.
Payment Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the payment is set to expire.
Payment Profile ID	The ID of the payment profile.
Status	The status of the payment.
Payment Method	The method of payment, such as Visa or Master-

Attribute	Description
	Card.
Country	The country associated with the payment profile.
ZIP/Postal Code	The ZIP Code associated with the payment profile.
Last Fare Split Name	The name of the person who the user last split a ride fare with.
Last Fare Split Phone Number	The number of the person who the user last split a ride fare with.

Additional Information

Uber Trips

Description	Uber Trips contains information about a user's Uber rides, as recovered from the Uber application (passenger only).
Recovery method	Parsing

Attribute	Description
Booking Date/Time UTC (yyyy-mm-dd)	The date and time when the trip was booked.
Origin Address	The address of the original start location.

Attribute	Description
Destination Address	The address of the final destination.
Arrival Date/Time UTC (yyyy-mm-dd)	The date and time when the vehicle arrived at the destination address.
Duration (Seconds)	The duration of the trip in seconds.
Distance	The distance of the trip (units unknown).
Driver Name	The first name of the driver.
Vehicle Make	The make of the driver's vehicle.
Vehicle Model	The model of the driver's vehicle.
Vehicle Type	The type of uber car service.
Driver Rating	The driver's rating.
Driver Picture URL	The URL to the driver's profile picture.
Cost	The cost of the trip.
Currency	The currency used to measure the cost of the trip.
Status	The status of the trip.
Route Map URL	The URL to the route taken in the trip.

Additional Information

Waze Events

Description	Waze Events can contain information about upcoming trips that a user

	has planned.
Recovery method	Parsing

Attribute	Description
Name	The name of the place.
Address	The house number and street name of the place.
City	The city of the address.
State	The state or province of the address.
Country	The country of the address.
Start Date/Time	The start date and time recommended for the planned drive.
End Date/Time	The date and time that the user has planned to arrive at the destination.
Created Date/Time	The date and time that the event was created.
Is All-day Event	Indicates whether the planned drive is an all-day event.
Latitude	The GPS latitude coordinates of the place.
Longitude	The GPS longitude coordinates of the place.

Additional Information

Waze Favorites

Description	Waze Favorites contains information about the locations that a user has

	bookmarked as a favorite.
Recovery method	Parsing

Attribute	Description
Name	The name of the place bookmarked as a favorite.
Address	The house number and street name of the place.
City	The city of the address.
State	The state or province of the address.
Country	The country of the address.
Created Date/Time	The date and time that the address was added as a favorite.
Modified Date/Time	The date and time that the favorite location was last modified by the user.
Accessed Date/Time	The date and time that the favorite location was last accessed in Waze.
Latitude	The GPS latitude coordinates of the place.
Longitude	The GPS longitude coordinates of the place.

Additional Information

Waze Places

Description	Waze Places contains all the places that the user has searched using

	Waze.
Recovery method	Parsing

Attribute	Description
Name	The name of the place.
Address	The house number and street name of the place.
City	The city of the address.
State	The state or province of the address.
Country	The country of the address.
Created Date/Time	The date and time that the address was entered in Waze.
Accessed Date/Time	The last date and time that the address was accessed in Waze.
Latitude	The GPS latitude coordinates of the place.
Longitude	The GPS longitude coordinates of the place.

Additional Information

WiFi Locations

Description	WiFi Locations contains records of WiFi Location detected by the mobile device at a given time.
Recovery method	Parsing

Attribute	Description
MAC Address	The MAC Address of the WiFi Location.
Channel	The channel the WiFi Location.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that this log was entered into cache.
Latitude	The latitude of the mobile device.
Longitude	The longitude of the mobile device.
Accuracy (meters)	The accuracy of the position information.
Confidence	The confidence of the data.

Additional Information

Media

AMR Files

Description	AMR Files contains voicemail messages or memos for both iOS and Android.
Recovery method	Carving

Attribute	Description
File Name	The name of the file the AMR was recovered from.

Attribute	Description
Size (Bytes)	The size of the AMR content.
MD5 Hash	An MD5 hash of the AMR content.
SHA1 Hash	A SHA1 hash of the AMR content.
Audio	The contents of an AMR file.
Media Duration (Seconds)	The duration of the audio clip in seconds.

Additional Information
For information about supported formats, see Supported media and file types. Media duration is calculated from the number of speech frames carved from the AMR data, where each speech frame has a duration of 20ms, as AMR files do not contain metadata for duration.

Audio

Description	Audio contains audio files that are recovered that use the .mp3 or .wav formats.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file.
File Extension	The extension of the file.
Created	The date and time that the audio file was created.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the audio file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the audio file was last modified.
File Size (Bytes)	The size of the audio file.
MD5 Hash	An MD5 hash of the audio content.
SHA1 Hash	A SHA1 hash of the audio content.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the audio clip in seconds (extracted from Exif data).
Exif Created Date/Time -	The date and time when the audio clip was first recorded (extracted from Exif data).

Attribute	Description
UTC (yyyy-mm-dd)	
Exif Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio clip was edited (extracted from Exif data).
Timezone	The timezone setting on the recorder at the time when the audio clip was recorded (extracted from Exif data).
Software	The software used to record or modify the audio clip. This could either be the OS version of the phone used to record the audio clip or the name of the software used to edit the audio clip in post-production (extracted from Exif data).
Latitude	The GPS latitude coordinates of where the audio clip was recorded (extracted from Exif data).
Longitude	The GPS longitude coordinates of where the audio clip was recorded (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of where the audio clip was recorded (extracted from Exif data).
Exif Data	A searchable field for all raw Exif properties.

Additional Information

For information about supported formats, see Supported media and file types.
To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Best Secret Folder Albums

Description	Best Secret Folder Albums contains information on the albums that the user has created in the application.
Recovery method	Parsing

Attribute	Description
Album Title	The title of the Album.
Created Date/Time - Local Time (yyyy-mm-dd)	The date and time when the album was created in local time.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the album was created in UTC.
User ID	The username assigned to the folder by the application. OtherUser indicates a user without access and VideoSafeValidUser indicates that a user has passcode access.
Type	The type of album (i.e. Photo, File or Video).

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Best Secret Folder Configuration Data

Description	Best Secret Folder Configuration Data contains information about the configuration of the application, including the locations where hidden media is stored.
Recovery method	Parsing

Attribute	Description
Password	The password used to access the application.
Password Hint	The hint for the password.
Root Notes Folder	The root folder in which all of the user's notes are stored.
Root Photos Folder	The root folder in which all of the user's photos are stored.
Root Videos Folder	The root folder in which all of the user's videos are stored.

Additional Information

Best Secret Folder Media

Description	Best Secret Folder Media contains information about the media files that the user has added in the application.
Recovery method	Parsing

Attribute	Description
File Name	The name of the media file.
File Type	The type of the media file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the media was added in UTC.
Created Date/Time - Local Time (yyyy-mm-dd)	The date and time when the media was added in local time.
Album Title	The title of the album.
User ID	The username assigned to the folder by the application. This is either 'OtherUser', indicating a user without access, or 'VideoSafeValidUser', indicating a user with passcode access.
File	The media file.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Carved Video

Description	Carved Video contains videos that are recovered using carving. Supported formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. Other container formats can also be recovered provided that their underlying packets

	are the same as one of the supported formats.
Recovery method	Parsing

Attribute	Description
Content Format	The format of the video.
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
File Size (Bytes)	The size of the container and file.
Container Format	The format of the video container.
Saved Video Size (Bytes)	The size of the video that was saved to the database.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Additional Information

As of February 20 2020, this artifact will no longer be included under Videos. Carved Video functionality will be included in the 'Videos' artifact instead.

Google Photos Albums

Description	Google Photos Albums contain information about the albums recovered from the device.
Recovery method	Parsing

Attribute	Description
Title	The name of the album.
Owner	The owner of the album.
User ID	The unique user ID of the owner of the album.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the album was created.
Shared With	A list of the IDs of users the album is shared with.
Shared	Indicates whether the album is shared with another user.
Album Cover URL	The url of the cover photo for the album. This data is unavailable for iOS.
Album URL	The url of the album. This data is unavailable for iOS.

Additional Information

Google Photos Comments

Description	Google Photos Comments contains information about comments left on an

	album or individual media by users.
Recovery method	Parsing

Attribute	Description
Author	The author of the album comment.
User ID	The unique user ID of the owner of the album comment.
Comment	The content of the comment. Comments include likes when the user clicks a heart-shaped like button.
Item Name	The name of the item that the comment belongs to. The user can comment on albums or individual media.
Type	The type of the item that the comment belongs to. The type can be Album or Media.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the comment was created.

Additional Information

Google Photos Media

Description	Contains information about media items added to Google Photos.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the media item.
Album	The album that the media item belongs to.
Owner	The owner of the media item.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the media item was created.
Size	The size of the media item in bytes.
Duration	The duration of the media item if it is a video.
Caption	The caption of the media item.
Latitude	The latitude of the media item.
Longitude	The longitude of the media item.
Deleted	Indicates whether or not the media item has been deleted. This data is unavailable in Android.
Picture URL	The url of the media item.
Profile Picture URL	The profile picture url of the owner of the media item.

Additional Information

iOS Device Wallpapers

Description	iOS Device Wallpapers contains the home screen and lock screen pictures and information about wallpaper configurations used on a device.
Recovery method	Parsing

Attribute	Description
GUID	The unique ID for a wallpaper configuration.
Type	Indicates if the wallpaper is a home screen or a lock screen.
Current	Indicates whether the wallpaper is currently being used on the device (i.e. Yes or No).
Last Used Date/Time - UTC (yyyy-mm-dd)	The last time the wallpaper was used on the device.
Paired Lock Screen ID	The unique ID for the coordinating lock screen that the user has chosen, if the wallpaper is a home screen. If the wallpaper is a lock screen, no paired ID will be displayed.
Attachment	The thumbnail of the wallpaper.

Additional Information

iOS Snapshots

Description	iOS Snapshots contains stored snapshots of an application's state taken by iOS when the application is suspended. An application is suspended when it is sent to the background, either by minimizing the application or by switching to a different application.
Recovery method	Not applicable

Attribute	Description
Application Package Name	The package name of the application.
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

This artifact can only return hits if the Pictures artifact is turned on.

Live Photos

Description	Live Photos contains Live Photos that were retrieved using parsing. Support exists for all versions of iOS.
Recovery method	Parsing

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
UUID	The ID of the picture and video. If the UUID is different for picture and a video, it is not associated with each other
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-	The last modified date and time of the picture in the file system.

Attribute	Description
mm-dd)	
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time when the picture was being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture, or the name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).

Attribute	Description
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The latitude coordinate in decimal degrees.
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS latitude (extracted from Exif data).
Longitude	The longitude coordinate in decimal degrees.
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the picture was taken (extracted from Exif data).
Exif Data	A searchable field for all raw exif properties.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.

Attribute	Description
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

If you're having issues previewing this artifact in your cases or exports, see Videos for Motion Photos and Live Photos do not play correctly.

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Photos Albums

Description	Photos Albums contains information about the albums that contain pictures and media in the Photos application on an iOS device.
Recovery method	Parsing

Attribute	Description
Album Title	The title of the album.
Created Date/Time	The date and time when the album was created on the local device.
Photo Count	The number of photos in the album.

Attribute	Description
Video Count	The number of videos in the album.
UUID	The UUID of the album.
Owner Name	The full name of the owner. This is only available when the album is a shared album.
Shared	Indicates whether the album is a shared album. Yes is displayed when the album is shared.
Invitees	The full names of those invited to view the shared album.

Additional Information

Photos Media Information

Description	Photos Media Information contains metadata about pictures and videos stored in the Photos application on an iOS device as well as any other accompanying media and modified media related to the original media file recovered.
Recovery method	Parsing

Attribute	Description
File Name	The name of the media file.
Type	The type of media. The value can be Picture or Video. This may be a picture instead of a video as the full video is not loaded from the cloud.

Attribute	Description
Album Title	The title of the media file's album.
Created Date/Time	The date and time when the media was created on the local device.
Favorited	Indicates whether a photo has been favorited.
Hidden	Indicates whether a photo has been hidden.
Deleted	Indicates whether a file has been recently deleted. Recently deleted files remain accessible for 30 days.
Bundle ID	The bundle identifier where the file is imported from.
Display Name	The display name of the bundle where the file is imported from.
Directory	The directory that the media file resides in.
UUID	The UUID of the media.
Latitude	The latitude of the location where the media was taken.
Longitude	The longitude of the location where the media was taken.
Modified Date/Time	The date and time when the media was modified on the local device.
Deleted Date/Time	The date and time when the media was deleted from the local device.
Media	The picture related to this photo media information.

Additional Information

To learn more about examining Photos Albums artifacts, see Find pictures or videos related to an iOS Photos Albums artifact.

Pictures

Description	Pictures contains pictures retrieved using either carving or parsing techniques.
Recovery method	Parsing and carving

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the that file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.

Attribute	Description
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from

Attribute	Description
	Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The latitude coordinate in decimal degrees.
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS latitude (extracted from Exif data).
Longitude	The longitude coordinate in decimal degrees.
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Exif Data	A searchable field for all raw exif properties.
MD5 Hash	An MD5 hash of the image content.

Attribute	Description
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicates whether the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

The supported formats are as follows: JPEG (.jpeg, .jpg, .jpe), PNG (.png), Bitmaps (.bmp), Graphics Interchange Format (.gif), Icons (.ico), and Tagged Image File Format (.tif, .tiff). For more information about supported formats, see Supported media and file types.

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Private Photo Vault Albums

Description	Private Photo Vault Albums contains information about the albums a user creates to organize their media in the Private Photo Vault application. The album information can be useful intelligence for how a user might have organized encrypted media.
Recovery method	Parsing

Attribute	Description
Album Title	The name of the album.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the album was created on the device.
Last Modified Date/Time - UTC (yyyy-mm-dd)	Not available on Android.
Decoy	Indicates whether the album is hidden (accessible with a different passcode) or not.
Password	The password protecting the album, if any. Does not affect encryption.
PIN	The value used to generate the encryption key. It can be either a numeric PIN (4 digits) or a sequence of values (2 to 9) of an unlock pattern.

Additional Information

Private Photo Vault Media

Description	Private Photo Vault Media contains information about encrypted media files that the user stores in the Private Photo Vault application. If decryption is successful, the decrypted media content is made available in this artifact. Metadata about the encrypted media files, such as timestamps, are always available. Users will often resort to encrypted media applications for storing illicit material. Being able to decrypt this media can be crucial to a case.
Recovery method	Parsing

Attribute	Description
File Path	The path to the encrypted media file.
Media Type	The type of media (photo or video).
Album Title	The associated album title.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the media was created on the device.
Last Modified Date/Time - UTC (yyyy-mm-dd)	Not available on Android.
Thumbnail Path	Not utilized on Android - see the 'Private Photo Vault Thumbnails - Android' artifact instead.
Picture	The encrypted media.
Thumbnail File	The thumbnail of the encrypted media.

Additional Information

Secret Photo Vault Albums

Description	Secret Photo Vault Albums contains information about the albums a user creates to organize their media in the Secret Photo Vault application. Users can create a fake account as a distraction from the content they want to hide in their main account.
Recovery method	Parsing

Attribute	Description
Album Title	The name of the album.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the album was created on the device.
Account Type	Indicates whether the album is in the user's main account or their fake account.

Additional Information

Secret Photo Vault Application Passwords

Description	Secret Photo Vault Application Passwords contains information about the passwords the user has set for the Secret Photo Vault Application. The fake password unlocks a sub-set of albums from the application, as determined by the user. The real password unlocks the entire application.
Recovery method	Parsing

Attribute	Description
Local User	The local username.
Password	The password.
Type	Indicates if the password is the real one or the fake one.
Application Name	The name of the application.

Additional Information

Secret Photo Vault Bookmarks

Description	Secret Photo Vault Bookmarks contains information about the webpages that a user has bookmarked while using the browser of the Secret Photo Vault application.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was added.
Name	The name of the bookmark.

Additional Information

Secret Photo Vault Break-In Alerts

Description	Secret Photo Vault Break-In Alerts contains forward-facing pictures that are taken when the incorrect login passcode is provided.
Recovery method	Parsing

Attribute	Description
File Path	The path to the break-in alerts.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the break-in alert was added.
Attachment	The picture the app takes when there has been a break-in alert.

Additional Information

Secret Photo Vault Contacts

Description	Secret Photo Vault Contacts contains information about the contacts a user saved in the Secret Photo Vault application. Users can create a fake account as a distraction from the content they want to hide in their main account.
Recovery method	Parsing

Attribute	Description
First Name	The first name of the saved contact.
Last Name	The last name of the saved contact.
Company	The company information of the saved contact.
Email Address	The email address of the saved contact.
Home Phone	The home phone number of the saved contact.
Business Phone	The busines or work phone number of the saved contact.

Attribute	Description
Mobile Phone	The mobile phone number of the saved contact.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact was added.
Notes	The notes added to the contact's information by the user.
URL	The URL added to the contact's information by the user.
Account Type	Indicates whether the saved contact is in the user's main account or their fake account.

Additional Information

Secret Photo Vault Media

Description	Secret Photo Vault Media contains information about the picture and video files that the user stores in the Secret Photo Vault application. Users can create a fake account as a distraction from the content they want to hide in their main account.
Recovery method	Parsing

Attribute	Description
File Path	The path to the media file.
Media	The media file.

Attribute	Description
Thumbnail	The thumbnail of the media file.
Media Type	The type of media (photo or video).
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the media was created on the device.
Deleted	Indicates whether or not the media file was deleted by the user.
Album Title	The associated album title.
Path	The path to the media file on the device.
Account Type	Indicates whether the saved contact is in the user's main account or their fake account.

Additional Information

Secret Photo Vault Saved Passwords

Description	Secret Photo Vault Saved Passwords contains information about the passwords a user has saved while using the browser of the Secret Photo Vault application. Users can create a fake account as a distraction from the content they want to hide in their main account.
Recovery method	Parsing

Attribute	Description
URL	The URL of the webpage that the saved password is associated with.
User Name	The saved username.
Password	The saved password.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the password was saved on the device.
Account Type	Indicates whether the saved password is in the user's main account or their fake account.

Additional Information

Secret Photo Vault Tabs

Description	Secret Photo Vault Tabs provides information about the currently open browser tabs in the Secret Photo Vault's built in browser.
Recovery method	Parsing

Attribute	Description
Tab ID	The unique ID of a tab in the browser.
Active	Indicates whether or not the tab is in focus and active.
Title	The title of the webpage that is currently open in the tab.

Attribute	Description
URL History	A list of URLs visited in chronological order prior to the current website URL.
Picture	A snapshot of the current website in the browser tab.

Additional Information

Videos

Description	Videos contains videos that are recovered using parsing or carving. Supported formats for parsing include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. Supported carving formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. For more information about supported video formats, see Supported media and file types.
Recovery method	Parsing

Attribute	Description
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
File Name	The name of the file.
File Extension	The extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was created.

Attribute	Description
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was last modified.
File Size (Bytes)	The size of the video.
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed, including potential metadata located at the end of the video. Partial indicates that only Exif information in the header section of the video file was recovered, which should only occur with very large videos (in excess of the limit set in the options screen). Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The resolution of the video (extracted from Exif data).
Original	The resolution of the video (extracted from Exif data).

Attribute	Description
Height	
Exif Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was first recorded (extracted from Exif data).
Exif Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the video being recored (extracted from Exif data).
Software	The software used to record or modify the video. This could either be the OS version of the phone used to record the video or name of the software used to edit the video in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to record the video (extracted from Exif data).
Model	The model of the camera used to record the video (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to record the video (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS coordinates of the camera where the video was recorded (extrac-

Attribute	Description
	ted from Exif data).
Longitude	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the video was recorded (extracted from Exif data).
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.
Content Format	The format of the carved video.
Container Format	The format of the carved video container.
Saved Video Size (Bytes)	The size of the carved video that was saved to the database.
Exif Data	A searchable field for all raw exif properties.

Additional Information

Supported formats include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. For more information about supported video formats, see Supported media and file types.

To learn more about Exif data for videos, see Extracting Exif data from videos.

To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Operating System

.DS_Store Records

Description	.DS_Store Records contains all of the records that were extracted from .DS_Store files found on the computer. Each record represents a property of a file or a folder. This artifact is an indicator of high likelihood that the user of the computer was aware of these files and folders with a possibility of attributing a date to that awareness.
Recovery method	Parsing

Attribute	Description
Record Name	The name of the file or folder as stored in the .DS_Store file.
Record Type	The type of the record, or property, that is being logged in the .DS_Store file for a particular file or folder.
Record Value	The value of the property for the given file or folder.
Record Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was modified.
Record Path	The full path to the file or folder
.DS_Store Created Date/Time - UTC (yyyy-mm-dd)	The created date of the .DS_Store file from which the record was extracted.
.DS_Store Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date of the .DS_Store file from which the record was extracted.

Attribute	Description
.DS_Store Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date of the .DS_Store file from which the record was extracted.

Additional Information

In the Apple macOS operating system, .DS_Store (Desktop Services Store) is a hidden file that stores the display information of its containing folder, similar to the file desktop.ini in Microsoft Windows. The file tracks information such as icon positions, view settings, cached file size, cached last modified date, and even the choice of a background image. The .DS_Store is created and maintained by the Finder application in any folder that it accesses, even on remote file systems mounted from servers that share files (for example, via Server Message Block (SMB) protocol or the Apple Filing Protocol (AFP)). .DS_Store files are also included in archives created by macOS users, such as ZIP files, and they are backed up by some cloud file backup services. This means that the presence of .DS_Store Records artifacts on non-Mac evidence such as Windows, Mobile, or Cloud indicates that some of the data may have originated or have been accessed from a macOS computer at some point. For more information on .DS_Store files and their forensic significance see: .DS_Stores: Like Shellbags but for Macs.

AirDrop Available Recipients

Description	AirDrop Available Recipients lists all available recipients for an AirDrop transfer that was outgoing from the local device. The devices need to be in Bluetooth and WiFi range to connect to each other. You can recover up to one week of AirDrop activity history as it is stored in the Apple Unified Logs.
Recovery method	Parsing

Attribute	Description
Name	The name of the user or the user's device.
User ID	The ID of the user as tracked by the AirDrop service.
Contact Added	Indicates whether the user is a contact on the local user's device.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the log entry.
Transaction Log	The log message that was extracted from Unified Logs.

Additional Information

Available users are only recorded in the Apple Unified Logs when the local user opens the AirDrop view in Finder or tries to send a file using the AirDrop sharing option. There is a record for each time a person "bubble" appears in the respective interface. This artifact can help place other devices in proximity of the device being investigated.

AirDrop Background Activity

Description	AirDrop Background Activity is a collection of logs that capture background events triggered by the AirDrop service.
Recovery method	Parsing

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	The date and time of the log entry.
Transaction Log	The log message that was extracted from Unified Logs.

Additional Information

This artifact does not capture every single background event that is described in the log. This artifact extracts what look to be the most relevant pieces of data, but it's up to the examiner to determine their forensic significance. If there are logs that are not included in this artifact that should be, please reach out to Magnet Technical Support.

AirDrop Discoverability

Description	AirDrop Discoverability lists changes to the discoverability status of device.
Recovery method	Parsing

Attribute	Description
Mode Changed Date/Time - UTC (yyyy-mm-dd)	The date and time of the log entry.
Mode	Indicates who can share files with the local machine (values include Off, Contacts Only, or Everyone).
Transaction Log	The log message extracted from Unified Logs.

Additional Information

While this artifact reflects changes that the user initiates a change to their discoverability, it does also capture system changes. The AirDrop service periodically resets which causes the status to toggle between the current status and off, typically within one second of each other. These changes are background system activities that are not representative of an action by the user.

AirDrop Incoming Transfers

Description	AirDrop Incoming Transfers lists information about AirDrop transfers incoming to the local device. The devices need to be in Bluetooth and WiFi range to connect to each other. You can recover up to one week of AirDrop activity history as it is stored in the Apple Unified Logs.
Recovery method	Parsing

Attribute	Description
Item Type	Typically these values are displayed as MIME types. However, if Apple doesn't have a friendly name reserved for a particular file type, you might see values like dyn.ah62d4rv4ge80nqbv.
Number of Items	The number of items of that type included in the transfer.
Is File	Indicates whether the items being transferred are files or not, such as whether the transferred items are folders or links.
Sender Name	The name of the sender.
Sender Device	The name of the sender's device.
Destination Folder	The location chosen by the user to save the incoming transfer to.
Status	Indicates whether the transfer is accepted, declined, or incomplete. Incomplete could either mean that the transaction timed out, or that the sender cancelled the transaction on their end.
Transfer Start	The date of the first log entry associated with the transfer.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date of the last log entry associated with the transfer.
Sender is Me	Indicates whether the sender is logged in under the same account as the recipient.
Auto Accept	Indicates whether the transfer was auto-accepted.
Sender ID	The ID of the sender as tracked by the AirDrop service.
Verifiable Identity	Indicates whether the identity of the user is verifiable. This is an internal flag and its up to the examiner to determine its forensic significance.
Partial Recovery	Identifies whether the transfer transaction log was incomplete. Yes indicates that some of the transaction log lines were missing before the end of the log file was encountered, so some fragment lines were left empty because they could not be properly recovered.
Transaction ID	An identifier for a given transaction. If multiple files are selected and transferred together, they're listed as separate hits but will have the same transaction ID.
Transaction Log	A raw dump of the logs between the first and last log relating to the transaction.

Additional Information
Incoming transfers are records pertaining to the files received on the local machine. A single transaction with multiple files will get split into multiple hits in AXIOM Examine and can be grouped by sorting on Transaction ID.

AirDrop Outgoing Transfers

Description	AirDrop Outgoing Transfers lists information about AirDrop transfers outgoing from the local device. The devices need to be in Bluetooth and WiFi range to connect to each other. You can recover up to one week of AirDrop activity history as it is stored in the Apple Unified Logs.
Recovery method	Parsing

Attribute	Description
Item Name	The file or folder name.
Item Type	Typically, these values are displayed as MIME types. However, if Apple doesn't have a friendly name reserved for a particular file type, you might see values like dyn.ah62d4rv4ge80nqbv.
Is File	Indicates whether the items being transferred are files or not, such as whether the transferred items are folders or links.
Recipient Name	The name of the recipient.
Recipient Device	The name of the recipient's device.

Attribute	Description
Status	Indicates whether the transfer is accepted, declined, or incomplete. A Declined/Incomplete status could indicate that the transfer was cancelled, declined, or timed out.
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date of the first log entry associated with the transfer.
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date of the last log entry associated with the transfer.
Recipient ID	The ID of the recipient as tracked by the AirDrop service.
Verifiable Identity	Indicates whether the identity of the user is verifiable. This is an internal flag and its up to the examiner to determine its forensic significance.
Partial Recovery	Identifies whether the transfer transaction log was incomplete. Yes indicates that some of the transaction log lines were missing before the end of the log file was encountered, so some fragment lines were left empty because they could not be properly recovered.
Transaction ID	An identifier for a given transaction. If multiple files are selected and transferred together, they're listed as separate hits but will have the same transaction ID.
Transaction Log	A raw dump of the logs between the first and last log relating to the transaction.

Additional Information
Outgoing transfers are records pertaining to the files sent by the local machine. A single transaction with multiple files will get split into multiple hits in AXIOM Examine and can be grouped by sorting on Transaction ID.

Apple Accounts

Description	Apple Accounts contains information about the Apple ID accounts used on the macOS computer. The account details contained can help investigators recover and correlate account information across applications, and provide information on what accounts to review and get more information from.
Recovery method	Parsing

Attribute	Description
Local Account	The local user's account name. This attribute is only available for macOS computers.
User Name	The email address or username used to log into the account.
Account ID	The UID used to identify accounts and files tied to a specific account.
Account Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the account was added to the database.
Parent Account ID	The UID used to match the account to its parent account if it has one.
Account Descrip-	A description of the account, as provided by the user.

Attribute	Description
tion	
Account Type	The type of user account.
Account Credential Type	The type of credentials used by the account. The account credential type can help to indicate which methods might be of use for recovering the credentials (and possibly aiding with a cloud acquisition of the account).
Owning Bundle ID	The unique bundle ID of the application that the account was setup with.
Last Credential Expiry Date/Time - UTC (yyyy-mm-dd)	The date and time when the credentials had to be re-entered for the account due to a password change or expiry of the token or credentials.

Additional Information

Cell Tower Locations

Description	Cell Tower Locations contains records of which cell towers a device connects to at a given time.
Recovery method	Parsing

Attribute	Description
CellID	A GSM Cell ID (CID) is a generally unique number used to identify each base tranceiver station (BTS) or sector of a BTS within a Location Area

Attribute	Description
	Code (LAC) if not within a GSM network.
Location Area Code	The Location Area Code (LAC) is a unique number describing the set of base stations that are grouped together to optimize signalling.
Mobile Country Code	The Mobile Country Code (MCC) is used in combination with Mobile Network Code (MNC) to uniquely identify a mobile network operator (carrier).
Mobile Network Code	The Mobile Network Code (MNC) is used in combination with Mobile Country Code (MCC) to uniquely identify a mobile network operator (carrier).
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that this log was entered into the cache.
Latitude	The latitude of the mobile device.
Longitude	The longitude of the mobile device.
Range	The distance that the phone is away from the cell base station.
Confidence	The confidence of the data.

Additional Information

File System Events

Description	File System Events contains information about the changes to file system objects on an iOS device. This artifact contains all system event files

	recovered from the .fseventsd folder.
Recovery method	Parsing

Attribute	Description
File Name	The name of the system object affected by the event.
File Path	The full path to the system object affected by the event.
Flags	Flags that indicate the type of system object and the changes that occured to the object.
Event ID	An Event ID for the record.
File ID	A system ID for the file system object that was affected by the event.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the event file is initially created. This file is recovered from the .fseventsd directory and can contain records for many different events, so this timestamp may not coincide with when the event actually occurred.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the event file was last updated. This file is recovered from the .fseventsd directory and can contain records for many different events, so this timestamp may not coincide with when the event actually occurred.

Additional Information

File System Information

Description	File System Information contains all of the relevant information about the hard drives in use by the operating system.
Recovery method	Parsing

Attribute	Description
ID	The identifier of the hard drive.
Volume Serial Number	This field only applies to FAT and NTFS file systems. This is a 32-bit unsigned int value that is stored in Bios Paramter Block (BPB) and is showed in a special hex format â€“ XXXX-XXXX e.g. EABB-6573. For other file systems, the value of this field should show "n/a".
Full Volume Serial Number	This field is a 64-bit volume serial number that is only present in BPB of NTFS file system, for example AABBCCDDEEFF0011. For non-NTFS file systems, "n/a" is displayed for this field.
File System	The type of the file system (e.g "Microsoft NTFS").
Sectors per cluster	The number of sectors in a file system cluster.
Bytes per sector	The number of bytes per sector.
Starting Sector	The starting sector for this partition.
Ending Sector	The ending sector for this partition.
Total Sectors	Encase shows different values for this field based on how a volume is

Attribute	Description
	added to the case. For example, if you add just a volume (e.g. your local C:\ drive), it shows 123410271 for the number of sectors, but if you add your local physical drive 0 to the case and then select your C:\ volume in the "Entries" tree (note: your C drive would most likely have another letter in this tree, e.g. E:), then total number of sectors would be one more that the other value, i.e. 123410272. the value show for this field is taken from BPB, which matches the first value. The other value is shown when the parent physical drive is present probably comes from the partition table, and it counts VBR as well.
Total Clusters	The number of clusters comprising the file system.
Free Clusters	The number of unallocated clusters in the file system.
Total Capacity (Bytes)	This value is calculated by (Total Clusters) x (Cluster Size), which shows the capacity of the file system and not the volume containing it. The size of the volume would be higher than this value.
Unallocated Area (Bytes)	The number of unallocated bytes on the file system, which is calculated by (Number of free clusters) x (cluster size).
Allocated Area (Bytes)	This value is calculated by (Number of allocated clusters) x (cluster size).
Volume Name	The volume label stored in Volume Boot Record (VBR).
Volume Offset (Bytes)	The offset (in bytes) of the volume containing this file system from beginning of the disk. "0" is displayed if the image and/or drive being searched is the image of one volume. Encase shows the number of sectors for this field instead of the number of bytes.
Drive Type	The type of the hard drive.

Additional Information

Google Accounts

Description	Google Accounts contains the Google accounts that are currently signed in on any Google application on the device.
Recovery method	Parsing

Attribute	Description
Account Name	The account name of the user.
Display Name	The display name of the user.
Profile ID	The GAIA ID.
Profile Image URL	The URL for the user's profile image.

Additional Information

iOS Home Screen Items

Description	iOS Home Screen Items contains information about the applications and folders on the Home screen, including their specific locations. This artifact shows how the user has organized applications on their Home screen and can help identify applications of interest.
Recovery method	Parsing

Attribute	Description
Desktop Icon Visibility	The location of the application or folder (either a specific page of the Home screen or the Button bar).
Position	The numbered position of the application or folder on the Button bar or Home screen page.
Type	The type of the item on the Home screen (either Application or Folder).
Application Name	The name of the application.
Folder Name	The name of the folder, if the item is a folder. Or, the name of the parent folder if the item is an application and it resides within a folder.
Folder Screen	The number of the screen the application is located on within the folder.
Folder Position	The numbered position of the application within the folder.

Additional Information

Network Interfaces - iOS, macOS

Description	Network Interfaces contains information about each of the networks the iOS device has been connected to.
Recovery method	Parsing

Attribute	Description
BSD Name	The BSD name for the network.
MAC Address	The MAC address for the network interface.
Network Type	The type of network, which can be ethernet or IEEE80211 (wireless).
Network Name (SSID)	The SSID for the network.
USB Device Name	The name of any external device that is connected to the phone and is using network connectivity. The value will be empty if there aren't any external devices connected.
IOPathMatch	An Apple-defined property list key that contains an IOService path that the device matches against during a driver request.

Additional Information

Network Usage - Application Data

Description	Network Usage Application Data contains information about how an application sends or receives data over the network.
Recovery method	Parsing

Attribute	Description
Process Name	The file name of the executable.

Attribute	Description
Type	The executable type (Process or App).
First Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the process was first run.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the process was last run.
Last Connected Date/Time - UTC (yyyy-mm-dd)	The date and time when the process was last connected to a network.
WiFi Bytes Sent	The number of bytes sent over a WiFi connection.
WiFi Bytes Received	The number of bytes received over a WiFi connection.
Mobile Bytes Sent	The number of bytes sent over a mobile cellular network.
Mobile Bytes Received	The number of bytes received over a mobile cellular network.
Wired Bytes Sent	The number of bytes sent over a wired connection.
Wired Bytes Received	The number of bytes received over a wired connection.

Additional Information

Network Usage - Connections

Description	Network Usage Connections contains information about the networks that

	a device connects to.
Recovery method	Parsing

Attribute	Description
Network Name	The SSID or mobile network name.
Connection Type	The connection type, such as WiFi or Cellular.
Cell ID/MAC Address	An identifier for the specific access point to the network, which can be either a cell tower identifier or a MAC address.
First Connected Date	The date that the device first connected to this network.
Last Connected Date	The date that the device last connected to this network.

Additional Information

Owner Information

Description	Owner Information contains information about the iOS device and the device owner. Information includes the device name, the phone number associated with the phone, and other details associated with iOS.
Recovery method	Parsing

Attribute	Description
Device Phone Name	The name of the device.
Device Phone Number	The phone number associated with the device.
Apple ID	The Apple ID associated with this owner.
DSID	The DSID associated with the Apple ID of the owner.
Model	The model of the device. For example, N41AP.
iTunes Version	The version of iTunes installed on the device.
Setup Date	The date and time that the iOS device was setup.
Setup Type	Indicates the method used for setting up the device. This could include using the setup assistant, iTunes, iCloud backup, and more.

Additional Information

PowerLog App Usage

Description	PowerLog App Usage contains information about the applications that were running on the device during a specified interval.
Recovery method	Parsing

Attribute	Description
Bundle ID	The ID of the application bundle.
Focus (Seconds)	The number of seconds that the application was on the screen during the interval.
Background (Seconds)	The number of seconds that the application was running in the background during the interval.
Monotonic Interval Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the interval started. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Interval Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the interval started. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Interval Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the interval started. The time stated in this column uses a system offset to calculate the time that is displayed on the device.
Interval Length (Seconds)	The length of the interval in seconds.

Additional Information

PowerLog Application State

Description	PowerLog Application State contains information about application state transition.
Recovery method	Parsing

Attribute	Description
Bundle ID	The ID of the application bundle.
Process ID	The process identifier of the application.
State	The current state of the application.
Monotonic Date/Time - UTC (yyyy-mm-dd)	The date and time that the state was recorded. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Date/Time - UTC (yyyy-mm-dd)	The date and time that the state was recorded. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Date/Time - UTC (yyyy-mm-dd)	The date and time that the state was recorded. The time stated in this column uses a system offset to calculate the time that is displayed on the device.

Additional Information

PowerLog Battery Level

Description	PowerLog Battery Level contains information about the phone's battery.
Recovery method	Parsing

Attribute	Description
Battery Level	The battery level displayed in the UI.
Raw Battery Level	The true battery level.
Charging	Indicates whether the phone is charging. This value is Yes if the phone is charging, or No if otherwise.
Fully Charged	Indicates whether the battery is fully charged. This value is Yes if the phone battery is fully charged, or No if otherwise.
Monotonic Date/Time - UTC (yyyy-mm-dd)	The date and time that the battery level was recorded. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Date/Time - UTC (yyyy-mm-dd)	The date and time that the battery level was recorded. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Date/Time - UTC (yyyy-mm-dd)	The date and time that the battery level was recorded. The time stated in this column uses a system offset to calculate the time that is displayed on the device.

Additional Information

PowerLog Battery Shutdown

Description	PowerLog Battery Shutdown contains information about when the phone's battery completely runs out and shuts down.
Recovery method	Parsing

Attribute	Description
Metadata	The low battery log details.
Monotonic Date/Time - UTC (yyyy-mm-dd)	The date and time that the battery shutdown was recorded. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer-.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Date/Time - UTC (yyyy-mm-dd)	The date and time that the battery shutdown was recorded. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Date/Time - UTC (yyyy-mm-dd)	The date and time that the battery shutdown was recorded. The time stated in this column uses a system offset to calculate the time that is displayed on the device.

Additional Information

PowerLog Camera State

Description	PowerLog Camera State contains information about changes to the camera state which indicate when a device's camera is in use.
Recovery method	Parsing

Attribute	Description
State	Indicates whether the camera was on or off.
Camera Type	Indicates which camera was being used (Front or Back).
Bundle ID	The ID of the application bundle.
Monotonic Date/Time - UTC (yyyy-mm-dd)	The date and time that the camera usage was recorded. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Date/Time - UTC (yyyy-mm-dd)	The date and time that the camera usage was recorded. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Date/Time - UTC (yyyy-mm-dd)	The date and time that the camera usage was recorded. The time stated in this column uses a system offset to calculate the time that is displayed on the device.

Additional Information

PowerLog Device Lock State

Description	PowerLog Device Lock State contains information about when the phone was locked or unlocked.
Recovery method	Parsing

Attribute	Description
State	The state of the phone (Locked or Unlocked).
Monotonic Date/Time - UTC (yyyy-mm-dd)	The date and time that the device lock state change was recorded. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer-.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Date/Time - UTC (yyyy-mm-dd)	The date and time that the device lock state change was recorded. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Date/Time - UTC (yyyy-mm-dd)	The date and time that the device lock state change was recorded. The time stated in this column uses a system offset to calculate the time that is displayed on the device.

Additional Information

PowerLog In Call Service

Description	PowerLog In Call Service contains information about when an application on the device was used to perform a call service.
Recovery method	Parsing

Attribute	Description
Bundle ID	The ID of the application bundle.
Application Name	The name of the application used to perform the call service.
Status	Indicates the status of the call, such as being started or stopped. Also indicates if the application that performed the call was running in the background or foreground of the device.
Type	Indicates the call type recorded to the PowerLog database (Audio Call or Video Call).
Monotonic Date/Time - UTC (yyyy-mm-dd)	The date and time that the in call service was recorded. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Date/Time - UTC (yyyy-mm-dd)	The date and time that the in call service was recorded. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time. It represents the value of the clock on the device's baseband hardware which is also the cellular modem.

Attribute	Description
Display Date/Time - UTC (yyyy-mm-dd)	The date and time that the in call service was recorded. The time stated in this column uses a system offset to calculate the time that is displayed on the device.

Additional Information

PowerLog Lightning Cable Status

Description	PowerLog Lightning Cable Status contains information about when the phone had a lightning cable connected or disconnected.
Recovery method	Parsing

Attribute	Description
Status	Indicates if the lightning cable was connected or disconnected.
Monotonic Date/Time - UTC (yyyy-mm-dd)	The date and time the lightning cable connection was recorded. The time stated in this column is based on a monotonic clock. In computing, a monotonic clock always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Date/Time - UTC (yyyy-	The date and time the lightning cable connection was recorded. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time. It represents the value of the clock on the device's baseband

Attribute	Description
mm-dd)	hardware which is also the cellular modem.
Display Date/Time - UTC (yyyy-mm-dd)	The date and time the lightning cable connection was recorded. The time stated in this column uses a system offset to calculate the time that is displayed on the device.

Additional Information

PowerLog Process Data Usage

Description	PowerLog Process Data Usage contains information about the processes that were running on the device, and the amount of data that was sent and received during the specified interval.
Recovery method	Parsing

Attribute	Description
Process Name	The name of the application that ran during the diagnostic period.
Bundle ID	The ID of the application bundle.
Monotonic Start Date/Time - UTC (yyyy-	The date and time that the time period started. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also:

Attribute	Description
mm-dd)	https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time period started. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time period started. The time stated in this column uses a system offset to calculate the time that is displayed on the device.
Monotonic End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time period ended. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time period ended. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time period ended. The time stated in this column uses a system offset to calculate the time that is displayed on the device.

Attribute	Description
Mobile Bytes Received	The number of bytes received over a mobile cellular network.
Mobile Bytes Sent	The number of bytes sent over a mobile cellular network.
WiFi Bytes Received	The number of bytes received over a WiFi connection.
WiFi Bytes Sent	The number of bytes sent over a WiFi connection.

Additional Information

PowerLog Screen Autolock

Description	PowerLog Screen Autolock contains information about when the phone autolocked.
Recovery method	Parsing

Attribute	Description
Monotonic Date/Time - UTC (yyyy-mm-dd)	The date and time that the device autolocked. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_abso-

Attribute	Description
	lute_time
Baseband Date/Time - UTC (yyyy-mm-dd)	The date and time that the device autolocked. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Date/Time - UTC (yyyy-mm-dd)	The date and time that the device autolocked. The time stated in this column uses a system offset to calculate the time that is displayed on the device.

Additional Information

PowerLog Timezone Information

Description	PowerLog Timezone Information contains information about the timezones that were registered on the device.
Recovery method	Parsing

Attribute	Description
Name	The name of the timezone.
Country Code	The code of the timezone's country.

Attribute	Description
Locale	The locale of the timezone.
GMT Offset	The number of hours that the timezone is away from Greenwich Mean Time (GMT).
Monotonic Date/Time - UTC (yyyy-mm-dd)	The date and time that the timezone was recorded. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Date/Time - UTC (yyyy-mm-dd)	The date and time that the timezone was recorded. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Date/Time - UTC (yyyy-mm-dd)	The date and time that the timezone was recorded. The time stated in this column uses a system offset to calculate the time that is displayed on the device.

Additional Information

Private MAC Addresses - iOS

Description	Private MAC Addresses saves details of the different MAC addresses used by the iOS device, which are added each time the user accesses a new network with the Private Wi-Fi Address setting enabled.

Recovery method	Parsing

Attribute	Description
Private MAC Address	The private MAC address for the device.
Network Name (SSID)	The SSID for the network.
Last Joined Date/Time - UTC (yyyy-mm-dd)	The last date and time that the wireless network was joined by the device.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the network was added.

Additional Information

Siri Message Search Suggestions

Description	Siri Message Search Suggestions contains the sent or received messages that Siri provides to the user as search results for a query. Queries can be typed in the search bar or spoken using Siri voice commands.
Recovery method	Parsing

Attribute	Description
Message	The message that appeared as a suggestion for a user's search.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message Direction	The direction of the message (either sent or received).
Conversation ID	The identifier of the conversation that the message is a part of.

Additional Information

Unified Logs

Description	Unified Logs contains parsed records of Apple Unified Logs from the default directory, including activity information for many different applications on an Apple device. It can be useful for determining a user's system interaction.
Recovery method	Parsing

Attribute	Description
Type	The type of the log.
Process Name	The process name related to the log message.
Process ID	The process ID associated with the log message.
Date/Time - UTC (yyyy-mm-dd)	The timestamp of the log message.

Attribute	Description
Message	The message of the log.
Primary Category	The category of the log.
Subsystem	The subsystem related to the log message.

Additional Information

User Notification Events

Description	User Notification Events contains data of notifications that have occurred on an iOS device.
Recovery method	Parsing

Attribute	Description
Title	The title of the notification even that appears on the device. Optional value.
Subtitle	The subtitle of the notification. Optional value.
Body	The body of the notification. Optional value.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the notification event was recorded to the file.
Notification Date/Time - UTC (yyyy-mm-dd)	The date and time at which the user received the notification.

Attribute	Description
GUID	The Global Unique Identifier (GUID) for the notification event.
Bundle ID	The Apple ecosystem's unique identifier for the application that generated the notification.
Optional Text	Optional text for the notification event.
UUID	The Universally Unique Identifier for the device associated with the notification event. Optional value.
User ID	The Apple ID, email address or phone number associated with the notification event. Optional value.

Additional Information

Peer to Peer

Beam Transactions

Description	Beam Transactions provides information about any logged transactions that have been sent by the user on the app.
Recovery method	Parsing

Attribute	Description
Transaction ID	The unique identifier associated with the transaction.
Event Type	The type of transaction that occurred.

Attribute	Description
Event Date/Time - UTC (yyyy-mm-dd)	The date and time when the cryptocurrency event took place.
Address	The cryptocurrency address the transaction was sent to.
Crypto Amount	The amount of cryptocurrency that was sent. The currency types are BEAM and GROTH.
Cost	The fee that was charged for the transaction.
Kernel ID	The unique identifier of the kernel associated with the transaction.
Note	The note that was sent with the transaction.

Additional Information

BRD Transactions

Description	BRD Transactions provides information about any logged transactions that have been sent by the user on the app.
Recovery method	Parsing

Attribute	Description
Transaction ID	The unique identifier associated with the transaction.
Event Date/Time - UTC (yyyy-mm-	The date and time when the cryptocurrency transaction took place.

Attribute	Description
dd)	
Address	The cryptocurrency address where the cryptocurrency transfer was deposited. Note: The address is currently only recovered for Bitcoin and Doge.
Crypto Amount	The amount and type of cryptocurrency that was transferred.

Additional Information

Coinbase Purchases

Description	Coinbase Purchases provides information about any cached crypto-currency purchases that have happened on the app. Cached purchase information may not exist in all cases.
Recovery method	Parsing

Attribute	Description
Crypto Amount	The amount of cryptocurrency that was purchased.
Cost	The total cost of the purchase.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the purchase action was cre-ated.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the purchase action was updated.

Attribute	Description
Payout Date/Time - UTC (yyyy-mm-dd)	The date and time when the purchase was paid out.
Unit Price	The price of the cryptocurrency unit at the time of the purchase.
Type	The type of purchase action that occurred.

Additional Information

Coinbase Transactions

Description	Coinbase Transactions provides information about any cached crypto-currency transactions that have been sent by the user on the app. Cached transaction information may not exist in all cases.
Recovery method	Parsing

Attribute	Description
Address	The cryptocurrency address the transaction was sent to.
Crypto Amount	The amount of cryptocurrency that was sent.
Value	The total value of the cryptocurrency that was sent at the time of the transaction.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time when the cryptocurrency event took place.
Note	The note that was sent with the transaction.

Additional Information

Coinbase Users

Description	Coinbase Users provides information about the cached local user.
Recovery method	Parsing

Attribute	Description
Name	The name of the user.
ID	The user ID.
User Name	The username associated with the user.
Email	The email of the user.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the user was created.
Avatar URL	The URL targeting the user's avatar image.
Biography	The user biography.
State	The state/province the user resides in.
Country	The country the user resides in.
Address	The address of the user.

Additional Information

Coinomi Transactions

Description	Coinomi Transactions provides information about any logged transactions that have been sent/received by the user of the application. These records are carved and should be verified as they may include compressed or truncated data.
Recovery method	Carving

Attribute	Description
Transaction ID	The unique identifier associated with the transaction.
Event Type	The type of transaction that occurred. E.g. BitCoin, Doge, LiteCoin, etc.
Address	The cryptocurrency address the transaction was sent to.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time when the cryptocurrency event took place.

Additional Information

Exodus Transactions

Description	Exodus Transactions provides information about any cached crypto-currency transactions that have been sent or received by the user on the app. Cached transaction information may not exist in all cases.
Recovery method	Parsing

Attribute	Description
Transaction ID	The ID of the transaction.
Address	The cryptocurrency address the transaction was sent to or received from.
Crypto Amount	The amount of cryptocurrency in the transaction.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time when the transaction took place.
Type	The type of transaction that occurred, either Sent or Received.

Additional Information

Peer-to-Peer

Torrent Active Transfers

Description	Torrent Active Transfers contains information about the torrents that are active on the user's system.
Recovery method	Parsing

Attribute	Description
Torrent Name	The name of the torrent file.
Potential App Name	The name of the application that the torrent was

Attribute	Description
	potentially downloaded with.
Download Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file download was started.
Download Completed Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file download was completed.
Download URL	The URL to download the torrent.
Downloaded Bytes	The total number of bytes that has been downloaded.
Download Location	The location on the disk to where the torrent was downloaded.
Bytes Uploaded	The total number of bytes that the system has uploaded for this torrent.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the active transfer was last modified.

Additional Information

Torrent Feeds

Description	Torrent Feeds contains information about RSS feeds that a user subscribes to that contains torrents available for download.
Recovery method	Parsing

Attribute	Description
Feed Name	The name of RSS subscription feed.
Feed URL	The URL of the RSS subscription feed.
Torrent Name	The name of the torrent available for download from the feed.
Download URL	The URL to download the torrent.
Description	A description of the contents of the torrent.
Published Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent feed item was published.
Status	The status of the feed item, either 'Downloaded' or 'Not Downloaded'.

Additional Information

Torrent File Fragments

Description	Torrent File Fragments contains data that is carved or parsed from .torrent files that are used to download torrents from various networks on the Internet.
Recovery method	Carving

Attribute	Description
Name	The name of the torrent file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file was modified.
Torrent Creation Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file was originally created.
Torrent Files	The files that are listed in the torrent to be downloaded.

Additional Information

Social Networking

Facebook

Facebook, being one of the most popular social networking sites in the world, presents numerous opportunities for gathering evidence. You can recover messages that are sent and received, status updates and wall posts, and pages and pictures that the user views. On mobile devices, you can also recover user profiles and contacts.

Facebook can provide background information about a user, as well as evidence of who they are communicating with or associated with. Status and location updates can provide details about where a user has been and what they've been doing.

Forensic notes

The Facebook Pictures artifact represents cached pictures found on the system that originated from Facebook. When caching pictures, Facebook names the pictures using a particular format which allows forensic tools to know that they come from Facebook. These pictures can be user profile pictures, friends' pictures, or any other picture that gets cached while browsing Facebook.

Artifacts

Related resources

How important are Facebook artifacts?

Recovering Facebook artifacts

Facebook Comments

Description	Facebook Comments contains information about comments that have been cached on the device. A cached comment does not necessarily imply that the local account interacted with the comment, just that it was cached on the device. Further investigation should be performed to confirm the user's activity.
Recovery method	Parsing

Attribute	Description
Author ID	The comment author's Facebook profile ID.
Comment	The message content of the comment.

Attribute	Description
Comment Created Date/Time - UTC (yyyy-mm-dd)	When the comment was created.
Post ID	The ID of the post on which the comment was made.

Additional Information

Facebook Posts

Description	Facebook Posts contains information about posts that have been cached on the device. A cached post does not necessarily imply that the local account interacted with the post, just that it was cached on the device. Further investigation should be performed to confirm the user's activity.
Recovery method	Parsing

Attribute	Description
Author	The author of the post. The author could be a user, a page, or a group.
Author ID	The author ID of the post.
Post	The body of the post.
Title	The title of the post.
Posted Date/Time - UTC (yyyy-mm-dd)	When the post was created.

Attribute	Description
Type	The type of the post.
Visibility	The visibility of the post.
Latitude	The latitude associated with the post.
Longitude	The longitude associated with the post.
Page ID	The page ID that the post was posted to.
Parent ID	The parent post ID of the post.
Attachment Type	The type of the content that was shared in the post.

Additional Information

iOS Facebook Friends

Description	iOS Facebook Friends contains the contact information of a user's friends stored by the Facebook application.
Recovery method	Parsing and carving

Attribute	Description
User ID	The unique ID for the friend.
Member Email	The mail address of the friend.
Member Name	The full name of the friend.
Nickname	The friend's nickname, if applicable.

Attribute	Description
Image URL	The URL of the friend's avatar.
Read Receipt Message ID	The message ID of the last read message from the friend.
Read Receipt Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the last message from the friend was read.

Additional Information

iOS Facebook Messages

Description	iOS Facebook Messages contains Facebook messages recovered from the device.
Recovery method	Parsing and carving

Attribute	Description
Text	The text message content.
Email	The sender's email address.
Name	The sender's name.
User ID	The unique ID of the sender.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The second timestamp associated with the message.

Attribute	Description
Send Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message ID	A string which uniquely identifies the message.
Message Source	Indicates which facebook platform was used to send the message.
Latitude	The latitude coordinate in decimal degrees associated with the message.
Longitude	The longitude coordinate in decimal degrees associated with the message.
Send State	Indicates whether a message was sent successfully or not. A value of 0 indicates a successful send, and value of 2 indicates a failed send.

Additional Information

Foursquare Check-ins

Description	Foursquare Check-ins contains check-ins made by the iOS Foursquare application.
Recovery method	Parsing and carving

Attribute	Description
User ID	The user ID.
User First Name	The user's first name.
User Last Name	The user's last name.
User Email	The email address of the account used to check in.
Check-In Date/Time - UTC (yyyy-mm-dd)	The date and time when the user checked-in to the specified locaiton.
Location Name	The name of the location the user checked into.
Comment	The comment a user left about their check-in for the location.
Address	The address of the check-in location.
Latitude	The latitude of the check-in location.
Longitude	The longitude of the check-in location.
City	The city of the check-in location.
State	The state of the check-in location.
Country	The country of the check-in location.
Been Here Count	The number of times the user has checked into this location.
User Gender	The user's gender.

Additional Information

Foursquare Locations

Description	Foursquare Locations contains locations cached by the iOS Foursquare application.
Recovery method	Parsing and carving

Attribute	Description
Location Name	The name of the location.
Address	The address of the location.
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Distance (meters)	The distance the user is from the location.
City	The city of the location.
State	The state of the location.
Country	The country of the location.

Additional Information

Grindr Buddies

Description	Grindr Buddies contains the buddies and their details within the current user's extracted iOS data.

Recovery method	Parsing and carving

Attribute	Description
Public ID	The ID of the user in the buddy list.
Display Name	The buddy's display name.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The date and time that the buddy was last seen.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time the last message from this buddy was received.
Description	The description of the buddy.
Age	The age of the buddy.
Height (cm)	The height of the buddy.
Weight (kg)	The weight of the buddy.
Ethnicity	The ethnicity of the buddy.
Type of User	The type of the user (local or non-local).
Distance	The distance of the buddy from the current user.
Favorited	Indicates if this buddy is a 'favorite buddy' of the current user.
Facebook Account	The name of the user's linked Facebook account.
Instagram Account	The name of the user's linked Instagram account.
Twitter Account	The name of the user's linked Twitter account.

Additional Information

Grindr Group Members

Description	Grindr Group Members contains the groups and their members within the current user's extracted iOS data.
Recovery method	Parsing

Attribute	Description
Member ID	The ID of the group member.
Member Name	The name of the group member.
Group ID	The ID of the group that the member is a part of.
Title	The title of the group.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the group was created.
Type	Indicate the user type. This value can be one of the following: Member, Invitee, Owner of the group.

Additional Information

Grindr Messages

Description	Grindr Messages contains the messages and their details within the cur-

	rent user's extracted iOS data.
Recovery method	Parsing and carving

Attribute	Description
Sender ID	The ID of the sender of the message.
Receiver ID	The ID of the receiver of the message.
Conversation Partner	The buddy's display name the message was with.
Group ID	The ID of the group the message was sent in.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received.
Message Body	The body of the message.
Has Attachment	Whether or not the message has an attachment.
Read Status	The status of the message (Read or Unread).
Message Direction	Indicates whether the message was incoming to the device, or outgoing from the device.

Additional Information

GROWLr Chat Messages

Description	GROWLr Chat Messages contains messages stored by the iOS GROWLr application.

Recovery method	Parsing and carving

Attribute	Description
Account ID	The ID of the other person that the message is with.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent or received.
Message	The body of the message.
Message Type	Indicates whether the message was incoming or outgoing.
Message Status	The status of the message (read or unread).
Image Filename	The path to the image associated with the message.
Image	The attached image.
Voice Filename	The filename of the attached voice message.
Voice	The attached voice data.

Additional Information

GROWLr Notes

Description	GROWLr Notes contains notes stored by the iOS GROWLr application.
Recovery method	Parsing

Attribute	Description
Text	The note text.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was last modified.

Additional Information

Instagram Direct Messages

Description	Instagram Direct Messages contains Instagram direct messages that are sent or received by the local user.
Recovery method	Parsing

Attribute	Description
Sender	The username of the sender of the message.
Recipient	The username of the recipient of the message.
Message	The message that was sent.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Direction	Indicates whether the message was incoming or outgoing.
Picture	Contains either the picture or a thumbnail of the video that was part of the message.

Attribute	Description
Attachment	The attachment that was sent.
Attachment Path	The path to the attachment that was sent.
Media URL	The URL to the media of the message.
Type	The message type.
Status	The status of the message.
Latitude	The latitude of the message.
Longitude	The longitude of the message.
Caption	The original message of a forwarded post.
Original Author	The original author of a forwarded post.
Original Date/Time - UTC (yyyy-mm-dd)	The original date and time of a forwarded post.
Chat ID	The ID of the chat.

Additional Information

The attachment path, latitude, and longitude are not recoverable on iOS devices. The Media URL attribute is only available for messages of the Forwarded Post type.

Instagram Group Members

Description	Instagram Group Members contains information about the Instagram groups that the local user is a member of.
Recovery method	Parsing

Attribute	Description
Group Member	The username of the group member.
Group Name	The name of the group.

Additional Information

Instagram Media

Description	Instagram Media contains the media files that have been found inside the Instagram application.
Recovery method	Parsing

Attribute	Description
Picture	The picture of the media, or a storyboard if the media is a video.
MIME Type	The MIME type of the media.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.

Attribute	Description
Size (Bytes)	The size of the media file.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
URL	The URL to the media.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

The com.burbn.instagram.IGSparseVideoCache directory contains many small snippets of videos which are not recovered in this artifact. These videos will be recovered by the Videos artifact.

Instagram Profiles

Description	Instagram Profiles contains all the profile information that the local user has had communications with, or have been referred to through direct mes-

	sages communication.
Recovery method	Parsing

Attribute	Description
User Name	The username of the profile.
Name	The name associated with the profile.
User ID	The user ID associated with the profile.
Profile Picture URL	The profile picture of the user's profile.
Local User	Indicates whether the profile belongs to a user logged into the device.
Is Private	Indicates whether the profile is private or not.
Biography	The biography of the user associated with the account.
Following	Indicates whether the user of this profile is following the local user.
Is Followed By	Indicates whether the local user is following this user profile.
Post Notifications	Indicates whether the local user has turned on post notifications for this user profile. This attribute is only populated if the local user is following this user profile.
Email	The public email address associated with this user profile.
Phone Number	The public phone number associated with the user profile.
Address	The public address associated with the user profile.
City	The city associated with the user profile.

Attribute	Description
ZIP/Postal Code	The ZIP or postal code associated with the user profile.
Latitude	The latitude of the location associated with the user profile.
Longitude	The longitude of the location associated with the user profile.

Additional Information
For iOS devices, the 'Post Notifications' attribute will always be empty.

iOS Instagram Posts

Description	iOS Instagram Posts contains information about posts that a user has recently viewed on Instagram for iOS, as well as comments that are present on those posts.
Recovery method	Parsing

Attribute	Description
ID	The post ID.
User Name	The username on Instagram.
Full Name	The full name of the user.
Comment Created Date/Time - UTC (yyyy-mm-dd)	The date that the comment was created.
Text	The text for the given image.

Attribute	Description
Profile Picture URL	The URL to the profile picture of the user.
Posted Image URL	The URL to the picture that was posted.
Type	The type of the post.
Taken Date/Time - UTC (yyyy-mm-dd)	The date and time that the media was taken.
Device Date/Time - UTC (yyyy-mm-dd)	The date that the user viewed the post.

Additional Information

The Device Date/Time and Downloaded Posted Images fragments are only available on Android.

iOS Tinder Accounts

Description	iOS Tinder Accounts contains all of the recovered iOS Tinder accounts.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the current account owner.
Local User	Indicates whether this is the local user's account (Yes or No).
First Name	The first name of the account user.
Last Activity Date/Time - UTC (yyyy-	The last date and time that the account user was act-

Attribute	Description
mm-dd)	ive.
Biography	A brief written biography about the user's account.
Birthday (yyyy-mm-dd)	The birthday of the account user.
Distance (Miles)	The distance that the user is searching for matches.
Gender	The gender of the account user.

Additional Information

iOS Tinder Matches

Description	iOS Tinder Matches contains all of a user's recovered iOS Tinder matches.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the user whom you are matched with.
User Name	The name of the user whom you are matched with.
Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time of the match entry.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The last date and time that there was activity with the match.

Attribute	Description
Gender	The gender of the matched user.
Message Count	The number of messages exchanged with the matched profile.
Viewed Profile	Indicates whether or not the user has viewed the matched profile.
Draft Message	The contents of a pending draft message.

Additional Information

iOS Tinder Messages

Description	iOS Tinder Messages contains all of a user's recovered iOS Tinder messages.
Recovery method	Parsing and carving

Attribute	Description
User ID	The user ID of the message sender.
Match ID	The user ID of the match who is part of the conversation.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.

Attribute	Description
Message Body	The body of the message.
Direction	The direction of the message (Outgoing or Incoming).

Additional Information

iOS Tinder Photos

Description	iOS Tinder Photos contains all of the recovered iOS Tinder photos.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the user whom the picture belongs to.
User Name	The name of the user whom this picture belongs to.
Image URL	The URL to the Tinder photo.
Downloaded Image	The downloaded image.

Additional Information

iOS Whisper Posts

Description	iOS Whisper Posts contains the posts stored by the Whisper applic-

	ation.
Recovery method	Parsing and carving

Attribute	Description
Poster Nickname	The username of the person at the time when the post was posted.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time that the post was posted.
Message Text	The content of the post.
Local Device Post	Indicates whether the post was created on the local device (Yes or No).
Locale	The location of the user when the post was posted.
Image URL	The URL to the image of the post.
Downloaded Image	The downloaded image from the post, if the option is turned on in Report Viewer.
Heart Count	The number of hearts that the post has received.
Reply Count	The number of replies to the post.
Hearted	Indicates whether the local user has hearted the post (Yes or No).

Additional Information

To learn more about Whisper, see Artifact profile: Whisper.

Life360 Circle Members

Description	Life30 Circle Members contains information about the members of a circle. A circle is comprised of a group of individuals, such as a family, that the local user has created or has been added to by another circle member.
Recovery method	Parsing

Attribute	Description
Member ID	The unique member ID of the circle member.
First Name	The first name of the member.
Last Name	The last name of the member.
Email Address	The email address of the member.
Phone Number	The phone number of the member.
Circle Name	The name the circle.
Circle ID	The ID of the circle.

Additional Information

Life360 Local User Account

Description	Life360 Local User Account contains information about the local user account.
Recovery method	Parsing

Attribute	Description
User ID	The unique ID of the local user.
First Name	The first name of the local user.
Last Name	The last name of the local user.
Email Address	The email address of the local user.
Phone Number	The phone number of the local user.

Additional Information

Life360 Messages

Description	Life360 Messages contains messages sent and received by the local user within a circle that they're a member of.
Recovery method	Parsing

Attribute	Description
Sender ID	The unique ID of the sender.
Sender Name	The name of the sender.
Recipient ID(s)	The ID(s) of the recipient(s).
Recipient Name(s)	The name(s) of the recipient(s).
Message Type	The type of the message.

Attribute	Description
Message	The message content.
Created Date/Time	The date and time when the message was created.
Picture URL	The URL of the picture on the Life360 server, if a picture is included in the message.
Read	The read status of the message.
Latitude	The latitude of the location, if the message is a map location.
Longitude	The longitude of the location, if the message is a map location.
Location Name	The name of the location if the message is a map location.
Location Acquired Date/Time	The date and time when the location was acquired if the message is a map location.

Additional Information

Life360 Places

Description	Life360 Places indicates favorite locations that are saved by the user or the application.
Recovery method	Parsing

Attribute	Description
Place Name	The name of the place. The name can be either user-defined or a default

Attribute	Description
	name defined by the application.
Place Address	The address of the place.
Circle ID	The ID of the circle where the place was found.
Owner ID	The owner ID of the place, if the place was created by the user.
Latitude	The latitude of the place.
Longitude	The longitude of the place.

Additional Information

Life360 Trip Locations

Description	Life360 Trip Locations indicates the locations that the user visits (or passes by on the way to a destination). During a trip, the application will log locations at regular intervals along the way.
Recovery method	Parsing

Attribute	Description
Updated Date/Time	The date and time that the trip details were last updated. Updates to the trip can be triggered by the user or the application.
Circle ID	The circle ID of the user who created this trip.

Attribute	Description
User ID	The unique ID of the user who created this trip.
Start Date	The date that the trip happened (days begin at 12:00 AM local time).
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Start Date/Time	The date and time when the user arrived at the location.
End Date/Time	The date and time when the user left the location.
Location Name	The name of the location if it is a user created place.
Location Address	The address of the location.

Additional Information

LinkedIn Messages

Description	LinkedIn Messages contains messages sent and received by the local user.
Recovery method	Parsing

Attribute	Description
Sender Name	The name of the sender.
Recipient Name(s)	The name(s) of the recipient(s).
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The body of the message.
Attachment Name	The name of attachment to the message.
Attachment URL	The URL of attachment to the message.
Attachment Type	The type of the attachment to the message.
File	The attachment file to the message.

Additional Information

LinkedIn Profile

Description	LinkedIn Profile contains information about the user accounts that the local user has used to log in on the device.
Recovery method	Parsing

Attribute	Description
UserName	The username of local user.
First Name	The first name of local user.

Attribute	Description
Last Name	The last name of local user.
Full Name	The full name of local user.
Summary	A summary of the local user. This information is provided by the user and could indicate a number of different things including their position or status.

Additional Information

Musical.ly Local Users

Description	Musical.ly Local Users contains all of the users that have logged in to Musical.ly on the local device.
Recovery method	Parsing

Attribute	Description
User Name	The user's login name.
User Nickname	The user's chosen nickname.
User ID	The ID of the user in Musical.ly systems.
Account Description	The description that the user has given themself.
Image URL	The URL of the user's profile picture.
Instagram	The user's Instagram account.

Attribute	Description
Account	
Google Account	The user's Google account.
YouTube Channel	The user's YouTube Channel.
IP Address	The public IP address of the device the user logged in with.
Is Private	Indicates whether the user prevented others from discovering their profile (Yes or No).
Hide Location	Indicates whether the user keeps their geolocation information hidden on their profile page (Yes or No).
Messaging Availability	Indicates who is able to message the user, as specified by the user (Public or Friends Only).
Country Code	The country code of the country that the user has set for themself.
Language	The language code of the language that the user has set for themself.

Additional Information

Musical.ly Messages

Description	Musical.ly Messages contains the messages sent or received via the in-app message system of Musical.ly.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message.
Recipient	The recipient of the message.
Message	The body of the message. This value is empty if a picture message was sent.
Direction	The direction of the message, relative to the source database.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was either received or sent on the local device.
Picture	The picture that was sent or received. This value is empty if a text message has been sent.
Read	Indicates whether or not the message has been read by the local device. This value is either Yes or No.
Message Status	The status of the message. This value is displayed as either Delivered or Pending Internet Connection.

Additional Information

Musical.ly Posts

Description	Musical.ly Posts contains posts that Musical.ly retrieved from the web.
Recovery method	Parsing

Attribute	Description
User Name	The username of the poster.
User Nickname	The nickname of the poster.
User ID	The ID of the poster.
Caption	The caption that the user wrote for their post.
Picture	The locally cached post's preview picture.
Cached Video Size (Bytes)	The size of the locally cached post's video.
Video URL	The URL of the post's video.
Picture URL	The URL of the post's preview picture.

Additional Information

Musical.ly Users

Description	Musical.ly Users contains all of the users that the local user has viewed in Musical.ly.
Recovery method	Parsing

Attribute	Description
User Name	The user's login name.
User Nickname	The user's chosen nickname.

Attribute	Description
User ID	The ID of the user in Musical.ly systems.
Account Description	The description that the user has given themself.
Profile Picture URL	The URL of the user's profile picture.
Instagram Account	The user's Instagram account.
Google Account	The user's Google account.
YouTube Channel	The user's YouTube Channel.
Is Private	Indicates whether the user prevented others from discovering their profile (Yes or No).
Is Friend	Indicates whether the user is a friend of the local user in the source database (Yes or No).
Following	Indicates whether the local user in the source database is following this user (Yes or No).
Post Notifications	Indicates whether the local user wants to receive notifications when this user makes a post (Yes or No).
Hide Location	Indicates whether the user keeps their geolocation information hidden on their profile page (Yes or No).
Messaging Availability	Indicates who is able to message the user, as specified by the user (Public or Friends Only).

Attribute	Description
Country Code	The country code of the country that the user has set for themself.
Language	The language code of the language that the user has set for themself.

Additional Information

Parler Activity - iOS

Description	Parler Activity contains information about the posts and comments that the local user has accessed or made.
Recovery method	Parsing

Attribute	Description
Entry ID	The activity ID of the request/response made by the Parler application.
URL	The API URL of the post or comment accessed.
Request Body	The request the application is making to the Parler API.
Request Content Type	The MIME type of data in the request.
Response Body	The body of the Parler API response.
Response Date/Time - UTC (yyyy-mm-dd)	The date and time that the Parler API responded.
Status	The HTTP method and HTTP status of the Parler API

Attribute	Description
	response.
Response Content Type	The MIME type of data in the response.

Additional Information

Parler Users - iOS

Description	Parler Users contains information about the local user account and any other users they've interacted with.
Recovery method	Parsing

Attribute	Description
Entry ID	The activity ID of the request/response made by the Parler application.
User Name	The user name of the user.
Name	The name of the user.
Password	The password of the local user.
Email Address	The email address of the local user.
Phone Number	The phone number of the local user.
Biography	The biography of the user.

Attribute	Description
Account Type	Indicates the type and source of the user details.
ID	The unique identifier associated with the user.
Device ID	The unique device identifier associated with the user.
Notification ID	The unique notification identifier associated with the user.
Joined Date/Time - Local Time	The local date and time the user joined Parler.
Verified	Indicates whether or not the user is verified on Parler.
Private	Indicates whether or not the user's account is private.
Following	The number of accounts the user is following.
Blocked	Indicates whether or not this user was blocked by the local user.
Outgoing Interaction Count	The number of potential interactions the user has made.
Comments Count	The number of comments the user has made.
Posts Count	The number of posts the user has made.
Likes Count	The number of likes the user has made.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Pinterest Accounts

Description	Pinterest Accounts contains information about the Pinterest accounts that the local user has logged in with on the device.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the local user.
Full Name	The full name of the local user.
Email	The email address of the local user.
Created Date/Time	The created date and time of the local user.
Gender	The gender of the local user.
Country	The country of the local user.
Locale	The location of the local user.
Profile Image URL	The profile image URL of the local user.
Active	The current status of the local user. This is indicated if the account is coming from an active database.

Additional Information

Pinterest Boards

Description	Pinterest Boards contains information about the Pinterest boards created by local user.
Recovery method	Parsing

Attribute	Description
ID	The ID of the board.
Name	The name of the board.
Type	The category type of the board.
Description	The description of the board.
Created Date/Time	The created date and time of the board.
Website URL	The URL of the board.
Owner ID	The owner ID of the board.
Active Account	Indicates whether the board is from the account that's currently logged in on the device.

Additional Information

Pinterest Messages

Description	Pinterest Messages contains messages or pins sent and received by the

	local user.
Recovery method	Parsing

Attribute	Description
Sender ID	The ID of the sender.
Sender Name	The name of the sender.
Recipient ID(s)	The user ID(s) of the recipient(s).
Recipient Name(s)	The name(s) of the recipient(s).
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The content of the message.
Pin Title	The title of the pin.
Pin Picture URL	The picture URL associated with the pin.
Attachment Name	The file name of the picture cache associated with the pin.
Attachment	The attachment associated with the pin.
Active Account	Active Account indicates whether the following user is of the account that's currently logged in on the device.

Additional Information

Pinterest Pins

Description	Pinterest Pins contains information about the items that the local user has pinned to their own board.
Recovery method	Parsing

Attribute	Description
Title	The title of the pin.
Description	The description of the pin.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the pin.
Website URL	The URL of the website associated with the pin.
Posted Image URL	The posted image URL associated with the pin.
Attachment Name	The name of the attachment associated with the pin.
Attachment	The attachment associated with the pin.
Pinner ID	The pinner ID of the pin.
Active Account	Active Account indicates whether the following user is of the account that's currently logged in on the device.

Additional Information

Reddit Accounts

Description	Reddit Accounts contains information about the user accounts that are used to log in to the Reddit application on the device.
Recovery method	Parsing

Attribute	Description
User ID	The reddit user ID.
Account ID	The unique account ID for the user.
Email Address	The email address of the user.
Icon URL	The URL to the user's account icon.
Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time of the Reddit account.

Additional Information

Reddit Posts

Description	Reddit Posts contains information about the posts recovered from the device. These posts might be ones that the user has read or created on their device.
Recovery method	Parsing

Attribute	Description
Title	The title of the Reddit post.
Subreddit Name	The subreddit name where the post was posted.
Author	The author of the post.
Over 18	Indicates whether or not the post was flagged as mature content.
Content Link	The URL to content from the post if applicable, or the URL to the post if there is no external content.
URL	The URL of the source. This URL is not recovered from the source as is, but is constructed using the Post ID.
Saved	Indicates whether or not the post was saved by the user.
Read Date/Time - UTC (yyyy-mm-dd)	The date and time that the user read the post.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the post was created.

Additional Information

Reddit Recently Visited Subreddits

Description	Reddit Recently Visited Subreddits contains information about the subreddits that a user has recently visited while on their device.
Recovery method	Parsing

Attribute	Description
Subreddit Name	The name of the subreddit.
Sort Order	The order in which posts were sorted within the subreddit (e.g. NEW, HOT, TOP, CONTROVERSIAL).
Sort Time Frame	The time frame in which posts were sorted within the subreddit (e.g. DAY, WEEK, MONTH, YEAR).
Description	The public facing description of the subreddit.
User Name	The user who visited the subreddit.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the user last visited the subreddit.
Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time of the subreddit.

Additional Information

Sina Weibo Posts

Description	Sina Weibo Posts contains user posts (similar to Twitter's tweets) on the Sina Weibo for iOS application.
Recovery method	Parsing

Attribute	Description
User ID	The unique identifier for the user posting.
User Nickname	The user's nickname.
Post Date/Time - UTC (yyyy-mm-dd)	The date and time that the content was posted.
Post	The content of the post.
Profile Image URL	The URL for the profile image of the user.
Downloaded Profile Image	The raw content of the user's profile image, downloaded from the URL shown in the Profile Image URL column.
Post Image URL	The URL of the image in the post, if applicable.
Downloaded Post Image	The raw content of the image in the post, if applicable. The raw content of the image is downloaded from the URL shown in the Post Image URL column.
Posted Source	Information describing the device from where the post was made.
Latitude	The latitude of the post's source device when the post was made.
Longitude	The longitude of the post's source device when the post was made.

Additional Information

Sina Weibo Private Messages

Description	Sina Weibo Private Messages contains stored data from private messages on the Sina Weibo for iOS application.
Recovery method	Parsing

Attribute	Description
Conversation Partner ID	The unique ID of the conversation partner.
Conversation Partner	The name of the conversation partner.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent or received.
Message	The actual private message content.
Profile Image URL	The URL for the profile image of the user.
Downloaded Profile Image	The raw content of the user's profile image, downloaded from the URL shown in the Profile Image URL column.
Attachment Type	The type of attachment associated with the message.
Attachment Local File Path	The local path to the file attachment.

Additional Information

TikTok Contacts

Description	TikTok Contacts contains information about a user's contacts in TikTok.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username of the contact.
Nickname	The nickname of the contact.
ID	The unique ID of the contact.
Profile Picture URL	The URL of the profile picture of the contact.

Additional Information

TikTok Media

Description	TikTok Media contains media that were either viewed or created by the user.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
File Extension	The extension of the file.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the media file was created. If the media file was published or drafted by the user, this date/time comes from the application data. If the application data date/time can't be found, or if the user only watched the media, the date/time comes from the file's metadata instead.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the media file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the media was last written to.
Type	The type of the media (Video or Photo). For some draft media files, if the type is photo, this indicates that the user selected a still photo for their TikTok video that will become a single frame video merged with a chosen accompanying audio when published.
Status	The status of the media (Cached, Draft, Published, Watched). Media that are reported as cached may not imply that the media was seen by the local user but that it was swiped on their Home feed. We recommend further investigation to confirm which videos were watched by the local user.
Skin Tone Percentage	The amount of skin tone found in the media.
File Size (Bytes)	The size of the media.
MD5 Hash	An MD5 hash of the media content. For videos, if frames are not generated

Attribute	Description
	properly for the video, then the file was truncated due to the entire video not being cached on the device. The reported MD5 hash is generated using the available portion of the video.
SHA1 Hash	A SHA1 hash of the media content. For videos, if frames are not generated properly for the video, then the file was truncated due to the entire video not being cached on the device. The reported SHA1 hash is generated using the available portion of the video.
Category	An integer that indicates the Project VIC category for the media.
Attachment	The media.
Recorded Audio	The audio track recorded with the media.
Sound	The sound file added to the media.
Duration	For videos only, the duration of the video in seconds.
Caption	The text for any captions that the media had.
Recorded From Camera	Indicates if the media was recorded from the camera of the device for iOS draft media.
Muted	Indicates if the microphone of the device was muted in iOS draft media.

Additional Information

For cached videos recovered from the cachev2 directory, AXIOM Process repairs the file header to enable video previewing in AXIOM Examine. If you create a report with attachments from the Artifacts explorer, the exported video attachment will contain the modified header. To export the original file, find the original source in the File System explorer in

Additional Information

AXIOM Examine and export from this location. The MD5 hash and SHA1 hash are generated using the repaired video file.
Draft videos may come in the form of separate files for the video, audio, and added sound. In these cases, the hit will include a complete video made from the combined video, audio, and sound, as well as each component file.

TikTok Messages

Description	TikTok Messages contains information about the messages a user sends or receives using TikTok.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the message.
Recipient	The recipient of the message.
Message	The content of the message.
Message Type	The type of the message.
Media URL	The URL of any media attached to the message.
Created Date/Time	The time that the message was sent.
Read	Indicates whether the recipient has read the message.
Deleted	Indicates whether the message has been deleted.

Additional Information

Tumblr Activity

Description	Tumblr Activity provides information of how the Tumblr application accessed API URLs and any media that may accompany these requests.
Recovery method	Parsing

Attribute	Description
Entry ID	The database ID of the request or response from the Tumblr application.
Request URL	The requested URL made by the Tumblr application.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was accessed.
Status	The HTTP response status code of the URL that was accessed.
MIME Type	The MIME Type of the data requested from the Tumblr Request URL.
Content Size (Bytes)	The size of the data requested in bytes.
Attachment	The picture or video media that was requested from the Tumblr Request URL.

Additional Information

Tumblr Blocked Blogs

Description	Tumblr Blocked Blogs contains information about the blogs blocked by the local user.
Recovery method	Parsing

Attribute	Description
Blog Title	The title of the blog.
Creator Name	The name of the blog's creator.
Blocked Date/Time - UTC (yyyy-mm-dd)	The date and time that the blog was blocked.

Additional Information

Tumblr Chat Messages

Description	Tumblr Chat Messages contains messages sent and received using Tumblr.
Recovery method	Parsing

Attribute	Description
Sender	The display name of the user who sent the message.
Recipient	The display name of the user who received the mes-

Attribute	Description
	sage.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The body of the message.
Media URL	The URL of any media attached to the message.
Entry ID	The database ID of the request or response from the Tumblr application.

Additional Information

Tumblr Created Posts

Description	Tumblr Created Posts contains information about the blog posts created by the local user.
Recovery method	Parsing

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the post was created.
Summary	The title of the post.
URL	The URL to the blog post.

Attribute	Description
Blog Title	The title of the post's blog.
Creator Name	The name of the post's creator.
Reblogged From	The name of the original creator, if this post was reblogged.
Tag	The tag or tags that are associated with the post.
Entry ID	The database ID of the request or response from the Tumblr application.

Additional Information

Tumblr Followed Blogs

Description	Tumblr Followed Blogs contains information about the blogs followed by the local user.
Recovery method	Parsing

Attribute	Description
Blog Title	The title of the blog.
Description	The description of the blog.
Creator Name	The name of the blog's creator.
URL	The URL to the blog.

Additional Information

Tumblr Profiles

Description	Tumblr Profiles contains information about the profiles encountered when using the Tumblr application.
Recovery method	Parsing

Attribute	Description
Entry ID	The database ID of the request or response from the Tumblr application.
URL	The URL of the Tumblr Blog profile page.
Blog Title	The title of the blog.
Posts Count	The number of posts the user has made. This does not always populate a value depending on the profile information available.
Description	The description text of the blog.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the blog was last updated.
Creator Name	The name of the blog's creator.
UUID	The universally unique identifier of the creator of the blog.
Local Account	Indicates whether or not the user is a local user. If unknown, the value will be empty.

Attribute	Description
Account Type	Indicates whether the Tumblr blog is a primary or secondary blog if it is determined to be a local account.
Notifications	This is the type of notifications the user will get from a particular blog.
Type	Indicates whether the blog is public or private.
Adult Blog	Indicates whether the account is marked as an adult blog.
NSFW Blog	Indicates whether the blog contains not safe for work content.
Admin	The admin status indicates if the local user has administrative rights to this blog.

Additional Information

Tumblr Tags

Description	Tumblr Tags contains information about the subject tags the local user has selected. Selecting a tags expresses the user's interest in a subject so they can see more content of that type.
Recovery method	Parsing

Attribute	Description
Tag	The tag that the local user selected.

Additional Information

Twitter Direct Messages

Description	Twitter Direct Messages contains carved and noncarved direct messages from the Twitter application. Note that carving may not retrieve the name and screen name of sender and receiver.
Recovery method	Parsing and carving

Attribute	Description
Text	The text of the direct message.
Sender ID	The Twitter ID of the sender.
Recipient ID(s)	The Twitter ID for the recipient(s).
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time that the direct message was sent or received.
Direction	Whether the message was sent or received.
Sender Name	The name of the person sending the direct message.
Sender Screen Name	The screen name or Twitter handle of the person sending the direct message.
Recipient Name(s)	The name(s) of the person(s) receiving the direct message.
Recipient Screen Name(s)	The screen name(s) or Twitter handle(s) of the person(s) receiving the direct message.
Attachments	The attachments associated with the direct message.

Additional Information

Twitter Tweets

Description	Twitter Tweets contains carved and noncarved tweets from the Twitter application. Note that carving older versions of the application will only recover the Tweet column.
Recovery method	Parsing and carving

Attribute	Description
Author ID	The numeric ID of the account that posted the tweet.
Status ID	The unique ID of the tweet.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the tweet was created.
Tweet	The text content of the tweet.
Favorited	Whether the tweet has been favorited.
Latitude	The latitude of the location from which the tweet was posted.
Longitude	The longitude of the location from which the tweet was posted.
Retweet Count	The number of times that the tweet has been retweeted.
Tweet Source	The interface that was used to post the tweet.

Additional Information

This artifact can recover Tweet data locally in versions up to Twitter 8.2.1.0. In later versions, Tweet data is stored in the cloud and cannot be recovered unless you're running a cloud acquisition.

Twitter Users

Description	Twitter Users contains information about users that were cached on the local user's device.
Recovery method	Parsing and carving

Attribute	Description
User ID	The user's Twitter user ID.
User Name	The user's Twitter username.
Full Name	The user's full name.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the user's Twitter profile was created.
Description	The short profile description that the user writes for themself.
Web URL	The user's website URL.
Following	'Yes' if the local user is following this account, 'No' otherwise. If this attribute is empty, it's undetermined whether the local user is following this account.

Attribute	Description
Locale	The location the user is from.
Protected	Whether or not the user's account was protected.
Followers	The number of followers that the user has.
Friends	The number of friends that the user has.
Statuses	The number of different statuses that the user has had.
Image URL	The URL to the user's profile picture.
Friend Metadata Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the user's meta information was last updated.
Header URL	The URL to the user's profile banner picture.

Additional Information

VK Messages

Description	This artifact contains VK messages (either private or group messages) as well as the details about pictures, video, and audio that may have been sent.
Recovery method	Parsing and carving

Attribute	Description
Sender ID	The user ID of the message sender.
Receiver ID(s)	The user ID of the message recipient. This column can contain multiple user IDs if the message is from a group conversation.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent/received.
Message Text	The message text that was sent/received.
Type	The type of message sent. The possible types are 'Private Message' for one-to-one conversations or 'Group Message' for one-to-many conversations.
Message Deleted	The deletion state of the message is unsupported in VK Android and will therefore be empty.
Read State	The read state of the message is unsupported in VK Android and will therefore be empty.
Forwarded Message Content	This column contains the original time that a message was sent, the user ID that originally sent the message, and the content (for example, text, video, or audio).
VK Attachment	This column contains details of the attachment that was sent. For picture attachments, a URL to a scaled picture is provided for downloading. When a video is sent, a thumbnail is provided with details of the video (title, date/-time, duration and description). When audio is sent, a URL to the audio is provided as well as the title, artist, and duration.
Latitude	The latitude in VK Android will be contained within VK Attachment or For-

Attribute	Description
	warded Message Content and this column will be empty.
Longitude	The longitude in VK Android will be contained within VK Attachment or Forwarded Message Content and this column will be empty.
Attachment	The attachment that was sent.

Additional Information
In this artifact, the latitude and longitude data can either represent the device's location at the time when an attachment was created, such as a photo or video, or it can represent a point that the user selected from the world map to send to another user.

VK Users

Description	This artifact contains the various VK users that the data owner has been in communication with, as well as the users own profile.
Recovery method	Parsing and carving

Attribute	Description
User ID	The user ID of the user.
Gender	Identifies whether the user is a male or female.
Birthdate (yyyy-mm-dd)	The birthdate of the user.
First Name	The first name/given name of the user.
Last Name	The last name/surname of the user.

Attribute	Description
Profile Image	The URL to the users profile image.
Downloaded Profile Image	

Additional Information

Whisper Messages

Description	Whisper Messages contains the messages that were sent and received between the local user and others.
Recovery method	Parsing and carving

Attribute	Description
Partner Name	The username of the person that the chat was with.
Message Text	The content of the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Status	The status of the message (received, sent, or send failed).
Read	Indicates whether or not the message has been read when the message was received.
Image	The image that was sent or received.

Additional Information

To learn more about Whisper, see Artifact profile: Whisper.

Yik Yak Notifications

Description	Yik Yak Notifications contains the notifications that have been generated for the user.
Recovery method	Parsing

Attribute	Description
Thing Content	The content of the object that the notification is about.
User ID	The identifier of the user the notification belongs to.
Thing Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the notification about the object was created.
Notification ID	The identifier of the notification.
Thing ID	The identifier of the thing the notification is about.
Thing Type	The type of object the notification is about (for example, a Yak or a Comment).
Subject	The subject of the notification.
Notification Body	The body of the notification.
Reason	The reason for the notification (for example, a Vote or a Comment).
Status	The status of the notification (New, Unread, or Read).

Additional Information

To learn more about Yik Yak, see Artifact profile: Yik Yak.

Yik Yak Yaks

Description	Yik Yak Yaks contains the Yaks the user has viewed on their homepage.
Recovery method	Parsing

Attribute	Description
Message	The content of the Yak.
Poster ID	The ID of the user who posted the Yak.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time the Yak was posted.
Message ID	The ID of the Yak.
Poster Handle	The handle of the user who posted the Yik Yak.
Image URL	The URL to the image associated with the Yak (if one exists).
Downloaded Image	The image of the Yak that was downloaded.
User Vote	Indicates whether the user has voted on the Yak (Down, None, or Up).
Latitude	The latitude of the Yak.
Longitude	The longitude of the Yak.

Attribute	Description
Likes Count	The number of likes the Yak has.
Re-Yaked Count	The number of times the Yak has been Re-Yaked.
Comments Count	The number of comments the Yak has.

Additional Information
To learn more about Yik Yak, see Artifact profile: Yik Yak.

Web Related

Aloha Browser Bookmarks

Description	Aloha Bookmarks contains the webpages that a user has bookmarked.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Title	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Is Folder	Indicates whether the bookmark entry is a folder.

Additional Information

Aloha Browser Downloads

Description	Aloha Browser Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download URL	The URL of the file that was downloaded.
File Path	The absolute path on the device to the file downloaded.
URL	The URL of the site in which the file was downloaded.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was downloaded.

Additional Information

Aloha Browser History

Description	Aloha Browser History contains information about the websites that the user visits.
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the user first visited the webpage.
Title	The title of the webpage.
Visit Count	The number of times the user has visited that webpage.

Additional Information

Bolt Browser Bookmarks

Description	Bolt Browser Bookmarks contains stored bookmark entries for the Bolt browser on iOS.
Recovery method	Parsing

Attribute	Description
URL	The URL of a bookmarked webpage.
Title	The title of the webpage.
Created Date/Time	The date and time when the URL was bookmarked.

Additional Information

Bolt Browser History

Description	Bolt Browser History contains stored history entries for the Bolt browser on iOS.
Recovery method	Parsing

Attribute	Description
URL	The URL of a visited webpage.
Title	The title of the webpage.
Created Date/Time	The date and time when the URL was visited.

Additional Information

Brave Bookmarks

Description	Brave Bookmarks contain bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Last Visited Date/Time - UTC (yyyy-	The date and time when the bookmark was last

Attribute	Description
mm-dd)	visited.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Brave FavIcons

Description	Brave Favicons contains the favicons that Brave displays in the address bar when visiting a website. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Brave Tab History

Description	Brave Tab History contains the websites that the user visits in a particular tab, sorted by order in which they were visited.
Recovery method	Parsing

Attribute	Description
Tab ID	The unique ID of the tab.
Visit Order	The order in which this URL was visited in the tab. Values start at 1 and increase with recency.
URL	The URL of the site visited in the tab.
Title	The title of the webpage that was most recently visited in the tab.

Additional Information

Brave Web History - iOS

Description	Brave Web History contains a history of all the websites that the user visits (includes unique visits only).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Domain	The title of the domain associated to the webpage.
Domain Visit Count	The number of times that the domain was visited.

Additional Information

Chrome

Google Chrome is free web browser developed by Google and is available on all major operating systems, for both mobile and desktop. As of 2016, Chrome usage represents over 70% of the world's total browser traffic.

Analyzing the websites a user visits and the time the visits occur can provide valuable insights about a user. One notable feature that Google Chrome has is that it allows users to sync their bookmarks, browsing history, and more across multiple platforms and devices by using cloud sync accounts.

Forensic notes

Web Visits vs Web History

Chrome has two distinct artifacts that are very similar nature: Chrome Web Visits and Chrome Web History. Both of these artifacts are recovered from the History database. Chrome Web History is parsed from the URLS table and only contains information for the last visited date of a

particular website. Chrome Web Visits can contain multiple entries for the same website, giving the examiner a more complete look at browser usage if the user visited a website multiple times. For example, if a user visits www.magnetforensics.com six times, the Chrome Web History artifact displays only the last time the site is visited, while the Chrome Web Visits artifact potentially displays records for all six instances. Chrome Web Visits was added in a later version of Chrome than Chrome Web History.

Carved web history

The Chrome / 360 Safe Browser / Opera Carved Web History is essentially the same as Chrome Web History except that it's recovered using carving and you may find additional deleted hits with it. The 360 Safe and Opera browsers are included in this artifact because when the data is carved, it's not possible to tell which browser the hit comes from as they're all formatted the same way.

Autofill and profile data

Chrome stores field data that the user has previously input as autofill and profile settings. For example, if you visit magnetforensics.com and login to the customer portal, browsers automatically save your username (and other details) so that you don't have to type it in each time you visit the site. This data is helpful for recovering usernames and other information that your user has filled out on various sites.

Sessions and tabs

When the system has an active session available, Chrome stores the browsing activity as the Chrome Current Session and any tabs that are open as Chrome Current tabs. The previous session and tabs are maintained in Chrome Last Session and Chrome Last Tabs so that the user can restore the last session and tabs if Chrome is closed.

Artifacts

Related resources

Artifact profile: Google Chrome

How does Chrome's 'incognito' mode affect digital forensics?

Forensic email analysis: browser artifacts you may find on a PC or laptop

Chrome Affiliations

Description	Chrome Affiliations contains information about visited pages and the domains their affiliated domains. Typical examples are; login page, advertiser, or CDN affiliated with a larger domain.
Recovery method	Parsing

Attribute	Description
Name	The name of the website visited.
URL	The url of the page visited.
Domain	The domain the visited page is affiliated with.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time of the last visit to the affiliated url.

Additional Information

Chrome Archived Keyword Search Terms

Description	Chrome Archived Keyword Search Terms contains keyword search terms that were archived by the browser.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Chrome Archived Web History

Description	Chrome Archived Web History contains an archived history of old webpage visits.
Recovery method	Parsing

Attribute	Description
URL	The URL where the archived web history is located.
Last Visited Date/Time -	The date and time when the URL was visited.

Attribute	Description
UTC (yyyy-mm-dd)	
Title	The title of the archived web history.
Visit Count	The total number of visits to the URL.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
ID	The ID for the web history archive.

Additional Information

Chrome Autofill Profiles

Description	Chrome Autofill Profiles contains profiles that Chrome uses to fill in forms with saved values.
Recovery method	Parsing

Attribute	Description
Name	The name for the autofill profile.
Email	The email used in the the autofill profile.
Number	The phone number used in the autofill profile.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the profile was last modified.

Attribute	Description
Company	The company name used in the autofill profile.
Address Line 1	The address Line 1 used in the autofill profile.
Address Line 2	The address Line 2 used in the autofill profile.
City	The city used in the autofill profile.
State	The state used in the autofill profile.
Zipcode	The ZIP code used in the autofill profile.
Country	The country used in the autofill profile.

Additional Information

Chrome Autofill

Description	Chrome Autofill contains records of the autofill values that Chrome saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-	The date and time when the autofill was last

Attribute	Description
dd)	used.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Chrome Bookmarks

Description	Chrome Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Chrome Cache Records

Description	Chrome Cache Records contains content that Chrome downloads and caches to speed up rendering times. Cached content can include pictures, text, HTML, JavaScript, and more.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached item.
Website	The website visted.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was first visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the record was last modified.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the cache was last synced with the server.
State	The state of the record. This may be Normal (Live), Doomed (Marked for Deletion), or Evicted (Deleted).
File Type	The type of file that was cached.
Content Size (Bytes)	The size of the cached file.
Picture	The cached picture if the file type is a picture. Otherwise, this

Attribute	Description
	column is empty.
Content	The cached file contents if the file type is not a picture. Otherwise, this column is empty.
File Name	The file name of the cached item.
MD5 Hash	An MD5 hash of the cached item if it is a picture. Otherwise, this column is empty.
SHA1 Hash	A SHA1 hash of the cached item if it is a picture. Otherwise, this column is empty.
PhotoDNA Hash	The hash of the cached item for PhotoDNA if it is a picture. Otherwise, this column is empty.

Additional Information

Chrome Cookies

Description	Chrome Cookies contains cookies that Chrome downloads from the Internet that contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	The domain of the cookie.
Name	The name of the cookie.

Attribute	Description
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Chrome Current Session

Description	Chrome Current Session contains information about the browser session that's currently underway.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Title	The title of the webpage.

Attribute	Description
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Current Tabs

Description	Chrome Current Tabs contains information about the tabs that are open in the current browser session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Title	The title of the webpage.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Downloads

Description	Chrome Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the file that was downloaded.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the download began.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the download ended.
Saved To	The local path where the file was downloaded.
State	The state of the downloaded file.
Opened	Whether or not the download was opened by the user.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Chrome FavIcons

Description	Chrome FavIcons contains the favicons that Chrome displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Chrome GPU Cache Records

Description	Chrome GPU Cache Records contains content that Chrome downloads and caches to speed up rendering times. Cached content can include textures, shader code, and other graphics related content.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached item.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was first visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the record was last modified.
State	The state of the record. This may be Normal (Live), Doomed (Marked for Deletion), or Evicted (Deleted).
Content Size (Bytes)	The size of the cached file.
Content	The cached file contents.

Additional Information

Chrome History Index

Description	Chrome History Index contains an index of the webpages that the user has visited in the past.
Recovery method	Parsing

Attribute	Description
Page URL	The URL of the webpage.

Attribute	Description
Visited On Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was visited.
Title	The title of the webpage.
Body	A snippet of the webpage.

Additional Information

Chrome Keyword Search Terms

Description	Chrome Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Chrome Last Session

Description	Chrome Last Session contains information about the previous browser session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Title	The title of the webpage.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Last Tabs

Description	Chrome Last Tabs contains information about the tabs that were open during the previous session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Title	The title of the webpage.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Logins

Description	Android Chrome Logins contains login information that a user provides in Chrome. Passwords are often encrypted, so you might not be able to recover them unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username of the login.
Password	The password of the login.
GUID	The GUID of the login found in the keychain.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the login was created.
Last Login Date/Time - UTC (yyyy-mm-dd)	The date and time when the login was last used successfully. If the login is unsuccessful for the page or account, this date and time will not be updated.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the login was last modified.
URL	The URL of the login page.

Additional Information

Chrome Saved Credit Cards

Description	Chrome Saved Credit Cards contains the credit card information saved by the user.
Recovery method	Parsing

Attribute	Description
Name On Card	The name of the person on the credit card.
Card Number	The number on the credit card.
Date Modified Date/Time - UTC	The date and time when the information was last mod-

Attribute	Description
(yyyy-mm-dd)	ified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the card was last used.
GUID	The GUID of the user.
Expiry Date	The date the credit card is supposed to expire in month-year format.

Additional Information

Chrome Shortcuts

Description	Chrome Shortcuts contains all of the shortcuts used by Google Chrome for user entered URLs.
Recovery method	Parsing

Attribute	Description
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - UTC	The last access time of the shortcut.

Attribute	Description
(yyyy-mm-dd)	
Web Page Title	The title of the webpage.
Times Used	The number of times that the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut, such as a typed URL or a bookmark.

Additional Information
To learn more about the Transition Type fragment, sign in to the Support Portal to read the article Google Chrome transition types.

Chrome Sync Accounts

Description	Chrome Sync Accounts contains information about the Chrome accounts that a user has logged in with. Chrome syncs data to the cloud so that a user can log in on multiple devices.
Recovery method	Parsing

Attribute	Description
Sync Id	The unique ID for the account that's used to sync data to the cloud.

Attribute	Description
Account Name	The name of the sync account.
Google Account	The GAIA ID of the sync account.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the sync account was synced.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the sync account was created.
Profile Picture URL	The profile picture URL of the sync account.
Active	Indicates whether or not the sync account is active.

Additional Information

Chrome Tab History

Description	Chrome Tab History contains a history of websites that the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the tab file. Android only.
Tab ID	The unique ID of a tab entry in a tab file.
Entry ID	The unique ID of a webpage entry in a tab.

Attribute	Description
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request open the webpage. For example, the referrer source might be from Google or another third-party application.
Originating URL	The URL of the webpage that led the user to the current URL. Android only.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Search Term	The value that the user entered into a search. Android only.

Additional Information

Chrome Top Sites

Description	A list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the site.

Attribute	Description
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the site.
Rank	The rank of the website, where the rank is based on how frequently the website was visited. A value of 1 indicates the most frequent and values increment to 8 as frequency decreases. A value of -1 indicates a site that the user manually added to the list of top sites.
Thumbnail	The thumbnail of the site.

Additional Information

Chrome Web History

Description	Chrome Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.

Attribute	Description
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Chrome Web Visits

Description	Chrome Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is link.

Attribute	Description
Visit Source	The source of the visit.

Additional Information
To learn more about the Transition Type fragment, sign in to the Support Portal to read the article Google Chrome transition types.

Dolphin Browser Bookmarks

Description	Dolphin Browser Bookmarks contains bookmarks from the Dolphin web browser on an iOS device.
Recovery method	Parsing

Attribute	Description
Title	The title of the bookmark.
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was modified.
Visits	The number of times that the user visited this bookmark.

Additional Information

The Visits field is always empty for iOS.

Dolphin Browser History

Description	Dolphin Browser History contains the webpage history from the Dolphin web browser on an iOS device.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the webpage.
URL	The URL of the webpage.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the user first visited the webpage.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the user last visited the webpage.
Visits	The number of times that the user visited the webpage.

Additional Information

DuckDuckGo Bookmarks

Description	DuckDuckGo Bookmarks contains information about the webpages that a user has bookmarked.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Name	The name of the bookmark.
Favorite	Indicates whether the link was added as a favorite.

Additional Information

DuckDuckGo Current Tabs

Description	DuckDuckGo Current Tabs contains information about the tabs that are open in the current DuckDuckGo browser session.
Recovery method	Parsing

Attribute	Description
URL	The URL of the webpage.
Title	The title of the webpage.

Attribute	Description
Was Viewed	Whether the tab was viewed on the local device or not.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that URL was accessed.
Attachment Path	If a snapshot was saved for that tab, this fragment stores the path of the snapshot image file.
Attachment	If a snapshot was saved for that tab, this is the attachment.

Additional Information

DuckDuckGo Whitelisted Websites

Description	DuckDuckGo Whitelisted Websites contains information on domains that have been added by the user to the whitelist or fireproof list of domains.
Recovery method	Parsing

Attribute	Description
Domain	The domain that was added by the user to either the whitelist or fireproof list of domains.
Status	The whitelisted or fireproofed status of a domain. The same domain may be added to one or both domain lists. A whitelisted domain allows for third-party trackers and a fireproofed domain saves cookies even after the application has been closed.

Additional Information

Ecosia Bookmarks

Description	Ecosia Bookmarks contains the webpages that a user has bookmarked in the browser.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Ecosia Current Tabs

Description	Ecosia Current Tabs contains information about the tabs that the user currently has open in the browser.
Recovery method	Parsing

Attribute	Description
Tab ID	The unique ID of the tab.
URL	The webpage URL.
Last Opened Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last opened.
Title	The title of the webpage.

Additional Information

Ecosia Web History

Description	Ecosia Web History contains information about the webpages that a user has visited (includes unique visits only).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the user accessed the URL.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Edge Chromium Bookmarks

Description	Edge Chromium Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Edge Chromium Current Session

Description	Edge Chromium Current Session contains information about the browser session that's currently underway.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Title	The title of the webpage.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Edge Chromium Current Tabs

Description	Edge Chromium Current Tabs contains information about the tabs that are open in the current browser session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Title	The title of the webpage.

Attribute	Description
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Edge Chromium FavIcons

Description	Edge Chromium FavIcons contains the favicons that Chrome displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite or bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Edge Chromium Last Session

Description	Chrome Last Session contains information about the previous browser session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Title	The title of the webpage.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Edge Chromium Last Tabs

Description	Edge Chromium Last Tabs contains information about the tabs that were open during the previous session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Title	The title of the webpage.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Edge Chromium Logins

Description	Edge Chromium Logins contains login information that a user provides in Chrome. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the data was created.
URL	The URL of the login page.

Additional Information

Edge Chromium Web History

Description	Edge Chromium Web History contains a history of the websites that a user has visited. Each artifact hit represents a unique webpage visit, whereas subsequent visits to the same page are tracked by the page's visit count.
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited. The value for this fragment is interpreted to show the actual visit count. The source data starts counting at 0 (0 indicates a single visit occurred), whereas the value that is displayed here is the actual visit count (1 indicates a single visit).
Typed Count	This fragment is not populated for iOS.

Additional Information

Edge Last Session

Description	Edge Last Session contains information about the last snapshot Edge took of the user's browsing session.
Recovery method	Parsing and carving

Attribute	Description
Page URL	The URL of the webpage.
Page Title	The title of the webpage.
Image	The snapshot that the browser took while the user was browsing the webage.
Body	The HTML body that was saved from the webpage.

Additional Information

At certain time intervals, Edge takes a snapshot of the user's browsing session. Using this artifact, an investigator is able to see exactly what the user was looking at, at the time of snapshot. The time interval between snapshots is unknown. Due to the interval, it's possible for a tab to be opened and closed quick enough that the tab isn't included in a snapshot.

Google Analytics First Visit Cookies

Description	Google Analytics First Visit Cookies contains information about Google Analytics first-visit cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Creation DateTime	The date and time when the site was first visited.
Most Recent Visit Date/Time	The date and time of the most recent session.
2nd Most Recent Visit Date/Time	The date and time of the previous session.
Hits	The number of visits.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics First Visit Cookies Carved

Description	Google Analytics First Visit Cookies Carved contains information about Google Analytics first-visit cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Most Recent Visit Date/Time	The date and time of the most recent session.

Attribute	Description
2nd Most Recent Visit Date/Time	The date and time of the previous session.
Hits	The number of visits.

Additional Information

Google Analytics Referral Cookies

Description	Google Analytics Referral Cookies contains information about Google Analytics referral cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Cookie Source	The source URL used to reach the site.
Host	The domain of the URL.
Update Date/Time	The last time that the cookie was updated.
Campaign	The method of referral.
Access Method	Indicates whether the site was accessed organically or was referred.
Keyword	The keywords that were used to arrive at the site.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics Referral Cookies Carved

Description	Google Analytics Referral Cookies Carved contains information about Google Analytics referral cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	Contains the domain of the URL.
Last Update Date/Time - UTC (yyyy-mm-dd)	The last time the cookie was updated.
Cookie Source	The source URL used to reach the site.
Access Method	Indicates whether the site was accessed organically or was referred.
Campaign	The method of referral.
Keyword	The keywords used to arrive at the site.
Path to Page	

Additional Information

Google Analytics Session Cookies

Description	Google Analytics Session Cookies contains information about Google Analytics session cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start time of the current sesion.
Outbound Link Events Left	
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics Session Cookies Carved

Description	Google Analytics Session Cookies Carved contains information about Google Analytics session cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	Contains the domain of the URL.
Start Current Session Date/Time	The start date and time of the current sesion.
Page Views	The number of visits to this page from the user.
Outbound Link Events Left	

Additional Information

Google Analytics URLs

Description	Google Analytics URLs contains URLs that are discovered in other artifacts that are related to Google Analytics.
Recovery method	Carving

Attribute	Description
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	The domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.

Attribute	Description
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics URLs Carved

Description	Google Analytics URLs Carved contains information about Google Analytics URLs that are recovered using carving.
Recovery method	Carving

Attribute	Description
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	The domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.

Attribute	Description
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.

Additional Information

iOS Safari Cache Records

Description	iOS Safari Cache contains Locally cached content from the Safari browser on iOS.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached content.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cached content was created on the local device.
Content	The raw cached content. This field is blank if the content is an image, in which case, the Image column will be populated instead.
File Type	The type of the cached file, such as HTML, JS, CSS, and JPEG.
Content Size (Bytes)	The size of the cached content, in bytes.
Image	The raw content of the cached image. This field is blank if the content is not an image.

Additional Information

iOS Safari Recent Search Terms

Description	iOS Safari Recent Search Terms contains the search terms that a user runs in the Safari browser.
Recovery method	Parsing

Attribute	Description
Search Term	The term that was searched.
Search Date/Time	The date and time of the search.

Additional Information

Malware/Phishing URLs

Description	Malware/Phishing URLs contains records that are believed to be either malware or phishing related URLs.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the website.

Attribute	Description
URL	The URL of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact that the URL belongs to.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Pornography URLs

Description	Pornography URLs contains records that are believed to be pornography related URLs.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the website.
URL	The URL of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact that the URL belongs to.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information
You can find a list of the domains that are supported by this refined result at Pornography URLs.

Potential Browser Activity

Description	The Potential Browser Activity artifact will recover browser-related URLs. This includes Chrome Incognito and Firefox Private Browsing URLs, HTTP request artifacts from multiple browsers, and regular web browsing artifacts. This does not include metadata such as the Windows username, dates and times, and so on. Note that some recovered URLs can be from background browser processes related to certificate authorities.
Recovery method	Carving

Attribute	Description
URL	The URL that the request was sent to.
User Agent	The string that represents the browser that sent the request.

Additional Information

Puffin Browser Bookmarks

Description	Puffin Browser Bookmarks contains bookmarks from the Puffin Browser for iOS.

Recovery method	Parsing

Attribute	Description
Title	The title of the bookmark.
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was added.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the user last visited the webpage.
Visits	The number of times that the user visited this bookmark.

Additional Information

The following columns are empty for iOS Puffin Browser Bookmarks: Created Date/Time, Last Accessed Date/Time, and Visits.

Puffin Browser History

Description	Puffin Browser History contains the web history for the Puffin Browser for iOS.
Recovery method	Parsing

Attribute	Description
Title	The title of the webpage.
URL	The URL of the webpage.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the user last visited the webpage.
Last Accessed Date/Time - Local Time (yyyy-mm-dd)	The date and time that the user last visited the webpage.
Visits	The number of times that the user visited that webpage.

Additional Information
Last Accessed Date/Time - UTC and Visits are empty for iOS Puffin Browser History. Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Rebuilt Webpages

Description	Rebuilt Webpages contains the data that allows for the reconstruction of webpages.
Recovery method	Not applicable

Attribute	Description
Page Title	The title of the webpage.

Attribute	Description
URL	The URL of the webpage.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the original record was created.
Domain	The domain of webpage.
Cache Table	The table that the data to re-construct the page came from.
Cache RowID	The row ID in the table that constructed the rebuilt webpage.

Additional Information

Safari Bookmarks

Description	Safari Bookmarks contains stored bookmarks for the Safari browser on iOS.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmarked webpage.
Title	The title of the bookmarked webpage.
Type	The type of bookmark (for example, Bookmark, Favorite, and Folder)

Attribute	Description
Read	If the bookmark type is a reading list item, this indicates whether the item has been read. This attribute is empty for all other types.
Added Date/Time - UTC (yyyy-mm-dd)	Indicates the date and time that the bookmark was added.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	Indicates the date and time that the bookmark was last visited.
Modified Date/Time - UTC (yyyy-mm-dd)	No data is populated for this fragment on iOS.
Locally Added	Indicates whether the bookmark was created on the local device or a synced device with the same Apple ID. The value in the database for locally_added is 0 to indicate 'Yes' and 1 for 'No'.

Additional Information

Safari Downloads

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for Windows. This table captures information related to files that have been downloaded from Safari.

Recovery method	Parsing

Attribute	Description
Download URL	The URL of the downloaded file.
Saved to Path	The local path where the download was saved.
Download Start Date/Time - UTC (yyyy-mm-dd)	The date and time the download started.
Download End Date/Time - UTC (yyyy-mm-dd)	The date and time the download finished.
Download Identifier	The unique identifier for the download.
Amount Downloaded (Bytes)	The number of bytes downloaded.
Size of Download (Bytes)	The size of the download in bytes.

Additional Information

Safari History

Description	Safari History contains stored history entries for the Safari browser on iOS.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of a visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Redirect URL	The URL that the user was redirected to.
Title	The title of the webpage.
Visit Count	The number of times that the URL was visited.
Visit Source	Indicates whether the website was viewed on the local device or on a synced device.

Additional Information

Safari iCloud Devices

Description	Safari iCloud Devices contains information about the devices that are synced to an iCloud account. Each device can access any browser tabs that are synced to the account.
Recovery method	Parsing

Attribute	Description
Unique Device Identifier	A unique ID for the device that is accessing the tab.
Device Name	The name of the device that is linked to the iCloud account.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the device first synced to the iCloud account.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the device last synced with the iCloud account.

Additional Information

Safari iCloud Tabs

Description	Safari iCloud Tabs contains information about tabs that have been opened in the browser and synced to an iCloud account. Synchronized tabs are available to any device that logs in to the iCloud account.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the tab.
URL	The URL address of the tab.
Unique Device Identifier	A unique ID for the device that is accessing the tab.
Device Name	The name of the device that is accessing the tab.
Tab ID	The unique ID of the tab.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was created.

Attribute	Description
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was last modified.
Modified By	The name of the device that last modified the tab.
Close Requested	Indicates whether a close request has been opened for the tab.
Close Request Date/Time - UTC (yyyy-mm-dd)	The date and time when the close request was created.

Additional Information

Safari Last Session

Description	Safari Last Session captures information related to the last time the user browsed the internet using Safari.
Recovery method	Parsing

Attribute	Description
Tab URL	The URL of the webpage.
Tab Title	The title of the webpage.

Additional Information

Safari Suspended State Tabs

Description	Safari Suspended State Tabs contains the current state of each browser tab in Safari that is currently open on the local device. The date and time are only updated when the user interacts with that tab on the local device. Since these are local tab states, results from this artifact may contain an earlier date and time compared to the results in the Safari History Artifact if iCloud Safari synchronization is enabled across multiple devices on one iCloud account.
Recovery method	Parsing and carving

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Interaction Date/Time - UTC (yyyy-mm-dd)	The date and time of the current tab's state when it was last interacted with on the local device. This date and time will reflect when the user has last interacted with this tab in Safari or if the tab auto-refreshed on the local device only.
Visit Order	The browsing order of the pages viewed in the tab where 0 indicates it is the earliest viewed tab and the highest number indicates the most recently viewed tab.
Private Browsing	Indicates whether the webpage was viewed using the private browsing setting.
Attachment	A thumbnail of the tab.
Tab ID	The ID of the tab that the webpage was visited in.

Additional Information

WebKit Browser Session/Tabs (Carved)

Description	WebKit Browser Sessions/Tabs contains information about the browser sessions and tabs that the user has open, while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers, such as Firefox and Safari, aren't likely to appear under this artifact.
Recovery method	Carving

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

WebKit Browser Web History (Carved)

Description	WebKit Browser Web History contains information about the websites that a user visits while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers aren't likely to appear under this artifact, however, some URLs found by other browsers may also be found by this artifact.
Recovery method	Carving

Attribute	Description
URL	The URL of the visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited
Title	The title of the visited webpage.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the webpage was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Whale Autofill

Description	Whale Autofill contains records of the autofill values that Whale saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Whale Bookmarks

Description	Whale Browser Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Whale Cookies

Description	Whale Cookies contains cookies that Whale downloads from the Internet that contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	The domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was last accessed.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie expires.
Path	The path of the cookie value.

Additional Information

Whale Downloads

Description	Whale Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the download finished.
Saved To	The absolute path on the device to the downloaded file.

Attribute	Description
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Whale FavIcons

Description	Whale Favicons contains the favicons that Whale displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite or bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Whale Keyword Search Terms

Description	Whale Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Additional Information

Whale Logins

Description	Whale Logins contains login information that a user provides in Whale. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username entered.
Password	The password entered.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the data was created.
URL	The URL of the login page.

Additional Information

Whale Top Sites

Description	Whale Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser homepage which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Additional Information

Whale Web History

Description	Whale Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Whale Web Visits

Description	Whale Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to the URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

Yandex Autofill

Description	Yandex Autofill contains records of the autofill values that Yandex saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.

Attribute	Description
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Yandex Bookmarks

Description	Yandex Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Yandex Cookies

Description	Yandex Cookies contains cookies that Yandex downloads from the Internet that contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	The domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie expires.
Path	The path of the cookie value.

Additional Information

Yandex Downloads

Description	Yandex Downloads contains information about the files that a user downloads from the Internet.

Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the downloaded was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the downloaded finished.
Saved To	The absolute path on the device to the file downloaded.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Yandex FavIcons

Description	Yandex Favicons contains the favicons that Yandex displays in the address bar for the website that's currently displayed. These icons are

	sometimes downloaded when you favorite or bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time when the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Yandex Keyword Search Terms

Description	Yandex Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.

Attribute	Description
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Yandex Logins

Description	Login information that a user provides in Yandex. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the data was created.
URL	The URL of the login page.

Additional Information

Yandex Shortcuts

Description	Contains all of the shortcuts used by Yandex for user entered URLs.
Recovery method	Parsing

Attribute	Description
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - UTC (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the web page.
Times Used	The number of times the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

Additional Information

Yandex Sync Data

Description	Yandex Sync Data contains information about the data that Yandex has synced to a user's account in the cloud.
Recovery method	Parsing

Attribute	Description
Name	The name of the sync key.
Local Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the local system.
Server Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the server.
Local Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the local system.
Server Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the server.
Type	The type of data that is synced (bookmark, favicon, type URL, and so on).
Parsed Content	The type parsed data.
Favicon Image	The actual favicon image.

Additional Information

Yandex Top Sites

Description	A list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the site was last updated.
Title	Title of the site.
Thumbnail	Thumbnail of the site

Additional Information

Yandex Web History

Description	A history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.

Attribute	Description
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Yandex Web Visits

Description	A history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Attribute	Description
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

YARA Rules

YARA Rule Matches

Description	The YARA artifact contains information about files and processes that matched with conditions specified in a YARA rule.
Recovery method	Parsing

Attribute	Description
File Name	The name and extension of the file whose content matched with the condition(s) from the YARA rule. The value is blank if the match came from a process (executable/application that was loaded into memory at the time of the memory dump) during memory analysis using the Comae plugin option.
File size (bytes)	The size of the file in bytes. The value is blank if the match came from a Process.
Process	The name of the process that matched with the condition(s) from the YARA

Attribute	Description
Name	rule. The value is blank if the match came from a file.
Process ID	The ID of the process (PID). The value is blank if the match came from a File.
Matched rule set(s)	List of the paths and respective YARA rule sets that had a match.
Matched rule	The YARA rule name that a match was found for.
Matching conditions	List of conditions for the YARA rule that had a match.

Additional Information

macOS

Additional Sources

Android Backups

Description	Android Backups contains information about any backups of Android devices that are recovered from the computer. If an Android backup is recovered during a search, you can search the contents of the backup for additional artifacts.
Recovery method	Parsing

Attribute	Description
File Name	The name of the backup file.
File Path	The path where the backup was stored on the computer.
Encryption	The type of encryption (if any) that was used on the backup.
File System Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time for the AB file from the file system.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time for the AB file from the file system.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time for the AB file from the file system.

Additional Information

Apple Disk Images

Description	Apple disk images are commonly stored as DMG or IMG files. These files are containers that may contain additional items of interest. This artifact identifies any Apple disk image found on the system.
Recovery method	Parsing

Attribute	Description
File Name	The name of the Apple disk image file.
File Path	The path where the Apple disk image was stored on the computer.
File Type	The type of Apple disk image file (DMG or IMG).
File System Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time for the file from the file system.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time for the file from the file system.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time for the file from the file system.

Additional Information

iOS Backups

Description	iOS Backups contains information about any backups of iOS devices that are recovered from the computer. If an iOS backup is recovered during a search, you can search the contents of the backup for additional artifacts.
Recovery method	Parsing

Attribute	Description
Device Phone Name	The name of the iOS device from which the backup originated.
Device Phone Number	The phone number of the iOS device from which the backup originated.
IMEI	The IMEI of the iOS device from which the backup originated.
ICCID	The ICCID of the iOS device from which the backup originated.
Backup File Creation Date/Time	The date and time when the backup was created.
Product Name	The model of the iOS device from which the backup originated.
Product Version	The version of iOS of the device at the time of the backup creation.
Serial Number	The serial number of the iOS device from which the backup originated.

Additional Information

Application Usage

Application Install States

Description	Application Install States contains a list of state changes that occur while an application installs or is uninstalled on an iOS device.
Recovery method	Parsing

Attribute	Description
Action	The type of change that occurred to the application.
Package Name	The internal name of the application.
Date/Time	The date and time that the event occurred.
Path	The file path to the package of the application.

Additional Information

Application Permissions - MacOS, iOS

Description	Application Permissions contains information about the app permissions that a user is prompted to accept or decline while using macOS applications.
Recovery method	Parsing

Attribute	Description
Application	The application that requests the permission.
Service Name	The permission service name.
Allowed	Indicates whether the application is allowed to use the service/permission.
Prompt Count	The number of times the user was prompted to give the permission to the application.

Additional Information

Biome Application Focus

Description	Biome Application Focus provides information about the applications that were in focus on the device screen, within a recorded interval.
Recovery method	Parsing

Attribute	Description
Bundle ID	The bundle name of the application, used to uniquely identify it in the application store.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time of when the application was brought into focus.
End Date/Time - UTC (yyyy-mm-dd)	The date and time of when the application was removed from focus.

Attribute	Description
Metadata	Metadata relating to the application in focus.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time of when the Biome record was created.
GUID	The GUID of the Biome record.

Additional Information

Biome Application Launch

Description	Biome Application Launch provides information about when applications were launched on the device.
Recovery method	Parsing

Attribute	Description
Bundle ID	The bundle name of the application, used to uniquely identify it in the application store.
Transition Type	The type of transition used to launch the application.
Type	Indicates where the application was launched (Local or Remote).
Device ID	The ID of the remote device presented as a GUID.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time of when the Biome record was created.

Attribute	Description
Display Version	The display version of the application.
Internal Version	The internal version of the application.

Additional Information

Biome Device Plugged-in States

Description	Biome Device Plugged-in States provides information about when the device was plugged in.
Recovery method	Parsing

Attribute	Description
GUID	The GUID of the Biome record.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the device was plugged in.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the device was unplugged.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time when the Biome record was logged.

Additional Information

Biome Device Screen Backlight States

Description	Biome Screen Backlight States provides information about the device backlight within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time. This information can help identify whether a device was in active use within a specific interval.
Recovery method	Parsing

Attribute	Description
State	The screen backlight state of the device. This value indicates whether the screen backlight is on or off.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started for First Backlight After Wakeup records.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended for First Backlight After Wakeup records.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.
Type	The type of record for the screen backlight state, which might have been retrieved from the public Backlight folder, or from the restricted _ DKEvent.User.IsFirstBacklightOnAfterWakeup folder.
GUID	The GUID of the Biome record.

Additional Information

Installed Applications - macOS

Description	Applications that are installed on the computer that's running macOS.
Recovery method	Parsing

Attribute	Description
Display Name	The display name of the installed application.
Package Name(s)	The application bundle(s), which represent the application package identifier(s) in the App Store.
Display Version	The version number of the application provided via the App Store.
Internal Version	The long version string of the application.
Installed/Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was last installed or updated.
App Store Action	The App Store action further describes the application installation or update.

Additional Information

KnowledgeC Activity Level

Description	KnowledgeC Activity Level provides information about the KnowledgeC

	stream type of activity level.
Recovery method	Parsing

Attribute	Description
Activity Type	The activity level.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Application Activities

Description	KnowledgeC Application Activities contains information about activities associated with specific applications.
Recovery method	Parsing

Attribute	Description
Activity	The description associated with the activity.
Application Name	The bundle name of the application associated with

Attribute	Description
	activity.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time that the activity occurred.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Application Focus

Description	KnowledgeC Application Focus provides information about the applications that were in focus on the device screen, within a recorded interval.
Recovery method	Parsing

Attribute	Description
Application Name	The bundle name of the application in focus.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Application Install States

Description	KnowledgeC Application Install States provides information about when applications were installed or uninstalled on the device.
Recovery method	Parsing

Attribute	Description
Application Name	The bundle name of the application that was installed or deleted.
Install State	The install state of the application (Installed or Uninstalled).
State Changed Date/Time - UTC (yyyy-mm-dd)	The date and time that install state last changed.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Application Usage

Description	KnowledgeC Application Usage provides information about the applications that were used on the device, within a recorded interval.
Recovery method	Parsing

Attribute	Description
Application Name	The bundle name of the application used.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Application Web Usage

Description	KnowledgeC Application Web Usage provides information about the applications that were used to access webpages on a iOS device, within a recorded interval.
Recovery method	Parsing

Attribute	Description
Application Name	The bundle name of the application that accessed the webpage.
Domain	The domain name of the webpage.
URL	The URL of the webpage.
Start Date/Time - UTC (yyyy-mm-	The date and time that the time interval started.

Attribute	Description
dd)	
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Device Lock States

Description	KnowledgeC Device Lock States provides information about whether the device is locked or unlocked within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time.
Recovery method	Parsing

Attribute	Description
State	The lock state of the device (Locked or Unlocked).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Device Orientation States

Description	KnowledgeC Device Orientation States provides information about the orientation of the device within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time.
Recovery method	Parsing

Attribute	Description
State	The orientation state of the device (Vertical or Sideways).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Device Plugged-in States

Description	KnowledgeC Device Plugged-in States provides information about the plugged-in state of a device within recorded intervals. An absence of a

	recorded interval might mean that device was turned off during that time. Knowing whenever a device is connected to charger or computer using USB can help identify how the device is used.
Recovery method	Parsing

Attribute	Description
State	The plugged-in state of the device. This value shows whether a device is plugged in and/or connected via USB (Plugged in or Unplugged).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Media History

Description	KnowledgeC Media History provides information about what type of audio or video media the user was engaging with at what time, as recovered from KnowledgeC.db

Recovery method	Parsing

Attribute	Description
Application Name	The bundle name of the application used to play the specified media.
Album	The album name of the specified media.
Title	The title of the specified media.
Artist	The artist of the specified media.
Duration	The duration of the specified media in seconds.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the media started playing.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the media stopped playing.

Additional Information

KnowledgeC Notification Usage

Description	KnowledgeC Notification Usage provides information about a user's notification usage within recorded intervals.
Recovery method	Parsing

Attribute	Description
Bundle ID	The bundle ID.
Type	The type of notification.
Device ID	The device ID.
Process ID	The process ID.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Safari History

Description	KnowledgeC Safari History provides information about webpages that were accessed using the Safari browser, as recovered from knowledgeC.db
Recovery method	Parsing

Attribute	Description
URL	The URL of the webpage that was accessed with Safari browser.

Attribute	Description
Title	The title of the webpage that was accessed with Safari browser.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was accessed with Safari browser.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

KnowledgeC Screen Backlight States

Description	KnowledgeC Screen Backlight States provides information about the device backlight within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time. This information can help identify whether a device was in active use within a specific interval.
Recovery method	Parsing

Attribute	Description
State	The screen backlight state of the device. This value indicates whether the screen backlight is on or off (Screen on or Screen off).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.

Attribute	Description
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Additional Information

Cloud Storage

iCloud Devices

Description	iCloud Devices show a list of devices that have access to the iCloud.
Recovery method	Parsing

Attribute	Description
Device Name	The name of the device.

Additional Information

iCloud Downloads

Description	iCloud Downloads show a list of files that have been either recently downloaded or are pending download.

Recovery method	Parsing

Attribute	Description
File Name	The name of the iCloud file.
Download State	Indicates whether the file is available on the local drive or is pending download.
File Size (Bytes)	The size of the file in bytes.
Download Request Date/Time - UTC (yyyy-mm-dd)	The date and time that the download was requested.

Additional Information

iCloud Local Files

Description	iCloud Local Files are files that have been imported from the local computer or synced remotely from the iCloud Drive folder on a macOS machine.
Recovery method	Parsing

Attribute	Description
File/Folder Name	The name of the iCloud file or folder.
iCloud Drive Path	The iCloud drive path to the file or folder.

Attribute	Description
Original File Name	The name of the file when it was first loaded to the iCloud Drive.
Package Name	The package ID of the application used to interact with the file.
File Size (Bytes)	The size of the file in bytes.
Item Type	Indicates whether an item is a file, a folder, or a hidden iCloud File. Hidden iCloud files are used as markers for upload and download sync states and are .iCloud files.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file or folder was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file or folder was modified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when that the file was last accessed on the iCloud Drive.
Device Name	The name of the device.

Additional Information

iCloud Server Files

Description	iCloud Server Files are files that exist on the iCloud server, and may not exist on the local macOS machine.

Recovery method	Parsing

Attribute	Description
File/Folder Name	The name of the iCloud file or folder.
iCloud Drive Path	The iCloud drive path to the file or folder.
Original File Name	The name of the file when it was first loaded to the iCloud Drive.
File Size (Bytes)	The size of the file in bytes.
Item Type	Indicates whether an item is a file, a folder, or a hidden iCloud File. Hidden iCloud files are used as markers for upload and download sync states and are .iCloud files.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file or folder was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file or folder was modified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when that the file was last accessed on the iCloud Drive.
Device Name	The name of the device.
Shared	Indicates whether the file was shared or not.

Additional Information

iCloud Uploads

Description	iCloud Uploads show a list of files that have been either recently uploaded or are pending upload.
Recovery method	Parsing

Attribute	Description
File Name	The name of the iCloud file.
Upload State	Indicates whether the file is available on the local drive or is pending upload.
File Size (Bytes)	The size of the file in bytes.
Upload Request Date/Time - UTC (yyyy-mm-dd)	The date and time that the upload was requested.

Additional Information

Communication

Apple Contacts - macOS

Description	Apple Contacts contains information about the contacts that a user has saved to their device.
Recovery method	Parsing

Attribute	Description
First Name	The first name of the contact.
Last Name	The last name of the contact.
Picture	The profile picture of the contact, in its full size.
Home Phone	The home phone numbers associated with the contact.
Mobile Phone	The mobile phone numbers associated with the contact.
Office Phone	The office phone numbers associated with the contact.
Phone Number(s)	Any additional phone numbers associated with the contact.
Home Email	The home email addresses associated with the contact.
Office Email	The office email addresses associated with the contact.
Email(s)	Any additional email addresses associated with the contact.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact's information was created.
Address	The physical addresses associated with the contact.
Website	The websites associated with the contact.
Middle Name	The middle name of the contact.
Source Account	The linked account that the contact was imported from.
Organization	The organization or business associated with the contact.
Company	Indicates whether or not the contact is a company.

Attribute	Description
Department	The department associated with the contact.
Note	Notes associated with the contact.
Birthday (yyyy-mm-dd)	The birthday of the contact.
Job Title	The job title associated with the contact.
Nickname	The nickname associated with the contact.
Prefix	Any prefix applied to the contact's name (such as Mr., Mrs., or Dr.).
Suffix	Any suffix applied to the contact's name (such as PH.D, Ed.D, LLD).
User Accounts	A comma separated list all the social media accounts associated with this contact.
First Name Phonetic	The phonetic spelling of the contact's first name.
Middle Name Phonetic	The phonetic spelling of the contact's middle name.
Last Name Phonetic	The phonetic spelling of the contact's last name.
Previous Last Name	The previous last name of the contact.
Relationship	Relationships that the contact shares with others (e.g. Mother, Father, or Spouse).
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact's information was last modified.

Additional Information

Apple Contacts Groups

Description	Apple Contacts Groups contains information about the groups that the user creates to organize their contacts.
Recovery method	Parsing

Attribute	Description
Name	The name of the contact group.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the group's information was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the group's information was last modified.
Group Member(s)	The contacts that have been added to the group.
Source Account	The linked account that the contact group was imported from.

Additional Information

Facebook Messenger Calls

Description	Facebook Messenger Calls contains call data recovered from Facebook Messenger.
Recovery method	Parsing

Attribute	Description
User Key	The user key of the call partner. If the call was made in a group chat, this field will be empty.
Thread Key	The thread key of the group where the call was made. If the call was made in a chat with only one other person, this field will be empty.
Partner Name	The name of the call partner. If the call was made in a group chat, this field will be empty.
Group Name	The name of the group where the call was made. If the call was made in a chat with only one other person, this field will be empty.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the call.
Call Duration	The duration of the call in a friendly text format. This field is left empty if the call wasn't answered.
Call Duration (Seconds)	The duration of the call in seconds. This field is left empty if the call wasn't answered.
Call Type	The type of the call. The call type is either a voice call or a group voice call.
Answered	Indicates whether the call was answered or not.
Direction	The direction of the call.
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).

Additional Information

Facebook Messenger Groups

Description	Facebook Messenger Groups contains data about group chats on Facebook Messenger.
Recovery method	Parsing

Attribute	Description
Application Name	The name of the application that generated the data (Facebook Messenger Desktop).
Thread Key	The thread key of the group.
Group Name	The display name of the group.
Participants	The IDs of the users that are a part of the group.
Participants User Names	The usernames associated with the participants of the group.
Sender(s)	The IDs of the users that recently participated in the group (for example, by sending a message).
Senders User Names	The usernames associated with the respective senders in the group.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The date and time of the last activity recorded in the group.
Message Count	The approximate number of messages in the group.

Additional Information

Facebook Messenger Messages

Description	Facebook Messenger Messages contains messages recovered from Facebook Messenger.
Recovery method	Parsing

Attribute	Description
Sender Name	The display name of the person sending the message.
Sender ID	The user ID of the person sending the message.
Receiver Name	The display name of the person receiving the message.
Group Name	The display name of the group receiving the message.
Receiver ID	The user ID of the person receiving the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time when message was sent.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time the message was deleted from the application.
Text	The text of the message.
Message Type	The type of message that was sent. If multiple attachments were sent together, this fragment indicates the number of attachments.

Attribute	Description
Send State	Represents whether the message was sent, received or queued.
Media Info	The information about the media that is found. This value can be a URL to the media, a file name, or a sticker ID.
Latitude	The latitude portion of the location data that is sent with the message.
Longitude	The longitude portion of the location data that is sent with the message.
Application Name	The name of the application that generated the data (Facebook Messenger Desktop).
Thread ID	The thread ID of the message. This is also the Facebook ID of the remote party.
Message ID	The internal unique message ID.
Message Source	The source of the message creation platform.
Attachment	The recovered attachment. If the attachment is a video, the video gets segmented into multiple files. Each segment gets collected for playback in Magnet AXIOM, but the actual file size might differ from the size that AXIOM reports due to the segmentation.

Additional Information

Facebook Messenger Users Contacted

Description	Facebook Messenger Users Contacted contains information about users contacted from the device using Facebook Messenger.

Recovery method	Parsing

Attribute	Description
User Key	The user key of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
Name	The display name of the user.
Username	The unique identifier of the user.
Profile Image	The profile image of the user.
Profile Picture URL	The URL of the user's profile picture.
Is App User	Identifies whether the user is using Facebook Messenger or not.
Is Friend	Identifies whenever the user is a friend of the local user.
Application Name	The name of the application that generated the data (Facebook Messenger Desktop).
Rank	User's rank within the app.

Additional Information

Houseparty Messages

Description	Houseparty Messages contains messages recovered from Houseparty.
Recovery method	Parsing

Attribute	Description
Sender	The username of the person sending the message.
Recipient	The username of the person receiving the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The content of the sent message.
Read Status	Indicates whether or not the message has been read.

Additional Information

Houseparty Users

Description	Houseparty Users contains information about the users contacted from the device using Houseparty.
Recovery method	Parsing

Attribute	Description
User Name	The username of the user.

Attribute	Description
Full Name	The full name of the user.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the user account was created.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the user account was last updated.

Additional Information

iMessage Archived Chats

Description	iMessage Archived Chats contains information from messages that have been archived on the macOS computer. iMessage allows users to chat using text, video, and audio and is a standard on almost all iOS and macOS devices.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message.
Recipient	The recipient of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message content.

Attribute	Description
Read Status	The read status of the message.
Attachment Name(s)	The attachment file names, recovered from the iChat file.

Additional Information

iMessage Archived Messages

Description	iMessage Archived Chats contains information from messages that have been archived on the macOS computer. iMessage allows users to chat using text, video, and audio and is a standard on almost all iOS and macOS devices.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message.
Recipient	The recipient of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message content.
Read Status	The read status of the message.

Additional Information

iMessage Chats

Description	iMessage (previously iChat) is a chat application for Apple products that allows users to share files and communicate via text chat, video, and audio. iMessage is standard on almost all Mac computers and iOS devices.
Recovery method	Parsing

Attribute	Description
Recipient	The recipient of the message.
Sender	The sender of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message content.
Type	The type of message.
Status	The sent status of the message.

Additional Information

iMessage Messages

Description	iMessage (previously iChat) is a chat application for Apple products that allows users to share files and communicate via text chat, video, and audio. iMessage is standard on almost all Mac computers and iOS devices.

Recovery method	Parsing

Attribute	Description
Recipient	The recipient of the message.
Sender	The sender of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message content.
Type	The type of message.
Status	The sent status of the message.

Additional Information

IP Addresses - Audio/Video Calls

Description	IP Addresses of web audio/video calls show who a user was communicating with. Each instance of this artifact represents a single hop in the communication chain. By showing the relationship between multiple hops, you can determine where a call originated from and what the final destination was.
Recovery method	Carving

Attribute	Description
Call ID	The ID of the call.
Message ID	The ID of the message.
Domain	The domain used for the call.
Connection Type	The type of connection.
Origin IP Address	The originating IP address for this hop in the call.
Origin Port	The originating port for this hop in the call.
Destination IP Address	The destination IP address for this hop in the call.
Destination Port	The destination port address for this hop in the call.
Date/Time - UTC (yyyy-mm-dd)	The timestamp associated with this hop in the call.
Remote User ID	The unique ID of the remote user.
Communication Protocol	The communication protocol for this call (either UDP or TCP).
Metadata	Any additional details about the call.

Additional Information

Signal Messages - macOS

Description	Signal Messages - macOS contains decrypted messages sent or received by a Signal user on macOS.
Recovery method	Parsing

Attribute	Description
Sender	The phone number of the sender.
Recipient(s)	The recipient(s) of the message. If this is not a phone number it will be a UUID tied to the recipient.
Conversation ID	A UUID identifying the conversation.
Conversation Name	The name of the conversation.
Conversation Type	The type of conversation.
Message	The message body.
Sent Date/Time - UTC (yyyy-mm-dd)	The date/time in UTC that the message was sent.
Received Date/Time - UTC (yyyy-mm-dd)	The date/time in UTC that the message was received.
Direction	The direction of the message.
File Name	The name of the attached file(s).
File Size (Bytes)	The size of the attached file(s).
File Type	The type of the attached file(s).
File Path	The path for the attached file(s).

Additional Information

Skype Accounts

Description	Skype Accounts contains information about the Skype accounts that are recovered, such as user information and when the account was created.
Recovery method	Parsing

Attribute	Description
Skype Name	The Skype name of the account.
Display Name	The display name of the account.
Full Name	The full name of the account.
Email(s)	The email of this account.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date when the profile was created.
Last Online Date/Time - UTC (yyyy-mm-dd)	The last time that the account was online.
Birthday (yyyy-mm-dd)	The birthday of the account.
Gender	The gender of the account.
City	The city where the account is located.
State/Province	The state/province where the account is located.
Country	The country where the account is located.
Home Phone	The home phone of this contact.
Office Phone	The office phone of this account.

Attribute	Description
Mobile Phone	The mobile phone of this account.
Homepage	The homepage of this contact.
About Info	The about info of this contact.
Profile Last Modified On Date/Time - UTC (yyyy-mm-dd)	The date when the profile was last modified.
Mood Text	The text used to express mood.
Last Used On Date/Time - UTC (yyyy-mm-dd)	The last time that the account was used.
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	The time that the avatar was created.
Picture	The avatar for this contact.

Additional Information

Skype Activity

Description	Skype Activity contains interactions that occur between users on Skype. These interactions include messages, group interactions, calls, files sent and received, and SMS. This artifact applies to Skype 8.1 and later.
Recovery method	Parsing

Attribute	Description
Conversation ID	The ID of this conversation.
Profile Name	The local user's profile name.
Sender	The username of the sender or initiator of the interaction.
Sender Email	The sender's email as given in the message (if available).
Recipient Name(s)	The recipients or targets of the interaction.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the interaction was initiated.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the interaction was last updated (for example, when a call ends).
Message Type	The type of the interaction.
Message	The content of the message or summary of the interaction.
Emotion Count	The number of reactions to the interaction. Some examples of interactions include likes, dislikes, and emojis.
File Name	The name of any attached files that are associated with the interaction.
File Size (Bytes)	The size in bytes of any attached files.
Attachment	The attachment file (if applicable).
Attachment Data Recovered	Indicates whether the attached file was recovered from the local filesystem.
Thumbnail URL	A URL that directs to the thumbnail picture (if applicable).
Call Duration (Seconds)	The length of the call in seconds (if applicable).

Attribute	Description
Metadata	The content of the message, if it consisted of interpreted data (that is, XML or JSON data, rather than plain text).

Additional Information

Skype Contacts

Description	Skype Contacts contains information about Skype contacts that are recovered, which may or may not be added contacts.
Recovery method	Parsing

Attribute	Description
Profile Name	The profile name of the user.
Skype Name	The Skype name of the contact.
Display Name	The display name of this account.
Is Blocked	Indicates whether a contact blocked.
Contact Added	Specifies whether the contact is an added contact or just cached into the database (1 if the contact was added, 0 otherwise). Contacts can be cached into the database for a variety of reasons (for example, as a 'suggested contact').
Full Name	The full name of this account.
Birthday (yyyy-	The birthday of this account.

Attribute	Description
mm-dd)	
Gender	The gender of this account.
City	The city where this account is located.
State/Province	The state or province where this account is located.
Country	The country where this account is located.
Home Phone	The home phone of this contact.
Office Phone	The office phone of this account.
Mobile Phone	The mobile phone of this account.
PSTN Number	The PSTN number of this contact.
Email(s)	The email of this account.
Homepage	The homepage of this contact.
About Info	The about info of this contact.
Profile Loaded Date/Time - UTC (yyyy-mm-dd)	The date and time when a contact's profile is first created on the user's device. When the profile information is updated by the contact, the date in the database is also updated. This fragment was previously called Profile Created On Date/Time.
Mood Text	The text used to express mood.
Last Online On Date/Time - UTC (yyyy-mm-dd)	The last time the account was online.
Last used On	The last time the account was used.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	The avatar created time.
Image	The image for this contact.

Additional Information

Skype Group Chat

Description	Skype Group Chat contains information about the Skype group chats that a user is a part of.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Chat ID	The group chat's unique identifier.
Participants	The participants of the chat.
Posters	The users that have posted to the chat.

Attribute	Description
Active Members	The currently active users of the group.
Chat name	The name of the chat.
Started Date/Time - UTC (yyyy-mm-dd)	The date and time when the chat started.
Last Changed Date/Time - UTC (yyyy-mm-dd)	The date and time when the chat was modified.
Source	The location where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Telegram Chats - macOS

Description	macOS Telegram Chats contains information about the chats that the suspect participates in using the Telegram application.
Recovery method	Parsing

Attribute	Description
Chat ID	The ID number for the chat.
Title	The title of the chat.
Last Sender	The full name of the user that sent the last message in the chat.
Last Sender Id	The user ID of the user that sent the last message in the chat.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message in the chat.
Last Message	The last message that was sent in the channel chat.
Flags	The status flags associated with the chat.
Number of Participants	The number of people who have actively participated in the chat.
Participant Information	A list of users who have participated in the chat. This data consists of the full name and user ID of each participant.

Additional Information

Telegram Messages - macOS

Description	macOS Telegram Messages contains individual chat messages that are sent and received using the Telegram application.
Recovery method	Parsing

Attribute	Description
Sender Name	The full name of the person who sent the message.
Sender ID	The user ID of the person who sent the message.
Recipient Name	The full name of the person who received the message.
Recipient ID	The user ID of the person who received the message.
Message	The content of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Image	The image that was sent or received.
Message Status	The status of the message (Received or Sent).
Read Status	Indicates whether or not the message has been read when the message was received.
Type	The type of the message that was sent or received. This value can be either a Message or Video Call.
Secret Chat	Indicates whether a message is sent as a secret chat. This field says 'Yes' if the message is a secret chat, and is empty if it isn't a secret chat.
Message ID	The ID number of the message.
Chat ID	The ID number for the chat that the message was sent in.
Flags	The status flags associated with the message.
Attachment Name(s)	The name of the attachments that were sent.

Additional Information

Telegram Users - macOS

Description	macOS Telegram Users contains information about the various users that the suspect has encountered using Telegram, either directly or as part of a channel chat.
Recovery method	Parsing

Attribute	Description
User ID	The ID number for the user.
First Name	The first name of the user.
Last Name	The last name of the user.
User Name	The user name of the user.
Phone Number	The phone number of the user.
Deleted	Indicates whether or not the user's account has been deleted.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The last time that the user was seen by the local user.

Additional Information

Connected Devices

Bluetooth Devices - macOS

Description	Bluetooth Devices contains information about the Bluetooth devices that have been connected to the user's macOS computer.
Recovery method	Parsing

Attribute	Description
Address	The MAC address of the associated Bluetooth Device that's connected to the macOS computer.
Type	The type of Bluetooth device.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The last date and time that the Bluetooth device was connected to the macOS computer.
UUID	The username GUID that's associated with the Bluetooth device.

Additional Information

Find My Devices

Description	A list of the Apple user's device and device info registered within the Find My application.
Recovery method	Parsing

Attribute	Description
Device Name	The name of the device.
Device ID	The device identifier.
Device Model	The internal device model.
Device Type	The device type. E.g. Accessory, Apple Watch, iPad, iPhone, MacBook, etc.
Family Shared	Indicates whether the device is shared using Apple Family Sharing.
Location Address	Last known full street address.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp logged for the last known location.
Pending Remote Wipe	Indicates whether a remote device wipe request was issued for this device.
Remote Wipe Request Timestamp - UTC (yyyy-mm-dd)	The timestamp logged for the remote device wipe request.
Remote Wipe Timestamp - UTC (yyyy-mm-dd)	The timestamp logged when a remote device wipe operation was performed.
Accuracy (meters)	GPS horizontal accuracy (in meters).
Latitude	Latitude of the last known location.
Longitude	Longitude of the last known location.

Additional Information

Find My Items

Description	A list of the Apple user's items registered within the Find My application.
Recovery method	Parsing

Attribute	Description
Device Name	The name of the item tracker.
Serial Number	The unique serial number of the tracker.
Device ID	The product identifier.
Role	The user assigned role for the item being tracked. E.g. Back-back, Keys, Luggage, etc.
Emoji	The user assigned emoji for the item.
Manufacturer	The manufacturer of the device.
Product ID	Product identifier.
Vendor ID	Vendor identifier.
Operating System Version	The firmware version of the tracker item.
Location Address	The last known full street address.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp logged for the last known location.
Accuracy (meters)	GPS horizontal accuracy (in meters).
Latitude	Latitude of the last known location.
Longitude	Longitude of the last known location.

Additional Information

Find My Locations

Description	A list of crowdsourced or safe locations for the Apple user's device/items registered within the Find My application.
Recovery method	Parsing

Attribute	Description
Device ID	The device or product item identifier.
Device Name	The name of the device or item.
Serial Number	The unique serial number.
Location Type	Type of the location for the device/item (crowdsourced or safe location).
Location Address	The last known full street address.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp logged for the last known location.
Accuracy (meters)	GPS horizontal accuracy (in meters).
Latitude	Latitude of the last known location.
Longitude	Longitude of the last known location.

Additional Information

LogMeIn Activity

Description	LogMeIn Activity records connection events that occur using the LogMeIn remote desktop client. These records can include remote sessions and file sharing events.
Recovery method	Parsing

Attribute	Description
Date/Time Local Time	The time in local time when the log line was recorded.
Activity Type	The type of the activity that was recorded. The Session type indicates that the event is a remote session. The SessionDateReport indicates that the recorded event is a session summary. The FileShare type indicates that the recorded event was a file being shared with other users.
Connection Type	The type of connection that was used.
Status	Indicates the status of the file sharing event (only applies to FileShare activities).
Remote IP Address	The public IP address of the client server.
Local IP Address	The public IP address of the host server.
Connection State	The login or logout state of the connection.
OS Version	The OS version of the host.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

USB Connection History

Description	USB Connection History contains a history of the USB devices that have been connected to the macOS computer.
Recovery method	Parsing

Attribute	Description
Connection Start Date/Time - UTC (yyyy-mm-dd)	The date and time when a connection was made to the macOS computer.
Connection End Date/Time - UTC (yyyy-mm-dd)	The date and time when a connection was ended on the macOS computer.
Serial Number	The serial number of the connected USB device.
Vendor ID	The vendor ID of the connected USB device.
Product ID	The product ID of the connected USB device.
Device Release Number	The release number of the connected USB device.
Device Name	The name of the connected USB device.

Additional Information

Your Phone Contacts

Description	Your Phone Contacts contains information about contacts synced from a mobile device to a computer using Your Phone. The Your Phone application can sync data from Android and iOS devices to computers running Windows 10.
Recovery method	Parsing

Attribute	Description
Display Name	The contact's display name.
Nickname	The contact's nickname.
Phone Number	The contact's phone number.
Type	The type of phone number associated with the contact, for example Home, Mobile, or Business.
Last Time Contacted Date/Time - UTC (yyyy-mm-dd)	The last time that this contact either sent a message to, or received a message from the synced device or local user since the Your Phone application was installed.
Number of Times Contacted	The number of times the synced device or local user either sent a message to, or received a message from the contact since the Your Phone application was installed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that this contact's details were modified.

Additional Information

Your Phone Devices

Description	Your Phone Devices contains information about the devices that are synced to the user's computer by using the Your Phone application.
Recovery method	Parsing

Attribute	Description
Application Version	The version of Your Phone running on the computer.
Last Run Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was last run on the computer.
Device Application Version	The version of the Your Phone companion application running on the device.
Device ID	A GUID identifier generated to uniquely identify devices within the Your Phone application.
Device Name	The name provided by the device and displayed in the user interface when referring to it.
Device Platform	The device's platform (Android or iOS).
Device Messages Synced Date	The date and time when the device last synchronized its messages data with Your Phone.
Computer Messages Synced Date	The date and time when the computer last synchronized its messages data with Your Phone.
Device Contacts Synced Date	The date and time when the device last synchronized its contacts data with Your Phone.

Attribute	Description
Computer Contacts Synced Date	The date and time when the computer last synchronized its contacts data with Your Phone.
Device Photos Synced Date	The date and time when the device last synchronized its picture data with Your Phone.
Computer Photos Synced Date	The date and time when the computer last synchronized its picture data with Your Phone.

Additional Information

Your Phone Pictures

Description	Your Phone Pictures contains information about pictures synced from a mobile device to a computer using Your Phone. The Your Phone application syncs the 25 most recently taken photos from Android and iOS devices to computers running Windows 10.
Recovery method	Not applicable

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.

Attribute	Description
Device ID	A GUID identifier generated to uniquely identify devices synced using the Your Phone application.
Device Name	The name of the device (as provided by the device) which is displayed in the user interface for Your Phone.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial

Attribute	Description
	indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
GPS Lon-	The GPS longitude coordinates of where the picture was taken (extracted

Attribute	Description
gitude	from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS Latitude (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicates whether the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.
Exif Data	A searchable field for all raw exif properties.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Your Phone SMS/MMS

Description	Your Phone SMS/MMS contains information about messages synced from a mobile device to a computer using Your Phone. The Your Phone application can sync data from Android and iOS devices to computers running Windows 10.
Recovery method	Parsing and carving

Attribute	Description
Sender	The phone number that sent the message.
Recipient(s)	The phone number(s) the message was sent to.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message content.
Message Direction	Indicates whether the message was sent or received by the synced device or local user.
Message Type	Indicates whether the message is SMS or MMS.
Message Status	Indicates whether the message has been read.
Attachment Name	The name of the attached file, if applicable (MMS only).

Additional Information

Custom

File Signature Mismatch (Audio)

Description	File Signature Mismatch (Audio) contains identified mismatches between a known file signature header and the extension (or lack thereof) for an audio file. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Container)

Description	File Signature Mismatch (Container) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a container. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Document)

Description	File Signature Mismatch (Document) contains identified mismatches

	between a known file signature header and the extension (or lack thereof) for a document. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Picture)

Description	File Signature Mismatch (Picture) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a picture. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.

Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file. If the MIME type is unknown, this defaults to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file. If the MIME type is unknown, this defaults to application/octet-stream. If there is no file extension, but the MIME type is known, a mismatch is is returned.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Video)

Description	File Signature Mismatch (Video) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a video. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

Documents

Apple Notes

Description	Apple Notes contains information about the notes a user has created on their macOS computer.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the note.

Attribute	Description
Folder	The folder that the note is stored in.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was last modified.
Summary	The summary of the note.
Encrypted	Indicates whether or not the note has been encrypted.
Password Hint	The hint to the encryption password.
Body	The body of the note. This fragment may contain the Object Replacement Character (U+FFFC) which indicates a non-text note is presented such as a picture, video, etc. If the non-text note is found, it will be presented as an attachment.
Attachments	A list of attachments contained in the note.
Note ID	The unique identifier of the note.

Additional Information

Apple Notes - Voice

Description	Contains the recovered voice notes from a macOS computer.
Recovery method	Parsing

Attribute	Description
Audio	The saved voice note.
Saved Date/Time - UTC (yyyy-mm-dd)	The date and time that the voice note was saved.
Duration (seconds)	The duration of the voice note in seconds.
Path	The path to the voice note on the device.
Version	The version of the note: Original, Duplicate (duplicate copy of the original), Duplicate - Edited (duplicate copy of the original and partly modified), Edited (edited copy of an original note).
Original Path	The path to the original version of an edited note.
Note ID	The ID of the note.
Label	The label of the note.

Additional Information

CSV Documents

Description	CSV documents (.csv) that are located on the system.
Recovery method	Parsing

Attribute	Description
File Name	The name of the CSV document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last modified.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was created.
File Content	The content of the CSV document.
Size (Bytes)	The size of the CSV document in bytes.
SHA1 Hash	The SHA1 hash of the contents of the document.
MD5 Hash	he MD5 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

Microsoft Excel Documents

Description	Microsoft Excel is a spreadsheet processor developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Size (Bytes)	The size of the document in bytes.
Saved Size (Bytes)	The size of the document (in bytes) that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title metadata.
Subject	The subject metadata.
Authors	The authors of the document.

Attribute	Description
Keywords	The keywords metadata in the document.
Comments	The comments metadata.
Last Author	The last author to edit the document.
Last printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

Microsoft PowerPoint Documents

Description	Micrsoft PowerPoint is a presentation creator developed by Microsoft. This table captures documents created with PowerPoint, extracted from the filesystem and carved from unallocated space.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
File	The actual file.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Comments	The comments in the metadata of the file.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

Microsoft Word Documents

Description	Microsoft Word is a word processor developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.

Attribute	Description
Size (bytes)	The size of the document.
Saved Size (bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title metadata.
Subject	The subject metadata.
Authors	The authors of the document.
Keywords	The keywords metadata in the document.
Comments	The comments metadata.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyy-mm-dd)	The date and time when the document was last printed extracted from metadata within the document.
Last Modified Date/Time - UTC (yyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the

Attribute	Description
	artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information
For information about supported formats, see Supported media and file types.

PDF Documents

Description	Portable Document Format (PDF) is a file format used to present documents in a manner independent of application software, hardware, and operating systems. This table captures documents in this file format, extracted from the filesystem and carved from unallocated space.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.

Attribute	Description
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
File	The PDF file.
MD5 Hash	An MD5 hash of the PDF content.
SHA1 Hash	A SHA1 hash of the PDF content.

Additional Information

For information about supported formats, see Supported media and file types.

RTF Documents

Description	The information for each RTF document that was recovered from the search.

Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the RTF document.
File Size (Bytes)	The size of the RTF document in bytes.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was last modified.
File Content	The contents of the RTF document.
MD5 Hash	A MD5 hash of the RTF content.
SHA1 Hash	A SHA1 hash of the RTF content.

Additional Information

For information about supported formats, see Supported media and file types.

Text Documents

Description	Text documents (.txt) that are located on the system.
Recovery method	Parsing

Attribute	Description
Filename	The name of the text document.
Size (Bytes)	The size of the text document in bytes.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was created.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.
File Content	The content of the text document.

Additional Information
For information about supported formats, see Supported media and file types.

Email and Calendar

Calendar Events (ICS)

Description	Calendar Events (ICS) contains information about events and appointments that are recovered from calendar .ics files. These files are used by many different email applications, including Outlook, Google Calendar, and Apple Calendar.

Recovery method	Parsing

Attribute	Description
ID	A unique ID for the calendar entry.
Type	The type of event, such as Event, TODO, or Journal.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was created.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the event starts.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the event ends.
Summary	A short summary of the event.
Description	A more complete description of the event.
Latitude	The latitude coordinates of the event's venue.
Longitude	The longitude coordinates of the event's venue.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time in which the event was last modified.
Location Name	The name of the venue in which the event is held.

Attribute	Description
Organizer	The organizer of the calendar event.
Status	The current pending status of the event (for example, NEEDS-ACTION, ACCEPTED, DECLINED, TENTATIVEB, DELEGATED, COMPLETED, IN-PROGRESS).
URL	The URL that is associated with the event.
Recurrence	Indicates whether the event is recurring.
Attendees	A list of attendees for the event.
Categories	The tags that are associated with the event.
Comment	A comment the organizer writes for to the user.
Contact Label	A reference of contacts associated with the event.
Resources	A list of resources and equipment required for the event.
Timezone	The timezone in which the event is held.

Additional Information

EML(X) Files

Description	EML(X) Files contains the emails in .eml and .emlx formats, that have been found on the device.
Recovery method	Parsing and carving

Attribute	Description
To	The recipients of the email.
From	The sender of the email.
Date/Time	The date and time that the email was sent or received.
Subject	The subject of the email.
Body	The body of the email.
CC	The recipients that receive the email by CC.
BCC	The recipients that receive the email by BCC.
Headers	The raw email headers.
Importance	The email importance setting.
Last Read Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was last read, if the data is available.
Attachment Name(s)	A list of attachments on the email.

Additional Information

Outlook Emails

Description	Microsoft Outlook is a personal information manager and email client. Outlook Messages captures information related to emails sent and received in Microsoft Outlook.
Recovery method	Parsing

Attribute	Description
Sender Name	The sender of the email.
Sender Email	The email address of the sender.
Recipients	The recipients of the email.
Subject	The subject of the email.
Sender Exchange Account	The sender's Exchange account name.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was created.
Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the email synced with the HxStore platform.
Submitted Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was submitted.
Delivered Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was delivered.
Last Modified	The date and time that the email was last modified.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Body	The body of the email. For HxStore data sources that include email bodies deleted when an account was removed, the displayed value is the path where the email body was located on the file system.
Folder Name	The name of the folder where the email is stored.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Attachments	The list of attachments on the email.
Headers	The raw email headers.
Priority	The priority of the email.
Importance	The importance of the email.
Sensitivity	The sensitivity of the email.
Read	Indicates whether the email was opened and therefore marked as Read. Note that Outlook users can also manually mark emails as either Read or Unread.
MD5 Hash	The MD5 hash of the email.
SHA1 Hash	The SHA1 hash of the email.

Additional Information

Encryption and Credentials

Apple Keychain Generic Passwords

Description	Apple Keychain Generic Passwords contains passwords for applications and services that are saved to the Keychain application. Analyzing results from this artifact can reveal valuable passwords and tokens that are associated with the user's accounts.
Recovery method	Parsing

Attribute	Description
Keychain Property	The keychain property of the keychain item.
Value	The secret value that's associated with the account. The values that have non-printable characters are converted to hex strings. To see what the raw data looks like before conversion, export the hit with attachments.
Service Name	The name of the service that has stored data in the keychain.
Account	The account identifier of the keychain item parsed from the 'Keychain Property'.
Password/Token	The password or token of the keychain item parsed from the 'Value'.
Access Group	The access group that the keychain item belongs to.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was created.

Attribute	Description
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was last modified.
Original Location	The offset of the keychain item in the keychain database.

Additional Information

Apple Keychain Internet Passwords

Description	Apple Keychain Internet Passwords contains passwords for websites and internet services that are saved to the Keychain applications. Analyzing results from this artifact can reveal valuable passwords and tokens that are associated with the user's accounts.
Recovery method	Parsing

Attribute	Description
Label	The label of the keychain item.
Description	The description of the keychain item.
Account	The account identifier of the keychain item.
Value	The secret value that's associated with the account. Values that have non-printable characters are converted to hex strings. To see what the raw data looks like before conversion, export the hit with attachments.

Attribute	Description
Access Group	The access group that the keychain item belongs to.
DSID	The Destination Signaling Identifier is a unique identifier assigned to a user when they register an iCloud account.
Server	The server address for an internet password item.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was last modified.
Original Location	The offset of the keychain item in the keychain database.

Additional Information

Location and Travel

Google Maps

Description	Google Maps is a free web service that allows users to get directions.
Recovery method	Carving

Attribute	Description
Search Query	The term that was searched for.
Starting Location	The starting location for navigation or directions.
Center of Map	Indicates where the map was centered.
Business Latitude and Longitude	The latitude and longitude of the business location.
Source Address	The source physical address.
Destination Address	The user's desired destination.
Route Type	Indicates how the user will travel (e.g. car, bus, bike).
Additional Address	Any additional addresses within the navigation.
Street View Latitude/Longitude	The latitude and longitude information in street view.

Additional Information

Google Maps Tiles

Description	Google maps is a free web service that allows users to get directions.
Recovery method	Parsing and carving

Attribute	Description
Image	The actual picture content.
X Coordinate	The X coordinate value that Google uses to download the right tile.

Attribute	Description
Y Coordinate	The Y coordinate value that Google uses to download the right tile.
Zoom Level	The level that the user was zoomed in to the map. This value can be understood as the Z coordinate value that Google uses to download the right tile.

Additional Information

Media

AMR Files

Description	AMR Files contains voicemail messages or memos for both iOS and Android.
Recovery method	Carving

Attribute	Description
File Name	The name of the file the AMR was recovered from.
Size (Bytes)	The size of the AMR content.
MD5 Hash	An MD5 hash of the AMR content.
SHA1 Hash	A SHA1 hash of the AMR content.
Audio	The contents of an AMR file.
Media Duration (Seconds)	The duration of the audio clip in seconds.

Additional Information

For information about supported formats, see Supported media and file types. Media duration is calculated from the number of speech frames carved from the AMR data, where each speech frame has a duration of 20ms, as AMR files do not contain metadata for duration.

Audio

Description	Audio contains Audio files that are recovered that use the .mp3 or .wav formats.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file.
File Extension	The extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was created.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was last accessed.
Last Modified Date/Time -	The date and time when the audio file was last modified.

Attribute	Description
UTC (yyyy-mm-dd)	
File Size (Bytes)	The size of the audio file.
MD5 Hash	An MD5 hash of the audio content.
SHA1 Hash	A SHA1 hash of the audio content.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the audio clip in seconds (extracted from Exif data).
Exif Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio clip was first recorded (extracted from Exif data).
Exif Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio clip was edited (extracted from Exif data).
Timezone	The timezone setting on the recorder at the time when the audio clip was recorded (extracted from Exif data).

Attribute	Description
Software	The software used to record or modify the audio clip. This could either be the OS version of the phone used to record the audio clip or the name of the software used to edit the audio clip in post-production (extracted from Exif data).
Latitude	The GPS latitude coordinates of where the audio clip was recorded (extracted from Exif data).
Longitude	The GPS longitude coordinates of where the audio clip was recorded (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of where the audio clip was recorded (extracted from Exif data).
Exif Data	A searchable field for all raw Exif properties.

Additional Information

For information about supported formats, see Supported media and file types.
To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Carved Video

Description	Carved Video contains videos that are recovered using carving. Supported formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. Other container formats can also be recovered provided that their underlying packets are the same as one of the supported formats.
Recovery method	Parsing

Attribute	Description
Content Format	The format of the video.
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
File Size (Bytes)	The size of the container and file.
Container Format	The format of the video container.
Saved Video Size (Bytes)	The size of the video that was saved to the database.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Additional Information

As of February 20 2020, this artifact will no longer be included under Videos. Carved Video functionality will be included in the 'Videos' artifact instead.

Live Photos

Description	Live Photos contains live photos that were retrieved using parsing.
Recovery method	Parsing

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
UUID	The ID of the picture and video. If the UUID is different for picture and a video, it is not associated with each other.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original	The original height of the picture, before any applied resizing.

Attribute	Description
Height	
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).

Attribute	Description
Latitude	The latitude coordinate in decimal degrees.
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS latitude (extracted from Exif data).
Longitude	The longitude coordinate in decimal degrees.
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the pciture was taken (extracted from Exif data).
Exif Data	A searchable field for all raw exif properties.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expec-

Additional Information
ted. To learn more, see Understanding sorting and filtering for artifacts with local timestamps. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Photos Albums

Description	Photos Albums contains information about the albums that contain pictures and media in the Photos application on macOS.
Recovery method	Parsing

Attribute	Description
Album Title	The title of the album.
Created Date/Time	The date and time when the album was created on the local device.
Photo Count	The number of photos in the album.
Video Count	The number of videos in the album.
UUID	The UUID of the album.
Owner Name	The full name of the owner. This is only available when the album is a shared album.
Shared	Indicates whether the album is a shared album. Yes is displayed when the album is shared.
Invitees	The full names of those invited to view the shared album.

Additional Information

To learn more about examining Photos Albums artifacts, see Find pictures or videos related to an iOS Photos Albums artifact.

Photos Media Information

Description	Photos Media Information contains metadata about pictures and media stored in the Photos application on macOS.
Recovery method	Parsing

Attribute	Description
File Name	The name of the media file.
Type	The type of media. The value can be Picture or Video.
Album Title	The title of the media file's album.
Created Date/Time	The date and time when the media was created on the local device.
Hidden	Indicates whether a photo has been hidden.
Favorited	Indicates whether a photo has been favorited.
Deleted	Indicates whether a file has been recently deleted. Recently deleted files remain accessible for 30 days.
Bundle ID	The bundle identifier where the file is imported from.
Display Name	The display name of the bundle where the file is imported from.

Attribute	Description
Directory	The directory that the media file resides in.
UUID	The UUID of the media.
Latitude	The latitude of the location where the media was taken.
Longitude	The longitude of the location where the media was taken.
Modified Date/Time	The date and time when the media was modified on the local device.
Deleted Date/Time	The date and time when the media was deleted from the local device.
Media	The picture related to this photo media information.

Additional Information

Pictures

Description	Pictures retrieved using either carving or parsing techniques. The supported formats are as follows: JPEG (.jpeg, .jpg, .jpe), PNG (.png), Bitmaps (.bmp), Graphics Interchange Format (.gif), Icons (.ico), and Tagged Image File Format (.tif, .tiff).
Recovery method	Parsing and carving

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction	The Exif extraction status indicates the level of Exif extraction that was per-

Attribute	Description
Status	formed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone that was used to take the picture, or name of the software that was used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial	The serial number of the lens (extracted from Exif data).

Attribute	Description
Number	
Latitude	The latitude coordinate in decimal degrees.
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS latitude (extracted from Exif data).
Longitude	The longitude coordinate in decimal degrees.
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the picture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicating if the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.
Exif Data	A searchable field for all raw exif properties.

Additional Information

For information about supported formats, see Supported media and file types.
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.
To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Quick Look Thumbnails

Description	Quick Look Thumbnails contains thumbnail previews that the macOS device creates and displays for items in the file system.
Recovery method	Parsing

Attribute	Description
Attachment	The picture used as the thumbnail.
Folder	The folder from which the thumbnail was generated.
File Name	The name of the file that the thumbnail was created for.
Filesystem ID	The unique ID provided to the file. This value can be used to verify file system attributes for the file.
Target File Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified timestamp of the file, from the file system. Once this value no longer matches the timestamp on the file, macOS generates a new thumbnail.
Thumbnail Size (bytes)	The thumbnail size in bytes. Negative values are ommitted until further investigation.

Attribute	Description
Thumbnail Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the thumbnail was last accessed by the user.
Thumbnail Access Count	The number of times that the thumbnail has been accessed.

Additional Information

Quicktime Player History

Description	Quicktime Player History provides information about the files that a user has viewed using the player. Quicktime is the default video player for macOS computers.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file played with Quicktime.
File Path	The full path to the file played with Quicktime.
Drive Name	The name of the drive where the played file was located.
Volume UUID	The UUID of volume where the played file was located.

Additional Information

Videos

Description	Videos contains videos that are recovered using parsing or carving. Supported formats for parsing include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. Supported carving formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. For more information about supported video formats, see Supported media and file types.
Recovery method	Parsing and carving

Attribute	Description
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
File Name	The name of the file.
File Extension	The extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the video was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the video was last accessed.
Last Modified Date/Time - UTC (yyyy-	The date and time that the video was last modified.

Attribute	Description
mm-dd)	
File Size (Bytes)	The size of the video.
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed, including potential metadata located at the end of the video. Partial indicates that only Exif information in the header section of the video file was recovered, which should only occur with very large videos (in excess of the limit set in the options screen). Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The resolution of the video (extracted from Exif data).
Original Height	The resolution of the video (extracted from Exif data).
Exif Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was first recorded (extracted from Exif data).
Exif Modified Date/Time -	The date and time when the video was edited (extracted from Exif data).

Attribute	Description
UTC (yyyy-mm-dd)	
Timezone	The timezone setting on the camera at the time of the video being recored (extracted from Exif data).
Software	The software used to record or modify the video. This could either be the OS version of the phone used to record the video or name of the software used to edit the video in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to record the video (extracted from Exif data).
Model	The model of the camera used to record the video (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to record the video (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS latitude coordinates of the camera where the video was recorded (extracted from Exif data).
Longitude	The GPS longitude coordinates of the camera where the video was recorded (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the video was recorded (extracted from Exif data).
MD5 Hash	An MD5 hash of the video content.

Attribute	Description
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.
Content Format	The format of the carved video.
Container Format	The format of the carved video container.
Saved Video Size (Bytes)	The size of the carved video that was saved to the database.
Exif Data	A searchable field for all raw exif properties.

Additional Information

If AXIOM Process is configured to save a set amount of data from carved videos, any generated MD5 and SHA1 hashes are based on the saved data, not the full video. This behavior might cause issues when searching for known video hashes, as the hash for a carved video will differ from the actual video if it exceeds the size limit set in AXIOM Process.

Supported formats include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. For information about supported formats, see Supported media and file types.

To learn more about Exif data for videos, see Extracting Exif data from videos.

To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

VLC Recently Played Files

Description	VLC Recently Played Files contains information about the media files that

	are played using the VLC Media Player. This artifact can reveal information on the user's interaction with the application.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file that was played in the player.
File Path	The file path to the recently played file.
Resume Time (seconds)	The number of seconds played before the media file is paused or stopped. If the duration is less than 5% or more than 95% of the total runtime, this value is set to 0.

Additional Information

Web Video Fragments

Description	This search recovers two distinct types of web-based videos. Fragments of Flash video can be left behind by many video streaming sites, such as YouTube. RTMP Frame Fragments are frames left behind by streaming sites using the RTMP protocol (widely used by webcam chat sites, including Chatroulette and Camstumble). In the case, a thumbnail from a recovered video is displayed, as well as any relevant metadata. Videos can be exported to .FLV format to be played. Due to the nature of the data recovered, some video players will have issues playing the exported files. We recommend trying FFmpeg, VLC, and the GOM player.
Recovery method	Carving

Attribute	Description
Preview	A thumbnail preview of the video.
Content Recovered	The raw bytes that were recovered.
Metadata	Any metadata about the video.
Recovered Duration	The length of the video that was recovered.

Additional Information

Operating System

.DS_Store Records

Description	.DS_Store Records contains all the records extracted from .DS_Store files found on the computer. Each record represents a property of a file or a folder. The significance of this artifact is an indicator of high likelihood that the user of the computer was aware of these files and folders with a possibility of attributing a date to that awareness.
Recovery method	Parsing

Attribute	Description
Record Name	The name of the file or folder as stored in the .DS_Store file.
Record Type	The type of the record, or property, that is being logged in the .DS_Store file for a particular file or folder.

Attribute	Description
Record Value	The value of the property for the given file or folder.
Record Path	The full path to the file or folder.
.DS_Store Created Date/Time - UTC (yyyy-mm-dd)	The created date of the .DS_Store file from which the record was extracted.
.DS_Store Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date of the .DS_Store file from which the record was extracted.
.DS_Store Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date of the .DS_Store file from which the record was extracted.

Additional Information

In the Apple macOS operating system, .DS_Store (Desktop Services Store) is a hidden file that stores the display information of its containing folder, similar to the file desktop.ini in Microsoft Windows. The file tracks information such as icon positions, view settings, cached file size, cached last modified date, and even the choice of a background image. The .DS_ Store is created and maintained by the Finder application in any folder that it accesses, even on remote file systems mounted from servers that share files (for example, via Server Message Block (SMB) protocol or the Apple Filing Protocol (AFP)). .DS_Store files are also included in archives created by macOS users, such as ZIP files, and they are backed up by some cloud file backup services. This means that the presence of .DS_Store Records artifacts on non-Mac evidence such as Windows, Mobile, or Cloud indicates that some of the data may have originated or have been accessed from a macOS computer at some point. For more information on .DS_Store files and their forensic significance see: .DS_Stores: Like Shellbags but for Macs.

AirDrop Available Recipients

Description	AirDrop Available Recipients lists all available recipients for an AirDrop transfer outgoing from the local device. The devices need to be in Bluetooth and WiFi range to connect to each other. You can recover up to one week of AirDrop activity history as it is stored in the Apple Unified Logs.
Recovery method	Parsing

Attribute	Description
Name	The name of the user or the user's device.
User ID	The ID of the user as tracked by the AirDrop service.
Contact Added	Indicates whether the user is a contact on the local user's device.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the log entry.
Transaction Log	The log message extracted from Unified Logs.

Additional Information

Available users are only recorded in the Apple Unified Logs when the local user opens the AirDrop view in Finder or tries to send a file using the AirDrop sharing option. There is a record for each time a person "bubble" appears in the respective interface. This artifact can help place other devices in proximity of the device being investigated.

AirDrop Background Activity

Description	Airdrop Background Activity is a collection of logs that capture background events triggered by the Airdrop service.
Recovery method	Parsing

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	The date and time of the log entry.
Transaction Log	The log message extracted from Unified Logs.

Additional Information

This artifact does not capture every single background event that is described in the log. This artifact extracts what look to be the most relevant pieces of data, but it's up to the examiner to determine their forensic significance. If there are logs that are not included in this artifact that should be, please reach out to Magnet Technical Support.

AirDrop Discoverability

Description	AirDrop Discoverability lists changes to the discoverability status of device.
Recovery method	Parsing

Attribute	Description
Mode Change Date/Time - UTC (yyyy-mm-dd)	The date and time of the log entry.
Mode	Mode is an indication of who can share files with the local machine (values include Off, Contacts Only, or Everyone).
Transaction Log	The log message extracted from Unified Logs.

Additional Information
While this artifact reflects changes that the user initiates a change to their discoverability, it does also capture system changes. The AirDrop service periodically resets which causes the status to toggle between the current status and off, typically within one second of each other. These changes are background system activities that are not representative of an action by the user.

AirDrop Incoming Transfers

Description	AirDrop Incoming Transfers lists information about AirDrop transfers incoming to the local device. The devices need to be in Bluetooth and WiFi range to connect to each other. You can recover up to one week of AirDrop activity history as it is stored in the Apple Unified Logs.
Recovery method	Parsing

Attribute	Description
Item Type	Typically these values are displayed as MIME types. However, if Apple doesn't have a friendly name reserved for a particular file type, you might

Attribute	Description
	see values like dyn.ah62d4rv4ge80nqbv.
Number of Items	The number of items of that type included in the transfer.
Is File	Indicates whether the items being transferred are files or not (e.g. folder, link, etc.).
Sender Name	The name of the sender.
Sender Device	The name of the sender's device.
Destination Folder	The location chosen by the user to save the incoming transfer to.
Status	Indicates whether the transfer is accepted, declined, or incomplete. Incomplete could mean either the transaction timed out, or the sender cancelled the transaction on their end.
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date of the first log entry associated with the transfer.
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date of the last log entry associated with the transfer.
Sender is Me	Indicates whether the sender is logged in under the same account as the recipient.
Auto Accepted	Indicates if the transfer was auto-accepted.

Attribute	Description
Sender ID	The ID of the sender as tracked by the AirDrop service.
Verifiable Identity	Indicates whether the identity of the user is verifiable. This is an internal flag and it's up to the examiner to determine its forensic significance.
Partial Recovery	Identifies whether the transfer transaction log was incomplete. Yes indicates that some of the transaction log lines were missing before the end of the log file was encountered, so some fragment lines were left empty because they could not be properly recovered.
Transaction ID	An identifier for a given transaction. If multiple files are selected and transferred together, they're listed as separate hits but will have the same transaction ID.
Transaction Log	A raw dump of the logs between the first and last log relating to the transaction.

Additional Information

Incoming transfers are records pertaining to the files received on the local machine. A single transaction with multiple files will get split into multiple hits in AXIOM Examine and can be grouped by sorting on Transaction ID.

AirDrop Outgoing Transfers

Description	AirDrop Outgoing Transfers lists information about AirDrop transfers outgoing from the local device. The devices need to be in Bluetooth and WiFi range to connect to each other. You can recover up to one week of AirDrop activity history as it is stored in the Apple Unified Logs.
Recovery method	Parsing

Attribute	Description
Item Name	The file or folder name.
Item Type	Typically, these values are displayed as MIME types. However, if Apple doesn't have a friendly name reserved for a particular file type, you might see values like dyn.ah62d4rv4ge80nqbv.
Is File	Indicates whether the items being transferred are files or not (e.g. folder, link, etc.).
Recipient Name	The name of the recipient.
Recipient Device	The name of the recipient's device.
Status	Indicates whether the transfer is accepted, declined, or incomplete. A Declined or Incomplete status could indicate that the transfer was cancelled, declined, or that the transfer timed out transfer.
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date of the first log entry associated with the transfer.
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date of the last log entry associated with the transfer.
Recipient ID	The ID of the recipient as tracked by the AirDrop service.
Verifiable Identity	Indicates whether the identity of the user is verifiable, this is an internal flag and its up to the examiner to determine its forensic significance.

Attribute	Description
Partial Recovery	Identifies whether the transfer transaction log was incomplete. Yes indicates that some of the transaction log lines were missing before the end of the log file was encountered, so some fragment lines were left empty because they could not be properly recovered.
Transaction ID	An identifier for a given transaction. If multiple files are selected and transferred together, they're listed as separate hits but will have the same transaction ID.
Transaction Log	A raw dump of the logs between the first and last log relating to the transaction.

Additional Information
Outgoing transfers are records pertaining to the files sent by the local machine. A single transaction with multiple files will get split into multiple hits in AXIOM Examine and can be grouped by sorting on Transaction ID.

Anacron Jobs

Description	Anacron jobs are used to execute tasks at a certain frequency on machines that may be powered off.
Recovery method	Parsing

Attribute	Description
Username	The username associated with the task.

Attribute	Description
Frequency	A description of how often the task is triggered.
Identifier	A specific job ID that is used when logging messages for the task.
Command	The command that will be performed when the task is triggered.
Command Shell	The path to the shell file that is used when the task is triggered.
Paths	An environment variable that specifies the paths of the directories used when the task is triggered.

Additional Information

Apple Accounts

Description	Apple Accounts contains information about the Apple ID accounts used on the macOS computer. The account details contained can help investigators recover and correlate account information across applications, and provide information on what accounts to review and get more information from.
Recovery method	Parsing

Attribute	Description
Local Account	The local user's account name, this attribute is only available for macOS computers.
User Name	The email address or username used to log into the account.

Attribute	Description
Account ID	The UID used to identify accounts and files tied to a specific account.
Account Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the account was added to the database.
Parent Account ID	The UID used to match the account to its parent account if it has one.
Account Description	A description of the account, as provided by the user.
Account Type	The type of user account.
Account Credential Type	The type of credentials used by the account. The account credential type can help to indicate which methods might be of use for recovering the credentials (and possibly aiding with a cloud acquisition of the account).
Owning Bundle ID	The unique bundle ID of the application that the account was setup with.
Last Credential Expiry Date/Time - UTC (yyyy-mm-dd)	The date and time of when the credentials had to be re-entered for the account due to a password change or expiry of the token or credentials.

Additional Information

Apple Contacts - macOS

Description	Apple Contacts contains information about the contacts that a user has

	saved to their device.
Notes	

Attribute	Description
First Name	The first name of the contact.
Last Name	The last name of the contact.
Picture	The profile picture of the contact, in its full size.
Home Phone	The home phone numbers associated with the contact.
Mobile Phone	The mobile phone numbers associated with the contact.
Office Phone	The office phone numbers associated with the contact.
Phone Number(s)	Any additional phone numbers associated with the contact.
Home Email	The home email addresses associated with the contact.
Office Email	The office email addresses associated with the contact.
Email(s)	Any additional email addresses associated with the contact.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact's information was created.
Address	The physical addresses associated with the contact.
Website	The websites associated with the contact.
Middle Name	The middle name of the contact.

Attribute	Description
Source Account	The linked account that the contact was imported from.
Organization	The organization or business associated with the contact.
Company	Indicates whether or not the contact is a company.
Department	The department associated with the contact.
Note	Notes associated with the contact.
Birthday (yyyy-mm-dd)	The birthday of the contact.
Job Title	The job title associated with the contact.
Nickname	The nickname associated with the contact.
Prefix	Any prefix applied to the contact's name (such as Mr., Mrs., or Dr.).
Suffix	Any suffix applied to the contact's name (such as PH.D, Ed.D, LLD).
User Accounts	A comma separated list all the social media accounts associated with this contact.
First Name Phonetic	The phonetic spelling of the contact's first name.
Middle Name Phonetic	The phonetic spelling of the contact's middle name.
Last Name Phonetic	The phonetic spelling of the contact's last name.
Previous Last Name	The previous last name of the contact.
Relationship	Relationships that the contact shares with others (e.g. Mother, Father, or Spouse).
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact's information was last modified.

Apple Contacts Groups

Description	Apple Contacts Groups contains information about the groups that the user creates to organize their contacts.
Notes	

Attribute	Description
Name	The name of the contact group.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the group's information was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the group's information was last modified.
Group Member(s)	The contacts that have been added to the group.
Source Account	The linked account that the contact group was imported from.

Apple Keychain Generic Passwords

Description	Apple Keychain Generic Passwords contains passwords for applications and services that are saved to the Keychain application. Analyzing results from this artifact can reveal valuable passwords and tokens that are associated with the user's accounts.
Notes	

Attribute	Description
Service Name	The name of the service that has stored data in the keychain.
Value	The secret value that's associated with the account. The values that have non-printable characters are converted to hex strings. To see what the raw data looks like before conversion, export the hit with attachments.
Account	The account identifier of the keychain item.
Access Group	The access group that the keychain item belongs to.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was last modified.
Original Location	The offset of the keychain item in the keychain database.

Apple Keychain Internet Passwords

Description	Apple Keychain Internet Passwords contains passwords for websites and internet services that are saved to the Keychain applications. Analyzing results from this artifact can reveal valuable passwords and tokens that are associated with the user's accounts.
Notes	

Attribute	Description
Label	The label of the keychain item.
Description	The description of the keychain item.
Account	The account identifier of the keychain item.
Value	The secret value that's associated with the account. Values that have non-printable characters are converted to hex strings. To see what the raw data looks like before conversion, export the hit with attachments.
Access Group	The access group that the keychain item belongs to.
DSID	The Destination Signaling Identifier is a unique identifier assigned to a user when they register an iCloud account.
Server	The server address for an internet password item.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the keychain item was last modified.
Original Location	The offset of the keychain item in the keychain database.

Apple Notes

Description	Apple Notes contains information about the notes a user has created on

	their macOS computer.
Notes	

Attribute	Description
Title	The title of the note.
Folder	The folder that the note is stored in.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was last modified.
Summary	The summary of the note.
Encrypted	Indicates whether or not the note has been encrypted.
Password Hint	The hint to the encryption password.
Body	The note body.
Attachments	A list of attachments contained in the note.
Note ID	The unique identifier of the note.

Apple Notes - Voice

Description	Contains the recovered voice notes from a macOS computer.
Notes	

Attribute	Description
Audio	The saved voice note.
Saved Date/Time - UTC (yyyy-mm-dd)	The date and time that the voice note was saved.
Duration (seconds)	The duration of the voice note in seconds.
Path	The path to the voice note on the device.
Version	The version of the note: Original, Duplicate (duplicate copy of the original), Duplicate - Edited (duplicate copy of the original and partly modified), Edited (edited copy of an original note).
Original Path	The path to the original version of an edited note.
Note ID	The ID of the note.
Label	The label of the note.

Application Permissions - MacOS, iOS

Description	Application Permissions contains information about the app permissions that a user is prompted to accept or decline while using macOS applications.
Notes	

Attribute	Description
Application	The application that requests the permission.
Service Name	The permission service name.
Allowed	Indicates whether the application is allowed to use the service/permission.
Prompt Count	The number of times the user was prompted to give the permission to the application.

Bash / ZSH Sessions

Description	Bash / ZSH Sessions contains information about terminal/Bash/ZSH sessions on a macOS computer, and the commands that are run during each session.
Recovery method	Parsing

Attribute	Description
Session ID	The ID of the session.
User	The user that started the session.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the session started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the session ended.
Session Command History	The command history of the session.

Additional Information

Bluetooth Devices - macOS

Description	Bluetooth Devices contains information about the Bluetooth devices that have been connected to the user's macOS computer.
Notes	

Attribute	Description
Address	The MAC address of the associated Bluetooth Device that's connected to the macOS computer.
Type	The type of Bluetooth device.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The last date and time that the Bluetooth device was connected to the macOS computer.
UUID	The username GUID that's associated with the Bluetooth device.

CoreAnalytics

Description	CoreAnalytics contains information about macOS system usage and application execution history. This artifact gives an overview of applications and processes used during historical and current activity periods.
Recovery method	Parsing

Attribute	Description
Process Name	The name of the application that ran during the diagnostic period.

Attribute	Description
Bundle ID	The unique bundle identifier for the application.
Application Version	The build and release versions for the application. This value is formatted as: Build Version (Release Version).
Ran in Foreground	Indicates whether the application had run in the foreground.
Number of Activations	The number of times that the application was brought to the foreground.
Uptime (seconds)	The total time that the application was awake including running in the background and foreground.
Active Time (seconds)	The number of seconds that the application was run in the foreground.
Number of Launches	The number of times that the application was launched during the diagnostic reporting period. The value of launches will remain at zero if the application was launched prior to the beginning of the diagnostic period.
Diagnostic Period Began	The date and time that the diagnostic log was started.
Diagnostic Period Ended	The date and time that the diagnostic log ended or will end.

Additional Information

Cron Jobs

Description	Cron jobs are used to execute tasks at a certain frequency on continuously running machines.
Recovery method	Parsing

Attribute	Description
Username	The username associated with the task.
Frequency	A description of how often the task is triggered.
Cron Frequency	The cron expression used to specify the task's frequency.
Command	The command that will be performed when the task is triggered.
Command Shell	The path to the shell file that is used when the task is triggered.
Paths	An environment variable that specifies the paths of the directories used when the task is triggered.

Additional Information

CUPS Print Jobs

Description	CUPS Print Jobs contains records of print jobs that were created by the Common Unix Printing System (CUPS).

Recovery method	Parsing

Attribute	Description
Job ID	The ID of the print job.
Job Name	The name of the print job.
Job UUID	The UUID of the print job.
Owner	The owner of the print job.
Application	The application that triggered the print job.
Cached File Name	The name of the cached file to print.
Document Format	The format of the document for the print job.
Copies	The number of copes that the user selected for printing.
Sheets Printed	The actual number of sheets that were printed.
Origin Host Name	The origin host name of the print job request.
Destination Printer	The printer used for the print job.
Printer URI	The URI of the printer used for the print job.
State	The state of the print job.
Printer State Message	The printer state message.
Printer State Reason	The printer state reason.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the print job was created.

Attribute	Description
Processed Date/Time - UTC (yyyy-mm-dd)	The date and time when the print job was processed.
Completion Date/Time - UTC (yyyy-mm-dd)	The date and time when the print job was completed.
Attachment	The cached document that was sent for printing, if it's available.

Additional Information

Daily Logs - Disk Status

Description	Daily Logs Disk Status contains information about daily disk status logs on a macOS computer.
Recovery method	Parsing

Attribute	Description
Log Date/Time - Local Time	The local date and time that the log was created.
Disk Device	The disk device that the log was created for.
Disk Size	The full size of the disk.
Disk Space Used	The amount of disk space that's used.
Disk Space Available	The amount of disk space that's still available.
Mount Point	The path the mounted disk.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Daily Logs - Local System Status

Description	Daily Logs Local System Status contains information about daily system status logs on a macOS computer.
Recovery method	Parsing

Attribute	Description
Log Date/Time - Local Time	The local date and time that the log was created.
System Up Time	The system up time at the time the log was created.
Number of Logged In Users	The number of logged in users.
Load Average (1 min)	The load average value over the last 1 minute.
Load Average (5 min)	The load average value over the last 5 minutes.
Load Average (15 min)	The load average value over the last 15 minutes.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Daily Logs - Network Interfaces Status

Description	Daily Logs Network Interfaces Status contains information about daily network interfaces status logs on a macOS computer.
Recovery method	Parsing

Attribute	Description
Log Date/Time - Local Time	The local date and time that the log was created.
BSD Name	The BSD name assigned to the network adapter.
MTU	The Maximum Transmission Unit value.
Network	The network interface type.
Address	The address of the network interface.
Incoming Packets	The number of packets received on this network interface.
Outgoing Packets	The number of packets sent on this network interface.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Deleted Accounts

Description	Deleted Accounts contains information about the accounts that have been deleted from the macOS computer.

Recovery method	Parsing

Attribute	Description
User Name	The account username.
Full Name	The full display name of the user.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time when the account was deleted.
UUID	The unique identifier for the user.
Home Directory	The user's home directory when still available.

Additional Information

Dock Items

Description	Dock Items contains information about the applications that have appeared in the dock. Usually, these items are recently or often used applications.
Recovery method	Parsing

Attribute	Description
Application Name	The name of the application.
Package Name	The package name of the application.

Attribute	Description
State	The positioning of the application in the dock (Persistent App, Recent App or Persistent Others).
User Name	The username of the account from where the dock items were parsed.
Folder Path	The folder path of the application.
GUID	The GUID of the application.

Additional Information

File Signature Mismatch (Audio)

Description	File Signature Mismatch (Audio) contains identified mismatches between a known file signature header and the extension (or lack thereof) for an audio file. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Exten-	The identified MIME type of the extension of the file, if we don't know what

Attribute	Description
sion Type	the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Container)

Description	File Signature Mismatch (Container) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a container. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

Attribute	Description
File Name	The file name of the identified mismatch.
File Exten-sion	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Exten-sion Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Document)

Description	File Signature Mismatch (Document) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a document. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Picture)

Description	File Signature Mismatch (Picture) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a picture. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file. If the MIME type is unknown, this defaults to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file. If the MIME type is unknown, this defaults to application/octet-stream. If there is no file extension, but the MIME type is known, a mismatch is is returned.
File Path	The path to the mismatched file.

File Signature Mismatch (Video)

Description	File Signature Mismatch (Video) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a video. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.

Attribute	Description
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

File System Events

Description	File System Events contains information about the changes to file system objects, occurring in volumes mounted on a macOS computer. This artifact contains all system event files recovered from the .fseventsd folder.
Recovery method	Parsing

Attribute	Description
File Name	The name of the system object affected by the event.
File Path	The full path to the system object affected by the event.
Flags	Flags that indicate the type of system object and the changes that occured to the object.
Event ID	An Event ID for the record.
File ID	A system ID for the file system object that was affected by the event.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the event file is initially created. This file is recovered from the .fseventsd directory and can contain records for many different events, so this timestamp may not coincide with when the event actually occurred.

Attribute	Description
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the event file was last updated. This file is recovered from the .fseventsd directory and can contain records for many different events, so this timestamp may not coincide with when the event actually occurred.

Additional Information

File System Information (APFS)

Description	File System Information (APFS) contains information about the file system of the macOS computer.
Recovery method	Parsing

Attribute	Description
Container GUID	The file system's container GUID.
Volume GUID	The file system's volume GUID.
Block Size	The block size of the file system.
Volume Name	The name of the volume of the file system.
Volume Size (bytes)	The size of the volume of the file system.
Next Object ID	The next allocated object ID in the file system.
Unmounted Date/Time - UTC (yyyy-mm-dd)	The date and time when the file system was last unmounted.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file system was created.
Volume Creator Program	The name of the program that was used to create the volume of the file system.
File Count	The number of files in the file system.
Symlink Count	The number of symbolic links in the file system.
Directory Count	The number of directories in the file system.
Snapshot Count	The number of snapshots in the file system.
Filesystem Object Count	The file system's object count.
Volume Count	The volume count.

Additional Information

Finder MRU

Description	Finder MRU lists the recently accessed paths from the Finder application on macOS.
Recovery method	Parsing

Attribute	Description
Path	The path that was accessed through the Finder.

Attribute	Description
Accessed Order	The order in which certain paths are accessed. 1 represents the location that was most recently accessed. The numbers then increase by 1 for each previous accessed location.
MRU Type	The type of MRU that is being reported.
Creator Name	The creator name for the path that was accessed.

Additional Information

Finder Sidebar Items

Description	Finder Sidebar Items contains information about each of the items featured in the Finder Sidebar on macOS. Items in the sidebar are often commonly-used items, and the user can customize the types of items they want to appear.
Recovery method	Parsing

Attribute	Description
Name	The name of the sidebar item.
Type	The type of the sidebar item.
Item Type	The category type that the sidebar item belongs to (Devices, Favorites, Shared, Tags).
Bookmark Data	The raw data contained within the sidebar item.

Additional Information

iCloud Downloads

Description	iCloud Downloads show a list of files that have been either recently downloaded or are pending download.
Notes	

Attribute	Description
File Name	The name of the iCloud file.
Download State	Indicates whether the file is available on the local drive or is pending download.
FileSize (bytes)	The size of the file in bytes.
Download Request Date/Time - UTC (yyyy-mm-dd)	The date and time that the download was requested.

iCloud Local Files

Description	iCloud Local Files are files that have been imported from the local computer or synced remotely from the iCloud Drive folder on a macOS machine.
Notes	

Attribute	Description
File Name	The name of the iCloud file.
Original File Name	The name of the file when it was first loaded to the iCloud Drive.
Package Name	The package ID of the application used to interact with the file.
FileSize (Bytes)	The size of the file in bytes.
Item Type	Indicates whether an item is a file, a folder, or a hidden iCloud File. Hidden iCloud files are used as markers for upload and download sync states, and are .iCloud files.
File Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created.
File Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was modified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when that the file was last accessed on the iCloud Drive.

iCloud Uploads

Description	iCloud Uploads show a list of files that have been either recently uploaded or are pending upload.
Notes	

Attribute	Description
File Name	The name of the iCloud file.
Upload State	Indicates whether the file is available on the local drive or is pending upload.
FileSize (Bytes)	The size of the file in bytes.
Upload Request Date/Time - UTC (yyyy-mm-dd)	The date and time that the upload was requested.

Installed Applications - macOS

Description	Applications that are installed on the computer that's running macOS.
Notes	

Attribute	Description
Display Name	The display name of the installed application.
Package Name(s)	The application bundle(s), which represent the application package identifier(s) in the App Store.
Display Version	The version number of the application provided via the App Store.
Internal Version	The long version string of the application.
Installed/Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was last installed or updated.
App Store Action	The App Store action further describes the application installation or update.

KnowledgeC Activity Level

Description	KnowledgeC Activity Level provides information about the KnowledgeC stream type of activity level.
Notes	

Attribute	Description
Activity Type	The activity level.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Application Activities

Description	KnowledgeC Application Activities contains information about activities associated with specific applications.
Notes	

Attribute	Description
Activity	The description associated with the activity.
Application Name	The bundle name of the application associated with activity.

Attribute	Description
Event Date/Time - UTC (yyyy-mm-dd)	The date and time that the activity occurred.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Application Focus

Description	KnowledgeC Application Focus provides information about the applications that were in focus on the device screen, within a recorded interval.
Notes	

Attribute	Description
Application Name	The bundle name of the application in focus.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Application Install States

Description	KnowledgeC Application Install States provides information about when applications were installed or uninstalled on the device.
Notes	

Attribute	Description
Application Name	The bundle name of the application that was installed or deleted.
Install State	The install state of the application (Installed or Uninstalled).
State Changed Date/Time - UTC (yyyy-mm-dd)	The date and time that install state last changed.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Application Usage

Description	KnowledgeC Application Usage provides information about the applications that were used on the device, within a recorded interval.
Notes	

Attribute	Description
Application Name	The bundle name of the application used.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Application Web Usage

Description	KnowledgeC Application Web Usage provides information about the applications that were used to access webpages on a iOS device, within a recorded interval.
Notes	

Attribute	Description
Application Name	The bundle name of the application that accessed the webpage.
Domain	The domain name of the webpage.
URL	The URL of the webpage.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Device Lock States

Description	KnowledgeC Device Lock States provides information about whether the device is locked or unlocked within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time.
Notes	

Attribute	Description
State	The lock state of the device (Locked or Unlocked).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Device Orientation States

Description	KnowledgeC Device Orientation States provides information about the orientation of the device within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time.
Notes	

Attribute	Description
State	The orientation state of the device (Vertical or Sideways).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Device Plugged-in States

Description	KnowledgeC Device Plugged-in States provides information about the plugged-in state of a device within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time. Knowing whenever a device is connected to charger or computer using USB can help identify how the device is used.
Notes	

Attribute	Description
State	The plugged-in state of the device. This value shows whether a device is plugged in and/or connected via USB (Plugged in or Unplugged).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Media History

Description	KnowledgeC Media History provides information about what type of audio or video media the user was engaging with at what time, as recovered from KnowledgeC.db
Notes	

Attribute	Description
Application Name	The bundle name of the application used to play the specified media.
Album	The album name of the specified media.
Title	The title of the specified media.
Artist	The artist of the specified media.
Duration	The duration of the specified media in seconds.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the media started playing.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the media stopped playing.

KnowledgeC Notification Usage

Description	KnowledgeC Notification Usage provides information about a user's notification usage within recorded intervals.
Notes	

Attribute	Description
Bundle ID	The bundle ID.
Type	The type of notification.
Device ID	The device ID.
Process ID	The process ID.

Attribute	Description
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Safari History

Description	KnowledgeC Safari History provides information about webpages that were accessed using the Safari browser, as recovered from knowledgeC.db
Notes	

Attribute	Description
URL	The URL of the webpage that was accessed with Safari browser.
Title	The title of the webpage that was accessed with Safari browser.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was accessed with Safari browser.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

KnowledgeC Screen Backlight States

Description	KnowledgeC Screen Backlight States provides information about the device backlight within recorded intervals. An absence of a recorded interval might mean that device was turned off during that time. This information can help identify whether a device was in active use within a specific interval.
Notes	

Attribute	Description
State	The screen backlight state of the device. This value indicates whether the screen backlight is on or off (Screen on or Screen off).
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time interval ended.
Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was created in the database.

Latent Wireless Geolocated WiFi Hotspots

Description	Latent Wireless Geolocated WiFi Hotspots contains information about WiFi hotspots that were discovered using a Latent Wireless device. Latent Wireless stores information about the hotspots in a database that Magnet AXIOM can parse for details about each hotspot.
Recovery method	Parsing

Attribute	Description
MAC Address	The MAC address of the detected WiFi hotspot.
First Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was first discovered.
Last Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was last seen.
Strongest Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was detected at its highest strength.
Network Name (SSID)	The SSID of the WiFi hotspot.
Channel	The WiFi hotspot channel.
RSSI	The received signal strength indicator for the WiFi hotspot.
Latitude	The latitude where the WiFi hotspot was detected.
Longitude	The longitude where the WiFi hotspot was detected.
Secure	Indicates whether the WiFi hotspot is secure.

Additional Information

Login History

Description	Login History contains information about the date and time when a user logged in or out of the macOS system.
Recovery method	Parsing

Attribute	Description
User Name	The account username.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the user logged in or out of the system in UTC format. These records are recovered from the .asl logs.
Date/Time - Local Time	The date and time when the user logged in or out of the system, in local time. Note that these records do not contain the year, so the exact date can only be inferred by using the Modified Date/Time of the respective accoun-tpolicy.log file.
Status	The logon or logoff event status.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expec-ted. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

LogMeIn Activity

Description	LogMeIn Activity records connection events that occur using the LogMeIn remote desktop client. These records can include remote sessions and file sharing events.
Notes	

Attribute	Description
Date/Time Local Time	The time in local time when the log line was recorded.

Attribute	Description
Activity Type	The type of the activity that was recorded. The Session type indicates that the event is a remote session. The SessionDateReport indicates that the recorded event is a session summary. The FileShare type indicates that the recorded event was a file being shared with other users.
Connection Type	The type of connection that was used.
Status	Indicates the status of the file sharing event (only applies to FileShare activities).
Remote IP Address	The public IP address of the client server.
Local IP Address	The public IP address of the host server.
Connection State	The login or logout state of the connection.
OS Version	The OS version of the host.

Menu Bar Apps

Description	Menu Bar Items lists the applications that are listed in the menu bar on macOS. The menu bar appears at the top of the screen and allows the user to open and interact with the applications that are displayed. Some menu bar items are displayed by default, while others might be added by the user.
Recovery method	Parsing

Attribute	Description
Application Name	The internal name of the application that's displayed in the menu bar.

Additional Information

Network Interfaces - iOS, macOS

Description	Network Interfaces contains information about each of the network the macOS computer has been connected to.
Recovery method	Parsing

Attribute	Description
BSD Name	The BSD name for the network.
MAC Address	The MAC address for the network interface.
Network Type	The type of network, which can be ethernet or IEEE80211 (wireless).
Network Name (SSID)	The SSID for the network.
USB Device Name	The name of any external device that is connected to the computer and is using network connectivity. The value will be empty if there aren't any external devices connected.
IOPathMatch	An Apple-defined property list key that contains an IOService path that the device matches against during a driver request.

Additional Information

Network Profiles - macOS

Description	Network Profiles contains information about networks that have been saved to the device. This artifact can reveal current networks that are frequently in use, as well as archived networks.
Recovery method	Parsing

Attribute	Description
Network Name (SSID)	The name of the saved network.
Last Connected Date/Time - UTC (yyyy-mm-dd)	The date and time of the last network connection.
Security Mode	The security mode of the network.
MAC Address	The list of MAC addresses that were accessed with the network.
Status	The network record status. Active indicates an up-to-date record from KnownNetworks, and 'Archived' an old record from UpdateHistory.

Additional Information

Network Usage - Application Data

Description	Network Usage Application Data contains information about how an application sends or receives data over the network.

Recovery method	Parsing

Attribute	Description
Process Name	The file name of the executable.
Type	The executable type (Process or App).
First Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the process was first run.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the process was last run.
Last Connected Date/Time - UTC (yyyy-mm-dd)	The date and time when the process last connected to a network.
WiFi Bytes Sent	The number of bytes sent over a WiFi connection.
WiFi Bytes Received	The number of bytes received over a WiFi connection.
Mobile Bytes Sent	The number of bytes sent over a mobile cellular network.
Mobile Bytes Received	The number of bytes received over a mobile cellular network.
Wired Bytes Sent	The number of bytes sent over a wired connection.
Wired Bytes Received	The number of bytes received over a wired connection.

Additional Information

Network Usage - Connections

Description	Network Usage Connections contains information about the networks that a device connects to.
Recovery method	Parsing

Attribute	Description
Network Name	The SSID or mobile network name.
Connection Type	The connection type, such as WiFi or Cellular.
Cell ID/MAC Address	An identifier for the specific access point to the network, which can be either a cell tower identifier or a MAC address.
First Connected Date	The date that the device first connected to this network.
Last Connected Date	The date that the device last connected to this network.

Additional Information

Network Utilities

Description	Network Utilities contains information about tools run in the Network Utilities application on macOS (Info, Ping, Netstat, Lookup, etc). Each instance

	of the artifact indicates the utility that's used and the query (or URL) passed in to the utility. The results of running the utility are not recoverable.
Recovery method	Parsing

Attribute	Description
Utility Tab	The specific utility that's used in the Network Utility application. The utilities include Ping Address, Lookup Address, Traceroute Address, Whois Address, User Finger Lookup Address, and Portscan Address.
Search Query	The query, or URL, that is run using the specified network utility.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the source file was last updated. The source file contains information about all user activity in the Network Utility application, so this timestamp may not represent the time that the event occurs, just the time that the file was last updated.

Additional Information

Operating System Information - macOS

Description	Operating System Information contains details about the macOS instance that's running on the user's computer.
Recovery method	Parsing

Attribute	Description
Operating System	The name of the operating system.
Version Number	The operating system version number.
Build Number	The operating system build number.
iOS Support Version	The version of iOS that the operating system supports.
Install Date/Time - UTC (yyyy-mm-dd)	The date and time when the operating system was installed.
Serial Number	The serial number of the drive that the operating system is installed on.
Computer Name	The name of the computer.
Local Hostname	The local hostname of the computer.
Timezone	The current timezone of the computer.
Country Code	The current country code of the computer.
Locale	The current locale of the computer.
Languages	The installed languages on the computer.

Additional Information

PowerLog App Usage

Description	PowerLog App Usage contains information about the applications that were running on the device during a specified interval.
Recovery method	Parsing

Attribute	Description
Bundle ID	The ID of the application bundle.
Focus (Seconds)	The number of seconds that the application was on the screen during the interval.
Background (Seconds)	The number of seconds that the application was running in the background during the interval.
Monotonic Interval Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the interval started. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Interval Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the interval started. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Interval Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the interval started. The time stated in this column uses a system offset to calculate the time that is displayed on the device.
Interval Length (Seconds)	The length of the interval in seconds.

Additional Information

PowerLog Application State

Description	PowerLog Application State contains information about application state transition.
Recovery method	Parsing

Attribute	Description
Bundle ID	The ID of the application bundle.
Process ID	The process identifier of the application.
State	The current state of the application.
Monotonic Date/Time - UTC (yyyy-mm-dd)	The date and time that the state was recorded. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Date/Time - UTC (yyyy-mm-dd)	The date and time that the state was recorded. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Date/Time - UTC (yyyy-mm-dd)	The date and time that the state was recorded. The time stated in this column uses a system offset to calculate the time that is displayed on the device.

Additional Information

PowerLog Battery Level

Description	PowerLog Battery Level contains information about the phone's battery.
Recovery method	Parsing

Attribute	Description
Battery Level	The battery level displayed in the UI.
Raw Battery Level	The true battery level.
Charging	Indicates whether the phone is charging. This value is Yes if the phone is charging, or No if otherwise.
Fully Charged	Indicates whether the battery is fully charged. This value is Yes if the phone battery is fully charged, or No if otherwise.
Monotonic Date/Time - UTC (yyyy-mm-dd)	The date and time that the battery level was recorded. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Date/Time - UTC (yyyy-mm-dd)	The date and time that the battery level was recorded. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Date/Time - UTC (yyyy-mm-dd)	The date and time that the battery level was recorded. The time stated in this column uses a system offset to calculate the time that is displayed on the device.

Additional Information

PowerLog Camera State

Description	PowerLog Camera State contains information about changes to the camera state which indicate when a device's camera is in use.
Recovery method	Parsing

Attribute	Description
State	Indicates whether the camera was on or off.
Camera Type	Indicates which camera was being used (Front or Back).
Bundle ID	The ID of the application bundle.
Monotonic Date/Time - UTC (yyyy-mm-dd)	The date and time that the camera usage was recorded. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Date/Time - UTC (yyyy-mm-dd)	The date and time that the camera usage was recorded. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Date/Time - UTC (yyyy-mm-dd)	The date and time that the camera usage was recorded. The time stated in this column uses a system offset to calculate the time that is displayed on the device.

Additional Information

PowerLog Device Lock State

Description	PowerLog Device Lock State contains information about when the phone was locked or unlocked.
Recovery method	Parsing

Attribute	Description
State	The state of the phone (Locked or Unlocked).
Monotonic Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the device lock state change was recorded. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer-.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the device lock state change was recorded. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Date/Time - UTC (yyyy-mm-dd)	The date and time that the device lock state change was recorded. The time stated in this column uses a system offset to calculate the time that is displayed on the device.

Additional Information

PowerLog Process Data Usage

Description	PowerLog Process Data Usage contains information about the processes that were running on the device, and the amount of data that was sent and received during the specified interval.
Recovery method	Parsing

Attribute	Description
Process Name	The name of the application that ran during the diagnostic period.
Bundle ID	The ID of the application bundle.
Monotonic Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time period started. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the time period started. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Start	The date and time that the time period started. The time stated in this column

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	uses a system offset to calculate the time that is displayed on the device.
Monotonic End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time period ended. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time period ended. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display End Date/Time - UTC (yyyy-mm-dd)	The date and time that the time period ended. The time stated in this column uses a system offset to calculate the time that is displayed on the device.
Mobile Bytes Received	The number of bytes received over a mobile cellular network.
Mobile Bytes Sent	The number of bytes sent over a mobile cellular network.
WiFi Bytes Received	The number of bytes received over a WiFi connection.
WiFi Bytes Sent	The number of bytes sent over a WiFi connection.

Additional Information

PowerLog Screen Autolock

Description	PowerLog Screen Autolock contains information about when the phone autolocked.
Recovery method	Parsing

Attribute	Description
Monotonic Date/Time - UTC (yyyy-mm-dd)	The date and time that the device autolocked. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Date/Time - UTC (yyyy-mm-dd)	The date and time that the device autolocked. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Date/Time - UTC (yyyy-mm-dd)	The date and time that the device autolocked. The time stated in this column uses a system offset to calculate the time that is displayed on the device.

Additional Information

PowerLog Timezone Information

Description	PowerLog Timezone Information contains information about the timezones that were registered on the device.
Recovery method	Parsing

Attribute	Description
Name	The name of the timezone.
Country Code	The code of the timezone's country.
Locale	The locale of the timezone.
GMT Offset	The number of hours that the timezone is away from Greenwich Mean Time (GMT).
Monotonic Date/Time - UTC (yyyy-mm-dd)	The date and time that the timezone was recorded. The time stored in this column is based on a monotonic clock. In computing, a monotonic clock is one that always increases in value, regardless of configurations to the system's date and time by a user, daylight savings, or any other changes. See also: https://developer.apple.com/documentation/kernel/1462446-mach_absolute_time
Baseband Date/Time - UTC (yyyy-mm-dd)	The date and time that the timezone was recorded. This value is computed by applying the appropriate 'Baseband' offset to the monotonic date and time, and represents the value of the clock on the device baseband hardware (cellular modem).
Display Date/Time -	The date and time that the timezone was recorded. The time stated in this column uses a system offset to calculate the time that is displayed on the

Attribute	Description
UTC (yyyy-mm-dd)	device.

Additional Information

Quarantined Files

Description	Quarantined Files contains information about the files that were flagged as quarantined in the macOS computer.
Recovery method	Parsing

Attribute	Description
Quarantined Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was flagged as quarantined.
Application Name	The name of the applicationthat was used to access or download the file.
Package Name	The package name of the application that was used to access or download the file.
Quarantined File identifier	A unique identifier of the quarantine event saved in the extended attributes of the quarantined file.
Download URL	The exact URL that the file was downloaded from.

Attribute	Description
Sender Name	The sender name of the email, when the flagged quarantined file originated from an email.
Sender Address	The sender email address, when the flagged quarantined file originated from an email.
Origin	When the flagged quarantined file originated from an email, this value is either the original URL that the file was downloaded from, or the email message ID.
Origin Title	The subject of the email, when the flagged quarantined file originated from an email.

Additional Information

Quick Look Thumbnails

Description	Quick Look Thumbnails contains thumbnail previews that the macOS device creates and displays for items in the file system.
Notes	

Attribute	Description
Attachment	The picture used as the thumbnail.
Folder	The folder from which the thumbnail was generated.
File Name	The name of the file that the thumbnail was created for.
Filesystem ID	The unique ID provided to the file. This value can be

Attribute	Description
	used to verify file system attributes for the file.
Thumbnail Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the thumbnail was generated.
Thumbnail Size (bytes)	The thumbnail size in bytes. Negative values are ommitted until further investigation.
Thumbnail Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the thumbnail was last accessed by the user.
Thumbnail Access Count	The number of times that the thumbnail has been accessed.

Rebuilt Desktops - macOS

Description	Rebuilt Desktops is an artifact that allows users to view an approximation of what a given macOS user's desktop looks like, including wallpapers, monitor configurations, and desktop icons, without having to virtualize the image.
Recovery method	Parsing

Attribute	Description
User Account	The user account that the desktop belongs to.
Wallpaper Path	The path that the wallpaper was located at as identified by the desktop-picture.db database.
Display Con-	Indicates whether the user had just a single screen, screens duplicated,

Attribute	Description
figuration	or a screen extended across connected monitors.
Monitor Identifier	A record identifier from the macOS system that indicates the type of monitors that were connected for a given configuration.
Preview	A preview of the rebuilt desktop image.

Additional Information
For more information about rebuilt desktops, see support.magnetforensics.com/s/article/Artifact-profile-Rebuilt-Desktops-macOS.

Recently Used Items

Description	Recently Used Items lists the most recently accessed items from a variety of sources. Each data source stores its recently used information in a separate file. For example, RecentDocuments aggregates information about all the documents that are opened, regardless of the application. RecentApplications contains information about each application that runs. And, app-specific sources can contain information specific to a particular application.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file that was accessed.
File Path	The full path of where the file was located.
UUID	The UUID of the accessed file.

Attribute	Description
Accessed Order	The order in which the files were accessed. A higher number indicates that the file was more recently accessed. For example, 1 represents the first item accessed, 2 represents the second item accessed, and so on.
MRU Type	The type of MRU that is being reported.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created.
Creator Name	The creator name of the file.
Volume Name	The name of the physical volume the file was recovered from.
Volume UUID	The UUID of the physical volume the file was recovered from.
Volume Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the physical volume where the file was recovered from.
Volume Size (bytes)	The size of the volume in bytes where the file was recovered from.
File System	The type of file system the file was recovered from.

Additional Information

Recovery Account Information

Description	Recovery Account Information lists the user accounts that have privileges to decrypt a FileVault encrypted volume in APFS.
Recovery method	Parsing

Attribute	Description
UUID	The unique identifier for the user.
Full Name	The full display name of the user.
Password Hint	The user's password hint.
Picture	The users profile image.
Is Admin Account	Indicates whether the user has administrative privileges on the computer.

Additional Information

Resumed Apps - macOS

Description	Resumed Apps has information about the applications that are set to reopen after the macOS computer restarts or resumes after going to sleep.
Recovery method	Parsing

Attribute	Description
Application Name	The name of the application that will be resumed when the computer resumes operations.
Bundle ID	The bundle name of the application, used to uniquely identify it in the application store.
Background State	A number that indicates the background state of the application. The values for this field are not translated into human-readable values, as it's not currently clear what each value represents.

Additional Information

Spotlight Shortcuts

Description	Spotlight Shortcuts contains information about the searches that a user performs in the Spotlight application on macOS. The display name can indicate a local file or folder, application, or online search results.
Recovery method	Parsing

Attribute	Description
Search Query	The query provided by the user.
Display Name	The name of the suggested result, provided by Spotlight.
URL	The URL associated with the suggested result.
Accessed Date/Time - UTC (yyyy-mm-dd)	Indicates when the displayed item was last accessed.

Additional Information

SSH Authorized Keys

Description	SSH Authorized keys are pre-configured keys used for logging into user accounts.
Recovery method	Parsing

Attribute	Description
Options	The list of options for the authorized key. This may be empty.
Encryption	The type of encryption used for the public key.
Public Key	The encrypted public key.
Comment	The comment added by the user for the authorized key. This may be empty.

Additional Information

SSH Keys

Description	SSH Keys are used to perform secure activities over the internet.
Recovery method	Parsing

Attribute	Description
File Name	The name of the SSH Keys file.
Type	The type of the SSH Key, either Public or Private.
Encryption	The type of encryption used on the SSH Key.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the file system.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the file system.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the file system.
File Content	The contents of the SSH Key file.

Additional Information

SSH Known Hosts

Description	SSH Known Hosts are public keys used to verify the identity of remote hosts. These are often automatically populated when the user connects to a host for the first time, but they can also be added manually.
Recovery method	Parsing

Attribute	Description
Host Names	The name or names of the specified host.
Marker	An optional tag used to indicate whether the host is a certificate authority.
Encryption	The type of encryption used for the public key.
Public Key	The encrypted public key.
Comment	The comment added by the user for the known host. This may be empty.

Additional Information

Startup Items - macOS

Description	Startup Items contains information about the processes and applications that are set to run at startup on a macOS computer.
Recovery method	Parsing

Attribute	Description
Application Package Name	A label that identifies the package name of the launch agent or daemon.
Startup Process Arguments	Any command line arguments that are run automatically when the application starts.
Type	The type of startup item (LaunchAgent if the plist file was found in the

Attribute	Description
	LaunchAgents folder and LaunchDaemon if the file is found in the LaunchDaemons folder).
Process Type	The type of process that's being launched (Background, Standard, Adaptive or Interactive).
Disabled	Indicates whether the job is enabled or disabled.

Additional Information

Trash Items

Description	Trash Items contains information about the items that a user has sent to the trash. There is also a potential of recovering items that have been cleared from the trash. This artifact does not recover folder or directory objects unless they're listed in the .DS_Store file.
Notes	

Attribute	Description
File Name	The name of the file or directory that's been deleted.
Type	The extension of the file. This attribute is not populated for files with no extensions. The type 'Folder' indicates that the item is a folder.
File Size (Bytes)	The size of the file in bytes.
Original Path	The original path of a file or directory recovered from the .DS_Store file. This

Attribute	Description
	path is used for restoring files to their original location.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that a file or directory was added to the trash bin. Typically, this timestamp represents the time the file or directory was deleted. However, this timestamp might be updated during data collection or transfer between volumes if the collection was not performed in a forensically sound manner. This attribute is not populated for files and directories that are not present in the filesystem but are mentioned in the .DS_Store file.

Trash Items - macOS

Description	Trash Items contains information about the items that a user has sent to the trash. There is also a potential of recovering items that have been cleared from the trash. This artifact does not recover folder or directory objects unless they're listed in the .DS_Store file.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file or directory that's been deleted.
Type	The extension of the file. This attribute is not populated for files with no extensions. The type 'Folder' indicates that the item is a folder.
File Size (Bytes)	The size of the file in bytes.
Original Path	The original path of a file or directory recovered from the .DS_Store file. This path is used for restoring files to their original location.

Attribute	Description
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that a file or directory was added to the trash bin. Typically, this timestamp represents the time the file or directory was deleted. However, this timestamp might be updated during data collection or transfer between volumes if the collection was not performed in a forensically sound manner. This attribute is not populated for files and directories that are not present in the filesystem but are mentioned in the .DS_Store file.

Additional Information

Unified Logs

Description	Unified Logs contains parsed records of Apple Unified Logs from the default directory, including activity information for many different applications on an Apple device. It can be useful for determining a user's system interaction.
Recovery method	Parsing

Attribute	Description
Type	The type of the log.
Process Name	The process name related to the log message.
Process ID	The process ID associated with the log message.
Date/Time - UTC (yyyy-mm-dd)	The timestamp of the log message.

Attribute	Description
Message	The message of the log.
Primary Category	The category of the log.
Subsystem	The subsystem related to the log message.

Additional Information

USB Connection History

Description	USB Connection History contains a history of the USB devices that have been connected to the macOS computer.
Notes	

Attribute	Description
Connection Start Date/Time - UTC (yyyy-mm-dd)	The date and time when a connection was made to the macOS computer.
Serial Number	The serial number of the connected USB device.
Vendor ID	The vendor ID of the connected USB device.
Product ID	The product ID of the connected USB device.
Device Release Number	The release number of the connected USB device.

User Accounts - macOS

Description	User Accounts contains information about the users that have logged in to the macOS computer, as recovered from the settings file.
Recovery method	Parsing

Attribute	Description
User Name	The account username.
Full Name	The full display name of the user.
User ID	The user's ID.
UUID	The unique identifier for the user.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the profile was created.
Home Directory	The user's home directory.
Password Hash	A hash of the user's password.
Password Hash Algorithm	The algorithm used to generate the user's password hash.
Password Hint	The user's password hint.
Login Failure Count	The number of failed logins for the account.
Last Incorrect Password Login Date/Time - UTC (yyyy-mm-dd)	The last date and time that an incorrect password was attempted.
Last Password Change Date/Time - UTC	The date and time that the password was last

Attribute	Description
(yyyy-mm-dd)	changed.
Profile Image	The user's profile image.
Profile Image Path	The path to the user's profile image.

Additional Information

Volume Information

Description	Volume Information contains information about the volumes that are connected to the macOS computer. Volumes can include mounted drives, CDs and DVDs, DMG files, external drives, or anything else that the computer detects as a mounted volume or device. You can find information about mapped networks volumes in the macOS Most Recently Used artifact.
Recovery method	Parsing

Attribute	Description
Volume Name	The volume name.
Volume Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the volume was created on the system.

Additional Information

Wi-Fi Logs

Description	WiFi Logs contains log entries extracted from the WiFi log on a macOS computer. This artifact can reveal WiFi activities, such as attempts to connect, autoconnect, and connection errors. This artifact can include data from networks that the user hasn't saved.
Recovery method	Parsing

Attribute	Description
Line	The line number within the log file where this record exists.
Network Name (SSID)	The name of the network that's associated with log entry.
Type	The type of event for the log entry.
Date/Time - Local Time (yyyy-mm-dd)	The local date and time for when the log entry was written.
Event	A brief description of the event from the log entry.
Original Text	The full text of the log entry.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Refined Results

Rebuilt Desktops - macOS

Description	Rebuilt Desktops is an artifact that allows users to view an approximation of what a given macOS user's desktop looks like, including wallpapers, monitor configurations, and desktop icons, without having to virtualize the image.
Notes	For more information about rebuilt desktops, see support.magnetforensics.com/s/article/Artifact-profile-Rebuilt-Desktops-macOS.

Attribute	Description
User Account	The user account that the desktop belongs to.
Wallpaper Path	The path that the wallpaper was located at as identified by the desktop-picture.db database.
Display Configuration	Indicates whether the user had just a single screen, screens duplicated, or a screen extended across connected monitors.
Monitor Identifier	A record identifier from the macOS system that indicates the type of monitors that were connected for a given configuration.
Preview	A preview of the rebuilt desktop image.

Social Networking

Houseparty Messages

Description	Houseparty Messages contains messages recovered from Houseparty.
Notes	

Attribute	Description
Sender	The username of the person sending the message.
Recipient	The username of the person receiving the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The content of the sent message.
Read Status	Indicates whether or not the message has been read.

Houseparty Users

Description	Houseparty Users contains information about the users contacted from the device using Houseparty.
Notes	

Attribute	Description
User Name	The username of the user.
Full Name	The full name of the user.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the user account was created.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the user account was last updated.

Volatile Artifacts

Active Connections

Description	Active Connections contains a list of all active and inactive connections, as well as the TCP and UDP ports the device is currently listening to.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
Protocol	The protocol used for the connection (UDP/TCP).
Local Address	The local address of the connection. This value can either be IPv4 or IPv6.
Local Port	The port that the connection is originating from.
Remote Address	The remote address of the connection. This value can either be IPv4 or IPv6.

Attribute	Description
Remote Port	The port that the connection is heading to.
State	The state of the connection.
Process ID	The process ID of the connection.

Additional Information

Network ARP Info

Description	Network ARP info contains a list of cached Address Resolution Protocol (ARP) entries.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
Local IP Address	Local IP address for the ARP cache entry.
Local MAC Address	Local MAC Address for the ARP cache entry.
Type	Type of ARP cache entry.
Seconds since ARP entry used	Number of seconds since the ARP entry was used. Fragment only populated for Linux.
Seconds since ARP entry	Number of seconds since the ARP entry was confirmed. Frag-

Attribute	Description
confirmed	ment only populated for Linux.
Seconds since ARP entry updated	Number of seconds since the ARP entry was updated. Fragment only populated for Linux.

Additional Information

Running Processes

Description	Running Processes contains a list of all processes currently running on the endpoint.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
Process Name	The name of the process.
Process ID	The process ID (PID).
User Name	The owner of the process.
Session ID	The associated session ID.
Session Name	The name of the associated session.
Memory Usage (KB)	The amount of memory used by the process, indicated in KB.

Attribute	Description
CPU Time (dd.HH:m-m:ss.ff)	The amount of time that the CPU has been running the process. Shown in dd.HH:mm:ss.ff format.
Command Line Call	The call to the command line that started the process.
Status	The status of the process.
Parent Process ID	The ID of the parent process (PPID).

Additional Information

Services

Description	Service List contains a list of all services currently running on the end-point.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
Service Name	The name of the service.
State	The state of the service.
Process ID	The process ID (PID).
Description	The description of the service.

Additional Information

Web Related

Chrome Archived Keyword Search Terms

Description	Chrome Archived Keyword Search Terms contains keyword search terms that were archived by the browser.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Chrome Archived Web History

Description	Chrome Archived Web History contains an archived history of old webpage visits.
Recovery method	Parsing

Attribute	Description
URL	The URL where the archived web history is located.
Title	The title of the archived web history.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.
Visit Count	The total visits to this URL.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
ID	The ID for the web history archive.

Additional Information

Chrome Autofill

Description	Chrome Autofill contains a collection of saved values that were used to fill in forms and fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Value	The value.
Count	The count of this autofill.

Attribute	Description
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.

Additional Information

Chrome Autofill Profiles

Description	Chrome Autofill Profiles contains profiles that Chrome uses to fill in forms with saved values.
Recovery method	Parsing

Attribute	Description
Name	The name for the autofill profile.
Email	The email used in the the autofill profile.
Number	The phone number used in the autofill profile.
Company	The company name used in the autofill profile.
Address Line 1	The address Line 1 used in the autofill profile.
Address Line 2	The address Line 2 used in the autofill profile.
City	The city used in the autofill profile.
State	The state used in the autofill profile.

Attribute	Description
Zipcode	The ZIP Code used in the autofill profile.
Country	The country used in the autofill profile.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the profile was last modified.

Additional Information

Chrome Bookmarks

Description	Chrome Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Parent	The name of the parent folder of the bookmark.

Additional Information

Chrome Cache Records

Description	Chrome Cache Records contains content that Chrome downloads and caches to speed up rendering times. Cached content can include pictures, text, HTML, JavaScript, and more.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached item.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was first visited.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the cache was last synced with the cloud.
File Type	The type of file that was cached.
Content Size (Bytes)	The size of the cached file.
Image	The cached image if the file type is an image. Otherwise, this column is empty.
Content	The cached file contents if the file type is not an image. Otherwise, this column is empty.
File Name	The file name of the cached item.
MD5 Hash	An MD5 hash of the cached item if it is a picture. Otherwise,

Attribute	Description
	this column is empty.
SHA1 Hash	A SHA1 hash of the cached item if it is a picture. Otherwise, this column is empty.
PhotoDNA Hash	The hash of the cached item for PhotoDNA if it is a picture. Otherwise, this column is empty.

Additional Information

Chrome Cookies

Description	Chrome Cookies contains cookies that Chrome downloads from the Internet that contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	The domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.

Attribute	Description
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Chrome Current Session

Description	Chrome Current Session contains information about the browser session that's currently underway.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times when the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Current Tabs

Description	Chrome Current Tabs contains information about the tabs that are open in the current browser session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times when the user accessed the URL.

Additional Information

Chrome Downloads

Description	Chrome Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the download.
Download Source	The URL of the file that was downloaded.
Saved To	The saved to location.
State	The state of the download.
Opened	Indicates whether the download is opened by the user.
Start Time Date/Time - UTC (yyyy-mm-dd)	The download start time.
End Time Date/Time - UTC (yyyy-mm-dd)	The download end time.
Bytes Downloaded	The bytes that were downloaded.
File Size(Bytes)	The file size of the download.

Additional Information

Chrome Extensions

Description	Chrome Extensions contains information about the extensions that a user has installed on their computer.
Recovery method	Parsing

Attribute	Description
Application Name	The name of the Chrome plugin or extension.
Version	The version number of the plugin or extension.
Description	The description of the plugin or extension.
Install Date/Time - UTC (yyyy-mm-dd)	The install time in the Chrome/Webkit time.
State	The state of the plugin or extension on the google account (Enabled or Disabled).
Permissions	The list of permissions that the plugin or extension has, as recorded in the 'manifest.json' file.
Active Permissions	The list of active permissions that the plugin or extension has, as recorded in the 'Preferences' file.
Granted Permissions	The list of all granted permissions that the plugin or extension has, as recorded in the 'Preferences' file.
Withholding Permissions	States whether the permissions are being withheld, as recorded in the 'Preferences' file.
Installed by OEM	States whether the plugin or extension is installed by OEM (True or False).
Installed by Default	States whether the plugin or extension is installed by default (True or False).
From Bookmark	States whether the plugin or extension was installed from a bookmark (True or False).
From Webstore	States whether the plugin or extension was installed from the chrome webstore (True or False).

Attribute	Description
Author	The author.
Homepage	The homepage.

Additional Information

Chrome FavIcons

Description	Chrome FavIcons contains the favicons that Chrome displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite or bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Icon URL	The icon URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.
Icon	A preview of the favicon.

Additional Information

Chrome History Index

Description	Chrome History Index contains an index of the webpages the user has visited in the past.
Recovery method	Parsing

Attribute	Description
Page URL	The URL of the webpage.
Title	The title of the webpage.
Visited On Date/Time - UTC (yyyy-mm-dd)	Indicates when the webpage was visited.
Body	A snippet of the webpage.

Additional Information

Chrome Keyword Search Terms

Description	Chrome Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user

Attribute	Description
	entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Chrome Last Session

Description	Chrome Last Session contains information about the previous browser session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times when the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Last Tabs

Description	Chrome Last Tabs contains information about the tabs that were open during the previous session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times when the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Logins

Description	Android Chrome Logins contains login information that a user provides in Chrome. Passwords are often encrypted, so you might not be able to

	recover them unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username of the login.
Password	The password of the login.
GUID	The GUID of the login found in the keychain.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the login was created.
Last Login Date/Time - UTC (yyyy-mm-dd)	The date and time when the login was last used successfully. If the login is unsuccessful for the page or account, this date and time will not be updated.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the login was last modified.
URL	The URL of the login page.

Additional Information

Chrome Saved Credit Cards

Description	Chrome Saved Credit Cards contains information about the credit cards

	that a user has saved to their device.
Recovery method	Parsing

Attribute	Description
Name On Card	The name of the person on the credit card.
Card Number	The number on the credit card.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the information was last modified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the credit card autofill information was last used.
GUID	An ID for the credit card.
Expiry Date	The date that the credit card is supposed to expire in the format of month-year.

Additional Information

Chrome Shortcuts

Description	Chrome Shortcuts contains all of the shortcuts used by Google Chrome for user entered URLs.
Recovery method	Parsing

Attribute	Description
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - UTC (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the webpage.
Times Used	The number of times that the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut, such as Typed URL or Bookmark.

Additional Information

To learn more about the Transition Type fragment, sign in to the Support Portal to read the article Google Chrome transition types.

Chrome Sync Accounts

Description	Chrome Sync Accounts contains information about the Chrome accounts that a user has logged in with. Chrome syncs data to the cloud so that a user can log in on multiple devices.
Recovery method	Parsing

Attribute	Description
Sync Id	The unique ID for the account that's used to sync data to the cloud.
Account Name	The name of the sync account.
Google Account	The GAIA ID of the sync account.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the sync account was synced.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the sync account was created.
Profile Picture URL	The profile picture URL of the sync account.
Active	Indicates whether or not the sync account is active.

Additional Information

Chrome Sync Data

Description	Chrome Sync Data contains information about the data that Chrome has synced to a user's account in the cloud.
Recovery method	Parsing and carving

Attribute	Description
Name	The name of the sync key.

Attribute	Description
Local Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the local system.
Server Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the server.
Local Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the local system.
Server Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the server.
Type	The type of data that is synced, such as bookmark, favicon, or type URL.
Parsed Content	The type of parsed data.
Favicon Image	The actual favicon image.

Additional Information

Chrome Top Sites

Description	Chrome Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser homepage which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the site.
Title	The title of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Rank	A ranking of the website, in terms of how frequently it was visited. A value of 1 indicates the most frequent and values increment to 8 as frequency decreases. A value of -1 indicates a site that the user manually added to the list of top sites.
Thumbnail	The thumbnail of the site.

Additional Information

Chrome Web History

Description	Chrome Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.

Attribute	Description
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times when the webpage was visited.
Typed Count	The number of times when the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Chrome Web Visits

Description	Chrome Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Attribute	Description
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information
To learn more about the Transition Type fragment, sign in to the Support Portal to read the article Google Chrome transition types.

Edge Chromium Autofill

Description	Edge Chrome Autofill contains records of the autofill values that Chrome saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was last used.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Edge Chromium Autofill Profiles

Description	Edge Chromium Autofill Profiles contains profiles that Chrome uses to fill in forms with saved values.
Recovery method	Parsing

Attribute	Description
Name	The name for the autofill profile.
Email	The email used in the the autofill profile.
Number	The phone number used in the autofill profile.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the profile was last modified.
Company	The company name used in the autofill profile.
Address Line 1	The address Line 1 used in the autofill profile.
Address Line 2	The address Line 2 used in the autofill profile.
City	The city used in the autofill profile.
State	The state used in the autofill profile.
ZIP/Postal Code	The ZIP Code or Postal Code used in the autofill profile.
Country	The country used in the autofill profile.

Additional Information

Edge Chromium Bookmarks

Description	Edge Chromium Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Edge Chromium Cache Records

Description	Edge Chromium Cache Records contains content that Chrome downloads and caches to speed up rendering times. Cached content can include pictures, text, HTML, JavaScript, and more.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached item.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was first visited.
Last Synced Date/Time - UTC (yyyy-mm-dd)	The date and time when the cache was last synced with the cloud.
File Type	The type of file that was cached.
Content Size (Bytes)	The size of the cached file.
Image	The cached image if the file type is an image. Otherwise, this column is empty.
Content	The cached file contents if the file type is not an image. Otherwise, this column is empty.

Additional Information

Edge Chromium Cookies

Description	Edge Chromium Cookies contains site usage information that websites send to the browser when a user visits their sites.
Recovery method	Parsing

Attribute	Description
Host	The host that created the cookie.
Name	The name of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.

Additional Information

Edge Chromium Downloads

Description	Edge Chromium Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The file name of the download.
Start Time Date/Time - UTC (yyyy-mm-dd)	The download start time.

Attribute	Description
End Time Date/Time - UTC (yyyy-mm-dd)	The download end time.
Saved To	The saved to location.
State	The state of the download.
Opened By User	Indicates whether the download is opened by the user.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Edge Chromium FavIcons

Description	Edge Chromium FavIcons contains the favicons that Chrome displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite or bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.

Attribute	Description
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Edge Chromium Keyword Search Terms

Description	Edge Chromium Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Additional Information

Edge Chromium Logins

Description	Edge Chromium Logins contains login information that a user provides in Chrome. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.

Recovery method	Parsing

Attribute	Description
User Name	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the data was created.
URL	The URL of the login page.

Additional Information

Edge Chromium Shortcuts

Description	Edge Chromium Shortcuts contains all of the shortcuts used by Google Chrome for user entered URLs.
Recovery method	Parsing

Attribute	Description
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.

Attribute	Description
Last Access Date/Time - UTC (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the webpage.
Times Used	The number of times that the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut, such as typed URL or bookmark.

Additional Information

Edge Chromium Web History

Description	Edge Chromium Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.

Attribute	Description
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Edge Chromium Web Visits

Description	Edge Chromium Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a

Attribute	Description
	user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.
_rawtime	The hidden raw time.

Additional Information

Firefox Add-ons

Description	Firefox Add-ons contains the add-ons from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
Name	The name of the add-on.
Version	The version the add-on.
Installed Date/Time - UTC (yyyy-mm-dd)	The date and time when the add-on was installed.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the add-on was updated.
Extension Enabled	Indicates whether the add-on is enabled by the user.
Description	The description of the add-on.

Additional Information

Firefox Bookmarks

Description	Firefox Bookmarks contains the bookmarks from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
URL	The URL of the website that was bookmarked.
Added Date/Time - UTC (yyyy-MM-dd)	The date and time when the bookmark was created.
Last Modified Date/Time - UTC (yyyy-MM-dd)	The date and time when the field was last modified.
Title	The title of the bookmark.
Bookmark Type	The type of bookmark, can be either Bookmark Item or Bookmark Folder.

Additional Information

Firefox Cache Records

Description	Firefox Cache Records contains all of the cached entries in the Firefox

	Cache Map.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cache entry.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cache entry was created.
MIME Type	The MIME type of the cache data.
Content Size (Bytes)	The content size of the cached data.
Image	The image, should one be associated with the cache entry.
Content	The content, should any be associated with the cache entry.

Additional Information

Firefox Cookies

Description	Firefox Cookies contains the cookies from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
Host	The host domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-MM-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-MM-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-MM-dd)	The date and time when the cookie will expire, if it is set to expire.
Path	The path to the cookie.

Additional Information

Firefox Downloads

Description	Firefox Downloads contains the downloads from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file being downloaded.

Attribute	Description
Download Source	The URL of the file being downloaded.
Start Date/Time - UTC (yyyy-MM-dd)	The date and time when the download was started.
End Date/Time - UTC (yyyy-MM-dd)	The date and time when the download was ended.
Saved To	The path to where the file was downloaded to.
Temp Path	The path to where the file was saved during downloading.
State	The state of the download can be Download In Progress, Download Complete, Download Stopped, or Download Paused.
Referrer	If the webpage used a mirror for downloading, the path to the original download URL.

Additional Information

Firefox FavIcons

Description	Firefox FavIcons contains the favicons from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
URL	The URL of the icon.

Additional Information

Firefox FormHistory

Description	Firefox FormHistory contains the form history from the Firefox web browser on a device.
Recovery method	Parsing and carving

Attribute	Description
Field Name	The name of the field.
Value	The value of the field.
First Used Date/Time - UTC (yyyy-MM-dd)	The date and time when the field was first used.
Last Used Date/Time - UTC (yyyy-MM-dd)	The date and time when the field was last used.
Times Used	The number of times that the field has been used.
ID	The unique ID of the field.

Additional Information

Firefox Input History

Description	Firefox Input History contains the input to forms from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
URL	The URL the input was given to.
Input	The value that was given.
Use Count	The number of times the input has been used.
ID	The unique ID of the input.

Additional Information

Firefox Logins

Description	Firefox Logins contains login information for websites that a user logs in to using the browser.
Recovery method	Parsing

Attribute	Description
URL	The URL of the login page.

Attribute	Description
Username	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the data was created.

Additional Information

Firefox Private Browsing History

Description	Firefox Private Browsing History contains the URLs that were loaded during a Private Browsing session from the Firefox web browser on a device.
Recovery method	Carving

Attribute	Description
URL	The URL.

Additional Information

Firefox SessionStore Artifacts

Description	Firefox SessionStore Artifacts contains the webpages from the last active session from the Firefox web browser on a device.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the webpage.
URL	The URL of the webpage.
Referrer URL	The URL of the webpage, if the webpage was a redirect.

Additional Information

Firefox Web History

Description	Firefox Web History contains the webpages from the last active session from the Firefox web browser on a device.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the webpage.
Last Visited Date/Time - UTC (yyyy-MM-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage.
Visit Count	The number of times that the webpage has been visited.
Typed	Indicates whether the user typed the URL (Yes or No).

Additional Information

Firefox Web Visits

Description	Firefox Web Visits contains all of the non-archived URL visits for Firefox.
Recovery method	Parsing

Attribute	Description
URL	The URL that was visited.
Title	The title of the page that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the page was visited.
Typed	Indicates whether the user typed the URL (Yes or No).
Transition Type	Indicates how the transition to the page happened.

Additional Information

Google Analytics First Visit Cookies

Description	Google Analytics First Visit Cookies contains information about Google Analytics first-visit cookies that are discovered in other artifacts.

Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Creation DateTime	The date and time when the site was first visited.
Most Recent Visit Date/Time	The date and time of most recent session.
2nd Most Recent Visit Date/Time	The date and time of the previous session.
Hits	The number of visits.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics First Visit Cookies Carved

Description	Google Analytics First Visit Cookies Carved contains information about Google Analytics first-visit cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.

Attribute	Description
Creation DateTime	The date and time when the cookie was created.
Most Recent Visit Date/Time	The date and time of most recent session.
2nd Most Recent Visit Date/Time	The date and time of the previous session.
Hits	The number of visits.

Additional Information

Google Analytics Referral Cookies

Description	Google Analytics Referral Cookies contains information about Google Analytics referral cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Cookie Source	The source URL used to reach the site.
Host	The domain of the URL.
Update Date/Time	The last time that the cookie was updated.
Campaign	The method of referral.
Access Method	Indicates whether the site was accessed organically or was referred.
Keyword	The keywords that were used to arrive at the site.

Attribute	Description
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics Referral Cookies Carved

Description	Google Analytics Referral Cookies Carved contains information about Google Analytics referral cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Cookie Source	The source URL used to reach the site.
Host	The domain of the URL.
Update Date/Time	The last time that the cookie was updated.
Campaign	The method of referral.
Access Method	Indicates whether the site was accessed organically or was referred.
Keyword	The keywords that were used to arrive at the site.

Additional Information

Google Analytics Session Cookies

Description	Google Analytics Session Cookies contains information about Google Analytics session cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start time of the current sesion.
Outbound Link Events Left	
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics Session Cookies Carved

Description	Google Analytics Session Cookies Carved contains information about Google Analytics session cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start date and time of the current sesion.
Outbound Link Events Left	

Additional Information

Google Analytics URLs

Description	Google Analytics URLs contains URLs that are discovered in other artifacts that are related to Google Analytics.
Recovery method	Carving

Attribute	Description
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	The domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.

Attribute	Description
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics URLs Carved

Description	Google Analytics URLs Carved contains information about Google Analytics URLs that are recovered using carving.
Recovery method	Carving

Attribute	Description
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	The domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.

Attribute	Description
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.

Additional Information

Google Maps

Description	Google Maps is a free web service that allows users to get directions.
Notes	

Attribute	Description
Search Query	The term that was searched for.
Starting Location	The starting location for navigation or directions.
Center of Map	Indicates where the map was centered.
Business Latitude and Longitude	The latitude and longitude of the business location.
Source Address	The source physical address.
Destination Address	The user's desired destination.
Route Type	Indicates how the user will travel (e.g. car, bus, bike).
Additional Address	Any additional addresses within the navigation.
Street View Latitude/Longitude	The latitude and longitude information in street view.

Google Maps Tiles

Description	Google maps is a free web service that allows users to get directions.
Notes	

Attribute	Description
Image	The actual picture content.
X Coordinate	The X coordinate value that Google uses to download the right tile.
Y Coordinate	The Y coordinate value that Google uses to download the right tile.
Zoom Level	The level that the user was zoomed in to the map. This value can be understood as the Z coordinate value that Google uses to download the right tile.

Malware/Phishing URLs

Description	Malware/Phishing URLs contains records that are believed to be either malware or phishing related URLs.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the website.
URL	The URL of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.

Attribute	Description
Artifact	The name of the artifact that the URL belongs to.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Pornography URLs

Description	Pornography URLs contains records that are believed to be pornography related URLs.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the website.
URL	The URL of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact that the URL belongs to.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

For a list of the URLs that are targeted by this artifact, see Pornography URLs.

Rebuilt Webpages

Description	Rebuilt Webpages contains the data that allows for the reconstruction of webpages.
Recovery method	Not applicable

Attribute	Description
Page Title	The title.
URL	The URL.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the original record was created.
Domain	The domain.
Cache Table	The table that the data to re-construct the page came from.
Cache RowID	The row ID in the table that constructed the rebuilt webpage.

Additional Information

Safari Bookmarks

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to webpages that have been bookmarked.

Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the bookmarked webpage.
Title	The title of the bookmarked webpage.
Type	The type of bookmark (for example, Bookmark, Favorite, and Folder)
Read	No data is populated for this fragment on macOS.
Added Date/Time - UTC (yyyy-mm-dd)	Indicates the date and time that the bookmark was added.
Last Visited Date/Time - UTC (yyyy-mm-dd)	No data is populated for this fragment on macOS.
Modified Date/Time - UTC (yyyy-mm-dd)	Indicates the date and time that the bookmark was modified.
Locally Added	Indicates whether the bookmark was created on the local device or a synced device with the same Apple ID. This data is not always available for every bookmark on macOS.

Additional Information

Safari Cache Records

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to webpages that have been cached on the local system.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL from which the file was downloaded.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cache file was created.
File Type	The type of the cached file.
Content Size	The size of the cached file.
Image	If the content file is an image, it will be displayed in this column.
Content	If the file is not an image (e.g. if it is a JavaScript file), the raw file content will be stored here.

Additional Information

Safari Downloads

Description	Safari is a web browser developed by Apple. Safari is installed by default

	on all Mac computers and is available for windows. This table captures information related to files that have been downloaded from Safari.
Recovery method	Parsing and carving

Attribute	Description
Download URL	The URL of the downloaded file.
Saved to Path	The local path where the download was saved.
Download Start Date/Time - UTC (yyyy-mm-dd)	The date and time the download started.
Download End Date/Time - UTC (yyyy-mm-dd)	The date and time the download finished.
Download Identifier	The unique identifier for the download.
Amount Downloaded (Bytes)	The number of bytes downloaded.
Size of Download (Bytes)	The size of the download in bytes.

Additional Information

Safari History

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures history entries which have been parsed from the filesystem.

Recovery method	Parsing and carving

Attribute	Description
URL	The URL of a visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Redirect URL	The URL that the user was redirected to.
Title	The title of the webpage.
Visit Count	The number of times that the URL was visited.
Visit Source	Indicates whether the website was viewed on the local device or on a synced device.

Additional Information

Safari iCloud Devices

Description	Safari iCloud Devices contains information about the devices that are synced to an iCloud account. Each device can access any browser tabs that are synced to the account.
Recovery method	Parsing and carving

Attribute	Description
Unique Device Identifier	A unique ID for the device that is accessing the tab.
Device Name	The name of the device that is linked to the iCloud account.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the device first synced to the iCloud account.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the device last synced with the iCloud account.

Additional Information

Safari iCloud Tabs

Description	Safari iCloud Tabs contains information about tabs that have been opened in the browser and synced to an iCloud account. Synchronized tabs are available to any device that logs in to the iCloud account.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the tab.
URL	The URL address of the tab.
Unique Device Identifier	A unique ID for the device that is accessing the tab.

Attribute	Description
Device Name	The name of the device that is accessing the tab.
Tab ID	The unique ID of the tab.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was last modified.
Modified By	The name of the device that last modified the tab.
Close Requested	Indicates whether a close request has been opened for the tab.
Close Request Date/Time - UTC (yyyy-mm-dd)	The date and time when the close request was created.

Additional Information

Safari Last Session

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to the user's last session with Safari.
Recovery method	Parsing and carving

Attribute	Description
Tab URL	The webpage URL.
Tab Title	The title of the webpage.

Additional Information

Safari Preferences

Description	Safari Preferences contains important Safari browser settings.
Recovery method	Parsing and carving

Attribute	Description
Homepage	The URL of the user's homepage.
Search Engine	The search engine used by the user to perform searches. The default search engine is Google.
Download Location	The folder location where downloaded items get saved. The user can specify a folder, or they may choose to manually select a download location with each download.
Remove Download Items Frequency	Indicates how frequently Safari should clear the download history. The default value is Manually.
Clear History Frequency	Indicates how frequently Safari should clear the browser history. The default value is Manually.
Open Safe	An option to automatically open safe download files, such as movies, pic-

Attribute	Description
Downloads	tures, sounds, PDF, text documents, and archives. The default value is True.

Additional Information

Safari Recently Closed Tabs

Description	Safary Recently Closed Tabs contains a history of recently closed tabs in the Safari browser.
Recovery method	Parsing and carving

Attribute	Description
Tab URL	The webpage URL.
Tab Title	The title of the webpage.
Close Request Date/Time - UTC (yyyy-mm-dd)	The date and time when the close request was created.

Additional Information

Safari Top Sites

Description	Safari is a web browser developed by Apple. Safari is installed by default

	on all Mac computers and is available for windows. This table captures information related to the user's top sites.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Feed Last Update Time	The date and time that the top site content was last updated.
Feed URL	The URL of the RSS feed.

Additional Information

Safari Website Preferences

Description	Safari Website Preferences contains important Safari browser settings that are configured on a site by site basis. Some of the preferences include allowing automatic downloads, sharing the user's location with the website, and receiving notifications. The user's preferences are saved by Safari to PerSitePreferences.db.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the website that the preference applies to.
Preference Type	The type of perference.
Value	The value of the preference.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the preference as added.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the preference expires.

Additional Information

WebKit Browser Session/Tabs (Carved)

Description	WebKit Browser Sessions/Tabs contains information about the browser sessions and tabs that the user has open, while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. The usage of other browsers, such as Firefox and Safari, aren't likely to appear under this artifact.
Recovery method	Carving

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

WebKit Browser Web History (Carved)

Description	WebKit Browser Web History contains information about the websites that a user visits while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. The usage of other browsers aren't likely to appear under this artifact, however, some URLs found by other browsers may also be found by this artifact.
Recovery method	Carving

Attribute	Description
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that this webpage was last visited
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

YARA Rules

YARA Rule Matches

Description	The YARA artifact contains information about files and processes that matched with conditions specified in a YARA rule.
Recovery method	Parsing

Attribute	Description
File Name	The name and extension of the file whose content matched with the condition(s) from the YARA rule. The value is blank if the match came from a process (executable/application that was loaded into memory at the time of the

Attribute	Description
	memory dump) during memory analysis using the Comae plugin option.
File size (bytes)	The size of the file in bytes. The value is blank if the match came from a Process.
Process Name	The name of the process that matched with the condition(s) from the YARA rule. The value is blank if the match came from a file.
Process ID	The ID of the process (PID). The value is blank if the match came from a File.
Matched rule set(s)	List of the paths and respective YARA rule sets that had a match.
Matched rule	The YARA rule name that a match was found for.
Matching conditions	List of conditions for the YARA rule that had a match.

Additional Information

Linux

Additional Sources

Android Backups

Description	Android Backups contains information about any backups of Android devices that are recovered from the computer. If an Android backup is recovered during a search, you can search the contents of the backup for additional artifacts.
Recovery method	Parsing

Attribute	Description
File Name	The name of the backup file.
File Path	The path where the backup was stored on the computer.
Encryption	The type of encryption (if any) that was used on the backup.
File System Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time for the AB file from the file system.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time for the AB file from the file system.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time for the AB file from the file system.

Additional Information

iOS Backups

Description	iOS Backups contains information about any backups of iOS devices that are recovered from the computer. If an iOS backup is recovered during a search, you can search the contents of the backup for additional artifacts.
Recovery method	Parsing

Attribute	Description
Device Phone Name	The name of the iOS device from which the backup originated.
Device Phone Number	The phone number of the iOS device from which the backup originated.
IMEI	The IMEI of the iOS device from which the backup originated.
ICCID	The ICCID of the iOS device from which the backup originated.
Backup File Creation Date/Time	The date and time that the backup was created.
Product Name	The model of the iOS device from which the backup originated.
Product Version	The version of iOS of the device at the time of the backup creation.
Serial Number	The serial number of the iOS device from which the backup originated.

Additional Information

Communication

IP Addresses - Audio/Video Calls

Description	IP Addresses of web audio/video calls show who a user was communicating with. Each instance of this artifact represents a single hop in the communication chain. By showing the relationship between multiple hops, you can determine where a call originated from and what the final destination was.
Recovery method	Carving

Attribute	Description
Call ID	The ID of the call.
Message ID	The ID of the message.
Domain	The domain used for the call.
Connection Type	The type of connection.
Origin IP Address	The originating IP address for this hop in the call.
Origin Port	The originating port for this hop in the call.
Destination IP Address	The destination IP address for this hop in the call.
Destination Port	The destination port address for this hop in the call.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	The timestamp associated with this hop in the call.
Remote User ID	The unique ID of the remote user.
Communication Protocol	The communication protocol for this call (either UDP or TCP).
Metadata	Any additional details about the call.

Additional Information

Skype Accounts

Description	Information about the Skype accounts that are recovered, such as user info and when the account was created.
Recovery method	Parsing

Attribute	Description
Skype Name	The Skype name of the account.
Display Name	The display name of the account.
Full Name	The full name of the account.
Email(s)	The email of this account.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date when the profile was created.

Attribute	Description
Last Online Date/Time - UTC (yyyy-mm-dd)	The last time that the account was online.
Birthday (yyyy-mm-dd)	The birthday of the account.
Gender	The gender of the account.
City	The city where the account is located.
State/Province	The state/province where the account is located.
Country	The country where the account is located.
Home Phone	The home phone of this contact.
Office Phone	The office phone of this account.
Mobile Phone	The mobile phone of this account.
Homepage	The homepage of this contact.
About Info	The about info of this contact.
Profile Last Modified On Date/Time - UTC (yyyy-mm-dd)	The date when the profile was last modified.
Mood Text	The text used to express mood.
Last Used On Date/Time - UTC (yyyy-mm-dd)	The last time that the account was used.
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	The time that the avatar was created.
Picture	The avatar for this contact.

Additional Information

Skype Activity

Description	Skype Activity contains interactions that occur between users on Skype. These interactions include messages, group interactions, calls, files sent/received, and SMS. Applies to Skype 8.1 and later.
Recovery method	Parsing

Attribute	Description
Conversation ID	ID of this conversation.
Profile Name	The local user's profile name.
Sender	The username of the sender/initiator of the interaction.
Sender Email	The sender's email as given in the message (if available).
Recipient Name(s)	The recipients or targets of the interaction.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was initiated.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the interaction was last updated (for example, when a call ends).
Message Type	The type of the interaction.
Message	The content of the message or summary of the interaction.
Emotion Count	The number of reactions to the interaction (for example, likes, dislikes, emojis, and so on).
File Name	The name of any attached files associated with the interaction.

Attribute	Description
File Size (Bytes)	The size in bytes of any attached files.
File	The attachment file (if applicable).
Attachment Data Recovered	Whether the attached file was recovered from the local filesystem.
Thumbnail URL	A URL that directs to the thumbnail picture (if applicable).
Call Duration (Seconds)	The length of the call in seconds (if applicable).
Metadata	The content of the message, if it consisted of interpreted data (that is, XML or JSON data, rather than plain text).

Additional Information

Skype Calls

Description	Information about Skype calls that occur between users.
Recovery method	Parsing and carving

Attribute	Description
Local Username	The user logged into Skype at the time of the call.
Call Initiator	The user who started the call.
Initiator Display Name	The display name of the user. This might be different from the username.
Recipient(s)	The users who accepted a call from the call initiator and participated

Attribute	Description
	in the call for a period of time.
Call Participants	The users who accepted and participated in the call from the call initiator for some duration.
Started Date/Time - UTC (yyyy-mm-dd)	Start time of the call.
Duration	Total duration of the Skype call.
Metadata	Additional details about the call extracted in XML format. This includes the duration of time each participant was in the call.

Additional Information

Skype Chat Messages

Description	Skype messages sent from one user to another.
Recovery method	Parsing and carving

Attribute	Description
Profile Name	Profile name of the caller
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent
Author	Author of the message

Attribute	Description
From Display Name	The display name of who sent the message
Message	The body of the message or a description of the action taken. For example, adding another participant to a group chat or sharing a file or picture.
Attachment Name	The name of the attachment that was sent. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Attachment Size (Bytes)	The size of the attached file, in bytes. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Metadata	Additional details about the action, extracted in its original XML format.
Message Status	The status of the message.
Message Type	Type of message
Chat ID	ID of this chat
Recipient	Recipient of the chat

Additional Information

Skype Chatsync Messages

Description	Skype messages sent from one user to another that are parsed from the chatsync directory.

Recovery method	Parsing and carving

Attribute	Description
Local User	The local Skype user
Chat Initiator	The user that started the conversation
Chat Partner/Group Chat ID	The other user in the chat, or a group chat identifier
Message Type	Indicates the sent status of the message
Message	The content or body of the message
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent

Additional Information

Skype Chatsync Messages Carved

Description	Skype messages sent from one user to another that are carved from the chatsync directory.
Recovery method	Parsing

Attribute	Description
Message Type	Indicates the sent status of the message
Message	The content or body of the message
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Skype Contacts

Description	Information about Skype contacts that are recovered, which may or may not be added contacts.
Recovery method	Parsing

Attribute	Description
Profile Name	Profile name of the user
Skype Name	Skype name of the contact

Attribute	Description
Display Name	Display name of this account
Is Blocked	Is this contact blocked?
Contact Added	Specifies whether the contact is an added contact or just cached into the database (1 if the contact was added, 0 otherwise). Contacts can be cached into the database for a variety of reasons (for example, as a 'suggested contact').
Full Name	Full Name of this account
Birthday (yyyy-mm-dd)	Birthday of this account
Gender	Gender of this account
City	City where this account is located
State/Province	State/Province this account is located
Country	Country this account is located
Home Phone	Home phone of this contact
Office Phone	Office phone of this account
Mobile Phone	Mobile phone of this account
PSTN Number	PSTN number of this contact
Email(s)	Email of this account
Homepage	Homepage of this contact
About Info	About info of this contact
Profile Loaded	Previously called "Profile Created On Date/Time", this attribute rep-

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	resents the date/time when a contact's profile is first created on the user's device. When the profile information is updated by the contact, the date in the database is also updated.
Mood Text	Text used to express mood
Last Online On Date/Time - UTC (yyyy-mm-dd)	Last time the account was online
Last used On Date/Time - UTC (yyyy-mm-dd)	Last time the account was used
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	Avatar created time
Image	Image for this contact

Additional Information

Skype File Transfers

Description	Files that are transferred from one user to another using Skype.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Partner Handle	The user name of the file transfer partner.
Partner Display Name	The display name of the file transfer partner
File Name	The file name being transferred
Type	The type of file being transferred
File Path	The path to the local file
Transferred File	The file that was transferred
File Size (Bytes)	The size of the file being transferred
Bytes Transferred	The number of bytes that were transferred
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date and time the file transfer was started
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date and time the file transfer completed
Status	The status of the file (for example, transfer, transferring or cancelled)

Additional Information

Skype Group Chat

Description	Information about the Skype group chats that a user is a part of.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Chat ID	The group chat's unique identifier.
Participants	The participants of the chat.
Posters	The users that have posted to the chat.
Active Members	The currently active users of the group.
Chat name	The name of the chat.
Started Date/Time - UTC (yyyy-mm-dd)	The date and time the chat started.
Last Changed Date/Time - UTC (yyyy-mm-dd)	The date and time the chat was modified.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the Source
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Skype IP Addresses

Description	IP addresses that are associated with a Skype user account.
Recovery method	Parsing and carving

Attribute	Description
Username	Username of Skype accounts
IP Addresses	IP Addresses for the Skype user
Date/Time - UTC (yyyy-mm-dd)	Date and time
IP Address Type	Type of IP address Local or Public

Additional Information
This artifact is no longer supported as of Skype 7.40.

Skype Media Cache

Description	Media content that gets sent from one Skype user to another.
Recovery method	Parsing

Attribute	Description
Chat ID	The group chat's unique identifier.
Profile Name	The name of the user.
Author	The author of the media message.
Recipient(s)	The recipient(s) of the media message.
From Display Name	The display name of the sender.
Message Sent Date/Time	The Date/Time the media message was sent.
MIME Type	The MIME type of the media sent.

Attribute	Description
File Size (Bytes)	The size of the media file sent in bytes.
Is Thumbnail	Whether the particular media recovered is a thumbnail.
Media URL	The URL of the media as stored in the Skype cloud.
Thumbnail URL	The URL of the thumbnail as stored in the Skype cloud.
Media	The media that was recovered.
Thumbnail	The thumbnail if the media recovered was a video file.

Additional Information

Skype Message History Exports

Description	Skype Message History Exports contains a history of a user's sent and received messages and attachments, as parsed from a message history export.
Recovery method	Parsing

Attribute	Description
Author	The Skype ID of the sender of the message.
Author Name	The display name of the sender of the message.
Recipient(s)	The recipient(s) of the message.
Message Sent Date/Time - UTC	The date and time that the message was sent.

Attribute	Description
(yyyy-mm-dd)	
Message	The body of the message.
Message Type	The data type of the message.
Conversation Name	The name of the group conversation the message was sent in.
Location Address	The name of the location in a geolocation message.
Temp File Name	The name of the attachment as it was downloaded in the export.
Attachment Name	The name of the attachment when it was sent in Skype.
Attachment Size (bytes)	The size of the attachment in bytes.
Attachment	The attachment file.
Local User ID	The Skype ID of the user whose data was exported.
_ThreadID	The Skype ID of the conversation.

Additional Information

Skype SMS

Description	SMS messages that a user sends or recieves using Skype.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Author	The author of the message
Message	The message content.
Target Number(s)	The recipient phone numbers
Status	The status of the message.
Reply-to Number	A phone number the recipients can reply to

Additional Information

Skype Voicemails

Description	Voicemails that a user sends or recieves using Skype.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Partner Handle	The user name of the conversation partner
Partner Display Name	The display name of the conversation partner
Subject	Identifies the subject of the voicemail
Message Sent Date/Time - UTC (yyyy-	The date and time the message was sent

Attribute	Description
mm-dd)	
Duration	The length of the voicemail
Allowed Duration	The maximum length allowed for the voicemail
Size	The size of the recording
Path	The file path of the voicemail
Type	Identifies whether the voicemail was received or sent.
Status	The status of the voicemail, recording or played for example.

Additional Information

Connected Devices

Your Phone Contacts

Description	Your Phone Contacts contains information about contacts synced from a mobile device to a computer using Your Phone. The Your Phone application can sync data from Android and iOS devices to computers running Windows 10.
Recovery method	Parsing

Attribute	Description
Display Name	The contact's display name.
Nickname	The contact's nickname.
Phone Number	The contact's phone number.
Type	The type of phone number associated with the contact, for example Home, Mobile, or Business.
Last Time Contacted Date/Time - UTC (yyyy-mm-dd)	The last time that this contact either sent a message to, or received a message from the synced device or local user since the Your Phone application was installed.
Number of Times Contacted	The number of times the synced device or local user either sent a message to, or received a message from the contact since the Your Phone application was installed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that this contact's details were modified.

Additional Information

Your Phone Devices

Description	Your Phone Devices contains information about the devices that are synced to the user's computer by using the Your Phone application.
Recovery method	Parsing

Attribute	Description
Application Version	The version of Your Phone running on the computer.
Last Run Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was last run on the computer.
Device Application Version	The version of the Your Phone companion application running on the device.
Device ID	A GUID identifier generated to uniquely identify devices within the Your Phone application.
Device Name	The name provided by the device and displayed in the user interface when referring to it.
Device Platform	The device's platform (Android or iOS).
Device Messages Synced Date	The date and time when the device last synchronized its messages data with Your Phone.
Computer Messages Synced Date	The date and time when the computer last synchronized its messages data with Your Phone.
Device Contacts Synced Date	The date and time when the device last synchronized its contacts data with Your Phone.
Computer Contacts Synced Date	The date and time when the computer last synchronized its contacts data with Your Phone.
Device Photos Synced Date	The date and time when the device last synchronized its picture data with Your Phone.
Computer Photos Synced Date	The date and time when the computer last synchronized its picture data with Your Phone.

Additional Information

Your Phone Pictures

Description	Your Phone Pictures contains information about pictures synced from a mobile device to a computer using Your Phone. The Your Phone application syncs the 25 most recently taken photos from Android and iOS devices to computers running Windows 10.
Recovery method	Not applicable

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Device ID	A GUID identifier generated to uniquely identify devices synced using the Your Phone application.
Device Name	The name of the device (as provided by the device) which is displayed in the user interface for Your Phone.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-	The last accessed date and time of the picture in the file system.

Attribute	Description
mm-dd)	
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken

Attribute	Description
	(extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS Latitude (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the pciture was taken (extracted from Exif data).

Attribute	Description
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicates whether the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.
Exif Data	A searchable field for all raw exif properties.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Your Phone SMS/MMS

Description	Your Phone SMS/MMS contains information about messages synced from a mobile device to a computer using Your Phone. The Your Phone application can sync data from Android and iOS devices to computers running Windows 10.
Recovery method	Parsing and carving

Attribute	Description
Sender	The phone number that sent the message.
Recipient(s)	The phone number(s) the message was sent to.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message content.
Message Direction	Indicates whether the message was sent or received by the synced device or local user.
Message Type	Indicates whether the message is SMS or MMS.
Message Status	Indicates whether the message has been read.
Attachment Name	The name of the attached file, if applicable (MMS only).

Additional Information

Custom

File Signature Mismatch (Audio)

Description	File Signature Mismatch (Audio) contains identified mismatches between a known file signature header and the extension (or lack thereof) for an audio file. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Container)

Description	File Signature Mismatch (Container) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a container. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.

Attribute	Description
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Document)

Description	File Signature Mismatch (Document) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a document. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.

Attribute	Description
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Picture)

Description	File Signature Mismatch (Picture) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a picture. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file. If the MIME type is unknown, this defaults to application/octet-stream.

Attribute	Description
File Extension Type	The identified MIME type of the extension of the file. If the MIME type is unknown, this defaults to application/octet-stream. If there is no file extension, but the MIME type is known, a mismatch is is returned.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Video)

Description	File Signature Mismatch (Video) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a video. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file

Attribute	Description
	extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

Documents

CSV Documents

Description	CSV Documents contains CSV documents (.csv) that are located on the system.
Recovery method	Parsing

Attribute	Description
File Name	The name of the CSV document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last modified.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was created.
File Content	The content of the CSV document.

Attribute	Description
Size (Bytes)	The size of the CSV document in bytes.
SHA1 Hash	The SHA1 hash of the contents of the document.
MD5 Hash	he MD5 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

Microsoft Excel Documents

Description	Microsoft Excel is a spreadsheet processor developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.

Attribute	Description
Size (Bytes)	The size of the document in bytes.
Saved Size (Bytes)	The size of the document (in bytes) that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title metadata.
Subject	The subject metadata.
Authors	The authors of the document.
Keywords	The keywords metadata in the document.
Comment	The comments metadata.
Last Author	The last author to edit the document.
Last printed Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

Microsoft PowerPoint Documents

Description	Microsoft PowerPoint is a presentation creator developed by Microsoft. This table captures documents created with PowerPoint, extracted from the filesystem and carved from unallocated space.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
File	The actual file.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.

Attribute	Description
Keywords	The keywords in the metadata of the file.
Comment	The comments in the metadata of the file.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

Microsoft Word Documents

Description	Microsoft Word is a word processor developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last modified on the filesystem.
Size (bytes)	The size of the document.
Saved Size (bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title metadata.
Subject	The subject metadata.
Authors	The authors of the document.
Keywords	The keywords metadata in the document.
Comment	The comments metadata.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyy-mm-dd)	The date and time when the document was last printed (extracted from metadata within the document).
Last Modified Date/Time - UTC (yyy-mm-dd)	The date and time when the document was last modified (extracted from meta-data within the document).

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created (extracted from metadata within the document).
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.
Source	The location where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

For information about supported formats, see Supported media and file types.

PDF Documents

Description	Portable Document Format (PDF) is a file format used to present documents in a manner independent of application software, hardware, and operating systems. This table captures documents in this file format, extracted from the filesystem and carved from unallocated space.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was created, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was last modified, extracted from metadata within the document.
File	The PDF file.
MD5 Hash	An MD5 hash of the PDF content.
SHA1 Hash	A SHA1 hash of the PDF content.

Additional Information

For information about supported formats, see Supported media and file types.

RTF Documents

Description	The information for each RTF document that was recovered from the search.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the RTF document.
File Size (Bytes)	The size of the RTF document in bytes.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the RTF document was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the RTF document was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the RTF document was last modified.
File Content	The contents of the RTF document.
MD5 Hash	A MD5 hash of the RTF content.
SHA1 Hash	A SHA1 hash of the RTF content.

Additional Information

For information about supported formats, see Supported media and file types.

Text Documents

Description	Text documents (.txt) that are located on the system.
Recovery method	Parsing

Attribute	Description
Filename	The name of the text document.
Size (Bytes)	The size of the text document in bytes.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was created.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.
File Content	The content of the text document.

Additional Information

For information about supported formats, see Supported media and file types.

Email and Calendar

Calendar Events

Description	The Android Calendar application is a default application on Android.
Recovery method	Parsing and carving

Attribute	Description
Summary	A summary of the calendar appointment.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the appointment starts.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the appointment ends.
Event Location	The location of the calendar appointment.
Notes	Notes about the calendar appointment.
Calendar	The name of the calendar from which the event was generated.
Attendees	The attendees of the event.
Timezone	The timezone the appointment is in.
URL	A URL associated with the event.

Additional Information

Calendar Events (UFED Agent)

Description	Calendar Events (UFED Agent) contains details about a user's calendar events on Android. These messages are recovered from <calendar> tag found in a UFED Report.xml
Recovery method	Parsing

Attribute	Description
Subject	The subject of the scheduled event. This data is retrieved from the <subject> tag within the calendar element in a UFED Report.xml.
Event Location	The location of the scheduled event. This data is retrieved from the <location> tag within the calendar element in a UFED Report.xml.
Notes	Notes about the scheduled event. This attribute is referred to as the <Description> in the evidence acquired from the UFED and is retrieved from the <description> tag within the calendar element in a UFED Report.xml.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the scheduled event. This data is retrieved from the <start> tag wihin the calendar element in a UFED Report.xml.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the scheduled event. This data is retrieved from the <end> tag within the calendar element in a UFED Report.xml.
Repeat Until Date/Time -	The date and time when this recurring scheduled event expires. This data is retrieved from the <repeat_until> tag within the calendar element in a UFED

Attribute	Description
UTC (yyyy-mm-dd)	Report.xml.
Repeat Interval	Describes the type of recurring event. This data is retrieved from the <repeat_type> tag within the calendar element in a UFED Report.xml.
Repeat Every	Describes the frequency of the recurring event. This data is retrieved from the <repeat_every> tag within the calendar element in a UFED Report.xml.
Repeat On	Indicates the specific day of occurrence of the recurring event. This data is retrieved from the <repeat_position> tag within the calendar element in a UFED Report.xml.

Additional Information

Live System

Logged on Users - Live System

Description	Logged on Users Live System contains the information for each logged on user on the live system.
Recovery method	Parsing

Attribute	Description
Account Type	The type of the user account and the MSDN information about that account type.

Attribute	Description
Description	The user generated description of the user account.
Account Disabled	Indicates whether the user account is disabled (Yes or No).
Domain	The domain that the user account belongs to.
Full Name	The full name of the user.
Installed Date/Time - UTC (yyyy-mm-dd)	Indicates when the user account was installed or created.
Local Account	Indicates whether the user account is a local account (Yes or No).
Locked Out	Indicates whether the user account is locked out (Yes or No).
Name	The name of the user account under the current domain.
Last Used Date/Time - UTC (yyyy-mm-dd)	The last date and time that the user account was used.
Last Login Date/Time - UTC (yyyy-mm-dd)	The last date and time that the user account was logged into.
Logon Type	Indicates how the user account was last logged into and the MSDN information about that logon type.
Password Changeable	Indicates whether the user's account password is changeable (Yes or No).
Will Password Expire	Indicates whether the user's account password will expire (Yes or No).
Password Required	Indicates whether the password is required to log in to the user's account (Yes or No).

Attribute	Description
Security Identifier	The security identifier of the account.
IP Address	The IP address that has logged in to the account. This value is either a valid IPv4 address or Local Host.
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the user's information was captured.

Additional Information

Running Processes - Live System

Description	Running Processes Live System contains the information for each process on the live system.
Recovery method	Parsing

Attribute	Description
Name	The name of the process, referred to as the 'Image Name' in task manager.
Description	The description of the executable file, can be blank and still be valid.
Full Path	The full path to the executable of the process.
Process ID	The ID of the process.
Parent Process ID	The process ID of the immediate parent of the process.

Attribute	Description
User Name	The owner of the process.
CPU Time (HH:mm:ss)	Indicates the amount of time that the process required of the CPU.
Elapsed Time (HH:mm:ss)	Indicates how long the process has lived for.
I/O Read Bytes	Indicates how many bytes have been read by the process.
I/O Write Bytes	Indicates how many bytes have been written by the process.
I/O Other Bytes	The number of bytes transferred in input and output operations generated by a process that are neither reads nor writes, including file, network, and device inputs and outputs.
Memory (Private Working Set) Bytes	The number of bytes that have been allocated for the process.
Command Line Call	The call to the command line that will start the process.
Start Date/Time - UTC (yyyy-mm-dd)	Indicates when the process was first started.
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the process information was captured.

Additional Information

Location and Travel

Google Maps

Description	Google Maps is a free web service that allows users to get directions.
Recovery method	Carving

Attribute	Description
Search Query	The term that was searched for.
Starting Location	The starting location for navigation/directions.
Center of Map	Indicates where the map was centered.
Business Latitude and Longitude	The latitude and longitude of the business location.
Source Address	The source physical address.
Destination Address	The user's desired destination.
Route Type	Indicates how the user will travel (e.g. Car, bus, or bike).
Additional Address	Any additional addresses within the navigation.
Street View Latitude/Longitude	The latitude and longitude information in street view.

Additional Information

Google Maps Tiles

Description	Google maps is a free web service that allows users to get directions.
Recovery method	Parsing and carving

Attribute	Description
Image	The actual picture content.
X Coordinate	The X coordinate value that Google uses to download the right tile.
Y Coordinate	The Y coordinate value that Google uses to download the right tile.
Zoom Level	The level that the user was zoomed in to the map. This value is the Z coordinate value that Google uses to download the right tile.

Additional Information

Media

AMR Files

Description	AMR Files contains voicemail messages or memos for both iOS and Android.
Recovery method	Carving

Attribute	Description
File Name	The name of the file the AMR was recovered from.
Size (Bytes)	The size of the AMR content.
MD5 Hash	An MD5 hash of the AMR content.
SHA1 Hash	A SHA1 hash of the AMR content.
Audio	The contents of an AMR file.
Media Duration (Seconds)	The duration of the audio clip in seconds.

Additional Information

For information about supported formats, see Supported media and file types. Media duration is calculated from the number of speech frames carved from the AMR data, where each speech frame has a duration of 20ms, as AMR files do not contain metadata for duration.

Audio

Description	Audio contains audio files that are recovered that use the .mp3 or .wav formats.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file.
File Extension	The extension of the file.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was created.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was last modified.
File Size (Bytes)	The size of the audio file.
MD5 Hash	An MD5 hash of the audio content.
SHA1 Hash	A SHA1 hash of the audio content.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the audio clip in seconds (extracted from Exif data).
Exif Created	The date and time when the audio clip was first recorded (extracted from Exif

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	data).
Exif Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio clip was edited (extracted from Exif data).
Timezone	The timezone setting on the recorder at the time when the audio clip was recorded (extracted from Exif data).
Software	The software used to record or modify the audio clip. This could either be the OS version of the phone used to record the audio clip or the name of the software used to edit the audio clip in post-production (extracted from Exif data).
Latitude	The GPS latitude coordinates of where the audio clip was recorded (extracted from Exif data).
Longitude	The GPS longitude coordinates of where the audio clip was recorded (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of where the audio clip was recorded (extracted from Exif data).
Exif Data	A searchable field for all raw Exif properties.

Additional Information

For information about supported formats, see Supported media and file types.
To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Carved Video

Description	Carved Video contains videos that are recovered using carving. Supported formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. Other container formats can also be recovered provided that their underlying packets are the same as one of the supported formats.
Recovery method	Parsing

Attribute	Description
Content Format	The format of the video.
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
File Size (Bytes)	The size of the container and file.
Container Format	The format of the video container.
Saved Video Size (Bytes)	The size of the video that was saved to the database.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Additional Information
As of February 20 2020, this artifact will no longer be included under Videos. Carved Video functionality will be included in the Videos artifact instead.

Pictures

Description	Pictures contains pictures retrieved using either carving or parsing techniques.
Recovery method	Parsing and carving

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.

Attribute	Description
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time when the picture was being taken (extracted from Exif data).

Attribute	Description
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The latitude coordinate in decimal degrees.
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS latitude (extracted from Exif data).
Longitude	The longitude coordinate in decimal degrees.
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
Altitude	The GPS coordinates of the camera where the pciture was taken (extracted

Attribute	Description
(meters)	from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicating if the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.
Exif Data	A searchable field for all raw exif properties.

Additional Information

For information about supported formats, see Supported media and file types.
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.
To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Videos

Description	Videos contains videos that are recovered using parsing or carving. Supported formats for parsing include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. Supported carving formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. For more information about supported video formats, see Supported media and file

	types.
Recovery method	Parsing

Attribute	Description
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
File Name	The name of the file.
File Extension	The extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was last modified.
File Size (Bytes)	The size of the video.
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
Exif Extraction	The Exif extraction status indicates the level of Exif extraction that was per-

Attribute	Description
Status	formed. Complete indicates that a full Exif extraction was performed, including potential metadata located at the end of the video. Partial indicates that only Exif information in the header section of the video file was recovered, which should only occur with very large videos (in excess of the limit set in the options screen). Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The resolution of the video (extracted from Exif data).
Original Height	The resolution of the video (extracted from Exif data).
Exif Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was first recorded (extracted from Exif data).
Exif Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the video being recored (extracted from Exif data).
Software	The software used to record or modify the video. This could either be the OS version of the phone used to record the video or name of the software

Attribute	Description
	used to edit the video in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to record the video (extracted from Exif data).
Model	The model of the camera used to record the video (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to record the video (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS latitude coordinates of the camera where the video was recorded (extracted from Exif data).
Longitude	The GPS longitude coordinates of the camera where the video was recorded (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the video was recorded (extracted from Exif data).
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.
Content Format	The format of the carved video.
Container	The format of the carved video container.

Attribute	Description
Format	
Saved Video Size (Bytes)	The size of the carved video that was saved to the database.
Exif Data	A searchable field for all raw exif properties.

Additional Information
If AXIOM Process is configured to save a set amount of data from carved videos, any generated MD5 and SHA1 hashes are based on the saved data, not the full video. This behavior might cause issues when searching for known video hashes, as the hash for a carved video will differ from the actual video if it exceeds the size limit set in AXIOM Process. To learn more about Exif data for videos, see Extracting Exif data from videos. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Operating System

.DS_Store Records

Description	.DS_Store Records contains all the records extracted from .DS_Store files found on the computer. Each record represents a property of a file or a folder. The significance of this artifact is an indicator of high likelihood that the user of the computer was aware of these files and folders with a possibility of attributing a date to that awareness.
Recovery method	Parsing

Attribute	Description
Record Name	The name of the file or folder as stored in the .DS_Store file.
Record Type	The type of the record, or property, that is being logged in the .DS_Store file for a particular file or folder.
Record Value	The value of the property for the given file or folder.
Record Path	The full path to the file or folder.
.DS_Store Created Date/Time - UTC (yyyy-mm-dd)	The created date of the .DS_Store file from which the record was extracted.
.DS_Store Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date of the .DS_Store file from which the record was extracted.
.DS_Store Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date of the .DS_Store file from which the record was extracted.

Additional Information

In the Apple macOS operating system, .DS_Store (Desktop Services Store) is a hidden file that stores the display information of its containing folder, similar to the file desktop.ini in Microsoft Windows. The file tracks information such as icon positions, view settings, cached file size, cached last modified date, and even the choice of a background image. The .DS_Store is created and maintained by the Finder application in any folder that it accesses, even on remote file systems mounted from servers that share files (for example, via Server Message Block protocol or the Apple Filing Protocol). .DS_Store files are also included in archives created by macOS users, such as ZIP files, and they are backed up by some cloud file backup services. This means that the presence of .DS_Store Records artifacts on non-Mac evidence such as Windows, mobile, or cloud indicates that some of the data may have

Additional Information
originated or have been accessed from a macOS computer at some point. For more information on .DS_Store files and their forensic significance see: .DS_Stores: Like Shellbags but for Macs.

Anacron Jobs

Description	Anacron jobs are used to execute tasks at a certain frequency on machines that may be powered off.
Recovery method	Parsing

Attribute	Description
Username	The username associated with the task.
Frequency	A description of how often the task is triggered.
Identifier	A specific job ID that is used when logging messages for the task.
Command	The command that will be performed when the task is triggered.
Command Shell	The path to the shell file that is used when the task is triggered.
Paths	An environment variable that specifies the paths of the directories used when the task is triggered.

Additional Information

Bash / ZSH Sessions

Description	Bash / ZSH Sessions contains information about terminal/Bash on a Linux computer, and the commands that are run during each session.
Recovery method	Parsing

Attribute	Description
Session ID	The ID of the session.
User	The user that started the session.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the session started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the session ended.
Session Command History	The command history of the session.

Additional Information

Cron Jobs

Description	Cron jobs are used to execute tasks at a certain frequency on continuously running machines.
Recovery method	Parsing

Attribute	Description
Username	The username associated with the task.
Frequency	A description of how often the task is triggered.
Cron Frequency	The cron expression used to specify the task's frequency.
Command	The command that will be performed when the task is triggered.
Command Shell	The path to the shell file that is used when the task is triggered.
Paths	An environment variable that specifies the paths of the directories used when the task is triggered.

Additional Information

CUPS Print Jobs

Description	CUPS Print Jobs contains records of print jobs that were created by the Common Unix Printing System (CUPS).
Recovery method	Parsing

Attribute	Description
Job ID	The ID of the print job.
Job Name	The name of the print job.

Attribute	Description
Job UUID	The UUID of the print job.
Owner	The owner of the print job.
Application	The application that triggered the print job.
Cached File Name	The name of the cached file to print.
Document Format	The format of the document for the print job.
Copies	The number of copes that the user selected for printing.
Sheets Printed	The actual number of sheets that were printed.
Origin Host Name	The origin host name of the print job request.
Destination Printer	The printer used for the print job.
Printer URI	The URI of the printer used for the print job.
State	The state of the print job.
Printer State Message	The printer state message.
Printer State Reason	The printer state reason.
Created Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the print job was created.
Processed Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the print job was processed.
Completed Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the print job was completed.
Attachment	The cached document that was sent for printing, if it's available.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

File Signature Mismatch (Audio)

Description	File Signature Mismatch (Audio) contains identified mismatches between a known file signature header and the extension (or lack thereof) for an audio file. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Container)

Description	File Signature Mismatch (Container) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a container. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Document)

Description	File Signature Mismatch (Document) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a document. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

File Signature Mismatch (Picture)

Description	File Signature Mismatch (Picture) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a picture. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file. If the MIME type is unknown, this defaults to application/octet-stream.

Attribute	Description
File Extension Type	The identified MIME type of the extension of the file. If the MIME type is unknown, this defaults to application/octet-stream. If there is no file extension, but the MIME type is known, a mismatch is is returned.
File Path	The path to the mismatched file.

File Signature Mismatch (Video)

Description	File Signature Mismatch (Video) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a video. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Notes	

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

File System Information

Description	Information pertaining to the File System that was searched
Recovery method	Parsing

Attribute	Description
Volume Serial Number	This field only applies to FAT and NTFS file systems. This is a 32-bit unsigned int value that is stored in Bios Paramter Block (BPB) and is showed in a special hex format ï¿½ XXXX-XXXX (e.g. EABB-6573). For other file systems, the value of this field should show "n/a".
Full Volume Serial Number	This field is a 64-bit volume serial number that is only present in BPB of NTFS file system, such as AABBCCDDEEFF0011. For non-NTFS file systems, "n/a" is displayed for this field.
File System	The type of the file system (e.g. "Microsoft NTFS").
Sectors per cluster	The number of sectors in a file system cluster (e.g. 8).
Starting Sector	The starting sector for this partition.
Ending Sector	The ending sector for this partition.
Total Sectors	Encase shows different values for this field based on how a volume is added to the case. For example, if you add just a volume (e.g. your local C:\ drive), the number of sectors is 12341027. However, if you add your local physical drive 0 to the case and then select your C:\ volume in the "Entries" tree (note that your C drive would most likely have another letter in this tree, such as E:), then the total number of sectors would be one more that the other value (i.e. 123410272). The value shown for this field is taken from BPB, which matches the first value. The other value is shown

Attribute	Description
	when the parent physical drive is present probably comes from the partition table, and it counts VBR as well.
Total Capacity	This value is calculated by multiplying the Total Clusters value by the Cluster Size value, which shows the capacity of the file system and not the volume containing it. The size of the volume would be higher than this value.
Total Clusters	The number of clusters comprising the file system.
Unallocated	The number of unallocated bytes on the file system, which is calculated by multiplying the number of free clusters by the cluster size.
Free clusters	The number of unallocated clusters in the file system.
Allocated	This value is determined by multiplying the allocated clusters by the cluster size.
Volume Name	This is the volume label stored in Volume Boot Record (VBR).
Volume Offset	The offset (in bytes) of the volume containing this file system from beginning of the disk. "0" is displayed if the image and/or drive being searched is the image of one volume. Encase shows the number of sectors for this field instead of the number of bytes.

Additional Information

Network Interfaces - Linux

Description	Network Interfaces lists all network interfaces and their DHCP leases assigned by the local DHCP server.

Recovery method	Parsing

Attribute	Description
Adapter Name	The name of the network adapter.
IPv4 Address	The IPv4 address of the interface.
IPv4 Subnet Mask	The IPv4 subnet mask of the interface
DNS Server(s)	The DNS server associated with this interface.
DHCP Server	The DHCP server associated with this interface.
Domain	The DNS domain of this interface.
Lease Obtained Date/Time - UTC (yyyy-mm-dd)	The date and time that the lease was obtained on this interface.
Lease Expires Date/Time - UTC (yyyy-mm-dd)	The date and time that the lease will expire on this interface.

Additional Information

Operating System Information - Linux

Description	This table contains information about the Linux installation.
Recovery method	Parsing

Attribute	Description
Operating System	The name of the operating system.
Operating System Version	The version of the operating system.
Local Hostname	The local hostname of the computer.
Adapter Name	The name of the network adapter device hosting the connection.
DHCP DNS Server(s)	A comma separated list of the DHCP assigned DNS servers. This fragment represents the Domain Name Server(s) (DNS) provided from the DHCP service.
IP	The local network IP address assigned to this computer.
Timezone	The current timezone of the computer.

Additional Information

Recent Files - Linux

Description	The Recent Files - Linux artifact contains information about the files that are accessed by a user. Most Linux distros store this information in XML format in the following location: ($home/.local/share/recently-used.xbel).
Recovery method	Parsing

Attribute	Description
File Path	The path to the file that was accessed.
MIME Type	The MIME type of the file that was accessed.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created.
Application Name	The name of the application that was used to access the file.
Command	The shell command used to access or execute the file, if applicable.
Application Run Count	The number of times the user has accessed the file.

Additional Information

SSH Authorized Keys

Description	SSH Authorized keys are pre-configured keys used for logging into user accounts.
Recovery method	Parsing

Attribute	Description
Options	The list of options for the authorized key. This may be empty.
Encryption	The type of encryption used for the public key.
Public Key	The encrypted public key.
Comment	The comment added by the user for the authorized key. This may be empty.

Additional Information

SSH Keys

Description	SSH Keys are used to perform secure activities over the internet.
Recovery method	Parsing

Attribute	Description
File Name	The name of the SSH Keys file.
Type	The type of the SSH Key, either Public or Private.
Encryption	The type of encryption used on the SSH Key.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the file system.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the file system.
File System Last Accessed Date/Time -	The date and time when the file was last

Attribute	Description
UTC (yyyy-mm-dd)	accessed on the file system.
File Content	The contents of the SSH Key file.

Additional Information

SSH Known Hosts

Description	SSH Known Hosts are public keys used to verify the identity of remote hosts. These are often automatically populated when the user connects to a host for the first time, but they can also be added manually.
Recovery method	Parsing

Attribute	Description
Host Names	The name or names of the specified host.
Marker	An optional tag used to indicate whether the host is a certificate authority.
Encryption	The type of encryption used for the public key.
Public Key	The encrypted public key.
Comment	The comment added by the user for the known host. This may be empty.

Additional Information

Startup Items - Linux

Description	Startup Items contains the configured auto-run scripts for the system at startup.
Recovery method	Parsing

Attribute	Description
Name	The name of the startup script file.
File Path	The path to the startup script file.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the script file was created.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the script file was last accessed.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the script file was last modified.
File Content	The contents of the script file.

Additional Information

System Logs - Linux

Description	System Logs contains the operating system-generated logs stored on the machine.

Recovery method	Parsing

Attribute	Description
File Path	The path to the system log file.
Log Date/Time - Local Time	The date and time that the log entry was written.
User Name	The user name of the user the logging application ran under.
Process Name	The name of the process that generated the log entry.
Process ID	The id of the process that generated the log entry.
Message	The log message.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

System Services - Linux

Description	The System Services artifact lists the current services that exist on the system.
Recovery method	Parsing

Attribute	Description
Name	The service name.
File Path	The path to the service definition file.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the service file was created.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the service file was last accessed.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the service file was last modified.
File Content	The contents of the service definition file.

Additional Information

Trash Items

Description	Trash Items contains information about the items that a user has sent to the trash. This artifact recovers both deleted files and deleted directories.
Recovery method	Parsing

Attribute	Description
Item Name	The name of the file or directory that has been deleted.
Item Type	The type of the deleted item. This can be Folder, File, or Item not found.

Attribute	Description
File Type	The extension of the file. This attribute is not populated for directories and files with no extensions.
File Size (Bytes)	The size of the file in bytes.
Original Path	The original path of a file or directory recovered from the .trashinfo file. This path is used for restoring files to their original location. Note that the original path of a folder is used as a starting point to which the relative path of each item found inside is appended.
Deleted Date/Time - Local Time (yyyy-mm-dd)	The date and time that a file or directory was added to the trash bin. This is recovered from the .trashinfo file.
Deleted Date/Time - Local Time (Format Unknown)	The date and time that a file or directory was added to the trash bin. This is recovered from the .trashinfo file.
Data	The preview card.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

User Accounts

Description	User Accounts contains user accounts information pulled from Linux system files.
Notes	

Attribute	Description
User Name	The username of the account.
Password Hash	A hash of the user's password.
Password Hash Algorithm	The algorithm used to generate the user's password hash.
Last Password Change Date/Time - UTC (yyyy-mm-dd)	The date and time that the user last changed their password.
User ID	The user's ID.
Group ID	The user's security group ID.
Account Description	A description of the account.
Home Directory	The user's home directory.
Command Shell	The base directory for shell commands.

User Accounts - Linux

Description	User Accounts contains user accounts information pulled from Linux system files.
Recovery method	Parsing

Attribute	Description
User Name	The username of the account.
Password Hash	A hash of the user's password.
Password Hash Algorithm	The algorithm used to generate the user's password hash.
Last Password Change Date/Time - UTC (yyyy-mm-dd)	The date and time that the user last changed their password.
User ID	The user's ID.
Group ID	The user's security group ID.
Account Description	A description of the account.
Home Directory	The user's home directory.
Command Shell	The base directory for shell commands.

Additional Information

Wi-Fi Logs - Android

Description	Wi-Fi Logs - Android contains information about the Wi-Fi networks that a device has connected to.
Recovery method	Parsing

Attribute	Description
Network Name (SSID)	The name of the saved network.
BSSID	A unique identifier for the specific access point, which is often represented as the MAC address for the access point's wireless adapter.
Date/Time - Local Time (yyyy-mm-dd)	The date and time of the network connection. In instances where the year is missing from the source data, this value is represented as a string instead of a date/time.
First Connected Date/Time - Local Time (yyyy-mm-dd)	The date and time of the connection event.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Volatile Artifacts

Active Connections

Description	Active Connections contains a list of all active and inactive connections, as well as the TCP and UDP ports the device is currently listening to.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
Protocol	The protocol used for the connection (UDP/TCP).
Local Address	The local address of the connection. This value can either be IPv4 or IPv6.
Local Port	The port that the connection is originating from.
Remote Address	The remote address of the connection. This value can either be IPv4 or IPv6.
Remote Port	The port that the connection is heading to.
State	The state of the connection.
Process ID	The process ID of the connection.

Additional Information

DNS Cache

Description	DNS Cache contains a list of all the cached DNS Records for the device.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-	The date and time that the information was cap-

Attribute	Description
dd)	tured.
Record Name	The name of the DNS record.
Record Type	The DNS record type.
Record Type ID	The DNS record type's ID.
Length	The length of the record in bytes.
Record Value	The value of the DNS record.

Additional Information

Network ARP Info

Description	Network ARP info contains a list of cached Address Resolution Protocol (ARP) entries.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
Local IP Address	Local IP address for the ARP cache entry.
Local MAC Address	Local MAC Address for the ARP cache entry.

Attribute	Description
Type	Type of ARP cache entry.
Seconds since ARP entry used	Number of seconds since the ARP entry was used. Fragment only populated for Linux.
Seconds since ARP entry confirmed	Number of seconds since the ARP entry was confirmed. Fragment only populated for Linux.
Seconds since ARP entry updated	Number of seconds since the ARP entry was updated. Fragment only populated for Linux.

Additional Information

Running Processes

Description	Running Processes contains a list of all processes currently running on the endpoint.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
Process Name	The name of the process.
Process ID	The process ID (PID).
User Name	The owner of the process.

Attribute	Description
Session ID	The associated session ID.
Session Name	The name of the associated session.
Memory Usage (KB)	The amount of memory used by the process, indicated in KB.
CPU Time (dd.HH:mm:ss.ff)	The amount of time that the CPU has been running the process. Shown in dd.HH:mm:ss.ff format.
Command Line Call	The call to the command line that started the process.
Status	The status of the process.
Parent Process ID	The ID of the parent process (PPID).

Additional Information

Services

Description	Service List contains a list of all services currently running on the endpoint.
Recovery method	Parsing

Attribute	Description
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the information was captured.
Service Name	The name of the service.

Attribute	Description
State	The state of the service.
Process ID	The process ID (PID).
Description	The description of the service.

Additional Information

Web Related

Google Analytics First Visit Cookies

Description	Google Analytics First Visit Cookies contains information about Google Analytics first-visit cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Creation DateTime	The date and time when the site was first visited.
Most Recent Visit Date/Time	The date and time of the most recent session.
2nd Most Recent Visit Date/Time	The date and time of the previous session.
Hits	The number of visits.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics First Visit Cookies Carved

Description	Google Analytics First Visit Cookies Carved contains information about Google Analytics first-visit cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Creation DateTime	The date and time when the cookie was created.
Most Recent Visit Date/Time	The date and time of most recent session.
2nd Most Recent Visit Date/Time	The date and time of the previous session.
Hits	The number of visits.

Additional Information

Google Analytics Referral Cookies

Description	Google Analytics Referral Cookies contains information about Google Analytics referral cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Cookie Source	The source URL used to reach the site.
Host	The domain of the URL.
Update Date/Time	The last time that the cookie was updated.
Campaign	The method of referral.
Access Method	Indicates whether the site was accessed organically or was referred.
Keyword	The keywords used to arrive at the site.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics Referral Cookies Carved

Description	Google Analytics Referral Cookies Carved contans information about Google Analytics referral cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Cookie Source	The source URL used to reach the site.
Host	The domain of the URL.

Attribute	Description
Update Date/Time	The last time that the cookie was updated.
Campaign	The method of referral.
Access Method	Indicates whether the site was accessed organically or was referred.
Keyword	The keywords used to arrive at the site.

Additional Information

Google Analytics Session Cookies

Description	Google Analytics Session Cookies contains information about Google Analytics session cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start time of the current sesion.
Outbound Link Events Left	
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics Session Cookies Carved

Description	Google Analytics Session Cookies Carved contains information about Google Analytics session cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start date and time of the current sesion.
Outbound Link Events Left	

Additional Information

Google Analytics URLs

Description	Google Analytics URLs contains URLs that are discovered in other artifacts that are related to Google Analytics.
Recovery method	Carving

Attribute	Description
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	The domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics URLs Carved

Description	Google Analytics URLs Carved contains information about Google Analytics URLs that are recovered using carving.
Recovery method	Carving

Attribute	Description
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	The domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.

Additional Information

Google Maps

Description	Google Maps is a free web service that allows users to get directions.
Notes	

Attribute	Description
Search Query	The term that was searched for.
Starting Location	The starting location for navigation/directions.
Center of Map	Indicates where the map was centered.

Attribute	Description
Business Latitude and Longitude	The latitude and longitude of the business location.
Source Address	The source physical address.
Destination Address	The user's desired destination.
Route Type	Indicates how the user will travel (e.g. Car, bus, or bike).
Additional Address	Any additional addresses within the navigation.
Street View Latitude/Longitude	The latitude and longitude information in street view.

Google Maps Tiles

Description	Google maps is a free web service that allows users to get directions.
Notes	

Attribute	Description
Image	The actual picture content.
X Coordinate	The X coordinate value that Google uses to download the right tile.
Y Coordinate	The Y coordinate value that Google uses to download the right tile.
Zoom Level	The level that the user was zoomed in to the map. This value is the Z coordinate value that Google uses to download the right tile.

IP Addresses - Audio/Video Calls

Description	IP Addresses of web audio/video calls show who a user was com-

municating with. Each instance of this artifact represents a single hop in the communication chain. By showing the relationship between multiple hops, you can determine where a call originated from and what the final destination was.

Notes

Attribute	Description
Call ID	The ID of the call.
Message ID	The ID of the message.
Domain	The domain used for the call.
Connection Type	The type of connection.
Origin IP Address	The originating IP address for this hop in the call.
Origin Port	The originating port for this hop in the call.
Destination IP Address	The destination IP address for this hop in the call.
Destination Port	The destination port address for this hop in the call.
Date/Time - UTC (yyyy-mm-dd)	The timestamp associated with this hop in the call.
Remote User ID	The unique ID of the remote user.
Communication Protocol	The communication protocol for this call (either UDP or TCP).
Metadata	Any additional details about the call.

YARA Rules

YARA Rule Matches

Description	The YARA artifact contains information about files and processes that matched with conditions specified in a YARA rule.
Recovery method	Parsing

Attribute	Description
File Name	The name and extension of the file whose content matched with the condition(s) from the YARA rule. The value is blank if the match came from a process (executable/application that was loaded into memory at the time of the memory dump) during memory analysis using the Comae plugin option.
File size (bytes)	The size of the file in bytes. The value is blank if the match came from a Process.
Process Name	The name of the process that matched with the condition(s) from the YARA rule. The value is blank if the match came from a file.
Process ID	The ID of the process (PID). The value is blank if the match came from a File.
Matched rule set(s)	List of the paths and respective YARA rule sets that had a match.
Matched rule	The YARA rule name that a match was found for.
Matching conditions	List of conditions for the YARA rule that had a match.

Additional Information

Cloud

Application Usage

Cloud Google Activity

Description	Cloud Google Activity contains Google activity entries retrieved from the Google Activity website.
Recovery method	Parsing

Attribute	Description
Action	The type of activity that occurred. For example, Visited or Searched for.
Description	Information about the activity. For example, the title of the website or the search criteria used.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the activity. This fragment is populated if the data was recovered using a live acquisition of the account.
Date/Time - Local Time (yyyy-mm-dd)	The date and time of the activity. This fragment is populated if the data was parsed from a Google Takeout export.
URL	The URL of the visited page.
Platform	The operating system or platform where the activity occurred. For example: Windows, Chrome OS, or Apple iPhone.
Latitude	The latitude of the location where the activity occurred.

Attribute	Description
Longitude	The longitude of the location where the activity occurred.
Attachments	The path to the downloaded file.
Attachment	The path to the file in the Cloud image.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Cloud Google Connected Apps

Description	Google Connected Apps recovered from the Cloud.
Recovery method	Parsing

Attribute	Description
Application Name	The name of the application.
Permissions	The application access permissions.
Authorization Date - Local Time	The date that authorization to use the application was granted.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Cloud Storage

Cloud Amazon EC2 Instances

Description	EC2 instances are virtual machines that corporations use for hosting secure services and storing data securely in the cloud. To acquire this data, Magnet AXIOM exports this instance to Amazon's S3 service and downloads it from there.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file after it's exported from EC2.
Instance ID	The unique ID of the EC2 instance.
Instance State	The status of the EC2 instace (running, stopped, or terminated).
Owner ID	The numerical ID of the user who launched the EC2 instance.
Instance Creation Date/Time	The date and time when the user launched the EC2 instance.
IP Address	The private IP address of the user who launched the EC2 instance.
Region	The region where the instance was launched.
Instance Type	The type of EC2 instance.
AMI ID	The ID of the AMI (Amazon Machine Image) with which the instance was launched.
Key Name	The name of the key pair that must be used to login to the instance

Attribute	Description
	securely.
File Path	The path from the root of S3 to the exported image.
Attachment	The path to the downloaded file.

Additional Information

Cloud Amazon S3 Files

Description	Cloud Amazon S3 Files contains information about files that are stored in Amazon S3 and are recovered from the cloud. Amazon S3 is a file hosting service that allows users to upload and sync files to the cloud and access them from multiple locations.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file on Amazon S3.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the file was last modified.
Owner Name	The username of the account that created the file.
Object Lock Legal Hold Status	The object lock status for the file.
Object Lock Retain Until Date/Time	The object lock retention date for the file.

Attribute	Description
Expiration Date/Time - UTC (yyyy-mm-dd)	The expiration date for the file.
Metadata	The metadata for the file.
S3 Tags	The list of tags for the file.
Storage Class	The Amazon S3 storage class of the file.
Version ID	The version ID of the file.
File Path	The file path of the file.
Attachment Name	The name of the attachment.
Attachment	The raw data of the file.

Additional Information

Cloud Azure Virtual Machine Snapshots

Description	Azure virtual machines are on-demand computing resources used by organizations for hosting services and storing data securely in the cloud. To acquire this data, Magnet AXIOM creates snapshots of all disks attached to a given virtual machine, and downloads the snapshots for analysis.
Recovery method	Parsing

Attribute	Description
Resource ID	The fully-qualified ID of the virtual machine resource.
Snapshot Name	The name of the snapshot created during processing.
Parent Virtual Machine Name	The name of the virtual machine that this disk belongs to.
Region	The region the targeted virtual machine was deployed to.
Disk Type	Indicates whether the targeted disk is an operating system disk or an attached data disk.
Disk Capacity in Gigabytes	Maximum capacity for the targeted disk in gigabytes.
Disk Creation Date/Time UTC	The date/time the disk was created and assigned to the targeted virtual machine (in UTC).
Snapshot Creation Date/Time UTC	The date/time that the disk snapshot was created (in UTC).
Attachment	The name of the snapshot downloaded as a VHD file.

Additional Information

Cloud Box.com Enterprise Events

Description	The Cloud Box Enterprise event contains information about administrative events that are triggered by user actions. Some examples of events include new user creation, successful login, and item syncs. You can see a full list at https://developer.box.com/v2.0/reference#enterprise-events.

Recovery method	Parsing

Attribute	Description
Initiator	The email address of the user the initiated the event.
Event Type	The type of the event that was created (for example, 'NEW_USER').
Subject	The email address of the user that was the subject of the event.
Server Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was initiated.
ID	The ID of the event.
IP Address	The IP address of the user that initiated the event.
Type	The type of the item that was targeted by the event (always a user or nothing).
Initiator Name	The name of the user that initiated the event.
Initiator ID	The ID of the user that initiated the event.
Subject Name	The name of the user that was the subject of the event.
Subject ID	The ID of the user that was the suject of the event.

Additional Information

Cloud Box.com Files

Description	Files that are stored in Box that are recovered from the cloud. Box is a file hosting service that allows users to upload and sync files to the cloud and access or share them from multiple locations.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
Description	The description attached to a file through Box.
File Size (Bytes)	The size of the file, in bytes, according to Box.
Type	The type of the file. Value is either 'file' or 'folder'.
Attachment Path	The path of an attachment.
Box File Path	The filepath of the file.
Attachments	The path to the downloaded file.
Attachment	The path to the file in the Cloud image.
Server Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the server.
Creator Name	The name of the original uploader of the file.
Creator Email Address	The email address of the original uploader of the file.

Attribute	Description
Creator ID	The unique Box ID of the original uploader of the file.
Server Modified Date/Time - UTC (yyyy-mm-dd)	The file's last modified date and time on the box.com server.
Last Modifier Name	The name of the latest user to modify the file.
Last Modified Email	The last modifying user's email address.
Last Modifier ID	The unique Box ID of the latest user to modify the file.
Owner Name	The name of the owner of the file.
Owner Email	The email address of the owner of the file.
Owner ID	The unique Box ID of the owner of the file.
Download Count	The number of times the file has been downloaded via a share link. This does not include downloads performed by API calls.
Preview Count	The number of times the file has been previewed via a share link.
Collaborator Emails	Email Address of Collaborators on the file.
Access	The permissions setting a file's share link. Null if no share link exists, 'open' if anyone with the link can access, and 'collaborators' if only collaborators on the file can access.
Download Permissions	True if users can download the file through a share link.

Attribute	Description
Preview Permissions	True if users can preview the file through a share link.
File Hash	The file's SHA1 hash, provided by Box.
File ID	The file's unique Box ID.
Revision ID	The unique identifier of the revision.

Additional Information

Cloud Box.com User Events

Description	The Cloud Box User Events artifact contains information about actions that are triggered by the user. Some examples of events include item creation, upload, and download. You can see a full list of events at https://developer-.box.com/v2.0/reference#user-events.
Recovery method	Parsing

Attribute	Description
Name	The name of the user that caused the event creation.
Event Type	The type of event that occurred (for example, 'ITEM_CREATE').
File Name	The name of the file that was targeted by the action/event.

Attribute	Description
File Path	The path to the folder that was targeted by the action/event.
Server Created Date/Time - UTC (yyyy-mm-dd)	The date and time in which the event was created.
Server Recorded Date/Time - UTC (yyyy-mm-dd)	The date and time in which the event was recorded.
User	The email address of the user that initiated the event.
User ID	The ID of the user that initiated the event.
Type	The type of the item that was targeted by the action (usually file or folder).
Source ID	The ID of the item that was targeted by the action.
ID	The ID of the user that initiated the event.

Additional Information

Cloud Dropbox Files

Description	Files that are stored in Dropbox that are recovered from the cloud. Dropbox is a file hosting service that allows users to upload and sync files to the cloud and access them from multiple locations.
Recovery method	Parsing

Attribute	Description
File Name	The original name of the file.
File ID	A unique identifier for the file.
Dropbox File Path	Path of the file in Dropbox
Server Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the server.
Client Modified Date/Time - UTC (yyyy-mm-dd)	The file's last modified date and time on the client application.
Photo Timestamp Date/Time - UTC (yyyy-mm-dd)	If the file is a photo, the date and time the photo was originally taken
File Hash	The hash of the file generated by Dropbox. For more information, see https://www.dropbox.com/developers/reference/content-hash.
File Version ID	The version ID of the file. This value is used to determine if there are any updates on the server that need to be synced locally.
File Type	The type of file
Attachments	The path to the downloaded file.
Attachment	The path to the file in the Cloud image.
Shared By	The email address of the user that shared the file.
Shared With	The email address(es) of the user(s) with whom the file has been shared.

Additional Information

Cloud Google Drive Activity

Description	Google Drive Activity contains information about actions performed on Google Drive files, folders, and drives.
Recovery method	Parsing

Attribute	Description
User	The user peforming the action.
Email	The user's email.
User ID	The unique identifier for the given user.
Actor Type	The type of actor performing the action, e.g. User, Impersonation, Anonymous, etc.
Date/Time	The time when the activity occurred.
Start Date/Time	The time when the activity started.
End Date/Time	The time when the activity ended.
Action	The activity performed by the user.
Action Type	The sub-category of the action performed.
File Name	The name of the file being acted upon.
File ID	The unique identifier for the file.

Attribute	Description
Old Value	The previous name of the item.
New Value	The new name of the item after the action was performed.
Source Name	The name of the item copied from.
Source ID	The unique identifier of the item copied from.
Mentions	The users referred to in a comment.
Origin Folder	The previous location(s) the target item was stored.
Destination Folder	The new location(s) the target item is stored.
Added Permissions	The permissions added to the target item.
Removed Permissions	The permissions removed from the target item.
Settings Changes	Setting changes made on the taget user account.
Folder Name	The name of the folder being acted upon.
Folder ID	The unique identifier for the folder.
Drive Name	The name of the drive being acted upon.
Drive ID	The unique identifier for the drive.
Comment ID	The unique identifier for a comment.
MIME Type	The mime type of the item.

Additional Information

Cloud Google Drive File Version History

Description	Cloud Google Drive File Version History contains file revisions that are stored in Google Drive and are recovered from the cloud. Google Drive is a file hosting service that allows users to upload and sync files to the cloud and access them from multiple locations.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file on Google Drive.
Original File Name	The name of the file used to create this revision.
Revision ID	The unique identifier of the revision. This can be an alphanumeric string or numeric value if the file in question does not have binary content in Drive.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the revision was modified.
Last Modified Name	The name of the last user to modify the revision.
Last Modified Email	The last modifying user's email address.
Last Modified ID	The last modifying user's ID.
MD5 Hash	The MD5 checksum of the revision's content.
File Size (Bytes)	The file size. This may be a false size of 0 if the file in question has no binary content in Google Drive.

Additional Information

Cloud Google Drive Files

Description	Cloud Google Drive Files contains files that are stored in Google Drive that are recovered from the cloud. Google Drive is a file hosting service that allows users to upload and sync files to the cloud and access them from multiple locations.
Recovery method	Parsing

Attribute	Description
ID	The ID of the file that was assigned by Google Drive.
File Name	The name of the file on Google Drive.
Folder Structure	The folder structure that the file resides in.
Drive Owner	The owner of the Google drive (e.g. testing@gmail.com).
Owner Name	The name of the author of the file.
Owner Email	The email address of the author of the file.
Shared	The number of accounts that the file is shared with.
MIME Type	An identifier that is used to described the type and format of the file (for example text/plain). For more information, see https://en.wikipedia.org/wiki/Media_type.
File Size (Bytes)	The file size.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created.
Last Viewed By Me Date/Time - UTC (yyyy-mm-dd)	The last date and time that the file was viewed by the user.
Last Modified By Me Date/Time - UTC (yyyy-mm-dd)	The last date and time that the file was modified by the user.
Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the file was modified.
Last Modified Name	The name of the last user to modify the file.
Last Modified Email	The last modifying user's email address.
Shared With Me Date/Time - UTC (yyyy-mm-dd)	The time when the file was shared with the user.
Trashed Date/Time (Team Drives) - UTC (yyyy-mm-dd)	The time that the file was trashed. This field is only populated for Team Drive files.
Source Locations	A list of the spaces where the file exists. The supported values are drive, appDataFolder, and photos.
Parent Folder	The parent of the folder where the file resides.
Web URL	The direct URL to the file.
Download URL	The direct URL to download the file.

Attribute	Description
Attachments	The raw data of the file.
Attachment Path	The path of an attachment.
Attachment	The path to the file in the Cloud image.

Additional Information

Cloud Google Workspace Drive Audit Events

Description	Google Workspace Drive Events contains event information about the Google Drive activity on a Google Workspace domain.
Recovery method	Parsing

Attribute	Description
ID	The unique identifier for each activity record.
Event Type	Type of the event.
Event Name	The name of the event.
Event Date/Time - UTC (yyyy-mm-dd)	The time when the activity occurred.
Actor Email	The primary email address of the actor. This value may be absent if there is no email address associated with the actor.

Attribute	Description
Actor Profile Id	The unique Google Workspace profile ID of the actor. This value may be absent if the actor is not a Google Workspace user.
Actor Caller Type	The type of actor.
Actor Key	The consumer_key of the requestor for OAuth 2LO API requests or an identifier for robot accounts.
Owner Domain	The domain that is affected by the report's event. For example, the domain of the Admin console or the Drive application's document owner.
IP Address	The IPv4 or IPv6 IP address of the user performing the action.
Document Title	The document title.
Document Type	The type of the document.
Document Id	The document ID.
Owner	The email address of the document's owner.
Owner Is Team Drive	Indicates whether the document's owner is a team drive.
Team Drive Id	The unique identifier of the Team Drive. Only populated for for events relating to a Team Drive or item contained inside a Team Drive.
Is Primary Event	Indicates whether this is a primary event.
Billable	Indicates whether the event is billable.
Originating App Id	The Google Cloud Project ID of the application that performed the action.
Visibility	The current visibility setting of the target file.

Attribute	Description
Old File Visibility	The previous visibility setting of the target file.
Visibility Change	The change in visibility setting of the target file.
Destination Folder ID	The destination folder ID.
Destination Folder Title	The destination folder title.
Old Value	The old name of the event.
New Value	The new name of the event.
Target Domain	The domain for which the acccess scope was changed.
Target User	The email address of the user or group whose access permissions were changed, or the name of the domain for which access permissions were changed.
Team Drive Membership Change Type	The type of change in Team Drive membership for the user or group.
Removed Role	The membership role that was removed for a user or group in a Team Drive.
Target	The target user or group.
New Team Drive Settings State	The new state of team drive settings.
Old Team Drive Settings State	The old state of team drive settings.

Attribute	Description
Team Drive Settings Change Type	The type of change that occurred to the team drive settings.

Additional Information

Cloud Google Workspace Login Audit Events

Description	Google Workspace Login Events contains information about the events and parameters for login activity on a Google Workspace domain.
Recovery method	Parsing

Attribute	Description
ID	Unique identifier for each activity record.
Event Type	The type of event that occurred.
Event Name	The name of the event.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time that the event occurred.
Actor Email	The primary email address of the actor that initiated the event. This value may be absent if there is no email address associated with the actor.
Actor Profile Id	The unique Google Workspace profile ID of the actor. This values may

Attribute	Description
	be absent if the actor is not a Google Workspace user.
Actor Caller Type	The type of actor.
Actor Key	The consumer_key of the requestor for OAuth 2LO API requests or an identifier for robot accounts.
Owner Domain	The domain that is affected by the report's event. For example, the domain could be for the Admin console or the Drive application's document owner.
IP Address	IPv4 or IPv6 IP address of the user doing the action.
Login Type	The type of credentials used to attempt the login.
Login Challenge Methods	Method(s) used to verify the logon.
Login Challenge Status	Whether the login challenge succeeded or failed.
Login Failure Type	The reason for the login failure.
Is Suspicious	The login attempt had some unusual characteristics, for example the user logged in from an unfamiliar IP address.

Additional Information

Cloud iCloud Backups

Description	Backups of iOS devices that the user creates, and which are recovered

	from the cloud.
Recovery method	Parsing

Attribute	Description
Created Date	The date and time the backup was created.
User Name	The Apple ID used to sign in to the account.
Cloudkit User ID	User ID for the CloudKit account - can be paired with the CloudkitToken to make authenticated requests to Cloudkit services.
Cloudkit Token	Token for the CloudKit account - can be used to make authenticated requests to Cloudkit services.
iCloud Account ID	The ID of the iCloud account.
Mme Auth Token	Token can be paired with the iCloud Account ID to make requests for other iCloud services.
Device Name	Name of the iOS device used to make the backup.
Device Hash	A unique hash value for the device (created by Apple).
Device Class	The type of device (for example, iPhone or iPad).
Model	The device model (for example, N61AP).
Friendly Name	A more friendly, recognizable name for the device model (for example, iPhone 6).
Product Type	An internal product identifier used by Apple (for example, iPhone7,2 which actually corresponds to the iPhone 6).

Attribute	Description
Quota Used	The number of bytes used by the backup.
Serial Number	Serial number of the device.
Snapshot Hash	Unique identifier of the backup (created by Apple).
System Domains Version	Backup system version.
Device Hardware Version	Device Backup version.
iOS Version	iOS version.
Was Passcode Set	Indicates whether the device was locked when the backup was created (True or False).
Attachment	The path to the downloaded backup file.

Additional Information

If an iOS Backup is discovered during the search of an image or another folder, the backup will be searched as a mobile search with all artifacts. This method will likely recover many more results than loading an iCloud Backup.

Cloud iCloud Drive Files

Description	Files that are stored in iCloud Drive that are recovered from the cloud. iCloud Drive is a file hosting service that allows users to upload and sync files to the cloud and access them from multiple locations.

Recovery method	Parsing

Attribute	Description
File Name	The name of the file on iCloud Drive.
File Path	The folder path the file resides in.
Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the file was modified.
Uploaded Date/Time - Local Time (yyyy-mm-dd)	The local date and time the file was uploaded to iCloud Drive.
File Size (Bytes)	The file size.
Type	The file type, like 'FILE' or 'FOLDER'
Download URL	The direct URL to download the file.
ID	The ID of the file assigned by iCloud Drive.
Attachment Path	The path of an attachment.
Attachments	The raw data of the file.
Attachment	The path to the file in the Cloud image.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Cloud Mega Files

Description	Cloud Mega Files contains files that are stored in Mega that are recovered from the cloud. Mega is a file hosting service that allows users to upload and sync files to the cloud and access them from multiple locations.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
Owner User Name	The user name of the owner of the file.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was added to cloud storage.
Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the file was modified.
File Size (Bytes)	The file size in bytes.
File ID	The file ID.
Parent ID	The file parent ID.
Owner ID	The unique identifier of the owner of the file.
Attachment Path	The path of the file in the Cloud image.
Attachments	The name of the downloaded file.
Attachment	The path of the file in the Cloud image.

Additional Information

Cloud Microsoft Unified Audit Logs

Description	Cloud Microsoft Unified Audit Logs contains events from Microsoft Unified Audit Log. This artifact collects information from SharePoint, Azure, and Exchange. SharePoint collects ItemType, SiteUrl, SourceFileName, and DestinationFileName information. Azure collects ResultStatus, and Client information. Exchange collects ClientInfoString, LogonType, MailboxOwnerUPN, Subject, and ExternalAccess information.
Recovery method	Parsing

Attribute	Description
ID	The unique identifier of an audit record (available on SharePoint, Azure, and Exchange).
Type	The type of operation that is indicated by the record. See the AuditLogRecordType table for details on the types of audit log records (available on SharePoint, Azure, and Exchange).
User	The User Principal Name (UPN) of the user who performed the action (specified in the operation property) that resulted in the record being logged. An example of this is my_name@my_domain_name. The records for activity performed by system accounts (such as SHAREPOINT/system or NT AUTHORITY/SYSTEM) are also included (available on SharePoint, Azure, and Exchange).
Action	The name of the user or administrative activity. For a description of the most common activities, see Search the audit log in the compliance portal. For Exchange administrative activity, this property identifies the name of the cmdlet that was run. For DLP events, this can be DlpRuleMatch,

Attribute	Description
	DlpRuleUndo or DlpInfo (available on SharePoint, Azure, and Exchange).
Event Date/Time - UTC (yyyy-mm-dd)	The date and time (in UTC) when the user performed the activity (available on SharePoint, Azure, and Exchange).
Object ID	The full path name of the file or folder accessed by the user on SharePoint and OneDrive Business activity. The name of the object that was modified by the cmdlet on Exchange administrative audit logging (available on SharePoint, Azure, and Exchange).
IP Address	The IP address of the device that was used when the activity was logged. The IP address is displayed in either an IPv4 or IPv6 address format (available on SharePoint, Azure, and Exchange).
Content Type	The type of object that was accessed or modified. See the ItemType table for details on the types of objects (available on SharePoint).
Resource URL	The URL of the site where the file or folder accessed by the user is located.
Original File Name	The original state of the file name.
Updated File Name	The filename when updated.
Status	Indicates whether the action (specified in the Operation property) was successful or not. For SharePoint and Azure, possible values are Succeeded, PartiallySucceeded, or Failed. For Exchange admin activity, possible values are True or False (available on SharePoint, Azure, and Exchange).

Attribute	Description
Client	The client device information, provided by the browser performing the login (available on Azure).
Device Description	Information about the email client that was used to perform the operation, such as a browser version, Outlook version, and mobile device information (available on Exchange).
Access Method	Indicates the type of user who accessed the mailbox and performed the operation that was logged (available on Exchange).
Owner Email	The email address of the user who is associated to the mailbox that was accessed (available on exchange).
Subject	The subject line of the message that was accessed (available on exchange).
External Access	Specifies whether the cmdlet was run by a user in your organization, by Microsoft datacenter personnel or a datacenter service account, or by a delegated administrator. The value False indicates that the cmdlet was run by someone in your organization. The value True indicates that the cmdlet was run by datacenter personnel, a datacenter service account, or a delegated administrator (available on Exchange).
Data	Multi-value data for multiple properties from the audit log record. Each of the multi-value properties has value pairs (available on SharePoint, Azure, and Exchange).

Additional Information

Cloud OneDrive File Version History

Description	Cloud Office 365 OneDrive File Version History contains information about previous versions of a file stored on OneDrive.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file on OneDrive.
Version Number	The version number of the file.
File Path	The path of the selected file.
Last Modified Name	The name of the person who last modified the file.
Last Modified Email	The email of the person who last modified the file.
Last Modified ID	The ID of the person who last modified the file.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last modified.
File Size (Bytes)	The file size in bytes.

Additional Information

Cloud OneDrive Files

Description	Cloud OneDrive Files contains files that are stored in OneDrive that are recovered from the cloud. OneDrive is a file hosting service that allows users to upload and sync files to the cloud and access them from multiple locations.
Recovery method	Parsing

Attribute	Description
File ID	The file ID on OneDrive.
File Name	The name of the file on OneDrive.
File Type	The type of file.
File Path	The path to the file on OneDrive.
File Size (Bytes)	The file size in bytes.
Owner ID	The unique identifer of the owner of the file.
Owner Name	The name of the owner of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was created.
Last Modified Name	The name of the person who last modified the file.
Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the file was modified.
Shared With Root User	Indicates whether the file was shared with the root user.

Attribute	Description
Sharing Scope	Indicates whom the file is shared with. E.g. Specific users.
Attachments	The path to the downloaded file.
Attachment	The path to the file in the Cloud image.

Additional Information

Communication

Cloud Apple Contacts

Description	Cloud Apple Contacts contains information about the contacts and services that a user has saved to their Apple account.
Recovery method	Parsing

Attribute	Description
Display Name	The display name of the contact.
Nickname	The nickname of the contact.
Birthday (yyyy-mm-dd)	The birth date of the contact.
Email Address(es)	The email addresses of the contact.
Mobile Phone	The mobile phone number of the contact.

Attribute	Description
Home Phone	The home phone number of the contact.
Home Address	The home address of this contact.
Title	The job title of this contact.
Organization	The organization or business that is associated with the contact.
Business Phone	A business phone number for the contact.
Business Address	The physical address of the business that is associated with the contact.
Phone Numbers	Any other phone numbers that are associated with the contact, excluding any home, business or cell phone number.
Additional Address	Any additional addresses associated with the contact.
Website URL	A list of website URLs that are associated with the contact.
Labels	Any tags that are associated with the contact (also known as labels).
Photo	The photo of the contact.
Relations	The relations of the contact.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date of the vcf file.

Additional Information

Cloud Apple iMessages

Description	Apple iMessages acquired from the cloud.
Recovery method	Parsing

Attribute	Description
Sender	The identifer of individual who sent the message.
Recipient	The recipient list of individuals who received the message.
Message Date/Time - UTC (yyyy-mm-dd)	The sent date and time of the message if the Service value is: SMS. The received date and time of the message if the Service value is: iMessage.
Message	The text content of the message.
Subject	The subject of the message.
Message ID	The identifier of the message.
Service	The service that delivers the message (SMS or iMessage).
Type	The type of the message.
Attachment	The attachment of the message.
Attachment Name	The file name of the attachment.

Additional Information

Cloud Apple iMessages (Warrant Return)

Description	Apple iMessages parsed from a Apple Warrant Return archive.
Recovery method	Parsing

Attribute	Description
Message Sender	The identifier of the individual who sent the message.
Chat ID	The identifer of the conversation, which the message belongs to.
Message Body	The text content of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The sent date and time (in UTC) of the message.
Message SVC	The type of the message.
User Account	The identifier of the individual who is the local user of the conversation
Message Delivered Date/Time - UTC (yyyy-mm-dd)	The delivered date and time (in UTC) of the message.
Message Read Date/Time - UTC (yyyy-mm-dd)	The read date and time (in UTC) of the message.
Message Played Date/Time - UTC (yyyy-mm-dd)	The played date and time (in UTC) of the message.
Message GUID	The unique identifer of the message.

Attribute	Description
Subject	The subject of the message.
Device ID	The unique identifier of the device which sent the message.

Additional Information

Cloud Facebook Messenger Messages

Description	Cloud Facebook Messenger Messages contains Facebook Messages recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Sender Name	The username of the person who sent the message.
Author ID	The unique Facebook ID of the author of the message.
Text	The content of the message.
HTML Body	The HTML body of the message.
Participants	The display names of the participants in the conversation.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Attachments	The file names of any locally downloaded files.

Attribute	Description
Attachment	The path to the file in the Cloud image.
Message Type	The type of the message (examples include 'Generic' which indicates a standard message, 'Call', and 'Share').

Additional Information

Cloud Google Chat (Takeout, Warrant Return)

Description	Google Chat parsed from a Google Takeout or Warrant Return archive.
Recovery method	Parsing

Attribute	Description
Creator Name	The message creator name.
Creator Email Address	The message creator email address.
Creator User Type	The message creator user type.
Participants	The conversation participants.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was created.
Text	The text content of the message.
Conversation ID	The generated ID of a conversation.
Annotations Type	The message type listed in annotations.

Attribute	Description
Original File Name	The original file name prior to export.
Attachment Path	The path to the attachment associated with the message, if one was recovered.
Attachment	The recovered attachment.
Attachment Data Recovered	Indicates whether the attached file was recovered from the local file system.
Updater Name	The name of the user that updated the message.
Updater Email Address	The email address of the user that updated the message.
Updater User Type	The user type of the user that updated the message.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was updated.
Last Edited Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was last updated.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was deleted.

Additional Information

Cloud Google Chats (Warrant Return)

Description	Google Chats parsed from a Google Warrant Return archive.
Recovery method	Parsing

Attribute	Description
Message	The message that was sent.
Sender Email	The sender's email address.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Participants	The email addresses of all participants in the conversation.
Attachment	The path to the file in the Warrant Return package.
Attachments	The name of the locally downloaded file.

Additional Information

Cloud Google Contacts

Description	Cloud Google Contacts contains information about the contacts and services that a user has saved to their Google account.
Recovery method	Parsing

Attribute	Description
Display Name	The display name of the contact.
Nickname	The nickname of the contact.
Birthday (yyyy-	The birth date of the contact.

Attribute	Description
mm-dd)	
Email Address (es)	The email addresses of the contact.
Mobile Phone	The mobile phone number of the contact.
Home Phone	The home phone number of the contact.
Home Address	The home address of this contact.
Title	The job title of this contact.
Organization	The organization or business that is associated with the contact.
Business Phone	A business phone number for the contact.
Business Address	The physical address of the business that is associated with the contact.
Phone Num-bers	Any other phone numbers that are associated with the contact, excluding any home, business or cell phone number.
Additional Address	Any additional addresses associated with the contact.
Website URL	A list of website URLs that are associated with the contact.
Labels	Any tags that are associated with the contact (also known as labels).

Additional Information

Cloud Google Hangouts Messages

Description	Cloud Google Hangouts Messages contains Google Hangouts messages that are sent or received by the logged in user and recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Conversation Name	The name of the conversation.
Sender Username	The username of the sender of the message.
Sender ID	The unique user ID of the sender.
Text	The message that was sent.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Participants	The name of the participants in that conversation.
Message Type	The message type.
Latitude	The latitude of a location that was shared through a message or attachment.
Longitude	The longitude of a location that was shared through a message or attachment.
Conversation Status	The status of the conversation.
Conversation View	Indicates where the conversation is located (Inbox or Archive).

Attribute	Description
Conversation ID	The conversation ID.
Attachments	The names of the locally downloaded files.
Attachment	The path to the file in the Cloud image.

Additional Information

Cloud Google Hangouts Messages (Warrant Return)

Description	Google Hangouts Messages parsed from a Google Warrant Return archive.
Recovery method	Parsing

Attribute	Description
Sender User Name	The email address of the individual who sent the message.
Active Participants	The email addresses of all participants who are active in the conversation.
Invited Participants	The email addresses of all participants who are invited, but have not become active in the conversation.
Text	The text content of the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time (in UTC) of the message.

Attribute	Description
Message Type	The type of the message.
User Account	The email of the individual who is the target of the Warrant Return.
Sender Display Name	The display name of the individual who sent the message.
Attachment Path	The path to the attachment associated with the message, if one was recovered.
Conversation Name	The name of the conversation.
Sender ID	The unique identifier of the individual who sent the message.
Conversation ID	The unique identifier of the conversation.
Attachment	The recovered attachment.
Attachment Data Recovered	Indicates whether the attached file was recovered from the local file system.

Additional Information

Cloud Microsoft Teams Conversations

Description	Cloud Microsoft Teams Conversations contains information about each of the channels and group messages that exist in a user's Teams environment, which were recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Conversation Name	The name of a channel or message group.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the message group was created.
Description	The optional description for the channel.
Participants	The names of the users in the message group. Channels do not have a participant list.
Email	The email address for sending messages to the channel.
Web URL	The URL for the channel in Microsoft Teams.
Conversation ID	The ID of a channel or message group.
Team ID	The team ID of the channel.

Additional Information

Cloud Microsoft Teams Messages

Description	Cloud Microsoft Teams Messages contains messages that were sent and received between Teams members and are recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Content Type	The type of the content.

Attribute	Description
HTML Body	The HTML body of the message.
Sender Name	The name of the sender.
Sender ID	The unique identifier of the sender.
Send Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time (in UTC) when the message was sent.
Parent ID	The ID of the parent conversation.
Conversation ID	The unique identifier of the conversation.
Message ID	The unique identifier of current message.
Attachment URL	The URL of the attachment.
Attachments	The attachments.
Attachment	The path to the file in the Cloud image.

Additional Information

Cloud Microsoft Teams Teams

Description	Cloud Microsoft Teams Teams contains information about Microsoft Teams as recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Team ID	The unique identifier for the team.
Team Name	Th name of the team.
Description	The description that is associated with the team.

Additional Information

Cloud Skype Account Details (Warrant Return)

Description	Cloud Skype Account Details (Warrant Return) contains information about the target account of the warrant return.
Recovery method	Parsing

Attribute	Description
User Name	The username of the user.
Account Creation Date/Time (yyyy-mm-dd)	The date and time that the account was created.
Account Creation IP Address	The IP Address of the device on which the account was created.
User Email	The email address of the user.
Language	The shortcode of the user account's language.
First Name	The first name of the user.

Attribute	Description
Last Name	The last name of the user.
Profile User ID	The unique ID that is associated with the profile.

Additional Information

Cloud Skype Chat History Records (Warrant Return)

Description	Cloud Skype Chat History Records (Warrant Return) contains the chat history of a user, including calls and shared attachments, as recovered from a warrant return.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message.
Recipient(s)	The recipient(s) of the message.
Message	The body of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Attachment Name	The name of the attachment that was sent.
Attachment Size (bytes)	The size of the attached file in bytes.
Message Type	The type of the message.

Attribute	Description
Metadata	Additional details about the record in XML format.
Attachment	The path to the file in the Warrant Return package.

Additional Information

Cloud Skype Connection History (Warrant Return)

Description	Cloud Skype Connection History (Warrant Return) contains information regarding the account activity that was extracted from warrant returns provided by Skype.
Recovery method	Parsing

Attribute	Description
User Name	The full username of the account holder.
First Name	The first name of the account holder.
Last Name	The surname of the account holder.
Record Type	The record type of this action.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the account activity occurred.
Action	The type of account activity that occurred.

Attribute	Description
IP Address	The IP address that is associated with the account action.
Service Name	The Microsoft service that was used for this action.

Additional Information

Cloud Skype Contacts (Warrant Return)

Description	Cloud Skype Contacts (Warrant return) contains the contacts of a user, as recovered from a warrant return.
Recovery method	Parsing

Attribute	Description
User	The username of the user.
Type	The type of contact. The GUID of the contact is displayed for service contacts.
Contact	The user ID of the contact.

Additional Information

Cloud Slack Channels

Description	Cloud Slack Channels contains information about each of the channels and conversations that exist in a user's Slack workspace. These Slack channels are recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Channel Name	The name of a channel or message group.
Channel ID	The ID of a channel or message group.
Channel Type	The type of the channel.
Created By	The name or user ID of whoever created the channel.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the channel was created.
Topic	The topic text for the channel.
Topic Author	The name or user ID of whoever last updated the topic text.
Purpose	The purpose of the channel.
Purpose Author	The author who set the channel purpose.
Channel Members	The usernames of the members in the channel.
Members Count	The number of members in the channel.
Last Read Date/Time - UTC (yyyy-	The date and time when the channel was last read.

Attribute	Description
mm-dd)	
Member	Indicates whether or not the local user is a member of the channel.

Additional Information

Cloud Slack Files

Description	Cloud Slack Files contains information about the files that a user has downloaded locally from the URLs that they've viewed within Slack, and that have been recovered from the cloud . Data about the downloads are recovered from Slack Workspace Corporate exports.
Recovery method	Parsing

Attribute	Description
Attachments	The name of the attached file.
Attachment URL	The download URL of the attached file.
Attachment ID	The unique ID of the attached file assigned to it by Slack.
Channel Name	The name of the Slack Channel in which the file was shared.
Attachment	The path to the file in the Slack Workspace Corporate export.

Additional Information

Cloud Slack Messages

Description	Cloud Slack Messages contains messages sent or received in channels in the user's Slack workspace, and that are recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Sender	The username of whoever sent the message.
Recipient(s)	If the message is a direct message, this attribute indicates the recipient's username. If the message is a group message, this attribute indicates the group or channel name.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message text.
Direction	The direction of the conversation relative to the signed in user.
Message Type	The type of message.
Message Status	The status of the message.
Channel Name	The name of the Slack conversation the message was sent to.
Message ID	The ID of the message that was sent.
Conversation ID	The Slack conversation ID for the chat.

Attribute	Description
Workspace ID	The unique identifier for the Slack workspace.
Attachment URL	The URL that is associated with a link attachment in the message.
Attachment Name	The name of the attachment that is associated with the message.
Attachment ID	The Slack ID that is used to identify the file.
Attachment	The path to the file in the Cloud image.

Additional Information

Cloud Slack Users

Description	Cloud Slack Users contains information about each user in the Slack workspace that is recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Workspace ID	The unique identifier for the Slack workspace.
Full Name	The full name of the user.
User Name	The unique username of the user.
Display Name	The Slack display name of the user.

Attribute	Description
Email	The user email.
Phone Number	The user phone number.
Member ID	The user ID.
Title	The user title.
Status Message	The status message for the user
Account Type	The type of account that the user has.
Local Account	Indicates whether the account belongs to the local user.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the user was last updated.
Timezone	The timezone that the user is in.

Additional Information

Cloud Slack Workspaces

Description	Cloud Slack Workspaces contains information about each of the work-spaces that the user is a member of. This information is recovered from the cloud.
Recovery method	Parsing

Attribute	Description
ID	The unique identifier for the Slack workspace.
Name	The name of the Slack workspace.
Domain	The domain of the Slack workspace.
Email Domain	The email domain of the Slack workspace.
Enterprise ID	If the team belongs to an Enterprise Grid, this field represents the enterprise ID for the organization.
Enterprise Name	If the team belongs to an Enterprise Grid, this field represents the enterprise name for the organization.

Additional Information

Cloud WhatsApp Backups

Description	Cloud WhatsApp Backups contains information about backups that are created by WhatsApp and stored in the cloud. Each backup is a database that contains information from the WhatsApp for Android application, such as the user's message history. Backups are recovered from the cloud through the user's Google Drive account.
Recovery method	Parsing

Attribute	Description
File ID	The unique ID for the WhatsApp backup recovered from Google Drive.
File Path	The parent folder and file name of the backup.
File Type	The MIME type of the file.
Description	The description of the file.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was uploaded to Google Drive.
File Hash	The unique MD5 hash calculated when uploaded to Google Drive.
FileSize	The total byte size of the file.

Additional Information

Cloud WhatsApp Chats

Description	Cloud WhatsApp Chats are messages that are retrieved from a subject's account using their WhatsApp QR code login.
Recovery method	Parsing

Attribute	Description
Message	The content of the message.

Attribute	Description
Author ID	The unique ID of the message author.
Display Name	The display name of the user.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent (UTC).
Message Type	The type of the message.
Conversation Name	The name of the conversation.
Conversation ID	The ID of the conversation
Message ID	The unique identifier of the message.
Attachment Name	The file names of any locally downloaded files.
Attachment	The path to the file in the Cloud image.

Additional Information

Facebook Messenger Messages (Warrant Return)

Description	Facebook Messenger Messages (Warrant Return) contains individual messages that are parsed from chat threads that Facebook has included in a warrant return. The 'messages' in a chat thread can include messages, shared files or links, calls, and audio messages.
Recovery method	Parsing

Attribute	Description
Sender	The user name of sender of the message.
Sender ID	The Facebook ID of the sender.
Active Participants	The active participants of the chat thread. These accounts were subscribed to the thread at the time when Facebook retrieved the records.
Inactive Participants	The inactive participants of the chat thread. These accounts were previously subscribed to the thread at some point before the records were retrieved, but were no longer subscribed at the time of retrieval.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Body	The text of the message.
IP	The IP address of the sender of the message.
Attachment	The message attachment.
Attachment Path	The file path of the attachment.
Attachment Data Recovered	Indicates whether attachment data was recovered.
Last Shared Date/Time - UTC (yyyy-mm-dd)	If the message was shared outside the chat, this value indicates the last date and time when it was shared.

Attribute	Description
Sharing Link	A link to the file, if the message contains a shared file.
Sharing Summary	A summary of the shared item, if the message contains a shared file or URL.
Sharing Text	A description of the shared item, if the message contains a shared file or URL.
Sharing Title	A title for the shared item, if the message contains a shared file or URL.
Sharing Url	A URL to the shared page, if the message contains a shared file or URL.
Call Type	If the message type is a call, this indicates whether the call is an audio or a video call.
Call Missed	Indicates whether the call was missed.
Call Duration	The duration of the call.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the chat thread was accessed by Facebook during the generation of the warrant return.
Deleted	Indicates whether the message was deleted.
Local User	The user name of the owner of the chat (identifies the local user for chat threading).
Local User ID	The Facebook ID of the owner of the chat (identifies the local user for chat threading).
Thread ID	The ID of the chat thread that the message is from.

Additional Information

Snapchat Account Information (Warrant Return)

Description	Cloud Snapchat Account Information (Warrant Return) contains information about the target account of the warrant return.
Recovery method	Parsing

Attribute	Description
Account ID	The handle of the target account of the warrant return.
Email Address	The registered email address of the target account of the warrant return.
Account Creation Date/Time (yyyy-mm-dd)	The date and time that the account was created.
Account Creation IP Address	The IP address of the device on which the account was created.
Phone Number	The registered phone number of the target account of the warrant return.
Display Name	The display name of the target account of the warrant return.

Additional Information

Snapchat Friends (Warrant Return)

Description	Cloud Snapchat Friends (Warrant Return) contains information about the

	user's friends, which are parsed from a warrant return.
Recovery method	Parsing

Attribute	Description
Target ID	The account handle of the target account for the warrant return.
Friend ID	The account handle of the target's friend.

Additional Information

Snapchat Geolocation (Warrant Return)

Description	Snapchat Geolocation (Warrant Return) contains information about the geolocation associated with the user's Snapchat activity.
Recovery method	Parsing

Attribute	Description
Name	The user name associated with the geolocation.
User ID	The account ID associated with the geolocation.
Latitude	The latitude of the geolocation.
Longitude	The longitude of the geolocation.
Date/Time	The timestamp of the geolocation.

Attribute	Description
Type	Indicates whether the data came from geolocation or memory location.
ID	ID of the memory if the type is memory.

Additional Information
Location row number starts counting at 0.

Snapchat Group Chat Messages (Warrant Return)

Description	Cloud Snapchat Group Chat Messages (Warrant Return) contains information about the messages sent and received by users participating in a group chat thread, and which are parsed from a warrant return.
Recovery method	Parsing

Attribute	Description
Message Type	The contents of the sent message.
From	The handle of the sender of the message.
Owner ID	The handle of the target account for the warrant return.
Group Chat ID	The unique identifier of the group chat thread.
Group Chat Name	The name of the group chat thread.
Body	The text that was included in the message.
HREF	The contents of the href column from the warrant return

Attribute	Description
	.CSV file.
Attachments	The media attached to the message.
Media ID	The sender and unique ID information for all media attached to a message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.

Additional Information

Snapchat IP History (Warrant Return)

Description	Cloud Snapchat IP History (Warrant Return) contains information about the IP addresses that are associated with a user's account logins, as recovered from a warrant return.
Recovery method	Parsing

Attribute	Description
User Account	The account name for the Snapchat user.
IP	The IP address of the device that logged in or out of the account.
Type	The type of account action the user performed (login or logout).

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	The date and time that the action was performed.

Additional Information

Snapchat Messages (Warrant Return)

Description	Cloud Snapchat Messages (Warrant Return) contains information about the messages that are sent or received by a user, and are parsed from a warrant return.
Recovery method	Parsing

Attribute	Description
Sender	User name of the user who sent the message.
Sender ID	User ID of the user who sent the message.
Recipient	User name of the user who received the message.
Recipient ID	User ID of the user who received the message.
Body	The text that was included in the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Direction	Indicates whether the message was sent or received.

Attribute	Description
Media ID	The identifier for any photo(s) that were sent in the message.
Message Type	The type of message.
Saved	The saved column found in the chat.
HREF	The href column that was found in the chat.
Potentially Harmful Material	The flag indicates whether media may be harmful. Supported in Warrant Returns following 2021.
Chat ID	An ID for the chat, which combines the account names of the two users participating in the chat.
Attachment Data Recovered	Indicates whether any attachment data was recovered.
Attachment	The recovered attachment.

Additional Information

Connected Devices

Cloud Google Devices

Description	Google Devices contains information about the target account of the warrant return.
Recovery method	Parsing

Attribute	Description
Google Account	The Google Account ID.
Device Type	The type of device that was used to access the Google Account.
Brand	The brand of the device that was used to access the Google Account.
Device Model	The model of the device that was used to access the Google Account.
IMEI(s)	The IMEI(s) associated with the device.
MEID(s)	The MEDI(s) associated with the device.
Operating System	The operating system of the device that was used to access the Google Account.
Device Last Country	The last country in which the device was used to access the Google Account.
Device Last Location Date/Time - UTC (yyyy-mm-dd)	The last location time that the device was used to access the Google Account.
Device First Activity Date/Time - UTC (yyyy-mm-dd)	The first time that the device was used to access the Google Account.
Device Last Activity Date/Time - UTC (yyyy-mm-dd)	The last time that the device was used to access the Google Account.

Additional Information

Cloud Google Recent Devices

Description	Cloud Google Recent Devices contains Google recent devices that were recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Device Name	The name of the device.
Device Location	The location of the device.
Last Access Date/Time - Local Time	The last time that Google was accessed from the device.
Device Status	The last time that the device was synced to Google.
Browser Name	The name of the browser that the device accessed.
Device Model	The device model number.
Computer Name	The name of the computer that the device was synced to.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Documents

Cloud Google Keep

Description	The Cloud Google Keep artifact contains notes and lists that the user wrote and saved to their Google account.
Recovery method	Parsing

Attribute	Description
Title	The title of the note, when specified.
Modified Date/Time - Local Time	The date and time when the note was modified.
Body	The body content of the note.
Pinned	Indicates whether the note was pinned.
Archived	Indicates whether the note was archived.
Labels	Any labels added to the note.
Has Attachments	Indicates whether the note has attachments.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Cloud Google Tasks

Description	Cloud Google Tasks contains information about the tasks that a user has saved to their Google account, and that were recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Title	The title of the task.
Type	The type of entry (a tasklist, a task or a subtask).
Task List	The title of the tasklist that the task belongs to.
Parent Task	The title of the parent task.
Status	Indicates whether a task has been completed (values are either needsAction or completed).
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the task was modified.
Due Date - UTC (yyyy-mm-dd)	The date and time that the task is due to be completed.
Completed Date - UTC (yyyy-mm-dd)	The data and time that the task was completed.
Notes	The notes describing the task.
ID	The ID of the task assigned by the system.
Parent ID	The ID of the task's parent task.

Attribute	Description
Version	The version tag of the task.
Content Link	The URL pointing to the task.

Additional Information

Email and Calendar

Cloud Gmail Messages

Description	Cloud Google Gmail Messages contains Gmail message contents and Gmail attachments that are recovered from the cloud.
Recovery method	Parsing

Attribute	Description
ID	An ID for the message.
Label	A list of the labels that are applied to the email (for example, IMPORTANT, SENT, UNREAD).
To Address(es)	The recipient(s) of the email.
From Address	The sender of the email.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.

Attribute	Description
Subject	The subject of the email.
Submitted Date/Time - UTC (yyyy-mm-dd)	The date and time the email was submitted. If a submitted date and time is not found, this value defaults to Unix epoch time.
Delivered Date/Time - UTC (yyyy-mm-dd)	The date and time the email was received. If a received date and time is not found, this value defaults to Unix epoch time.
Headers	The header information of the email.
Email Body	The body of the email.
HTML Body	The body of the email in HTML format where applicable.
Thread ID	The ID of the thread that the message is from.
Attachments	The list of files that are attached to the email.
Attachment	The path to the file in the Cloud image.
Message Owner	The Owner of the Message.
Attachment Path	The path of an attachment.

Additional Information

Cloud Google Calendar Events

Description	Cloud Google Calendar Events contains information about the entries a user has saved to their Google Calendar.
Recovery method	Parsing

Attribute	Description
Title	The title of the event.
Calendar Display Name	The name of the calendar.
Calendar Owner	The email of the owner of the calendar.
Status	The status of the event (Confirmed, Tentative, or Cancelled).
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was created in the calendar.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the event was last updated.
Description	A more complete description of the event.
Event Location	A free-form text description of the location/venue of the event.
Created By	The email of the user who created the event.
Organizer	The organizer's email of the calendar event.
Start Date/Time - Local (yyyy-mm-dd)	The local date and time that the event is scheduled to start.
Event Start Timezone	The timezone of the start date/time.
End Date/Time - Local (yyyy-mm-dd)	The local date and time that the event is scheduled to end.
Event End Timezone	The timezone of the end date/time.
Attendees	The list of attendee emails that are associated with the event.
User Response	The user response for the calendar event (Needs Action, Accepted, Declined, Tentative).

Attribute	Description
Recurrence	The recurrence rules for the event.
Visibility	The visibility of the event (Default, Public, Private, or Confidential).
Web URL	The URL associated with the event.
Hangout URL	An absolute link to the Google+ hangout that is associated with this event.
PrivateCopy	Indicates whether the event is private.
Locked	Indicates whether the event is locked.
Guests Can Invite Others	Indicates whether guests can invite others to the event.
Guests Can Modify	Indicates whether guests can modify the event.
Guests Can See Other Guests	Indicates whether guests can see the list of other guests that are attending.
Source URL	The source URL from which the event was created.
ID	The unique ID within the calendar for this event.
Calendar ID	The unique ID for this calendar.
Attachments	The name(s) of the downloaded file(s).
Attachment	The path to the file in the Cloud image.

Additional Information

Cloud Google Calendar Events (Takeout)

Description	Cloud Google Calendar Events (Takeout) contains information about the entries that a user has saved to their Google Calendar.
Recovery method	Parsing

Attribute	Description
ID	The unique ID within the calendar for this object.
Type	The Calendar entry type. This value is one of the following: Event, Todo or Journal.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time (in UTC) that the entry was created in the calendar.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time (in UTC) when this entry is scheduled to start.
End Date/Time - UTC (yyyy-mm-dd)	The date and Time (in UTC) when this entry is scheduled to end.
Summary	A short summary of the entry.
Description	A more complete description of the entry.
Latitude	The latitude attached to the entry. This could be where the event will occur.
Longitude	The longitude attached to the entry. This could be where the event will

Attribute	Description
	occur.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time (in UTC) when this entry was last modified.
Event Location	Free form text defining the intended venue for the entry.
Organizer	The organizer's email of the calendar entry.
Status	The status of the entry within the calendar. This value is one of the following: Needs Action, Accepted, Declined, Tentative, Delegated, Completed, or In Progress.
URL	A URL associated with the event.
Recurrence	Indicates whether the event is recurring.
Attendees	A list of attendee emails that are associated with the entry.
Categories	The tags that are associated with this event.
Comment	Specifies a comment to the user for this entry.
Contact Label	Contact information or alternately a reference to contact information that is associated with the entry.
Resources	The equipment or resources that are required for the entry.
Timezone	The name of timezone that is associated with this entry.

Additional Information

Cloud iCloud Mail

Description	Cloud iCloud Mail contains the messages and attachments recovered from an iCloud Mail account.
Recovery method	Parsing

Attribute	Description
To	The recipients of the email.
From	The sender of the email.
Date/Time - UTC (yyyy-mm-dd)	The date and time the email was created.
Subject	The subject of the email.
Body	The body of the email.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Folder Path	The folder path of where the email is stored.
Headers	The raw email headers.
Attachments	The list of attachments on the email.

Additional Information

Cloud IMAP/POP Emails

Description	Cloud IMAP/POP Emails contains messages and attachments from an IMAP/POP account that are recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Sender Name	The sender of the email.
Recipients	The recipients of the email.
Subject	The subject of the email.
Delivery Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was delivered.
Body	The body of the email.
Folder Name	The name of the folder where the email is stored.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Attachments	The list of attachments on the email.
Headers	The raw email headers.
Importance	The importance of the email.

Additional Information

Cloud MBOX Emails

Description	Cloud MBOX Emails contains the messages and attachments that were recovered from an MBOX file and from the cloud.
Recovery method	Parsing

Attribute	Description
To	The recipients of the email.
From	The sender of the email.
Submitted Date/Time - UTC (yyyy-mm-dd)	The date and time the email was submitted. If a submitted date and time is not found, this value defaults to Unix epoch time.
Delivered Date/Time - UTC (yyyy-mm-dd)	The date and time the email was received. If a received date and time is not found, this value defaults to Unix epoch time.
Subject	The subject of the email.
Body	The body of the email.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Headers	The raw email headers.
Attachments	The list of attachments on the email.

Additional Information

Cloud Outlook Calendar

Description	Cloud Outlook Calendar contains information about the entries a user has saved to their Outlook Calendar, which are recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Event ID	The unique identifier of a calendar event.
Subject	The subject of the event.
Body	A more complete description of the entry.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the entry was created in the calendar.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when this entry was last modified.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when this entry is scheduled to start.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when this entry is scheduled to end.
Attendees	The list of attendee emails that are associated with the entry.
Has Attachment	Indicates whether there is an attachment associated with the entry.
Is All-day Event	Indicates whether the event is an all-day event.

Attribute	Description
Sent By Organizer	Indicates whether the sender of the event is the organizer.
Event Location	Free form text defining the intended venue for the entry.
Organizer	The organizer's email of the calendar event.
Recurrence	Indicates whether the event is recurring.
Sensitivity	Indicates the sensitivity of the event.
Importance	Indicates the importance of the entry.

Additional Information

Cloud Outlook Contacts

Description	Cloud Outlook Contacts contains information about the entries that a user has saved to their Outlook contacts, which are recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Contact Owner	The owner account of the contact.
Contact Display Name	The display name of the contact.
Contact Family Name	The family name of the contact.

Attribute	Description
Contact Middle Name	The middle name of the contact.
Contact Given Name	The given name of the contact.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact was last modified.
Contact Email	The email address of the contact.
Contact ID	A unique identifier of a contact.
Profession	The profession of the contact.
Company Name	The company of the contact.
Department	The department of the contact.
Job Title	The job title of the contact.
Manager Name	The manager of the contact.
Office Location	A free form description of the contact's office location.
Business Homepage	The business homepage of the contact.
Business Address	The business address of the contact.
Business Phone	The business phone number of the contact.
Home Address	The home adress of the contact.
Home Phone	The home phone number of the contact.
Mobile Phone	The mobile phone number of the contact.

Additional Information

Cloud Outlook Mail

Description	Cloud Outlook Mail contains email messages and attachments that were sent and received using Microsoft mail services (such as Hotmail, or Outlook), which are recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Sender Name	The sender of the email.
Recipients	The recipients of the email.
Subject	The subject of the email.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the email was Created.
Submitted Date/Time - UTC (yyyy-mm-dd)	The date and time when the email was Submitted.
Delivered Date/Time - UTC (yyyy-mm-dd)	The date and time when the email was Delivered.
Body	The body of the email.
Folder Name	The name of the folder where the email is stored.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.

Attribute	Description
Attachments	The list of attachments on the email.
Headers	The raw email headers.
Importance	The importance of the email.

Additional Information

Encryption and Credentials

Cloud Google Passwords

Description	Cloud Google Passwords contains Google Passwords that are recovered from the Cloud.
Recovery method	Parsing

Attribute	Description
Application Name	The name of the application that saved the passwords.
User Name	The username that is associated with the application.
Password	The saved password.

Additional Information

Location and Travel

Cloud Google Location History

Description	Cloud Google Timeline Locations contains information about the locations that a user visits. The location history is captured by Google Timeline and recovered using Google Takeout. Google Timeline is a web service that allows a user to view the locations that they visit and the routes that they take.
Recovery method	Parsing

Attribute	Description
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time when the user was at the location.
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Accuracy	The accuracy of the latitude and longitude values.
Altitude	The location's distance above sea level.
Altitude Accuracy	The accuracy of the altitude.
Velocity	The speed at which the user was moving at, when captured at the location.
Heading	The direction the user was moving in, when captured at the location.

Attribute	Description
Activity Confidence Scores	A collection of Google inferred activities that the user may have been doing at that location, along with respective confidence scores reported at the time in UTC.

Additional Information

Cloud Google Location History (Warrant Return)

Description	Google Location History (Warrant Return) contains information about the locations that a user visits. The location history is associated with the Device Tag that Google assigns to the device.
Recovery method	Parsing

Attribute	Description
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time when the user was at the location.
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Accuracy (meters)	The accuracy of the position.
Source Information	The source medium from which the position was obtained. For example: WIFI, CELL, or GPS.
Device ID	The ID of the device that captured the location history.

Attribute	Description
Platform	The operating system or platform in which the activity occurred. For example: Windows, Chrome OS, Android, or iOS.

Additional Information

Cloud Google Maps Activity (Warrant Return)

Description	Google Maps Activity (Warrant Return) contains information about the Google Maps actions that were executed by the account holder and found within a Warrant Return package.
Recovery method	Parsing

Attribute	Description
Description	A description of the Google Maps action made by the subject of the Warrant Return.
URL	The Google Maps URL associated with the action.
Search Date/Time - UTC (yyyy-mm-dd)	The date/time when the search was entered.
Latitude	The GPS latitude coordinate of the area viewed, or the journey destination (depending on the action).
Longitude	The GPS longitude coordinate of the area viewed, the location that was searched for, or the journey destination (depending on the action).

Additional Information

Cloud Google Semantic Location History - Activity Segment

Description	Cloud Google Semantic Location History - Activity Segment contains information about the activities that involved a change in location for a duration of time. The semantic location history is captured by Google Timeline and recovered using Google Takeout. Google Timeline is a web service that allows a user to view the locations that they visit and the routes that they take.
Recovery method	Parsing

Attribute	Description
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the user started the activity segment.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the user ended the activity segment.
Activity Type	The activity type describes how the user traveled from orgin location to destination. e.g. WALKING.
Origin Latitude	The latitude of the origin location.
Origin Longitude	The longitude of the origin location.
Destination Lat-	The latitude of the destination location.

Attribute	Description
itude	
Destination Longitude	The longitude of the destination location.
Distance	The distance in meters the user traveled from origin to destination.
Origin Place Address	The place address where the user started the activity segment.
Origin Place Name	The place name where the user started the activity segment.
Origin Place Map URL	The map URL of the place where the user started the activity segment.
Destination Place Address	The place address where the user ended the activity segment.
Destination Place Name	The place name where the user ended the activity segment.
Destination Place Map URL	The map URL of the place where the user ended the activity segment.
Confidence	Indicates how confident the Google application was in determining that the activity type is correct. One of: LOW, MEDIUM, HIGH, or UNKNOWN_CONFIDENCE.
Edit Confirmation Status	Indicates whether the user has manually edited the activity segment. Can be NOT_CONFIRMED or CONFIRMED.
Candidate Activity Types	A collection of all the activity types that were considered during the acquisition, and the probability of each activity type being the correct

Attribute	Description
	one.
Simplified Raw Path	A collection of Google recorded locations that the user may have been visiting or stopping at during the activity segment, reported in UTC.
Waypoint Path	A collection of the coordinates of any waypoints along the activity segment.

Additional Information

Cloud Google Semantic Location History - Place Visit

Description	Cloud Google Semantic Location History - Place Visit contains information about the locations that a user visited or stayed for a duration of time. The semantic location history is captured by Google Timeline and recovered using Google Takeout. Google Timeline is a web service that allows a user to view the locations that they visit and the routes that they take.
Recovery method	Parsing

Attribute	Description
ID	The ID of the place visit or child visit.
Parent ID	The Parent ID of the child visit.
Start Time Date/Time - UTC (yyyy-mm-	The date and time when the user arrived at the location.

Attribute	Description
dd)	
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the user left the location.
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Place Address	The address of the place that the user visited.
Place Name	The name of the place that the user visited.
Center Latitude	The latitude of the map center.
Center Longitude	The longitude of the map center.
Location Confidence	A number that indicates how confident the Google application was in determining that the user was at the location. A higher number indicates a higher confidence.
Place Confidence	Indicates how confident the Google application was in determining that the user visited the place. One of: LOW_CONFIDENCE, MEDIUM_CONFIDENCE, HIGH_CONFIDENCE, or USER_CONFIRMED.
Visit Confidence	A percentage that indicates how confident the Google application was in determining that the user was visiting the location.
Edit Confirmation Status	Whether the user has manually edited the place visit. Can be NOT_CONFIRMED or CONFIRMED.
Device Tag	An integer identifier that is associated with the device that obtained the loc-

Attribute	Description
	ation data. This data is specific to the Location History artifact.
Semantic Type	Place type based on semantic information specific to the user. One of: TYPE_ALIASED_LOCATION, TYPE_HOME, TYPE_SEARCHED_ADDRESS, or TYPE_WORK.
Place Visit Importance	Place visit importance. One of MAIN or TRANSITIONAL.
Place Visit Type	Place visit type. Can be SINGLE_PLACE.
Calibrated Probability	A number that indicates calibrated probability when the Google application process all collected locations.
Other Candidate Locations	A collection of all the other locations that Google considered during its acquisition, which the user may have visited.
Simplified Raw Path	A collection of Google recorded locations that the user may have been visiting at the reported time in UTC.

Additional Information

Cloud Google Timeline Locations

Description	Cloud Google Timeline Locations contains the locations that a user visits that are captured by Google Timeline, and recovered from the cloud. Google Timeline is a web service that allows a user to view the locations they travel and the routes that they take.

Recovery method	Parsing

Attribute	Description
Location Name	The name of the location.
Location Address	The address of the location.
Arrival Date/Time UTC (yyyy-mm-dd)	The time that the user arrived at the location.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The time that the user was last seen at this location.
Latitude	The GPS latitude coordinates of the location.
Longitude	The GPS longitude coordinates of the location.
Location Type	A description of the location, as determined by Google (for example, home, bar, cafe, or generic).
Location Type Inference	Indicates how the location type was determined. A value of inferred suggests that Google inferred the location type based on the person's position and the types of places nearby (for example, Google might infer that a person is at a restaurant if there's a restaurant at the same approximate location). A value of inferred-alias is used when the person visits a place that they explicitly set as destination type (i.e. home or work).

Additional Information

Cloud Lyft Profile Information

Description	Cloud Lyft Profile Information contains profile information recovered from the cloud.
Recovery method	Parsing

Attribute	Description
User ID	The unique ID of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
Email	The email address of the user.
Phone Number	The phone number of the user.
Email Verification Date/Time - UTC (yyyy-mm-dd)	The date and time that the user verified their account with their registered email.
Has Taken Ride	Indicates whether the user has taken a ride.
Photo URL	The URL of the user's profile photo.

Additional Information

Cloud Lyft Trip Information

Description	Cloud Lyft Trip Information contains summaries of the trips taken by a Lyft user, and recovered from the cloud using their account credentials.
Recovery method	Parsing

Attribute	Description
Ride ID	The unique ID for the ride.
Pickup Address	The pickup location address, as specified by the user.
Pickup Latitude	The GPS latitude coordinates of the specified pickup location.
Pickup Longitude	The GPS longitude coordinates of the specified pickup location.
Departure Date/Time - UTC (yyyy-mm-dd)	The date and time that the rider was picked up from their pickup location.
Dropoff Address	The address that was specified by the rider for drop-off.
Dropoff Latitude	The GPS latitude coordinates of the specified drop-off location.
Dropoff Longitude	The GPS longitude coordinates of the specified drop-off location.
Arrival Date/Time - UTC (yyyy-mm-dd)	The date and time that the rider was dropped off at their destination.

Attribute	Description
Origin Address	The original address that was specified by the rider for pickup.
Origin Latitude	The original GPS latitude coordinates of the specified pickup location.
Origin Longitude	The original GPS longitude coordinates of the specified pickup location.
Destination Address	The original address specified by the rider for drop-off.
Destination Latitude	The original GPS latitude coordinates of the specified drop-off location.
Destination Longitude	The original GPS longitude coordinates of the specified drop-off location.
Driver ID	The unique ID of the driver.
Driver Name	The first name of the driver.
Driver Phone Number	The phone number of the driver.
Account Activation Date/Time - UTC (yyyy-mm-dd)	The date and time that the driver activated their account.
Driver Picture URL	The URL of the driver's picture.
Vehicle Make	The make of the driver's vehicle.
Vehicle Model	The model of the driver's vehicle.
Vehicle Year	The year of the driver's vehicle.
License Plate Number	The license plate number of the driver's vehicle.

Attribute	Description
License Plate State	The license plate state of the driver's vehicle.
Cost	The cost of the rider's trip and the currency used.
Distance	The distance in miles that was covered on the rider's trip.
Duration	The duration of the rider's trip in hours, mins and seconds.
Trip Status	The status of the trip at the time of acquisition.

Additional Information

Cloud Uber Trip History

Description	Cloud Uber Trip History contains summaries of the trips that were taken by an Uber user, and were recovered from the cloud using their account credentials.
Recovery method	Parsing

Attribute	Description
Origin Address	The pickup location address, as specified by the user.
Origin Latitude	The GPS latitude coordinates of the specified pickup location.
Origin Longitude	The GPS longitude coordinates of the specified pickup

Attribute	Description
	location.
Departure Date/Time - UTC (yyyy-mm-dd)	The date and time that the rider was picked up from their pickup location.
Destination Address	The address specified by the rider for drop-off.
Destination Latitude	The GPS latitude coordinates of the specified drop-off location.
Destination Longitude	The GPS longitude coordinates of the specified drop-off location.
Arrival Date/Time - UTC (yyyy-mm-dd)	The date and time that the rider was dropped off at their destination.
Rider ID	The unique ID that is assigned to the rider's account.
Distance	The distance that was covered on the rider's trip.
Duration	The duration of the rider's trip.
Cost	The cost of the rider's trip and the currency used.
Trip Status	The status of the trip at the time of acquisition.
Trip ID	The unique ID for the trip.
Driver Name	The first name of the driver.
Driver ID	The unique ID of the driver.
Vehicle Make	The make of the driver's vehicle.
Vehicle Year	The year of the driver's vehicle.
Map Tile URL	The URL of the map tile that displays the route taken.

Attribute	Description
Attachments	The name of the downloaded Map Tile that displays the route taken.
Attachment	The path to the file in the Cloud image.

Additional Information

Media

Cloud Google Photos

Description	Cloud Google Photos contains pictures stored in Google Photos which are recovered from the cloud. Google Photos is a cloud-based photo storage service that allows users to store, view and share their photos.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the photo was created.
Album	The album that the photo is stored in.
MIME Type	The MIME type of the media.
Description	A description of the photo, if one exists.

Attribute	Description
Make	The make of the camera that was used to take the picture, as recovered from the Exif data.
Model	The model of the camera that was used to take the picture, as recovered from the Exif data.
ID	The ID of the photo.
Shared	Indicates if the album is shared with another user.
Web URL	The URL associated with the photo.
Attachment Path	The path of an attachment.
Attachments	The name of the locally downloaded file.
Attachment	The path to the file in the Cloud image.

Additional Information

Cloud Google Photos (Warrant Return)

Description	Google Photos (Warrant Return) contains information about pictures recovered from the target user's Google account.
Recovery method	Parsing

Attribute	Description
HexID	The Hex ID of the photo in the warrant return.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The universal date and time that the photo was last modified.
Modified Date/Time - UTC (yyyy-mm-dd)	The universal date and time that the photo was last modified.
Created Date/Time - Local Time (yyyy-mm-dd)	The local date and time that the photo was created.
Modified Date/Time - Local Time	The local date and time that the photo was last modified.
Upload IP	The IP address of the user who uploaded the photo.
Title	The title of the photo.
Description	A description of the photo, if one exists.
Status	The status of the user who uploaded the photo.
Caption	The caption of the photo.
Locale	The location where the photo was taken.
Album ID	The ID of the photo album.
Album URL	The URL for the photo album.
Album Title	The title of the photo album.
Access	The access level set for the photo album.
Media Key	The media key for the photo album.
Comment	The comments that are associated with the photo.
Tag	The tags that are associated with the photo.

Attribute	Description
Latitude	The GPS latitude coordinates of where the picture was taken, as recovered from the Exif data.
Longitude	The cardinal coordinates of the GPS longitude, as recovered from the Exif data.
People	The people who are identified in the photo.
EXIF - Camera	The camera that was used to take the photo (as extracted from the picture's EXIF Data).
EXIF - Width	The width of the image (as extracted from the picture's EXIF Data).
EXIF - Length	The length of the image (as extracted from the picture's EXIF Data).

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Cloud Google Photos - AXIOM 2.8

Description	Cloud Google Photos contains pictures stored in Google Photos which are recovered from the cloud. Google Photos is a cloud-based photo storage service that allows users to store, view and share their photos. This artifact applies to Magnet AXIOM 2.8 and earlier.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
Published Date/Time - UTC (yyyy-mm-dd)	The date that the photo was published to Google Photos.
Updated Date/Time - UTC (yyyy-mm-dd)	The date that the photo was last updated.
Photo Timestamp Date/Time - UTC (yyyy-mm-dd)	The photo's timestamp contains the date and time of the photo, either set externally or retrieved from the Exif data.
Exif Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the photo was taken.
Album	The album that the photo is stored in.
Description	A description of the photo, if one exists.
Make	The make of the camera used to take the picture, as recovered from the Exif data.
Model	The model of the camera used to take the picture, as recovered from the Exif data.
ID	The ID of the photo.
Latitude	The GPS latitude coordinates of where the picture was taken, as recovered from the Exif data.
Longitude	The cardinal coordinates of the GPS longitude, as recovered from the Exif data.
Access	The current sharing permission assigned to the photo.

Attribute	Description
File Size (Bytes)	The size of the photo in bytes.
Image Unique Id	The unique ID assigned to the photo.
Download URL	A download URL for the photo.
Attachment Path	The location of the attachment.
Attachments	The name of the locally downloaded file.
Attachment	The path to the file in the Cloud image.

Additional Information

Cloud iCloud Photos

Description	Photos that are stored in iCloud Photo Library that are recovered from the cloud.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the photo in iCloud Photo Library.
File Size (Bytes)	The file size.
Taken Date/Time - UTC (yyyy-mm-dd)	The time the photo was taken.
Added Date/Time - UTC (yyyy-	The time the photo was added to the phone.

Attribute	Description
mm-dd)	
Published Date/Time - UTC (yyyy-mm-dd)	The time the photo was published to iCloud Photo Library.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the photo was changed on iCloud Photo Library.
Caption	The description user added in iCloud Photo Library to describe the photo.
Albums	The albums the photo belongs to.
ID	The ID of the file assigned by iCloud Photo Library.
Attachments	The raw data of the file.
Attachment	The raw data of the file.

Additional Information

Operating System

Cloud Accounts Information

Description	Cloud Accounts Information contains the credentials of the acquired target account.
Recovery method	Parsing

Attribute	Description
User Name	The user name of the target account.
Password/Token	The password/token of the target account.
Platform	The platform of interest. For example: Google, Facebook, Slack e.t.c.

Additional Information

Cloud Google Account Information (Warrant Return)

Description	Google Account Information (Warrant Return) contains information about the target account of the warrant return.
Recovery method	Parsing

Attribute	Description
Name	The name of the user who created the account.
Email Address	The registered email address of the target account of the warrant return.
Services	The list of Google services associated with the user account.
Recovery Email	The recovery email address of the target account of the warrant return.
Account Creation Date/Time (yyyy-mm-dd)	The date and time that the account was created.

Attribute	Description
Terms of Service IP	The IP Address of the device on which the account was created.
Terms of Service Date/Time - UTC (yyyy-mm-dd)	The Date/Time the terms of service was accepted.
SMS	The phone number associated with the target account of the warrant return.
Account ID	The handle of the account target account of the warrant return.
Last Login Date/Time - UTC (yyyy-mm-dd)	The date and time of the last successful login.
Phone Numbers	Phone numbers associated with the user account, such as the phone number used to sign in and other phone numbers belonging to that user.
Youtube URL	The YouTube URL associated with the target account of the warrant return.
Youtube Creation DateTime	The date and time that the user created the associated YouTube account.
Youtube Creation IP Address	The IP Address of the device on which the YouTube account was created.

Additional Information

Cloud Google Login History (Warrant Return)

Description	Google Login History (Warrant Return) contains information about the logins and logouts made by the user account of the warrant return.
Recovery method	Parsing

Attribute	Description
IP Address	The IP address of the device on which the action was executed.
Type	The type of action executed.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the action.
Device Type	The type of the device on which the action was executed, such as Android or iOS.
Device ID	The unique identifier of the device on which the action was executed. Depending on the type of the device, this may be an Android ID or an Apple iOS IDFV.
Details	Information about the action that occurred.

Additional Information

Social Networking

Cloud Facebook Friends

Description	Cloud Facebook Friends contains information about the user's Facebook friends that was recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Name	The name of the user's friend.
Tagline	A string containing a tagline for the friend (this can contain the friend count for that user, the mutual friend count, or another piece of information about the friend).
Permanent Link	The URL of the friend's profile.
Attachments	The profile picture of the friend.
Attachment	The path to the file in the Cloud image.
HTML Body	An HTML card for the friend, which appears in the user's Friends list.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the friend was added, deleted or requested.
Status	The friend's relationship status with the user (for example 'deleted friends' if the user is no longer a friend, or 'friends' if they are currently friends).

Additional Information

Cloud Facebook Messenger Messages

Description	Cloud Facebook Messenger Messages contains Facebook Messages recovered from the cloud.
Notes	In cases where the sender account is suspended by Facebook pending a user ID verification, the body of a message is not recoverable. Only the sender name, sender ID, participants, and timestamp for the message is available.

Attribute	Description
Thread ID	The unique ID for the message thread that the message is recovered from.
Local User Account	The unique Facebook ID associated with the local user account.
Sender Name	The username of the person who sent the message.
Author ID	The unique Facebook ID of the author of the message.
Text	The content of the message.
HTML Body	The HTML body of the message.
Participants	The display names of the participants in the conversation.
Date/Time	The date and time when the message was sent.
Attachments	The file names of any locally downloaded files.
Message Type	The type of the message (examples include 'Generic' which indicates a standard message, 'Call', and 'Share').
Source	The location of where the artifact was found.
Location	A byte offset within the source where the Facebook Message data has been acquired.

Cloud Facebook Mobile Timeline

Description	Cloud Facebook Mobile Timeline contains Facebook timelines and their content, which are recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Name	The authenticated user's name.
Text	The content of the post.
Post Type	The type of post (for example: post, comment, reply).
Post ID	The Facebook ID of the post.
Comment ID	The Facebook ID of the comment (if the entry is a comment). This fragment is empty if the entry is a post.
Posted Timestamp	The displayed timestamp of when the post was created.
Parsed Date/Time - UTC (yyyy-mm-dd)	The date and time parsed by Magnet AXIOM of the posted timestamp.
Acquired Timestamp	The timestamp of when the post was acquired by Magnet AXIOM.
Source URL	A URL to the post.
Picture URL	The URL(s) to pictures from any link included with the post.
HTML Body	The HTML body of the post.
Attachments	A list of relative file paths to downloaded media.
Attachment	The path to the file in the Cloud image.

Additional Information

Cloud Facebook Profile Info

Description	Cloud Facebook Profile Info contains Facebook profile information recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Address	The full address of the user.
Additional Address	The name of the neighborhood that the user lives in.
Email Address(es)	A list of the user's email addresses.
Public Key	The user's PGP public key.
Phone Number	A list of the user's phone numbers.
Website URL	A list of website URLs that are associated with the user's profile.
Website	A list of other websites and account names that are associated with the user's profile.
Birthday (yyyy-mm-dd)	The user's birthday.
Gender	The user's gender.
Sexual Orientation	The user's sexual orientation (Men, Women, or Men and Women).

Attribute	Description
Language	A list of the languages that the user has specified.
Religion	A title and description indicating the user's religious views.
Political Party	A title and description indicating the user's political views.
HTML Body	The HTML of the user's profile info page.

Additional Information

Cloud Facebook Timeline

Description	Cloud Facebook Timeline contains Facebook timelines and their content, which are recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Message ID	The Facebook ID of the post.
Name	The authenticated user's name.
Title	The title of the post.
Text	The content of the post.
Type	The type of post (for example: photo, video, status, or link).
Permanent Link	A URL to the post that is intented to remain unchanged

Attribute	Description
	for many years.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the post was created.
HTML Body	The HTML body of the post.
Attachments	A list of relative file paths to downloaded media.
Attachment	The path to the file in the Cloud image.

Additional Information

Cloud Instagram Direct Messages

Description	Cloud Instagram direct messages that are sent or received by the logged in user and recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Thread Title	The title of the conversation.
Sender Username	The username of the sender of the message.
Author	The username of the original author of the message.
Text	The message that was sent.
Sent Date/Time - UTC (yyyy-	The date and time when the message was sent.

Attribute	Description
mm-dd)	
Participants	The username of the participants in the conversation.
Message Type	The message type.
Direction	The direction of the message, relative to the source of the hit.
Latitude	The latitude of a location shared through the message or attachment.
Longitude	The longitude of a location shared through the message or attachment.
Thread ID	The conversation ID.
Message ID	The message ID.
Attachment Name	The name of the locally downloaded file.
Attachment Data Recovered	Indicates whether attachment data was recovered.
Attachment	Attachment data associated with the message.

Additional Information

Cloud Instagram Posts

Description	Cloud Instagram Posts contains Instagram posts that are published by the logged in user and recovered from the cloud.
Recovery method	Parsing

Attribute	Description
ID	The post ID.
Sender Username	The username of the publisher of the post.
Sender Full Name	The full name of the publisher of the post.
Sender ID	The user ID of the publisher of the post.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time that the post was created.
Archived	Indicates whether the post was archived.
Text	The caption of the post.
Likes Count	The number of likes the post has.
Likers	The usernames of the users that like the post.
Comments Count	The number of comments that the post has.
Comments Preview	A preview of the comments on the post.
Tagged Users	The users that were tagged in the post.
Permanent Link	The direct link to the post.
Latitude	The latitude of a location added to the post.
Longitude	The longitude of a location added to the post.
Attachments	The names of any locally downloaded files attached to the post.
Attachment	The names of any locally downloaded files attached to the post.

Additional Information

Cloud Instagram Posts - AXIOM 2.1

Description	Cloud Instagram Posts - AXIOM 2.1 contains instagram posts that are published by the logged in user and recovered from the cloud.
Recovery method	Parsing

Attribute	Description
Message ID	The post ID.
Name	The username of the publisher of the post.
Text	The caption of the post.
Permanent Link	The direct link to the post.
Web URL	The web URL of the post.
Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time of the post.
HTML Body	The HTML body of the post.
Attachments	The names of any locally downloaded files attached to the post.
Attachment	The names of any locally downloaded files attached to the post.

Additional Information

Cloud Twitter Direct Messages

Description	Cloud Twitter Direct Messages contains direct messages between an authenticated Twitter user and another user, which are recovered from the cloud (limited to 20 sent and 20 received messages).
Recovery method	Parsing

Attribute	Description
Message ID	The unique identifier for the direct message.
Sender Screen Name	The Twitter handle for the message sender.
Recipient Screen Name(s)	The Twitter handle for the message recipient.
Text	The content of the direct message.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The UTC date and time that the message was sent.
Sender ID	The unique identifier for the sender.
Sender Name	The name of the Twitter sender, as they've defined it, but is not necessarily the person's name.
Sender Location	The name of the place from where the message was sent.
Recipient ID(s)	The unique identifier for the recipient.
Recipient Name(s)	The name of the Twitter recipient, as they've defined it, but is not necessarily the person's name.
Recipient Location	The name of the place from where the message was received.

Attribute	Description
Media URL	A list of media URLs that are attached to the message.
Media Type	A list of media types corresponding to each media URL.
Type	Indicates whether the message was sent to a group or a user.
Attachments	A list of relative file paths to the media that was downloaded from Twitter servers.
Attachment	The path to the file in the Cloud image.

Additional Information

Cloud Twitter Direct Messages (Warrant Return)

Description	Cloud Twitter Direct Messages (Warrant Return) contain information about those messages sent or received by a user, and are parsed from a warrant return.
Recovery method	Parsing

Attribute	Description
Sender ID	The unique identifier of the account who sent the message.
Sender Name	The user name of the account who sent the message.
Recipient ID	The unique identifier of the account that received the message.

Attribute	Description
Recipient Name	The user name of the account that received the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Text	The textual content of the message.
Message ID	The unique identifier of the message.
Message Deleted	True, if the message was parsed from a deleted-direct-messages. Otherwise, false.
Conversation ID	The unique identifier for the conversation. This identifier is a combination of the account IDs of both participants.
Media URL	The URL links to media included in the message, if applicable.
URL	The expanded URL links included in the message, if applicable.
Attachment Name(s)	Paths to attachments included in the message, if applicable.
Attachment	A .zip file of attachments included in the message, if applicable.

Additional Information

Cloud Twitter Posts

Description	Cloud Twitter Posts contains an authenticated Twitter user's tweets, recovered from the cloud (limited to 1200 of the user's most recent Tweets).
Recovery method	Parsing

Attribute	Description
Status ID	The unique identifier of the tweet.
User ID	The unique identifier of the Twitter user.
Screen Name	The Twitter handle of the user (ie. @username).
Name	The name of the Twitter user, as they've provided in their user profile.
Tweet Text	The content of the tweet.
Posted Date/Time - UTC (yyyy-mm-dd)	The UTC date and time that the tweet was posted.
Favorited	Indicates whether this tweet was liked by the authenticated user.
Retweet Count	The number of times this tweet has been retweeted.
Tweet Source	The type of device/application that was used to create the tweet.
URL	The URL of the tweet.
Locale	The name of the location where the tweet was posted.
Country	The name of the country where the tweet was posted.
Latitude	The latitude of the location where the tweet was posted (values are between -90.0 to +90.0, where North is positive).
Longitude	The longitude of the location where the tweet was posted (values are between -180.0 to +180.0 where East is positive).
Location Bounding Box	A series of longitude and latitude points, which define a box around around the tweet location.
Media URL	A list of media URLs for media included in the tweet.

Attribute	Description
Media Type	The media types of the media included in the tweet.
Attachments	A list of relative file paths to downloaded media attached to the tweet.
Attachment	The path to the file in the Cloud image.

Additional Information

Cloud Twitter Posts (Warrant Return)

Description	Cloud Twitter Posts (Warrant Return) containing data describing a user's posted tweets, as recovered from a Warrant Return.
Recovery method	Parsing

Attribute	Description
Status ID	The unique identifier of the tweet.
User ID	The unique identifier of the tweet author.
Screen Name	The Twitter handle of the tweet author (i.e. @username).
Tweet Text	The content of the tweet.
Posted Date/Time - UTC (yyyy-mm-dd)	The UTC date and time that the tweet was posted.
Favorited	The number of times the tweet was favorited by other Twitter users.

Attribute	Description
Retweet Count	The number of times the tweet was retweeted by other Twitter users.
Tweet Source	The Twitter client the tweet was published from.
Media URL	A list of URLs for the media linked to in the tweet, if applicable.
Attachment Name(s)	A list of the attachment names and paths to their locations in the Warrant Return package, if applicable.
Attachment	A .zip file containing the media attachments within the Warrant Return package for a given tweet, if applicable.

Additional Information

Cloud Twitter Posts Public

Description	Cloud Twitter Posts Public contains publicly-accessible tweets which are recovered from the cloud. The data structure is defined in https://-github.com/twintproject/twint/blob/master/twint/tweet.py.
Recovery method	Parsing

Attribute	Description
Screen Name	The Twitter handle for the user (@username).
Name	The name of the Twitter user, as they've provided in their user profile.

Attribute	Description
Tweet Text	The content of the tweet.
Retweeted by Target User	The screen name of the targeted user that retweeted the original tweet.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time when the tweet was originally created.
Attachments	A list of relative file paths to downloaded media attached to the tweet.
Reply Count	The number of times that people replied to this tweet.
Retweet Count	The number of times this tweet has been retweeted.
Likes Count	The number of times this tweet has been liked.
Locale	The location of the tweet's author.
Mentions	An array of user's that were mentioned within this post.
Status ID	The unique identifier for the Twitter tweet.
Conversation ID	The unique identifier for the conversation of the Twitter tweet.
User ID	The unique identifier of the Twitter user.
Location Name	The name of the place where the Tweet was posted.
Web URL	An array of URLs contained inline within this tweet.
Photo URL	An array of URLs to photos contained inline within this tweet.
HashTags	An array of hashtags used within this tweet.

Attribute	Description
URL	The URL for the tweet.
Retweeted	Indicates whether this tweet is a retweet of another user's tweet.
Quote URL	The URL to the a tweet which is being quoted in this user's tweet.
Has Video	Indicates whether this tweet has an inline video included.
Attachment	The path to the file in the Cloud image.

Additional Information

Cloud Twitter Users

Description	Twitter users (followers, friends, and personal profile) information. The data structure is defined in https://dev.twitter.com/overview/api/users.
Recovery method	Parsing

Attribute	Description
User ID	The integer representation of the unique identifier for this User. Int64.
Name	The name of the Twitter user, as they've provided in their user profile.
User Name	The screen name, handle, or alias that this user uses to identify

Attribute	Description
	themself. Screen names are unique but subject to change.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date and time (in UTC) that the user account was created on Twitter.
Description	Nullable. The user-defined UTF-8 string describing their account.
Web URL	Nullable. A URL provided by the user in association with their profile.
Locale	Nullable. The user-defined location for this account's profile. This value is not necessarily a location, nor machine-parseable.
Protected	If true, this indicates that this user has chosen to protect their tweets.
Followers	The number of followers that this account currently has. Under certain conditions of duress, this field will temporarily indicate 0.
Friends	The number of users this account is following. Under certain conditions of duress, this field will temporarily indicate 0.
Statuses	The number of tweets (including retweets) issued by the user.
Timezone	Nullable. A string describing the Time Zone that this user declares themselves to be in.
Following	Nullable. The screen name of a user that this account is following.
Followed By	Nullable. The screen name of a user that is following this account.
Profile Picture URL	A HTTP-based URL pointing to the user's profile image.
Profile Background Pic-	A HTTP-based URL pointing to the background image the user

Attribute	Description
ture URL	has uploaded for their profile.
Profile Banner URL	The HTTPS-based URL pointing to the standard web representation of the user's uploaded profile banner.

Additional Information

Cloud Twitter Users (Warrant Return)

Description	Twitter users' (followers, friends, and personal user) information. The data structure is defined by the followers.txt and following.txt in a Twitter Warrant return.
Recovery method	Parsing

Attribute	Description
User ID	The integer representation of the unique identifier for this User. Int64.
User Link	A URL provided by the user in their profile.
Following	Nullable. The user id of a user that this account is following.
Followed By	Nullable. The user id of a user that is following this account.

Additional Information

Cloud Twitter Users Public

Description	Cloud Twitter Users Public contains information about publicly-accessible Twitter users (followers, friends, and personal profile) which are recovered from the cloud. The data structure is defined in https://-github.com/twintproject/twint/blob/master/twint/user.py.
Recovery method	Parsing

Attribute	Description
User ID	The integer representation of the unique identifier for this User. Int64.
Name	The name of the Twitter user, as they've provided in their user profile.
Screen Name	The name of the Twitter user, as they've provided in their user profile.
Biography	Nullable. The user-defined UTF-8 string describing their account.
Bio URL	Nullable. A URL provided by the user in association with their profile.
Locale	Nullable. The user-defined location for this account's profile. This value is not necessarily a location, nor machine-parseable.
Statuses	The number of tweets (including retweets) that are issued by the user.
Friends	The number of users that this account is following. Under cer-

Attribute	Description
	tain conditions of duress, this field will temporarily indicate 0.
Followers	The number of followers that this account currently has. Under certain conditions of duress, this field will temporarily indicate 0.
Likes Count	The number of tweets that this user has liked.
Media Count	Indicates the number of posts with media embedded in them, such as all Twitter posts that contain inline photos or video.
Protected	Indicates whether a user has chosen to protect their tweets.
Verified	Indicates whether this user has been marked as verified by Twitter.
Profile Picture URL	A HTTP-based URL that points to the user's profile image.
Following	Nullable. The screen names of the users that this account is following.
Followed By	Nullable. The screen names of the users that are following this account.
Web URL	The HTTPS-based URL that points to the user's profile.
Profile Created Date/Time - Local Time (yyyy-mm-dd)	The date and time (in UTC) that the user account was created on Twitter.
Attachments	A list of relative file paths to the media that was downloaded from Twitter servers.
Attachment	The path to the file in the Cloud image.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Facebook - Instagram Messages (Download Your Data)

Description	Facebook - Instagram Messages contains the Facebook or Instagram messages sent or received by a user and recovered from that user's Download Your Data package.
Recovery method	Parsing

Attribute	Description
Sender Name	The name of the person who sent the message.
Participants	The names of the participants in the conversation.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message Sent Date/Time - Local Time (Date Format Unknown)	The date and time the message was sent, as parsed from a Download Your Data package in the HTML format.
Message Text	The content of the message that was sent.
Message Type	The type of the message (for example, 'Generic,' which indicates a standard message, 'Call', and 'Share').
Shared Link	The link that was shared.

Attribute	Description
Shared Text	The description of the link that was shared.
Shared Content Original Owner	The original owner of the content that was shared.
Attachments	The path to the file(s) in the Download Your Data package.
Attachment Path	The path to the attached files.
Local User Display Name	The display name of the local user account.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Facebook Account Actions (Warrant Return)

Description	Facebook Account Actions (Warrant Return) contains the list of actions made by the user that Facebook has included in a warrant return.
Recovery method	Parsing

Attribute	Description
Action	A description of the action executed on the account.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the action.
IP Address	The IP address of the device on which the action was executed.

Additional Information

Facebook Audit Log (Warrant Return)

Description	Facebook Audit Logs (Warrant Return) contains information activities the user has performed on Facebook which are parsed from a warrant return.
Recovery method	Parsing

Attribute	Description
Type	The type of activity that occurred.
Summary	A summary of what happened.
Date/Time - UTC (yyyy-mm-dd)	The time the activity occurred.
Object ID	The ID of the activity.

Additional Information

Facebook Friend Requests (Warrant Return)

Description	Facebook Friend Requests (Warrant Return) contains friend requests that are parsed from friend_requests file that Facebook has included in a warrant return.
Recovery method	Parsing

Attribute	Description
Sender Name	The name of the sender of the friend request.
Sender ID	The Facebook ID of the sender.
Recipient Name	The name of the recipient of the friend request.
Recipient ID	The Facebook ID of the recipient.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the friends request was received.
Requests Accepted	Indicates whether the friend request is accepted.
Is Rejected	Indicates whether the friend request is rejected.
Marked As Spam	Indicates whether the friend request is marked as spam.
Hidden	Indicates whether the friend request is hidden.

Additional Information

Facebook Friends (Warrant Return)

Description	Facebook Friends (Warrant Return) contains information about a user's Facebook friends which are parsed from a warrant return.
Recovery method	Parsing

Attribute	Description
Name	The name of the user's friend.
ID	The Facebook ID of the user's friend.

Additional Information

Facebook Photos (Warrant Return)

Description	Facebook Photos (Warrant Return) contains information about the pictures that a user has posted to Facebook, which are parsed from a warrant return.
Recovery method	Parsing

Attribute	Description
Picture	The image data that was recovered.
Album	The name of the album that the picture belongs to.
Title	The title of the picture.
ID	The Facebook ID of the picture.
Photo URL	The URL of the picture on Facebook.
Web URL	The URL of the picture post on Facebook.
IP	The IP address of the device that was used to upload the photo.
Uploaded Date/Time	The date and time the photo was uploaded to Facebook.
Modified Date/Time - UTC (yyyy-mm-dd)	The modification date and time of the photo as reported by Facebook.
Make	The make of the camera used to take the picture, as

Attribute	Description
	recovered from the Facebook data.
Model	The model of the camera used to take the picture, as recovered from the Facebook data.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Primary Category	An integer that indicates the Project VIC category for the picture.
Tag	Any Facebook tags applied to the picture by the user.

Additional Information

Facebook Status Updates (Warrant Return)

Description	Facebook Status Updates (Warrant Return) contains status updates and comments from a user's status update that Facebook has included in a warrant return.
Recovery method	Parsing

Attribute	Description
Author	The author of the status update or comment.
Author ID	The Facebook ID of the author of the status update or comment.
Content	The content of the status update or comment.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time when the status update or comment was made.
Type	Indicates whether this instance is a status update or comment.
Mobile	Indicates if the status update was posted via mobile phone
Local User	The local user ID.
Attachment	The attachment for the status update or comment.
Attachment Path	The path to the attachment for the status update or comment.
Attachment Data Recovered	Indicates whether attachment data was recovered.

Additional Information

Facebook Wallpost (Warrant Return)

Description	Facebook Wallposts (Warrant Return) contains posts and comments from a user's wall that Facebook has included in a warrant return.
Recovery method	Parsing

Attribute	Description
Sender ID	The Facebook ID of the person who made the post.
Sender Name	The name of the person who made the post.
Recipient ID	The Facebook ID of the post recipient.
Recipient Name	The name of the post recipient.
Date/Time - UTC (yyyy-mm-dd)	The time that the post was made.
Content	The content of the post.
Message ID	The ID of the post. Both the post and the comments on a post share the same ID.
Message Type	Indicates whether this instance is a wall post or a comment on a post.

Additional Information

Instagram Account Actions (Warrant Return)

Description	Cloud Instagram Account Actions (Warrant Return) contains the list of actions that were made by the user, and that Instagram has included in a warrant return.
Recovery method	Parsing

Attribute	Description
Action	A description of the action executed on the account.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the action.
IP Address	The IP address of the device on which the action was executed.
Account Name	The handle of the user.
ID	The unique ID of the account.

Additional Information

Instagram Account History (Download Your Data)

Description	Cloud Instagram Account History contains log in or log out information that can be recovered through the user's Download Your Data package.
Recovery method	Parsing

Attribute	Description
Type	Indicate whether an event occurred while logging in or logging out.
Date/Time - UTC (yyyy-mm-dd)	The date and time the event occurred.

Attribute	Description
IP Address	The IP address of the device used during the current event.
User Agent	The application that was used during the current event.
Device ID	The ID of the device used during the current event.

Additional Information

Instagram Comments (Download Your Data)

Description	Cloud Instagram Comments (Download Your Data) contains comments on other users' posts that were sent by the user whose Download Your Data package is acquired.
Recovery method	Parsing

Attribute	Description
Sender User Name	The username of the person who sent the comment.
Original Post Author	The username of the person who authored the original post.
Comment	The content of the comment.
HREF	The url of the post the liked comment resides.
Comment Created Date/Time - UTC (yyyy-mm-dd)	The time that the comment was posted by the sender.

Additional Information

Instagram Comments (Warrant Return)

Description	Cloud Instagram Comments (Warrant Return) contains the list of comments that Instagram has included in a warrant return.
Recovery method	Parsing

Attribute	Description
Author ID	The ID of the target user.
Author Name	The name of the target user.
Comment ID	The ID of the comment.
Content	The content of the comment.
Date/Time Created - UTC (yyyy-mm-dd)	The UTC date and time that the comment was posted.
Status	The status of the comment.
Media ID	The ID of the media related to the comment.
Media Owner Name	The owner name of the media related to the comment.
Media Owner ID	The owner ID of the media related to the comment.

Additional Information

Instagram Direct Messages (Download Your Data)

Description	Cloud Instagram direct messages that are sent or received by a user and recovered from that user's Download Your Data package.
Recovery method	Parsing

Attribute	Description
Sender	The username of the sender of the message.
Participants	The username of the participants in the conversation.
Message	The message that was sent.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Likers	The usernames of the users that like the post.
Media Owner Name	The owner name of the media related to the message.
Sharing Summary	The media share caption.
Sharing Url	The media share URL.
Sharing Text	The story share description.
Action	The video call action, if applicable.

Additional Information

If the user linked their Instagram account to Facebook Messenger, Instagram direct messages can appear as Facebook Messenger Messages artifacts rather than Instagram Direct Messages artifacts. You can confirm whether the accounts are linked in the Instagram app. If accounts are not linked, the direct message icon in Instagram is an arrow. If accounts are linked, the direct message icon in Instagram is the Facebook Messenger icon. Note that media associated with messages is not included in the Download Your Data package from Instagram.

Instagram Direct Shares (Warrant Return)

Description	Cloud Instagram Direct Shares (Warrant Return) contains the list of direct shares of the user that Instagram has included in a warrant return.
Recovery method	Parsing

Attribute	Description
Sender ID	The Instagram ID of the sender of the direct share message.
Sender	The user name of the sender of the direct share message.
Recipient ID(s)	The Instagram ID of the recipient(s) of the direct share message.
Recipient(s)	The user name of the recipient(s) of the direct share message.
Content	The content of the direct share message.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the direct share message was sent.

Attribute	Description
Direction	Indicates whether the direct share message was sent or received by the user.
Type	The type of the direct share message.
Attachment Data Recovered	Indicates whether attachment data was recovered.
Attachment	The attachment associated with the direct share message.
IP Address	The IP address of the user that sent the direct share message.
URL	The URL of the content that was shared.
ID	The ID of the direct share message.
Thread ID	The ID of the thread that the direct share was a part of.

Additional Information

Instagram Direct Stories (Warrant Return)

Description	Cloud Instagram Direct Stories (Warrant Return) contains the list of direct stories that were sent by the user, and that Instagram has included in a warrant return.
Recovery method	Parsing

Attribute	Description
Author Name	The name of the author of the story.
Author ID	The Instagram ID of the author of the story.
Recipient(s)	The recipient(s) of the direct story.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the story was sent.
Media ID	The ID of the picture or video featured in the story.
Attachment Name	The picture or video featured in the story.
Attachment	The path to the file(s) in the Warrant Return package.

Additional Information

Instagram Followers and Following (Warrant Return)

Description	Cloud Instagram Followers and Following (Warrant Return) provides information about who the user is following and who their followers are, which is parsed from an Instagram warrant return.
Recovery method	Parsing

Attribute	Description
User Name	The Instagram handle for the user.
User ID	The unique identifier for this user.

Attribute	Description
Display Name	The name of the Instagram user, as they've provided in their user profile.
Followed By	Nullable. The username of the user that is following this account.
Following	Nullable. The username of the user that this account is following.

Additional Information

Instagram Media (Download Your Data)

Description	Cloud Instagram media that is uploaded by a user and recovered from that user's Download Your Data package.
Recovery method	Parsing

Attribute	Description
Type	The media type.
Caption	The caption that the user added to the media item.
Title	The title that the user added to the post.
Uploaded Date/Time - UTC (yyyy-mm-dd)	The date and time that the media was uploaded.
Location Name	The name of the location that the user added to the media.
Path	The path to the media in the Download Your Data

Attribute	Description
	archive.
Exif Data	The media's Exif Data serialized.
Device ID	The ID of the device that was used to upload the media.
Created Date/Time - Local Time	The media's Exif Data created date.
Source Type	The media's Exif Data source type.
Latitude	The media's Exif Data latitude coordinate in decimal degrees.
Longitude	The media's Exif Data longitude coordinate in decimal degrees.
Attachment	The path to the file in the Download your data package.

Additional Information

Instagram Photos (Warrant Return)

Description	Cloud Instagram Photos (Warrant Return) contains the list of all of the user's photos and any comments that are attached to the photo, and that Instagram has included in a warrant return. Each comment is displayed as an individual hit and you can view a thread of the comments in the chat threading view in AXIOM Examine. You can identify the photo that a comment belongs to using the Photo ID attribute.
Recovery method	Parsing

Attribute	Description
Picture	The picture data that was recovered.
Comment	A comment posted on the photo (by another user or the photo's author).
Author Name	The name of the author of the comment.
Author ID	The ID of the author of the comment.
Comment Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the comment was posted on the photo.
Comment ID	The ID of the comment.
Message Status	The status of the comment. The values of this attribute might indicate cases where a comment has been edited or removed, but this has not been verifiable.
Photo Id	The ID of the photo that the user posted to Instagram.
Image Date/Time - UTC (yyyy-mm-dd)	The date and time that the photo was uploaded.
IP Address	The IP Address of the user that uploaded the photo.
Web URL	The Instagram URL of the photo that was uploaded
Draft	Indicates whether the post is public or still a draft. Yes indicates that the post is a draft, and No indicates that the post is public.
Shared	Indicates whether the photo was shared with another user.
Status	The status of the photo.
Source Locations	The device or location from which the photo was uploaded.

Attribute	Description
Image Filter	The Instagram filter that was applied to the photo.
Local Name	The name of the local user.
Local User ID	The Instagram ID of the local user.
Type	Indicates whether this instance is a comment or a photo.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
MD5 Hash	An MD5 hash of the picture content.
SHA1 Hash	A SHA1 hash of the picture content.
PhotoDNA Hash	The hash of the picture content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

Web Related

Cloud Google Browsing History (Warrant Return)

Description	Google Browsing History (Warrant Return) contains information about the target account of the warrant return.
Recovery method	Parsing

Attribute	Description
Search Date/Time - UTC (yyyy-mm-dd)	The date and time that the website was visited.
Browsing History Event	The website that the user visited or the browsing history event that occurred.
URL	The URL of the website that the user visited.

Additional Information

Cloud Google Chrome Autofill

Description	Cloud Google Chrome Autofill contains information used in Google Chrome to automatically fill out contact information forms on the web. A user's account can contain multiple sets of autofill data, and this artifact creates a hit for each set it discovers.
Recovery method	Parsing

Attribute	Description
Name	Full names that the user has saved to this autofill identity.
First Name	First names that the user has saved to this autofill identity.
Last Name	Last names that the user has saved to this autofill identity.
Middle Name	Middle names that the user has saved to this autofill identity.

Attribute	Description
Email Address	Email addresses that the user has saved to this autofill identity.
Home Phone	Phone numbers that the user has saved to this autofill identity.
Home Address	The home street address that the user has saved to this autofill identity.
Address Line 1	The address line 1 that the user has saved to this autofill identity.
Address Line 2	The address line 2 that the user has saved to this autofill identity.
City	The city of residence that the user has saved to this autofill identity.
State/Province	The state or province of residence that the user has saved to this autofill identity.
ZIP/Postal Code	The ZIP or postal code that the user has saved to this autofill identity.
Country Code	The country code that the user has saved to this autofill identity.
Sorting Code	The sorting code that the user has saved to this autofill identity. The sorting code serves as additional information around the postal code, such as a CEDEX code.
Dependent Locality	The dependent locality that the user has saved to this autofill identity. More specific city locations such as village, township, neighbourhood, and district belong here.
Language Code	The abbreviated language code that the user has saved to this autofill identity.
Company	The company of employment that the user has saved to this autofill identity.
Use Count	The number of times that this autofill identity has been used.
Last Used	The time when this autofill identity was last used.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Source Information	The origin of this autofill identity. This value is usually the URL of the website on which this information was first entered, or 'Chrome Settings' if it was entered through Chrome's autofill page.
GUID	A unique ID for this autofill identity.

Additional Information

Cloud Google Chrome Bookmarks

Description	Cloud Google Chrome Bookmarks contains information about the bookmarks that a user has saved to their Google Account. Saved bookmarks can be synced across multiple devices.
Recovery method	Parsing

Attribute	Description
Title	The name of the bookmark or bookmark folder.
URL	The URL for the bookmark.
Icon URL	The icon URL for the bookmark.
Path	The absolute folder path to the bookmark.
Last Modified Date/Time - UTC (yyyy-	The last date and time that the bookmark was

Attribute	Description
mm-dd)	modified.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was added.

Additional Information

Cloud Google Chrome Browser History

Description	Cloud Google Chrome Browser History contains information about all URLs that were visited using Google Chrome.
Recovery method	Parsing

Attribute	Description
Event Type	The event that caused this page to be visited. Some examples of event type are LINK, TYPED, and FORM_SUBMIT.
Title	The title of the webpage.
URL	The URL of the webpage.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The time when the webpage was visited.
ID	The ID of the client which caused this visit. This value is unique per installation of Google Chrome.
Favicon URL	The URL for the favicon of the webpage.

Additional Information

Cloud Google Chrome Extension Settings

Description	Cloud Google Chrome Extension Settings contains configuration settings for Chrome Extensions.
Recovery method	Parsing

Attribute	Description
ID	The ID of the extension. This value is unique per extension, and is the same between users with the same extension.
Value	The value of the setting.
Key	The name of the setting.

Additional Information

Cloud Google Chrome Extensions

Description	Cloud Google Chrome Extensions contains information about installed Chrome Extensions.
Recovery method	Parsing

Attribute	Description
Extension Name	The extension name.
ID	The ID of the extension. This value is unique per extension, and is the same between users with the same extension.
Version Number	The version number of the extension.
Extension Enabled	Indicates whether the extension is enabled by the user.
Incognito Enabled	Indicates whether the extension is enabled in incognito browsing mode by the user.
Disable Reasons	The reason why the extension has been disabled. Possible values are as follows: DISABLE_USER_ACTION: Disabled by the user DISABLE_PERMISSIONS_INCREASE: Disabled due to an increase in required permissions DISABLE_RELOAD: Disabled until extension is reloaded DISABLE_UNSUPPORTED_REQUIREMENT: Disabled because of an unsupported requirement DISABLE_SIDELOAD_WIPEOUT: Disabled during a mass disabling of 3rd party extensions DEPRECATED_DISABLE_UNKNOWN_FROM_SYNC: Disabled because of synced disable state DISABLE_NOT_VERIFIED: Disable because Chrome could not verify the install DISABLE_GREYLIST: Disabled because the extension is blacklisted in the Windows registry DISABLE_CORRUPTED: Disabled because the extension is corrupted DISABLE_REMOTE_INSTALL: Disabled because it was remotely installed and must be enabled by the user DISABLE_EXTERNAL_EXTENSION: Disabled because it is an external extension and must be enabled by the user DISABLE_UPDATE_REQUIRED_BY_POLICY: Disabled because an update is required for the extension

Attribute	Description
	DISABLE_CUSTODIAN_APPROVAL_REQUIRED: Disabled because user requires approval by custodian DISABLE_BLOCKED_BY_POLICY: Disabled because management policy blocks the extension.
Remote Install	Indicates whether this extension was remotely installed from an Android device.
Installed by Custodian	Indicates whether this extension was installed by the custodian managing this user.
Update URL	The update URL for this extension.

Additional Information

Cloud Google Chrome Search Engines

Description	Cloud Google Chrome Search Engines contains information about search engines the user has used.
Recovery method	Parsing

Attribute	Description
Short Name	The name of the search engine.
URL	The URL of the search engine.
Suggestions URL	The URL which returns suggested searches.
Originating URL	The URL of the XML configuration file for the search engine.

Attribute	Description
Instant URL	The URL used by the Chrome Instant feature.
New Tab URL	The URL for the search engine upon opening a new browser tab.
Alternate URL	A list of alternate URLs for the search engine.
Favicon URL	The URL for the favicon associated with the search engine.
Picture URL	The URL for the image associated with the search engine.
Image URLPost Params	The post parameters to be used with the image URL.
Search Terms Replacement Key	The keyword for activating Chrome Instant feature.
Show in Default List	Indicates whether this search engine will appear in the default search engines list in Chrome.
Created Date/Time - UTC (yyyy-mm-dd)	The time when this search engine was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time for this search engine.
Sync GUID	The unique ID for this search engine.
Keyword	A keyword used to activate this search engine in Chrome.
Input Encodings	Encodings for the input into this search engine, such as UTF-8.

Additional Information

Cloud Google Chrome Sync Settings - App Settings

Description	Cloud Google Chrome Sync Settings - App Settings contains information about Chrome application settings to sync between devices.
Recovery method	Parsing

Attribute	Description
ID	The ID of the application. This value is unique per application, and is the same between users with the same application.
Key	The name of the setting.
Value	The value of the setting.

Additional Information

Cloud Google Chrome Sync Settings - Apps

Description	Cloud Google Chrome Sync Settings - Apps contains information about Chrome applications to sync between devices.
Recovery method	Parsing

Attribute	Description
Extension Name	The application name.

Attribute	Description
ID	The ID of the application. This value is unique per application, and is the same between users with the same application.
Version Number	The version number of the application.
Extension Enabled	Indicates whether the application is enabled by the user.
Incognito Enabled	Indicates whether the application is enabled in incognito browsing mode by the user.
Disable Reasons	The reason why the application has been disabled. Possible values are as follows: DISABLE_USER_ACTION: Disabled by the user DISABLE_PERMISSIONS_INCREASE: Disabled due to an increase in required permissions DISABLE_RELOAD: Disabled until app is reloaded DISABLE_UNSUPPORTED_REQUIREMENT: Disabled because of an unsupported requirement DISABLE_SIDELOAD_WIPEOUT: Disabled during a mass disabling of 3rd party apps DEPRECATED_DISABLE_UNKNOWN_FROM_SYNC: Disabled because of synced disable state DISABLE_NOT_VERIFIED: Disable because Chrome could not verify the install DISABLE_GREYLIST: Disabled because the app is blacklisted in the Windows registry DISABLE_CORRUPTED: Disabled because the app is corrupted DISABLE_REMOTE_INSTALL: Disabled because it was remotely installed and must be enabled by the user DISABLE_EXTERNAL_EXTENSION: Disabled because it is an external app and must be enabled by the user DISABLE_UPDATE_REQUIRED_BY_POLICY: Disabled because an update is required for the app DISABLE_CUSTODIAN_APPROVAL_REQUIRED: Disabled because user requires approval by custodian DISABLE_BLOCKED_BY_POLICY: Disabled because management policy blocks the application.

Attribute	Description
Remote Install	Indicates whether this application was remotely installed from an android device.
Installed by Custodian	Inidcates whether this application was installed by the custodian managing this user.
Update URL	The update URL for this application.

Additional Information

Cloud Google Chrome Sync Settings - Preferences

Description	Cloud Google Chrome Sync Settings - Preferences contains information about Chrome settings to sync between devices.
Recovery method	Parsing

Attribute	Description
Key	The name of the setting.
Value	The value of the setting.

Additional Information

Cloud Google Search History

Description	Google Search History contains information about the searches that were made by the account holder, and found within a Warrant Return or Takeout package.
Recovery method	Parsing

Attribute	Description
Search Type	The type of Google search that the user used.
Search Term	The search term that the user used.
URL	The URL of the search generated by Google.
Search Date/Time - UTC (yyyy-mm-dd)	The date/time when the search was entered.
Latitude	The GPS latitude coordinates of the location at which the search was made.
Longitude	The GPS longitude coordinates of the location at which the search was made.

Additional Information

Google Search URLs can contain important insight for your investigation. To learn more about Google Search URLs, sign in to the Support Portal to read the article Analyzing timestamps in Google Search URLs.

Cloud SharePoint Content

Description	content that is hosted on a SharePoint service and is recovered from the cloud. SharePoint is a web-based, collaborative platform that integrates with Microsoft Office.
Recovery method	Parsing

Attribute	Description
File Name	The name of the content that is hosted by SharePoint service.
Type	The type of content.
File Path	The path to the content on the SharePoint service.
Creator Name	The name of the content creator.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the the content was created.
Last Modified Name	The name of the individual that last modified the content.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the content was last modified.
Web URL	A direct URL to the content
ID	Content ID hosted by SharePoint services.
Data	Meta data, json data of the SharePoint item.

Attribute	Description
Attachments	A path to the downloaded content.
Attachment	The path to the file in the Cloud image.
Creator ID	A unique identifier for the content Creator.
Last Modified ID	An ID for the individual that last modified the content.

Additional Information

Cloud SharePoint Documents

Description	Files that are stored in SharePoint Documents library that are recovered from the cloud. SharePoint is a web-based, collaborative platform that integrates with Microsoft Office.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file in the SharePoint Documents library.
File Type	The type of file.
File Path	Path to the file in the SharePoint Documents library.
File Size (Bytes)	The file size in bytes.
Owner ID	The unique identifer of the owner of the file.

Attribute	Description
Owner Name	The name of the owner of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the file was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the file was modified.
Shared With Root User	Indicates whether the file was shared with the root user.
Sharing Scope	Indicates with whom the file is shared. E.g. Specific users.
File ID	File ID in SharePoint Documents library.
Attachments	Path to the downloaded file.
Attachment	The path to the file in the Cloud image.

Additional Information

Cloud SharePoint Site Pages

Description	Cloud Sharepoint Site Pages contains site pages that are hosted on a SharePoint service and are recovered from the cloud. SharePoint is a web-based, collaborative platform that integrates with Microsoft Office.
Recovery method	Parsing

Attribute	Description
File Name	The name of the site page.
File Path	The path to the site page on the SharePoint service. This is the hierarchy of the site page that is hosted by SharePoint services.
Creator Name	The name of the site page creator.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the the site page was created.
Last Modified Name	The name of the individual that last modified the site page.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the site page was last modified.
Web URL	A direct URL to the site page
ID	The SharePoint ID of the site page.
Data	Meta data, json data of the SharePoint item.
Attachments	A path to the downloaded site page.
Attachment	The path to the file in the Cloud image.
Creator ID	A unique ID for the page Creator.
Last Modified ID	An ID for the individual that last modified the site page.

Additional Information

YARA Rules

YARA Rule Matches

Description	The YARA artifact contains information about files and processes that matched with conditions specified in a YARA rule.
Recovery method	Parsing

Attribute	Description
File Name	The name and extension of the file whose content matched with the condition(s) from the YARA rule. The value is blank if the match came from a process (executable/application that was loaded into memory at the time of the memory dump) during memory analysis using the Comae plugin option.
File size (bytes)	The size of the file in bytes. The value is blank if the match came from a Process.
Process Name	The name of the process that matched with the condition(s) from the YARA rule. The value is blank if the match came from a file.
Process ID	The ID of the process (PID). The value is blank if the match came from a File.
Matched rule set(s)	List of the paths and respective YARA rule sets that had a match.
Matched rule	The YARA rule name that a match was found for.
Matching conditions	List of conditions for the YARA rule that had a match.

Additional Information

Chromebook

Additional Sources

Android Backups

Description	Android Backups contains information about any backups of Android devices that are recovered from the computer. If an Android backup is recovered during a search, you can search the contents of the backup for additional artifacts.
Recovery method	Parsing

Attribute	Description
File Name	The name of the backup file.
File Path	The path where the backup was stored on the computer.
Encryption	The type of encryption (if any) that was used on the backup.
File System Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time for the AB file from the file system.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time for the AB file from the file system.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time for the AB file from the file system.

Additional Information

Apple Disk Images

Description	Apple disk images are commonly stored as DMG or IMG files. These files are containers that may contain additional items of interest. This artifact identifies any Apple disk image found on the system.
Recovery method	Parsing

Attribute	Description
File Name	The name of the Apple disk image file.
File Path	The path where the Apple disk image was stored on the computer.
File Type	The type of Apple disk image file (DMG or IMG).
File System Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time for the file from the file system.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time for the file from the file system.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time for the file from the file system.

Additional Information

iOS Backups

Description	iOS Backups contains information about any backups of iOS devices that are recovered from the computer. If an iOS backup is recovered during a search, you can search the contents of the backup for additional artifacts.
Recovery method	Parsing

Attribute	Description
Device Phone Name	The name of the iOS device from which the backup originated.
Device Phone Number	The phone number of the iOS device from which the backup originated.
IMEI	The IMEI of the iOS device from which the backup originated.
ICCID	The ICCID of the iOS device from which the backup originated.
Backup File Creation Date/Time	The date and time that the backup was created.
Product Name	The model of the iOS device from which the backup originated.
Product Version	The version of iOS of the device at the time of the backup creation.
Serial Number	The serial number of the iOS device from which the backup originated.

Additional Information

Virtual Machines

Description	Virtual Machine files that have been found on the object being searched.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the virtual machine.
Virtual Machine Software	The software that is associated with the virtual machine.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the virtual machine was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the virtual machine was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the virtual machine was last modified.

Additional Information

Advanced Search Tools

Dynamic Application Finder

Description	Artifacts found using the Dynamic Application Finder vary depending on your case's evidence. To learn more, see Processing details > Find more

	artifacts in the AXIOM User Guide.
Recovery method	Parsing

Attribute	Description

Additional Information

Application Usage

Activity Manager History

Description	Activity Manager History contains a list of recent activity manager events, identified by the package name that triggered the event.
Recovery method	Parsing

Attribute	Description
Date/Time - Local Time (yyyy-mm-dd)	The date and time of the activity.
Type	The type of activity.
Event	The name of the event.
Package Name	The name of the package that triggered the event.
Process ID	The process ID of the package.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Android Application Roles

Description	Android Application Roles contains a list of the default set application for specific functions in Android.
Recovery method	Parsing

Attribute	Description
Package Name	The internal name of the application.
Role	The role assigned to the application.

Additional Information

Android Device Information

Description	Android Device Information contains the phone identification values.
Recovery method	Parsing

Attribute	Description
Device ID	The unique identifier that is displayed when rooting the device.

Attribute	Description
IMSI	The IMSI associated with the device.
IMEI	The IMEI associated with the device.
MEID	The MEID associated with the device.
ICCID	The ICCID associated with the device.
Serial Number	The serial number associated with the device.
Manufacturer	The manufacturer of the device.
Model	The model of the device.
Product Name	The secret codename that the manufacturer gave to the device.
Advertising ID	The advertising ID of the primary user account.
Chip Name	The name of the processor within the device.
Bootloader	The bootloader associated with the device.
SIM Card State	The state of the SIM card when the device was acquired (for example, READY).
Service Provider Country Code	The country code associated with the service provider of the device.
Mobile Country Code	The mobile country code of the provider of the SIM.
Mobile Network Code	The mobile network code of the provider of the SIM.
Service Provider Name	The name of the SIM service provider.
Device Phone Number	The phone number of the device.
Device Phone Type	The type of radio used to transmit voice calls (for example, GSM)

Attribute	Description
Voice Mail Identifier	The alphabetic identifier associated with the voice mail number.
Voice Mail Number	The phone number the device calls to access voice mail.
Current Network Country ISO Code	The ISO country code of the network that the device was registered on during acquisition.
Current Network Operator Name	The name of the network operator that the device was registered on during acquisition.
Network Type	The type of network that the device was registered on during acquisition.
Host Name	The hostname associated with the device.
Device Software Version	The software version of the device.
Security Patch	The current installed security patch of the device.
Roaming	Indicates whether the device was considered to be roaming during acquisition.
MAC Address	The WiFi hardware address of the device.
Bluetooth Address	The Bluetooth hardware address of the device.
Bluetooth Name	The Bluetooth name that appears upon pairing the device.
Timezone	The timezone for the device.

Additional Information

Android Usage History

Description	Android Usage History contains information about the usage and activity of applications that are running on the device.
Recovery method	Parsing

Attribute	Description
Event Name	The category of event that is occurring.
Package Name	The package name defined by the publisher/developer of the application (for example, com.example.mypackage).
Event	The event that is running within the application.
Event Date/Time - UTC (yyyy-mm-dd)	The last time that the event was actively being engaged either by a user or by the system.
Last Active Date/Time - UTC (yyyy-mm-dd)	The last time that the package was active on the device.
Last System Active Date/Time - UTC (yyyy-mm-dd)	The last time that the package was being utilized on or by the system.
Total Time	The amount of time that the application/package was open and being inter-

Attribute	Description
(Seconds)	acted with by the user.
Type	The type of event representing a state of change, for example, configuration change or shortcut invocation. For a complete list of events, visit https://developer-.android.com/reference/android/app/usage/UsageEvents.Event.

Additional Information

Android Usage History (Dumpsys)

Description	Android Usage History (Dumpsys) contains information about the usage and activity of applications running on the device, recovered using the dumpsys utility. The dates and times that were recovered by this artifact reflect the local time of the device.
Recovery method	Parsing

Attribute	Description
Event Name	The category of event that is occurring.
Package Name	The package name that was defined by the publisher/developer of the application (for example, com.example.mypackage).
Event	The event that is running within the application.
Configuration	The Android configuration that is currently active.

Attribute	Description
Time Range - Local Time (yyyy-mm-dd)	The time range that the data was aggregated within.
Total Time (Seconds)	The amount of time that the application/package was open and being interacted with by the user.
Event Date/Time - Local Time (yyyy-mm-dd)	The last time that the event was actively being engaged either by a user or by the system.
Last Active Date/Time - Local Time (yyyy-mm-dd)	The last time that the package was active on the device.
Last System Active Date/Time - Local Time (yyyy-mm-dd)	The last time that the package was being utilized on or by the system.
Type	The type of event representing a state of change, for example, configuration change or shortcut invocation. For a complete list of events, visit https://developer-.android.com/reference/android/app/usage/UsageEvents.Event.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Android User Dictionary

Description	Contains the shortcuts and words the user has on his or her device.
Recovery method	Parsing

Attribute	Description
Word	A word entered by a user to auto-complete a shortcut (a desired word or phrase). For example, a user may type the word, "Hello," prompting the short-cut, "Hello World."
Shortcut	The symbols that the user types to cause the word to be written.

Additional Information

Application Activity - Android

Description	Application Activity represents the applications that are active in the back-ground of the operating system.
Recovery method	Parsing

Attribute	Description
Package Name	The application package name.
First Active Date/Time -	The date and time when the application was first active.

Attribute	Description
UTC (yyyy-mm-dd)	
Last Active Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was last active.
Last Moved Date/Time - UTC (yyyy-mm-dd)	The date and time when the application last changed positions in the list of running applications. An application moves to the front of the list when it starts.
Application Activity	The activity the application is performing.
Application Data	The application data.
Origin Activity	The Android activity where the currently running activity originated from. For example, if the current activity describes opening a website in the browser, the origin activity might be from a messaging application where the link was opened from.
Device User ID	A unique user ID associated with the user account.
Preview	The snapshot preview of the active application.

Additional Information

Application Permissions - Android

Description	Application Permissions contains information about the application permissions that a user has granted or declined.
Recovery method	Parsing

Attribute	Description
Package Name	The package that requests the permission.
Permission	The permission name.
Allowed	Indicates whether the package is allowed to use the service/permission.

Additional Information

Application Power Usage

Description	Application Power Usage represents the amount of battery power consumed by each application since the device's last full charge.
Recovery method	Parsing

Attribute	Description
Application Name	The application package name.
Application ID	The unique ID associated with the application package.
Power Usage	The amount of power (in mAh) that the application consumes.

Additional Information

Application Runtime Permissions

Description	Application Runtime Permissions contains information about the application permissions that a user has granted or declined while the application is running.
Recovery method	Parsing

Attribute	Description
Package Name	The package that requests the permission.
Permission	The permission name.
Allowed	Indicates whether the package is allowed to use the service/permission.

Additional Information

Digital Wellbeing Events

Description	Digital Wellbeing Events contains information about events that are tracked by the Digital Wellbeing app. Events describe state changes such as when an application pauses or resumes. Digital Wellbeing is a system application that's available on most Android 9 and 10 devices. The app is used to track events and provide the user with options to limit their usage of applications and set up a sleep schedule to reduce device usage.

Recovery method	Parsing

Attribute	Description
Event ID	The unique ID of the event.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time of the event.
Package Name	The package name of the application associated with the event.
Event Type	An event representing a state change in the application associated with the event.
Source Package Name	The package name of the application that triggered the event. The application that triggers the event can be different from the application that the event is associated with. For example, opening one application might cause an activity in a tracked application to pause.

Additional Information

Digital Wellbeing Limits

Description	Digital Wellbeing Limits is used for restricting the amount of time for application usage. An application is suspended once the time limit has been reached.

Recovery method	Parsing

Attribute	Description
Package Name	The package name of the application.
Time Limit (m)	The time limit configured for the application, in minutes (converted from milliseconds).
Suspended	Indicates whether the application is currently suspended.

Additional Information

Google Play Application Details

Description	Google Play Application Details contains more detailed information about the applications that a user has downloaded from Google Play. This information includes when the user last installed or updated an application, and how the user was referred to the application.
Recovery method	Parsing

Attribute	Description
Package Name	The package name of the application that is installed.
Title	The name of the application as it is currently represented in the Google Play Store.

Attribute	Description
Account	The signed in Google Play Store account that is used to install the application.
Last Updated Date/Time	The date and time when the application was last updated through the Google Play Store.
Downloaded Date/Time	The date and time when the application was last downloaded through the Google Play Store.
Download Request Date/Time	The date and time when the application was last requested for installation through the Google Play Store.
First Install Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was first installed through the Google Play Store.
Update Discovered Date/Time	The last time Google Play discovered an available update for the installed application.
Automatically Update	Indicates whether the application is set to automatically update in Google Play.
Referrer	The original source that referred the user to the application in Google Play.

Additional Information

Google Play Installed Applications

Description	Google Play Installed Applications lists each of the applications that were downloaded and installed from Google Play.
Recovery method	Parsing

Attribute	Description
Package Name	The package name of the application that is installed.
Account	The signed in Google Play Store account that is used to install the application.
Purchased Date/Time	The time that the application was purchased from the Google Play Store.

Additional Information

Google Play Searches

Description	Google Play Searches contains the search queries that a user has performed in Google Play, and the date and time of when they were performed.
Recovery method	Parsing

Attribute	Description
Search Query	The search query entered by the user.
Query Date/Time	The date and time when the user made the search.

Additional Information

Installed Applications

Description	Installed Applications contains a list of all of the applications on an Android device, including their versions.
Recovery method	Parsing

Attribute	Description
Package Name	The internal name of the application.
Installed Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was installed.
Platform	The platform of the application.
Internal Version	The internal version of the application.
Display Name	The display name of the application.
Display Version	The display version of the application.
AppSource	The path of where the .app file application is located for the installed application.
Application Data	The path of where the user data is stored for the installed application
Type	The type of application (either System or User).

Additional Information

Cloud Storage

Android Dropbox

Description	Android Dropbox contains Dropbox file information recovered from a Kindle device.
Recovery method	Parsing

Attribute	Description
File Path	The path to the file.
Updated Modified Date/Time - UTC (yyyy-mm-dd)	The updated date and time that the file/folder was modified.
Local Modified Date/Time - UTC (yyyy-mm-dd)	The local date and time that the file/folder was modified.
Updated File Name	The name of the file/folder being updated.
Displayed Modified Date/Time	The displayed modified date and time.
Local File Size (Bytes)	The size of the file on the local machine.
Updated File Size (Bytes)	The updated size of the file.
Favorited	Indicates whether or not the file has been favorited.
File Version	The file version.

Additional Information

Android Dropbox Account Info

Description	Android Dropbox Account Info contains Dropbox account information recovered from a Kindle device.
Recovery method	Parsing

Attribute	Description
Email	The email address associated with the account.
User ID	The Dropbox user account ID.
Display Name	The Dropbox user account display name.
Country	The country that the user account is set for.

Additional Information

MEGA Accounts

Description	MEGA Accounts contains information about the accounts that the local user has logged in with on the device.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the local user.

Attribute	Description
Email Address	The email address of the local user.
First Name	The first name of the local user.
Last Name	The last name of the local user.

Additional Information

MEGA Chat

Description	MEGA Chat contains messages sent and received by the local user.
Recovery method	Parsing

Attribute	Description
Sender ID	The ID of the sender.
Sender Email	The email address of the sender.
Recipient ID(s)	The user ID(s) of the recipient(s).
Recipient Email(s)	The email address of the recipient of the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message Body	The body of the message.
Message Type	The type of the message.
Attachment Name	The file name of the attachment in a message.
File	The attachment in the message.

Additional Information

MEGA Contacts

Description	MEGA Contacts contains information about MEGA users that have communicated with the local user account.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the contact.
Email Address	The email address of the contact.
First Name	The first name of the contact.
Last Name	The last name of the contact.

Additional Information

Communication

AIM Buddies

Description	Contains the AIM buddies that were recovered from an Android device.
Recovery method	Parsing

Attribute	Description
User AIM ID	The AIM ID of the local user.
Buddy Name	The name of the buddy.
Buddy Display ID	The display ID of the buddy.
Buddy AIM ID	The AIM ID of the buddy.
Buddy Icon URL	The URL of the buddy's icon.
Downloaded Buddy Icon	The dowloaded icon of the buddy.
Buddy Group	Identifies if the row is a buddy or group chat. The possible values are Buddies or groupcht.
Group Chat ID	The ID of the group chat, if applicable.

Additional Information

AIM Messages

Description	Contains the AIM messages that were recovered from and Android device.
Recovery method	Parsing and carving

Attribute	Description
Sender	The AIM ID of the sender of the message

Attribute	Description
Receiver	The AIM ID of the user receiving the message or the group chat ID if in a chat.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Message	The message that was sent/received.
Latitude	The latitude of the message sender.
Longitude	The longitude of the message sender.

Additional Information

Android Burner Conversations

Description	Android Burner Conversations contains the Burner conversations that were recovered from an Android device.
Recovery method	Parsing

Attribute	Description
Burner Number	The Burner number on the device that is a part of the conversation.
Conversation Partner	The phone number of the other person in the conversation.
Message	The last message of the conversation.

Attribute	Description
Account Number	The Burner ID on the device that is a part of the conversation.
Conversation Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message in the conversation.
Conversation Name	The name of the conversation.
Type	The type of the last interaction in the conversation. The possible values are Outgoing Text Message, Incoming Text Message, Incoming Phone Call, Missed Incoming Phone Call, Outgoing Phone Call, and Incoming Voice Mail.
Voice Mail URI	The URI to the voice mail, if applicable.

Additional Information

Android Burner Numbers

Description	Android Burner Numbers contains the Burner numbers that were recovered from an Android device.
Recovery method	Parsing and carving

Attribute	Description
User ID	The ID of the user's Burner account.
Burner ID	The ID of the Burner number.
Burner Number	The phone number that was generated by Burner.
Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time when the Burner number was updated.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the Burner number was generated.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the Burner number will expire.
About	Information about the Burner number.

Additional Information

Android Call Logs

Description	Android Call Logs contains information about the phone calls that occur using the Android Phone application.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where the data was recovered from.

Attribute	Description
Partner	The phone number of the conversation partner.
Partner Name	The name of the conversation partner.
Direction	The direction of the call (Incoming or Outgoing).
Call Status	The status of the call (Answered, Unanswered, Missed or Declined).
Call Date/Time - UTC (yyyy-mm-dd)	The date/time of the call.
Call Duration (Seconds)	The duration of the call.
Partner Location	The location of the other participant of the call, can be a province or state.
Service Provider Country Code	The country code of the service provider that handled the call.
ICCID	The ICCID number of the SIM card inside the device.

Additional Information

Android Call Logs (UFED Agent)

Description	Android Call Logs (UFED Agent) contains calling logs from the Phone application on Android. These logs are recovered from <incoming_calls>, <outgoing_calls>, <missed_calls>, <unknown_calls> tags found in a UFED Report.xml.
Recovery method	Parsing

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Type	The type of call (Incoming, Outgoing, or Missed). This data is retrieved from the <incoming_calls>, <outgoing_calls>, <missed_calls>, <unknown_calls> tags in a UFED Report.xml.
Partner Phone Number	The phone number of the conversation partner. This data is retrieved from the <number> tag within each call element in a UFED Report.xml.
Partner Name	The name of the conversation partner. This data is retrieved from the <name> tag within each call element in a UFED Report.xml.
Date/Time - UTC (yyyy-MM-dd)	The date/time of the call. This data is retrieved from the <timestamp> tag within each call element in a Report.xml.
Duration (Seconds)	The duration of the call. This data is retrieved from the <duration> tag within each call element in a Report.xml.

Additional Information

Android Contacts

Description	Android Contacts contains contact information from a recovered Android device.
Recovery method	Parsing and carving

Attribute	Description
Display Name	The display name of the contact.
Phone Number(s)	The phone number of the contact.
Email Address(es)	The email address of the contact.
Address	The postal address of the contact.
Website	The website of the contact.
Starred	Indicates whether or not the contact has been starred.
Deleted	Indicates whether or not the contact has been deleted.
Last Time Contacted Date/Time - UTC (yyyy-mm-dd)	The last date and time when the contact was contacted.
Number of Times Contacted	The number of times that the contact has been contacted.
Total Contact Call Duration (Seconds)	The sum of the call durations for a given contact.
Notes	Notes associated with the contact.
Source Account Name(s)	The name of the account.
Source Account Type(s)	The type of account that the contact information is for.
Image	The image associated with the contact.

Additional Information

Android Contacts (UFED Agent)

Description	Android Contacts (UFED Agent) contains information recovered from the Contacts application on Android. These contacts are recovered from <contacts> tag found in a UFED Report.xml.
Recovery method	Parsing

Attribute	Description
Contact Name	The name of the contact. This data is retrieved from the <name> tag within contact elements in a UFED Report.xml.
Phone Numbers	The phone number of the contact. This data is retrieved from the <phone_number> tags within the contact elements in a UFED Report.xml.
Email Address(es)	Any email addresses associated with the contact. This data is retrived from the <extra_field> tags within the contact elements in a UFED Report.xml.
Company	The company name of the contact. This data is retrived from the <extra_field> tags within the contact elements in a UFED Report.xml.
Address	The mailing address of the contact. This data is retrieved from the <extra_field> tags within the contact elements in a UFED Report.xml.
Source Account Type(s)	The source from where the contact information is saved (that is, whether the contact is saved to the SIM card, the device, or another account). This data is retrieved from the <memory> tag within the contact elements in a UFED Report.xml.
Notes	The data from the notes field for the contact. This data is retrieved from the <extra_field> tag within calendar elements in a UFED Report.xml.

Attribute	Description
Additional Data	Any additional data that is recovered that's related to the contact. This field is in XML format as the data recovered is directly from the Report.xml without any further interpretation.

Additional Information

Android Google Hangouts Messages

Description	Android Google Hangouts Messages contains the messages from Google Hangouts from an Android device.
Recovery method	Parsing

Attribute	Description
Sender Phone ID	The identifier of the device for who sent the message.
Sender Full Name	The full name of the sender who sent the message.
Sender Fall-back Name	The name of the sender, if they don't have a full name.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.

Attribute	Description
Recipient Phone ID	The identifier of the recipient of the message.
Recipient Full Name	The full name of the recipient of the message.
Recipient Fallback Name	The name of the recipient, if they don't have a full name.
Message	The body of the message.
Message Type	The type of the message. The message type value can be 'Sent Message', 'Received Message', 'Participant joined/left the Hangout', 'Video Chat Started', 'Video Chat Ended', 'History Turned Off', 'History Turned On', 'Participant left the Hangout', or 'Participant joined the Hangout'.
Sender Profile Photo URL	The URL to the profile photo of the sender of the message.
Recipient Profile Photo URL	The URL to the profile photo of the recipient of the message.
Remote Attachment URL	The URL to the attachment of a message.
Attachment Type	The type of the attachment.
Latitude	The latitude of the message. It has not been determined whether this is the sender of the message, the recipient of the message, or just where the device received the message.
Longitude	The longitude of the message. It has not been determined whether this is

Attribute	Description
	the sender of the message, the recipient of the message, or just where the device received the message.
Location URL	The URL to a location on Google maps of the image.
Location Thumbnail URL	The URL to a thumbnail picture of the location of the message on Google Maps.

Additional Information

Android Kik Messenger Attachments

Description	Android Kik Messenger Attachments contains the attachments of messages from Kik Messenger from an Android device.
Recovery method	Parsing

Attribute	Description
Media ID	The ID of the attachment.
Attachment	The attachment.
File Metadata	Any metadata from the file.

Additional Information

Android Kik Messenger Contacts

Description	Android Kik Messenger Contacts contains information about a user's Kik Messenger contacts.
Recovery method	Parsing

Attribute	Description
Contact ID	The ID of the contact.
Display Name	The display name of the contact.
Local Name	The local name of the person on the device.
User Name	The username of the contact.
Photo Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the contact's profile photo.
Photo URL	The URL to the profile photo of the contact.
Group Member	Indicates whether the contact is a member of a group (Yes or No).
Blocked	Indicates whether the contact is blocked by the local user.

Additional Information

Android Kik Messenger Messages

Description	Android Kik Messenger Messages contains Kik Messenger messages that were sent or received by the local user.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Partner	The person the local user sent a message to or received a message from.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the message.
Message Body	The body of the message.
Message Status	The status of the message. The possible values are Trying to establish connection, Message has been sent to recipient, Message has been delivered to recipient, Message has been read by recipient and Unknown message status.
Message Type	The type of the message. The possible values are Message Received, Message Sent and Unknown Message Type.
Media ID	The ID of the attachment.
Media Info	The description of the attached media.
Attachment	The attachment sent with the message.

Additional Information

Android Messages

Description	SMS/MMS messages sent and received using Android Messages.
Recovery method	Parsing and carving

Attribute	Description
Sender	The name of the sender or the phone number if the name is not available.
Sender Phone Number	The phone number of the sender.
Recipient	The recipient of the message.
Message Sent Date/Time	The date and time when the message was sent.
Message Received Date/Time	The date and time when the message was received.
Message	The content of the message.
Message Status	The read status of the message.
Message Type	The message type. An example of message type is Text/plain.
Message Direction	Indicates whether the message was sent by or recieved on the local user's device.
Attachment Path	The path of an attachment.
Attachment Data	Indicates whether attachment data was recovered (Yes or No).

Attribute	Description
Recovered	
Subject	The optional subject line provided for an MMS message.
Target File Size (Bytes)	The size of attachments.
Latitude	The latitude associated with a location message.
Longitude	The longitude associated with a location message.
Avatar Path	The path to the contact icon used for the sender.

Additional Information

Android MMS

Description	MMS messages sent or received using an Android device. These messages are recovered from mmssms.db.
Recovery method	Parsing and carving

Attribute	Description
Sender	The phone number of the device that sent the message.
Recipient(s)	The phone numbers of the devices that received the message.
Message Direction	Indicates whether the message was incoming or outgoing. If the direction is not recognized, the value will be an integer.
Original Transmit	The date and time when the message was first sent from the

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	sender.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent (only for out-going messages).
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received (only for incoming messages).
Message	The message body of the MMS message.
Attachments	The file names of all recovered attachments.
Attachment Data Recovered	Indicates whether attachment data was recovered (Yes, No, or Partial).

Additional Information

Android MMS (UFED Agent)

Description	Android MMS (UFED Agent) contains MMS messages sent or received using the Messages app on Android. These messages are recovered from <mms_messages> tags found in a UFED Report.xml
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where the data was recovered from.

Attribute	Description
Partner Name	The name of the person who communicated with the local user. This data is retrieved from the <to> or <from> tags within mms_message elements in a UFED Report.xml.
Partner Phone Number	The phone number of the person who communicated with the local user. This data is retrieved from the <to> or <from> tags within mms_message elements in a UFED Report.xml.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the message, though it is unclear whether this represents the sent or received time. This data is retrieved from the <timestamp> tag within mms_message elements in a UFED Report.xml.
Subject	The subject of the message. This data is retrieved from the <subject> tag within mms_message elements in a UFED Report.xml.
Message	The body of the message, excluding any attachments. This data is retrieved from the <body> tag within mms_message elements in a UFED Report.xml.
Message Direction	The direction of the message relative to the Local User. This data is retrieved from the <to> or <from> tags within mms_message elements in a UFED Report.xml.
Message Status	The status of the message. This data is retrieved from <status> tag within mms_message elements in a UFED Report.xml. However, if the value in the <folder> tag is Draft, this attribute will indicate Draft.
Priority	The priority of the message. This data is retrieved from <priority> tags within mms_message elements in a UFED Report.xml.
Attachment Name(s)	The attachment file name. This data is recovered from the <attachments> tag within mms_message elements in a UFED Report.xml.
Attachment	The attachment file.

Additional Information

Android Sim Card Information

Description	Android SIM Card Information is information about the device's SIM card that is recoverable if the user has the Android Messages application installed on the device.
Recovery method	Parsing

Attribute	Description
ICCID	The ICCID (Integrated Circuit Card Identifier) is a serial number stored in the SIM card.
Service Provider Name	The name of the mobile service provider.
Phone Number	The phone number associated with the SIM card.
IMSI	The IMSI (International Mobile Subscriber Identity) is a unique number identifying a GSM (Global System for Mobile Communications) subscriber.

Additional Information

Android SMS

Description	SMS messages sent using the Messages app on Android.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Partner	An identifier for the person who communicated with the local user.
Received Date/Time-(UTC)(dd/MM/yyyy)	The time the message is received.
Sent Date/Time-(UTC)(dd/MM/yyyy)	The time the message is sent. This value will also display the time when the message has a direction of queued, failed or outbox.
Original Transmit Date/Time-(UTC)(dd/MM/yyyy)	Original transmit timestamp.
Message	The message body of the SMS message.
Message Direction	Indicates whether the message was incoming or outgoing.
Application	The application from which the message was sent.

Additional Information

Android SMS (UFED Agent)

Description	Android SMS (UFED Agent) contains SMS messages sent or received

	using the Messages app on Android. These messages are recovered from <sms_messages> tags found in a UFED Report.xml.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Partner Name	The name of the person who communicated with the local user. This data is retrieved from the <name> tag within sms_message elements in a UFED Report.xml.
Partner Phone Number	The phone number of the person who communicated with the local user. This data is retrieved from the <number> tag within sms_message elements in a UFED Report.xml.
Message Date/Time - UTC (yyyy-mm-dd)	A date and time associated with the message, though it is unclear whether this represents the sent or received time. This data is retrieved from the <timestamp> tag within the sms_message elements in a UFED Report.xml.
Message	The message content for the message. This data is retrieved from the <text> tag within sms_message elements in a UFED Report.xml.
Message Direction	The direction of the message (either incoming or outgoing). This data is retrieved from the <type> tag within sms_message elements in a UFED Report.xml.
Message Status	The status of the message. Values can be Read, Unread, or Sent. This data is retrieved from the <status> tag within sms_message elements in the UFED Report.xml.

Attribute	Description
SMSC	The Short Message Service Center (SMSC) associated with the message. This data is retrieved from the <smsc> tag within sms_message elements in a UFED Report.xml.

Additional Information

Android SMS/MMS

Description	SMS and MMS messages sent or received using an Android device. These messages are recovered from mmssms.db.
Recovery method	Parsing and carving

Attribute	Description
Sender	The phone number of the device that sent the message.
Recipient(s)	The phone number(s) of the device(s) that received the message.
Message	The message that was sent.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent (only for out-going messages).
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received (only for incoming messages).
Original Transmit Date/Time -	The date and time when the message was first sent from

Attribute	Description
UTC (yyyy-mm-dd)	the sender.
Direction	Indicates if the message is incoming, outgoing, draft, out-box, failed, queued, unknown, or alert.
Status	The status of the message.
Type	Whether the message was SMS or MMS.
Attachments	The file names of all recovered attachments.
Attachment Data Recovered	Indicates whether attachment data was recovered (Yes, No, or Partial).
Application	The application from which the message was sent.

Additional Information

Android SMS/MMS (Content Provider)

Description	SMS/MMS messages sent or received using an Android device. Data for this artifact is recovered during the acquisition process using an Android Content Provider.
Recovery method	Parsing

Attribute	Description
Participants	The phone numbers of the people in the conversation.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was either received if it was incoming or sent if it was outgoing.
Original Transmit Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was first sent from the sender to the local user.
Message	The message body of the MMS message.
Message Status	The status of the message.
MIME Type	The MIME type for the attachment.
Attachment	The recovered attachment.

Additional Information

Android SMS/MMS (Google Play Services)

Description	SMS and MMS messages sent or received using an Android device. These messages are recovered from icing_mmssms.db.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Partner	An identifier for the person who communicated with the local user.

Attribute	Description
Sent Date/Time - UTC (yyyy-mm-dd)	The time the message is sent.
Received Date/Time - UTC (yyyy-mm-dd)	The time the message is received.
Message	The message body of the SMS message.
Message Type	The type of message. Possible values are MMS and SMS.
Message Direction	Indicates whether the message was incoming, outgoing, draft, sent, outbox, failed, or queued.
Message Status	The status of the message (Read or Unread).

Additional Information

Android Snapchat Accounts Information

Description	Android Snapchat Accounts Information contains information about the accounts that the user has logged in on the device with.
Recovery method	Parsing and carving

Attribute	Description
User ID	The ID of the user.
User Name	The username of the user.

Attribute	Description
Display Name	The display name of the user.
Email Address	The email address of the user.
Phone Number	The phone number of the user.
Country	The location of the user, specified by country.
Birthday	The birthday of the user.
Last Login Date	The most recent date and time that the user used the application.
Account Creation Date/Time	The date and time that the user created the account

Additional Information

Android Snapchat Event Logs

Description	Android Snapchat Event Logs contains the events performed by the user.
Recovery method	Parsing and carving

Attribute	Description
Event	The event that the user performed.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time that the event occurred.
Event Parameters	The parameters of the performed event.

Additional Information

Android Snapchat Friends

Description	Android Snapchat Friends contains the friends of the user.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username of the friend.
Display Name	The name that is displayed for that friend on the local device.
Added Them Date/Time - UTC (yyyy-mm-dd)	The date and time that the friend added the user on the device.
Added Me Date/Time - UTC (yyyy-mm-dd)	The date and time that the user on the device added the friend.

Additional Information

Android Snapchat Photo Transfers

Description	Android Snapchat Photo Transfers contains attributes of the photos sent between users.
Recovery method	Parsing and carving

Attribute	Description
Sender	The person that sent the photo.
Receiver	The person that received the photo.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the photo was sent/received.
Was Viewed	Indicates whether or not the receiver has viewed the sent photo.
Type	The type specifies if the photo was sent or received.
Send Succeeded	Whether the message was successfully sent to the recipient.
Screenshot Taken	Indicates if a screenshot was taken or not.
Photo Id	The identifier of the photo.

Additional Information

Android Snapchat Received Images

Description	Android Snapchat Received Images contains the photos that the user on device has received.
Recovery method	Parsing and carving

Attribute	Description
Image	The actual picture content.
Snapchat Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time of the picture according to Snapchat.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the picture was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time whent he picture was created.
Size (Bytes)	The size of the picture
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Skin Tone Percentage	The percentage of the image that is skin tone.
MD5 Hash	The MD5 hash of the image.
SHA1 Hash	The SHA1 hash of the image.
PhotoDNA Hash	The PhotoDNA hash of the image.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

Android Snapchat Received Snaps

Description	Android Snapchat Received Snaps contains Snaps containing pictures and videos that have been sent to the local user.
Recovery method	Parsing

Attribute	Description
Sender	The user who sent the snap.
Picture	A picture or thumbnail of the video that was received as the snap.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the snap was sent.
Media Type	Whether the snap was a picture or video snap.
Skin Tone Percentage	The percentage of the video snap that contains what appears to be visible skin.
Status	The status of the snap.
Display Time (seconds)	Indicates how long the snap can be viewed for, in seconds.
Broadcast URL	The URL of a broadcasted snap.
Broadcast Text	The text of a broadcasted snap.

Additional Information

Android Snapchat Sent Snaps

Description	Android Snapchat Sent Snaps contains the snaps that have been sent by the user.
Recovery method	Parsing and carving

Attribute	Description
Recipient	The recipient of the snap.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the snap was sent.
Status	The status of the snap.

Additional Information

Android Snapchat Stories

Description	Android Snapchat Stories contains information about Snapchat Stories that are recovered, along with any decrypted media content.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username of the owner of the story.
Caption	The caption text associated with the story.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the story was first posted.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time when the local user viewed the story.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the story expires.
Screenshot Taken	Indicates the number of screenshots that the local user takes of the story.
Display Time (seconds)	The duration of the snap story.
Attachment Path	The path to an encrypted attachment.
Media URL	A URL to the location of the attachment. The URL will expire after some time.
Picture	The decrypted picture attachment.
Attachment	The decrypted attachment (if it's not a picture).

Additional Information

Android Telegram Chats

Description	Information about the conversations that the suspect participates in using the Telegram application.
Recovery method	Parsing

Attribute	Description
Chat ID	The ID of the chat.
Chat Type	The type of the chat.
Chat Name	The name of the chat.
Unread Count	The number of unread messages.
Last Message ID	The ID of the last message in the chat.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message in the chat.
User ID	The ID of the other user in the chat.
RSA Key	The RSA key of the chat, if it is encrypted.
RSA Key Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the RSA key was created.

Additional Information

This table doesn't contain any of the actual text from the conversations that occur. However, the table does contain some useful metadata about group chats such as the RSA ID.

Android Telegram Contacts

Description	Information about a subject's contacts that are displayed in Telegram. The application pulls the list of potential contacts from Android Contacts, meaning that these users may or may not be Telegram users.
Recovery method	Parsing

Attribute	Description
User ID	The ID of the user.
First Name	The user's first name.
Last Name	The user's last name.
Phone Number	The phone number associated with the user's account.
Second Phone Number	The second phone number associated with the user's account. If there is no second phone associated with the account, this value is the same as the above Phone column.
Deleted	Whether the suspect marked the user's information for deletion.

Additional Information

Android Telegram Messages

Description	Individual chat messages that are sent and received using the Telegram application.
Recovery method	Parsing

Attribute	Description
Partner	The name of the conversation partner. In case the name is not available, it displays 'Chat Type:id', where the ID is the telegram ID of the partner (or conversation ID)

Attribute	Description
Chat Type	The type of chat that the message belongs to.
Direction	The direction of the message.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the message was created on the local device.
Message Body	The body of the message.
Action	The action that occurred.
Type	The type of the message that was sent or received. This value can be one of the following: Text, Completed Call, Geo Location, Service, Video call.
Call Duration (Seconds)	The duration of the call.
Latitude	The latitude of a location message.
Longitude	The longitude of a location message.
Local Media Path	The path to the content of the media file on the local phone.
Attachment	The attachment sent with the message.

Additional Information

Android Telegram Users

Description	Information about the users that a subject has interacted with using Telegram.
Recovery method	Parsing

Attribute	Description
User ID	The ID of the user.
First Name	The user's first name.
Last Name	The user's last name.
User Name	The user's user name.
Phone Number	The phone number associated with the user's account.
Last Seen Date/Time	The date and time of the user's last seen.
Contact Added	Indicates whether the subject has added the user as a contact.
Deleted	Indicates whether the contact was deleted by the subject.
Verified	Indicates whether the user has verified their account.
Bot Account	Indicates whether the user is a bot account.
Mutual Contact	Indicates whether the subject has a mutual contact with the user.
Self Contact	Indicates whether the contact is the subject's own user account.

Additional Information

Android TextNow Calls

Description	Android TextNow Calls contains information about calls and voicemails that are sent and received through the TextNow application.
Recovery method	Parsing and carving

Attribute	Description
Call Type	The type of call or voicemail.
Direction	Whether the call was incoming or outgoing.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the call or voicemail.
Duration (Seconds)	The duration of the call.
Contact ID	The ID of the other call participant.
Contact Type	The other participant's contact type.
Conversation Partner	The name of the other call participant.
Voicemail URL	The URL of the voicemail.
Message Status	The status of the message ('Read' or 'Unread').
Attachment Path	The voicemail attachment path.

Additional Information

If the Contact Name cannot be determined, the Local Contact Key may be used to locate the corresponding entry in the iOS TextNow Contacts artifact.

Android TextNow Chat

Description	Android TextNow Chat contains chat messages that are sent and received through the TextNow application.
Recovery method	Parsing and carving

Attribute	Description
Message	The body of the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Contact ID	The ID of the other message participant.
Contact Type	The other participant's contact type.
Message Partner	The phone number or username of the other participant.
Message Type	The type of message.
Message Direction	Whether the message was incoming or outgoing.
Group Name	The group name, if the message was sent to a group chat.
Message Status	The status of the message ('Read' or 'Unread').
Attachment Path	The attachment path.
Attachment	The attachment.

Additional Information

If the Contact Name cannot be determined, the Local Contact Key may be used to locate the corresponding entry in the iOS TextNow Contacts artifact.

Android TextNow Contacts

Description	Android TextNow Contacts contains the application, phone, email and group contacts that a user has in the TextNow application.
Recovery method	Parsing

Attribute	Description
Contact ID	The name of the contact.
Contact Type	The contact's type.
Contact Name	The display name contact.

Additional Information

Android TextNow Groups

Description	Android TextNow Groups contains membership information for TextNow group chats.
Recovery method	Parsing and carving

Attribute	Description
Contact ID	The ID for the group.
Group	The name of the group.

Attribute	Description
Member Name	The username of a group member.
Type	The group member's contact type.
Display Name	The display name of the group member.
Contact Uri	The Android resource URI of the group member.

Additional Information

Android TextNow Profile

Description	Android TextNow Profile contains TextNow user profiles and application preference settings.
Recovery method	Parsing and carving

Attribute	Description
First Name	The first name of the TextNow user.
Last Name	The last name of the TextNow user.
Email	The email of the TextNow user.
User Name	The username of the TextNow user.
Phone Number	The phone number of the TextNow user.
Signature	The signature automatically appended to the end of each TextNow message sent by the user.

Attribute	Description
Last Number Called	The last number called using the TextNow application by the user.
TextNow Credit	The TextNow credit held by the user.
Balance	The TextNow cash balance held by the user.

Additional Information

Android TigerText Messages

Description	Android TigerText Messages contains messages from the TigerText Android application.
Recovery method	Parsing

Attribute	Description
Sender Display Name	The display name of the message sender.
Sender First Name	The first name of the message sender.
Sender Last Name	The last name of the message sender.
Sender Email	The email address of the message sender.
Sender Phone Number	The phone number of the message sender.
Recipient Display Name	The display name of the message recipient.

Attribute	Description
Recipient First Name	The first name of the message recipient.
Recipient Last Name	The last name of the message recipient.
Recipient Email	The email address of the message recipient.
Recipient Phone Number	The phone number of the message recipient.
Message Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message Expiry Date/Time - UTC (yyyy-mm-dd)	The date and time that the message will expire.
Message Text	The text content of the message.
Message Recalled	Whether the message was recalled. This value is 'True' for recalled, and 'False' for not recalled.
Attachment Type	The file type of the attachment (if any).
Attachment	Attachment data.
Message Status	The status of the message (sent, delivered or read).

Additional Information

Android WhatsApp Accounts Information

Description	WhatsApp Accounts Information Contains the login information for the user's account, including the private key used for authentication.
Recovery method	Parsing

Attribute	Description
WhatsApp Name	The WhatsApp username that is associated with the account.
Phone Number	The phone number used to register the account.
Private Key	The decryption key of the account.

Additional Information

Android WhatsApp Chats

Description	WhatsApp Chats contains information about chat sessions that occur between the local user and another user or group. This artifact indicates the IDs of each participant as well as information about unread messages and the time when the last message was sent.
Recovery method	Parsing

Attribute	Description
Individual Chat Name	If the chat is with an individual, this value indicates the name of the participant.
Group Chat Name	If the chat is a group chat, this value indicates the name of the group.
Chat ID	The ID of the individual or group involved in the chat.
Phone Number	The phone number associated with an individual contact.

Attribute	Description
Last Message	The text body of the last message sent in the chat.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the last message in the chat was sent.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the conversation was created.
Unread Message Count	The number of unread messages in the chat.
Missed Call Count	The number of missed calls in the chat.

Additional Information

Android WhatsApp Contacts

Description	Android WhatsApp Contacts contains contacts that were added to WhatsApp by the local user.
Recovery method	Parsing

Attribute	Description
Image	The actual picture content.
ID	The unique identifier for the contact.
Phone Number	The contact's phone number.
Display Name	The contact's full name.

Attribute	Description
Given Name	The contact's given (i.e. first) name.
Family Name	The contact's family (i.e. last) name.
WhatsApp Name	The contact's name that is displayed to other users.
Status	The contact's status message.
Status Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the status message was updated.
Is WhatsApp User	Identifies whether the user is using WhatsApp or not.
Frequently Contacted	Indicates whether this contact is contacted frequently by the user.

Additional Information

To learn more about artifacts from WhatsApp Messenger, sign in to the Support Portal to read the article Artifact profile: WhatsApp Messenger.

Android WhatsApp Groups

Description	Android WhatsApp Groups contains information about the WhatsApp Group chats that the user participates in.
Recovery method	Parsing and carving

Attribute	Description
Picture	The profile picture associated with this group.
Group Chat ID	The unique identifier for group chats. The Group Chat ID format is creator phone number-creation epoch time@g.us.
Group Name	The name of the group that is seen by users in the chat list and the conversation view.
Description	The description of the group.
Admin IDs	The IDs of the administrators of the group chat.
Admin Names	The names of the administrators of the group chat.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the group was created.
Group Member(s)	The list of contact IDs for the members of the group.

Additional Information

Android WhatsApp Live Locations

Description	Android WhatsApp Live Locations captures Live Locations that are shared with the local device user. The coordinates in each result represent the sender's last shared location. Once a Live Location expires, it is no longer recoverable.
Recovery method	Parsing

Attribute	Description
ID	The user ID of the contact that is sharing their live location.
Phone Number	The phone number of the contact.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the live location coordinate was captured.
Latitude	The latitude associated with the live location.
Longitude	The longitude associated with the live location.
Speed (m/s)	The speed of the contact at the time the live location was captured.
Direction	The direction of travel for the contact at the time the live location was captured.

Additional Information

Android WhatsApp Messages

Description	Android WhatsApp Messages contains messages that were sent and received using WhatsApp.
Recovery method	Parsing and carving

Attribute	Description
Sender	The phone number of the message sender.

Attribute	Description
Sender Nick-name	The name of the message sender, retrieved from display_name.
Receiver	The phone number of the message recipient.
Receiver Nick-name	The name of the message recipient, retrieved from display_name.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent.
Message Received Date/Time - UTC (yyyy-mm-dd)	The date and time the message was received locally.
Recipient Received Date/Time - UTC (yyyy-mm-dd)	The date and time the message was received by the remote recipient.
Server Received Date/Time - UTC (yyyy-mm-dd)	The date and time the message was received by the server.
Message	The message text.

Attribute	Description
Type	The format of the message or the MIME type of the media attachment.
Chat Type	Defines the audience for the message/call. 'Individual' indicates one-on-one messages/calls, 'Group' indicates that the message/call involves more than one user, and 'Broadcast' indicates a message with multiple recipients.
Media Duration (Seconds)	The duration of the attached media.
Call Duration (Seconds)	The duration of the audio/video call.
Message Status	The sent/received status.
Latitude	The latitude of the location from which the message was sent.
Longitude	The longitude of the location from which the message was sent.
Attachment	The media attached to the message.
Media URL	The source URL of the attached media.
Starred	Indicates whether the user bookmarked (or 'starred') a message.
Forwarded	Indicates whether the user forwarded a message to another conversation

Additional Information

To learn more about artifacts from WhatsApp Messenger, sign in to the Support Portal to read the article Artifact profile: WhatsApp Messenger.

Android WhatsApp Profile Pictures

Description	Android WhatsApp Profile contains profile pictures that WhatsApp uses that are stored locally.
Recovery method	Parsing

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date/time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date/time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date/time of the picture in the file system.

Attribute	Description
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed. "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera that was used to take the picture (extracted from

Attribute	Description
	Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Longitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Exif Data	A searchable field for all raw exif properties.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Android WhatsApp User Profiles

Description	WhatsApp User Profiles contains profile information about the local WhatsApp user.
Recovery method	Parsing

Attribute	Description
Image	The user's profile image.
WhatsApp Name	The WhatsApp username that is associated with the account.
Phone Number	The phone number used to register the account.
Status	The current status that the user shares
Version	The version of the WhatsApp application.
Latitude	The latitude associated with the last location the user shared.
Longitude	The longitude associated with the last location the user shared.
Private Key	The decryption key of the account.

Additional Information

BlackBerry Messenger Contacts

Description	Contains the BBM Contacts recovered from an Android device.
Recovery method	Parsing

Attribute	Description
BlackBerry PIN	Contains the contacts BlackBerry PIN.
Display Name	Contains the contacts display name.
Personal Message	Contains the contacts personal message.
Personal Message Last Update Date/Time - UTC (yyyy-mm-dd)	The data and time the contacts personal message was updated.
Avatar	The contacts avatar.
Avatar Content Type	The avatar content type. An example is 'image/jpeg'
Locale	The contacts location.
Timezone	The contacts timezone.

Additional Information

BlackBerry Messenger File Transfers

Description	Contains the BBM File Transfers recovered from an Android device.
Recovery method	Parsing

Attribute	Description
BlackBerry PIN	BlackBerry PIN of the contact who the transfer is with.
Display Name	Display name of the contact who the transfer is with.

Attribute	Description
Transfer Date/Time - UTC (yyyy-mm-dd)	The date and time the transfer took place.
Transfer Direction	Indicates whether a file was sent or received.
Transfer State	Indicates whether a file transfer is 'Pending Approval' or 'Complete'.
Local File Path	The path on the device to the data transferred.
Content Type	The type of data that was transferred.
Transfer Description	Description of what is being transferred.
Attachment	The file that was transferred.
Total Transfer Size (Bytes)	The number of bytes the transferred file is.
Bytes Transferred	The number of bytes that were transferred.

Additional Information

BlackBerry Messenger Invitations

Description	BlackBerry Messenger Invitations contains BBM invite requests recovered from an Android device.
Recovery method	Parsing

Attribute	Description
BlackBerry PIN	The BlackBerry PIN of the user sending the invite request.
Display Name	The display name of the user sending the invite request.
Local Email Address	The local email address of the user.
Remote Email Address	The remote email address of the user.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date/time when the invite was sent/received.
Direction	This column states if the invite is a received invite or a sent invite.
Invitation Status	Contains the status of the invite request. The value can be Pending Approval or Unknown.
Invite Method	The method used for sending the invite request. The value can be Via PIN or Unknown.
Subject	The subject used for the invite request.
Greeting	The message sent with the invite request.

Additional Information

BlackBerry Messenger Locations

Description	BlackBerry Messenger Locations contains BBM locations recovered from an Android device.
Recovery method	Parsing

Attribute	Description
BlackBerry PIN	The BlackBerry PIN of the location sender.
Display Name	The display name of the location sender.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date/time when the location was sent/received.
Message Type	Indicates whether the message was sent or received.
Location Name	The name of the location
Latitude	The latitude of the location
Longitude	The longitude of the location
Altitude (meters)	The altitude of the location.
Accuracy (meters)	The accuracy in meters.
Street	The street address of the location.
City	The city of the location.
State/Province	The state/province of the location.
Country	The country of the location.
ZIP/Postal Code	The postal code/ZIP of the location.

Additional Information

BlackBerry Messenger Messages

Description	Contains the BBM messages recovered from an Android device.
Recovery method	Parsing and carving

Attribute	Description
Conversation ID	The conversation identifier.
BlackBerry PIN	The BlackBerry PIN of who sent the message to the device or who's receiving a message from the device.
Display Name	The display name of who sent the message to the device or who's receiving a message from the device.
Participants	The display names of the people in the conversation.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time the message was sent/received.
Message Content	The message sent/received.
Message Type	Contains the type of message that was sent. This can be one of the following: Message, Ping, File, Picture, Notification, Location.
Message Status	The status of the message (received or sent).
Message State	Contains the state of the message. This can be one of the following: 'Sent', 'Undelivered', 'Delivered, Unread', 'Read'.
Attachment	The attachment that was sent/received.

Additional Information

BlackBerry Messenger Profile

Description	Contains the BBM Profiles recovered from an Android device.
Recovery method	Parsing

Attribute	Description
BlackBerry PIN	The BlackBerry PIN associated with the profile.
Display Name	The display name associated with the profile.
Personal Message	The profiles personal message.
Personal Message Last Update Date/Time - UTC (yyyy-mm-dd)	The date and time the profile message was last updated.
Avatar	The profiles avatar.
Avatar Content Type	The avatar content type. An example is 'image/jpeg'.
Locale	The location of the profile.
Timezone	The timezone of the profile.
Keeps Chat History	Indicates whether or not the user keeps chat history.

Additional Information

Burner Contacts

Description	Burner Contacts contains information about a subject's Burner Contacts, as recovered from their Android device.
Recovery method	Parsing

Attribute	Description
Contact ID	The ID of the contact.
Contact Name	The name of the contact.
Phone Number	The phone number of the contact.
Burner ID	The ID of the Burner application associated with the contact.
Date/Time Created - UTC (yyyy-mm-dd)	The date and time when the contact was created.

Additional Information

Burner Messages

Description	Burner Messages contains information about messages and calls that are sent and received using Burner.
Recovery method	Parsing

Attribute	Description
Sender	The phone number of the sender.
Recipient	The phone number of the recipient.
Message	The body of the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Direction	Indicates whether the message was incoming or out-going.
Message Type	The type of message.
Media URL	The URL to the media file attached to the message.
Voicemail URL	The URL of the voicemail.

Additional Information

Burner Numbers

Description	Burner Numbers contains information about the burner numbers that the local user created.
Recovery method	Parsing

Attribute	Description
Burner ID	The ID of the Burner number.

Attribute	Description
Burner Number	The Burner phone number.
Display Name	The display name associated with the Burner number.
Created Date/Time	Indicates when the Burner number was created.
Expiration Date/Time	Indicates when the number will expire.
Mobile Phone	The phone number used to sign in to the Burner App.
User ID	The user id of the signed in user.

Additional Information

Cake Local User Account

Description	Cake Local User Account contains information about the logged in local user.
Recovery method	Parsing

Attribute	Description
Local User ID	The unique ID of the local user.
Local User Display Name	The display name of the local user.
Gender	The gender of the local user.
Birthday	The birthday of the local user.
Email Address	The email address of the local user.

Additional Information

Cake Messages

Description	Cake Messages contains messages sent and received by the local user.
Recovery method	Parsing

Attribute	Description
Sender ID	The unique user ID of the sender.
Sender Display Name	The display name of the sender.
Recipient ID	The Cake ID of the message recipient. If the chat type is Group chat, the recipient ID is the group ID.
Recipient Display Name	The display name of the message recipient. If the chat type is Group chat, the recipient display name is the group display name.
Message	The body of the message.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was created.
Chat Type	The type of chat where the message was sent (Group chat or One to one).
Picture URL	The URL of the picture, if one is attached to the message.
File	The attachment file.

Additional Information

Chatous Chat Messages

Description	Chatous Chat Messages contains messages that were sent and received using the Chatous application.
Recovery method	Parsing

Attribute	Description
Sender	The display name of the user who sent the message (Local User if it was the local user).
Recipient	The display name of the user who received the message (Local User if it was the local user).
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The body of the message.
Attachment Name	The name of the attachment that was sent.
Attachment Data Recovered	Indicates whether attachment data was recovered (Yes or No).

Additional Information

Chatous Chat Partners

Description	Chatous Chat Partners contains information about the users that the local user has communicated with.
Recovery method	Parsing

Attribute	Description
Screen Name	The name of the chat partner.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message in the chat.
Age	The age of the chat partner.
Gender	The gender of the chat partner. A blank value indicates that the chat partner is the Team Chatous account.
Locale	The location of the chat partner.
About	A summary of the chat partner.
Tag	The tag that matched the local user and the chat partner for a chat.
Profile Tags	The hashtags that the chat partner uses to describe themselves.

Additional Information

Discord Logged-in Account

Description	Discord Logged-in Account contains information about the user that is currently logged into Discord on the device. Information about other accounts that were previously logged into are not recoverable.
Recovery method	Parsing

Attribute	Description
User ID	The ID of the logged-in user.
User Name	The name of the logged-in user.
Email	The email address of the logged-in user.
Phone Number	The phone number of the logged-in user.
Locale	The locale of the logged-in user.
User Token	The authentication token of the logged-in user.
Platform	The cloud platform name.

Additional Information

Discord Messages

Description	Discord Messages contains information about messages and calls that are sent and received using Discord. Messages from some channels might be missing if they haven't been cached by the application. This artifact uses

	both parsing and carving techniques to recover messages.
Recovery method	Parsing and carving

Attribute	Description
Sender	The username of the message sender.
Sender ID	The ID of the message sender.
Message	The message content. If the message sent is a sticker, the message will display 'Sticker(sticker name)'.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Last Edited Date/Time - UTC (yyyy-mm-dd)	If the message has been edited then this indicates the date and time when the last edit has occurred.
Message Type	The type of the message (Message or Call).
Channel ID	The ID of the channel that the message was sent in.
Attachment URL	If the message includes an attachment, then this value indicates the saved URL of the attachment.
Attachment Name	If the message includes an attachment, then this value indicates the file name of the attachment.
Embedded Content Title	If the message contains a link, then this then this value indicates the title that's displayed in the link preview.
Embedded Content	If the message contains a link, then this value indicates the descrip-

Attribute	Description
Description	tion that's displayed in the link preview.
Call End Date/Time - UTC (yyyy-mm-dd)	If the message was a call, this indicates the date and time that the call ended.
Message ID	The Message ID of the message that this message is replying to.
Pinned	Indicates whether a message is pinned (True or False).
Mentions	The user mentioned in the message, if present.
In Reply To	The Message ID of the message that this message is replying to.
Reactors	The users who reacted to this message, if any. The order of reactors does not correspond to the reactions used.
Reaction	The emojis that were used to react to the message, if any. If a custom emoji is used, the name of that emoji will be listed instead of the emoji itself.

Additional Information

Facebook Messenger Calls

Description	Facebook Messenger Calls contains call data recovered from Facebook Messenger.
Recovery method	Parsing and carving

Attribute	Description
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
User Key	The user key of the call partner.
Thread Key	The thread key of the group where the call was made.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the call.
Call Duration (Seconds)	The duration of the call. If the call wasn't answered this field is Empty.
Call Type	The type of call. The types of calls are voice calls and group voice calls.
Answered	Indicates whether the call was answered or not.
Direction	The direction of the call.

Additional Information

Facebook Messenger Groups

Description	Facebook Messenger Groups contains data about group chats on Facebook Messenger.
Recovery method	Parsing and carving

Attribute	Description
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
Thread Key	The thread key of the group.
Group Name	The display name of the group.
Participants	The users that are a part of the group.
Participants User Names	The user names of the users that are a part of the group.
Sender(s)	The users that recently participated in the group (for example, by sending a message).
Senders User Names	The user names of the users that recently participated in the group.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The date and time of the last activity recorded in the group.
Message Count	The approximate number of messages in the group.

Additional Information

Facebook Messenger Messages

Description	Facebook Messenger Messages contains messages recovered from Facebook Messenger.
Recovery method	Parsing and carving

Attribute	Description
Sender Name	The display name of the person sending the message.
Sender ID	The user ID of the person sending the message.
Receiver Name	The display name of the person receiving the message.
Group Name	The display name of the group receiving the message.
Receiver ID	The user ID of the person receiving the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time when message was sent.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time the message was deleted from the application.
Text	The text of the message.
Message Type	The type of message that was sent. If multiple attachments were sent together, this fragment indicates the number of attachments.
Send State	Represents whether the message was sent, received or queued. This field is always empty for Android.
Media Info	The information about the media that is found. This value can be a URL to the media, a file name, or a sticker ID.
Latitude	The latitude portion of the location data that is sent with the message.
Longitude	The longitude portion of the location data that is sent with the message.

Attribute	Description
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
Thread ID	The thread ID of the message. This is also the Facebook ID of the remote party.
Message ID	The internal unique message ID.
Message Source	The source of the message creation platform.
Attachment	The recovered attachment. If the attachment is a video, the video gets segmented into multiple files. Each segment gets collected for playback in Magnet AXIOM, but the actual file size might differ from the size that AXIOM reports due to the segmentation.

Additional Information

Facebook Messenger Users Contacted

Description	Facebook Messenger Users Contacted contains information about users contacted from the device using Facebook Messenger.
Recovery method	Parsing and carving

Attribute	Description
User Key	The user key of the user.

Attribute	Description
First Name	the first name of the user.
Last Name	The last name of the user.
Name	The display name of the user.
Username	The unique identifier of the user.
Profile Picture URL	The URL of the user's profile picture.
Is App User	Identifies whether the user is using Facebook Messenger or not.
Is Friend	Identifies whenever the user is a friend of the local user.
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
Rank	User's rank within the app.

Additional Information

Glide Messages

Description	Glide Messages contains messages sent and received by the local user.
Recovery method	Parsing

Attribute	Description
Sender ID	The unique user ID of the sender.
Sender Name	The name of the sender.
Recipient ID(s)	The Glide IDs of the message recipients.
Recipient Name(s)	The names of the message recipients.
Message	The body of the message.
Message Type	The type of message.
Created Date/Time	The date and time when the message was created.
Read	The read status of the message.
Media URL	The URL to any media that's attached to the message.
Chat Type	The type of chat where the message was sent (group or oneToOne).

Additional Information

Glide Users

Description	Glide Users contains information about the contacts that the local user has added using Glide. The local user's contact information is also recovered by this artifact.
Recovery method	Parsing

Attribute	Description
User ID	The unique ID of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
Email Address	The email address of the user.
Gender	The gender of the user.
Account Type	The type of account associated with the user.
Last Seen Date/Time	The last time the user was seen online.

Additional Information

Google Duo Activity

Description	Google Duo Activity contains details about audio calls, video calls, and messages sent and received by the user.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message or call.
Recipient(s)	The recipient(s) of the message or call. The recipients of a group call are the users who joined the call. If no one joined the group call, this fragment will be empty.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	The date and time of the message or call.
Activity Type	The type of activity. Possible values include Audio Call, Video Call, and Message.
Direction	The direction of the activity.
Call Status	The status of the call. Possible values include Answered, Not Answered, and Rejected.
Call Duration (Seconds)	The duration of the call.
Message ID	The ID of the message (if the Activity Type is Message).
Message	The content of the message.
Attachment Name	The name of the attachment from the message.
Reaction	The reaction to a message. You can associate the reaction to the message through the Message ID. In the Google Duo app, the reaction is overlaid on the message, but in AXIOM Examine, the reaction is presented on its own.
Attachment	The attachment from the message.

Additional Information

Google Duo Group Calls

Description	Google Duo Group Calls contains details about the video calls made and received by the user.
Recovery method	Parsing

Attribute	Description
Session ID	The session ID of the group call.
Call Status	The status of the call. 'Incoming Initiated' indicates an incoming call request, 'Incoming Cancelled' indicates that the caller cancelled the request before connecting, and 'Call' indicates an incoming call that was connected or an outgoing call that is unknown if any participants joined the call.
Caller	The phone number of the caller.
Recipient(s)	The recipients of the call.
Call Date/Time - UTC (yyyy-mm-dd)	The date and time of the call.
Call Duration (Seconds)	The duration of the call.
Call Type	The type of call.

Additional Information

Google Duo Groups

Description	Google Duo Groups contains membership information of Google Duo Groups.
Recovery method	Parsing

Attribute	Description
Group Chat ID	The ID of the group.
Group Name	The display name of the group.
Group Member Name(s)	The display names of the group members.
Group Member ID(s)	The IDs of the group members.

Additional Information

Google Hangouts Cached Images

Description	Google Hangouts Cached Images contains the cached images from Google Hangouts from an Android device.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the cached image.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	The date and time of the image. The significance of the date and time is unknown to us.
Image	The cached image.

Additional Information

Google Hangouts Voice Calls

Description	Google Hangouts Voice Calls contains a history of voice calls between the local user and other users.
Recovery method	Parsing

Attribute	Description
Phone Number	The phone number of the call participant.
Call Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the call started.

Additional Information

Google Meet Meeting History

Description	Google Meet Meeting History contains the meetings that any local user on the device has joined.

Recovery method	Carving

Attribute	Description
Meeting ID	The unique ID for the meeting.
Meeting Code	The code that was used to join the meeting.
URL	The URL for the meeting.
Joined Date/Time - Local Time	The local date and time that the local user joined the meeting.
Type	Whether the local user created or joined the meeting.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

GroupMe Accounts

Description	GroupMe Accounts contains information about the accounts that the local user has logged in with on the device.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the local user.

Attribute	Description
Display Name	The display name of the local user.
Email Address	The email address of the local user.
Phone Number	The phone number of the local user.
Created Date/Time	The date and time that the account was created (specific to iOS).
Login Date/Time	The date and time that the account was logged in on the device (specific to Android).
Profile Picture URL	The URL of the profile picture of the local user.
Password/Token	The local user password/token.

Additional Information

GroupMe Contacts

Description	GroupMe Contacts contains information about a user's contacts.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the contact.
Display Name	The display name of the contact.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact was added.

Additional Information

GroupMe Groups

Description	GroupMe Groups contains information about the groups that the logged-in user is a member of.
Recovery method	Parsing

Attribute	Description
Group	The group number.
Group Name	The name of the group.
Topic	The topic of the group.
Creator ID	The creator identifier of the group.
Created Date/Time	The date and time when the group was created
Group Member ID(s)	The IDs of all of the group's participants.
Group Member Name(s)	The names of all of the group's participants.

Additional Information

GroupMe Messages

Description	GroupMe Messages contains the messages sent and received using GroupMe.
Recovery method	Parsing

Attribute	Description
Sender Name	The name of the message sender.
Sender ID	The user ID of the message sender.
Recipient Name(s)	The user name(s) of the message recipient(s).
Recipient ID(s)	The user ID(s) of the message recipient(s).
Sent Date/Time	The date and time when the message was sent.
Message	The message text.
Photo URL	The URL to the photo associated with the message.
Video URL	The URL to the video associated with the message.
Locale	The name of the location in the location data sent with the message.
Latitude	The latitude part of location data sent with the message.
Longitude	The longitude part of location data sent with the message.
Event	The event sent with the message.
Document Title	The document details sent with the message.
Poll	The poll details sent with the message.

Additional Information

Gtalk Contacts

Description	Gtalk Contacts contains contact information that was recovered from Gtalk.

Recovery method	Parsing

Attribute	Description
Username	The username/Gmail address of the contact.
Nickname	The nickname of the contact.
Local Account	The user account of the user logged into Gtalk.

Additional Information

Gtalk Messages

Description	Gtalk Message contains the details of messages that were recovered from Gtalk.
Recovery method	Parsing

Attribute	Description
Sender	The user who sent the message.
Receiver	The user who received the message.
Local User	The local user ID.
Date/Time - UTC (yyyy-mm-dd)	The timestamp for the message.
Message	The message that was sent.
Sent/Received	The type of the message.

Additional Information

Houseparty Messages

Description	Houseparty Messages contains messages recovered from Houseparty.
Recovery method	Parsing

Attribute	Description
Sender	The username of the person sending the message.
Recipient	The username of the person receiving the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The content of the sent message.
Read Status	Indicates whether or not the message has been read.

Additional Information

Houseparty Users

Description	Houseparty Users contains information about the users that were contacted from the device using Houseparty.
Recovery method	Parsing

Attribute	Description
User Name	The username of the user.
Full Name	The full name of the user.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the user account was created.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the user account was last updated.

Additional Information

imo Contacts

Description	imo Contacts contains information about a user's contacts.
Recovery method	Parsing

Attribute	Description
User ID	The unique user ID of the contact.
Display Name	The display name of the contact.
Name	The full name of the contact.
Phone Number	The phone number of the contact.
Number of Times Contacted	The number of times that the local user initiates contact (by message or call) with the contact.

Additional Information

imo Messages

Description	imo Messages contains information about sent and received messages and calls made using the imo application.
Recovery method	Parsing

Attribute	Description
Local User	Indicates the local user identifier of the account.
Remote User ID	The user ID of the remote conversation partner.
Remote User Display Name	The display name of the remote conversation partner.
Direction	The direction of the message.
Message	The message content.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message Type	The type of the message (either call or message).
Attachment Path	The path to locate any attachments on the device.
Attachment	The attachment on the device.

Additional Information

IP Addresses - Audio/Video Calls

Description	IP Addresses of web audio/video calls show who a user was communicating with. Each instance of this artifact represents a single hop in the communication chain. By showing the relationship between multiple hops, you can determine where a call originated from and what the final destination was.
Recovery method	Carving

Attribute	Description
Call ID	The ID of the call.
Message ID	The ID of the message.
Domain	The domain used for the call.
Connection Type	The type of connection.
Origin IP Address	The originating IP address for this hop in the call.
Origin Port	The originating port for this hop in the call.
Destination IP Address	The destination IP address for this hop in the call.
Destination Port	The destination port address for this hop in the call.
Date/Time - UTC (yyyy-mm-dd)	The timestamp associated with this hop in the call.
Remote User ID	The unique ID of the remote user.
Communication Protocol	The communication protocol for this call (either UDP or TCP).
Metadata	Any additional details about the call.

Additional Information

Jott Groups

Description	Jott Groups contains information about the groups that the Jott user is a member of.
Recovery method	Parsing

Attribute	Description
Group Chat ID	The ID of the group chat.
Group Name	The display name of the group.
Participants	The users that are a part of the group.
Picture Path	The path to the group's picture, if one exists.

Additional Information

Jott Messages

Description	Jott Messages contains information about the messages sent or received by the Jott user.
Recovery method	Parsing

Attribute	Description
Sender	The username of the person sending the message.
Recipient	The username of the person receiving the message, or the group chat ID if the message is being sent to a group.
Message	The message being sent.
Direction	The direction of the message being sent.
Read Status	Indicates whether or not the message has been read.
Group Chat	Indicates whether or not this is a group chat.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received.
Attachment Path	The path to the attachment, if one exists.

Additional Information

KakaoTalk Browsing History

Description	KakaoTalk Browsing History contains the web browsing history on any links visited within the KakaoTalk application.
Recovery method	Parsing

Attribute	Description
URL	The URL of the webpage link opened in KakaoTalk.
Title	The title of the webpage link opened in KakaoTalk.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage link was accessed in KakaoTalk.

Additional Information
Sometimes, the web browsing history is duplicated in the database this artifact is recovered from. This behavior is expected, though the cause is unknown. The duplicated data and its associated timestamps are identical.

KakaoTalk Calls

Description	KakaoTalk Calls contains audio calls and/or video calls sent or received using KakaoTalk.
Recovery method	Parsing and carving

Attribute	Description
Call Status	Information about the call.
Duration (Seconds)	The duration of the call in seconds.
Sender ID	The KakaoTalk ID of the sender.
Sender Name	The name of the sender.
Chat ID	The ID of the KakaoTalk chat room session.

Attribute	Description
Call Type	Indicates whether the call was a voice call or a video call.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the call was made.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time that the call was deleted from the application.
Direction	Indicates whether the call was incoming or outgoing.

Additional Information
Call Status and Sender information are not available for deleted calls.

KakaoTalk Chat Rooms

Description	KakaoTalk Chat Rooms contains KakaoTalk chat rooms that the user participates in.
Recovery method	Parsing

Attribute	Description
Group Chat ID	The ID of the KakaoTalk chat room session.
Other Participants	The names or KakaoTalk IDs of the other chat room participants.
Chat Type	The type of chat room session.

Attribute	Description
Last Message	The last message sent by any participant in the chat room session.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the chat room session was last updated.
Unsent Message	Messages that the local user has written, but not sent to the chat room.
Group Name	The name of the group, if the chat room session is a group chat.
Invitation Status	The status of any invitations to the chat room.

Additional Information

KakaoTalk Detected Wifi

Description	KakaoTalk Detected Wifi contains the network name of any WiFi networks detected by KakaoTalk.
Recovery method	Parsing

Attribute	Description
Network Name (SSID)	The network name.

Additional Information
As of KakaoTalk 8.4.0, the data in this artifact is no longer available.

KakaoTalk Friends

Description	KakaoTalk Friends contains the user's KakaoTalk friends and contacts.
Recovery method	Parsing

Attribute	Description
ID	The KakaoTalk ID of the friend.
Name	The friend's name.
Contact Name	The friend's full contact name.
Nickname	The friend's nickname as set by the local user.
Status Message	The status message of the friend.
Favorite	Indicates whether the friend has been marked as a favorite.
Hidden	Indicates whether the friend has been hidden in the local user's application.
Phone Number	The friend's phone number.
Profile Picture URL	The URL for the friend's profile picture.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the friend's account was created.
User ID	The friend's KakaoTalk user ID.
Group Chat ID	The chat room session IDs that the friend shares with the local user.

Additional Information

KakaoTalk Messages

Description	KakaoTalk Messages contains messages sent or received using KakaoTalk.
Recovery method	Parsing and carving

Attribute	Description
Sender ID	The KakaoTalk ID of the sender.
Sender Name	The name of the sender.
Message	The message contents.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was created.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was deleted from the application.
Chat ID	The ID of the KakaoTalk chat.
Message Type	The type of the message sent.
Message Direction	Indicates whether the message was sent or received.
Additional Information	Additional information attached to the message.
Latitude	The latitude of location type messages.
Longitude	The longitude of location type messages.
Attachment	The attachment sent with the message.
Attachment Name	The file name of the attachment sent with the message.
Attachment Path	The file path of the attachment sent with the message.

Additional Information

Message and Sender information are not available for deleted messages.

LINE Chats

Description	LINE Chats contains the chats that the local user is a part of.
Recovery method	Parsing

Attribute	Description
Participants	The users in the chat (other than the local user).
Chat Name	The name of the chat.
Owner	The owner of the chat.
Last Message	The last message that was sent in the chat.
Sender	The user who sent the last message.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the last message was received.
Message Count	The number of messages that were sent in the chat.
Read Count	The number of messages that were read in the chat by the local user.

Additional Information

LINE Contacts

Description	LINE Contacts contains the user's LINE contacts.
Recovery method	Parsing

Attribute	Description
Line ID	The LINE ID of the contact.
Name	The name of the LINE contact.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the user contact was added.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact was last updated.
Status Message	The status of the contact.
Hidden	Indicates whether the contact has been marked as hidden.
Favorite	Indicates whether the contact has been marked as favorite.

Additional Information

LINE Messages

Description	LINE Messages contains messages that were sent and received through LINE on Android.

Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the message. The sender value can be the sender's name or Local User.
Recipient(s)	The recipient(s) of the message.
Message Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was created.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The body of the message.
Message Type	The type of the message. The Message Type value can be Audio, Call, Contact Card, File, Location, Note, Picture, Sticker, or Text.
Contact Card Name	The first and last name of the contact.
Read Count	The number of times that the message has been read.
Location Address	The address of the location.
Latitude	The latitude of the location when message type is Location.
Longitude	The longitude of the location when the message type is Location.
Audio Length (Seconds)	The length of the audio in seconds when the message type column is Audio.

Attribute	Description
Call Duration (Seconds)	The duration of the call in seconds when the message type is Call.
File Attachment	The name of the file that's sent when the message type is File.
File Size (Bytes)	The size of the file sent in bytes.
Attachment	The attachment sent with the message.
Thumbnail	A thumbnail of the image (if available).

Additional Information

LINE Pictures

Description	LINE Pictures contains pictures originating from LINE.
Recovery method	Parsing

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-	The created date and time of the picture in the file system.

Attribute	Description
mm-dd)	
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time -	The local date and time when the picture was edited (extracted from Exif data).

Attribute	Description
Local Time	
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture, or the name of the software that was used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Longitude	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Exif Data	A searchable field for all raw exif properties.
MD5 Hash	An MD5 hash of the image content.

Attribute	Description
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Mail.Ru Agent Contacts

Description	Mail.Ru Agent Contacts contains contact info for the Agent application on Android.
Recovery method	Parsing

Attribute	Description
Contact ID	The user ID of contact.
Display Name	The display name of contact.
Account Type	The type of the contact. The value can be Agent ID or Agent Channel.
Local User ID	The unique ID of the local user.

Additional Information

Mail.Ru Agent Messages

Description	Mail.Ru Agent Messages contains messages sent or received by the Agent user on Android.
Recovery method	Parsing

Attribute	Description
Local User ID	The unique ID of the local user.
Remote User ID	The user ID of the remote participant of the chat.
Remote Participant Display Name	The display name of remote participant.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was created.
Message	The content of the message.
Type	The type of the message. The value can be Text Message, Voice Call, Video Call or File Transfer.
Duration (Seconds)	The duration of voice or video call.
Direction	The direction of the message.
File Name	The file name of the attachment.
File	The attachment associated with the message.

Additional Information

Mail.Ru Agent User Accounts

Description	Mail.Ru Agent User Accounts contains information about the Agent user accounts that are saved locally on the Android device.
Recovery method	Parsing

Attribute	Description
User ID	The unique ID of the local user.
Active	Whether or not the account is currently logged in.
First Name	The first name of the account.
Last Name	The last name of the account.
Display Name	The display name of the account.
Birthday	The birthday of the account.
Phone Number	The phone number of the account.
Gender	The gender of the account.
Home Address	The home address of the account.

Additional Information

QQ File Transfers

Description	QQ File Transfers contains file transfers recovered from the QQ application.
Recovery method	Parsing

Attribute	Description
Local User ID	The local user ID who the file was transferred with.
Chat Partner / Group Chat ID	The unique ID of the chat partner or group the file was transferred with.
Partner Display Name	The name displayed for the partner the file was transferred with.
Server Date/Time - UTC (yyyy-mm-dd)	The server date and time that the file was transferred.
Direction	Sent/Received: Indicates the direction of the file transfer relative to the local user.
File Name	The file name of the file transferred.
File Path	The file path of the file transferred.
File Size (bytes)	The size of the file transferred.
MD5 Hash	The MD5 hash of the file.
SHA1 Hash	The SHA1 hash of the file.

Additional Information

QQ Local Users

Description	QQ Local Users contains local users recovered from the QQ application.
Recovery method	Parsing

Attribute	Description
Local User ID	The user ID of the local user.
Local User Display Name	The name displayed for the local user.
Country	The country of the user.
City	The city of the user.
Age	The user's age in years.
Birthday (yyyy-mm-dd)	The user's birthday in YYYY-MM-DD format.
Email	The user's email address.

Additional Information

QQ Messages

Description	QQ Messages contains messages stored by the QQ application.
Recovery method	Parsing

Attribute	Description
Local User ID	The unique ID of the local user.
Local User Display Name	The name displayed for the local user.
Chat Partner / Group Chat ID	The unique ID of the chat partner or group.
Sender User ID	The unique ID of the sender.
Sender Display Name	The name displayed for the sender.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the message.
Message	The text of the message.
Type	The type of content in the message.
Sent/Received	Indicates whether the message is incoming or outgoing (Sent or Recieved).
Read	Indicates whether the message has been read (Read or Unread).

Additional Information

Samsung Messages

Description	Samsung Messages is an application that is installed by default on Samsung Android devices and is used for sending SMS and MMS messages.
Recovery method	Parsing

Attribute	Description
Conversation Partner	The phone number of the other person in the conversation.
Contact Name	The name of the contact. This will display if we can get the contact name from the file contact_simple_name.dat.xml.
Group Member(s)	The list of phone numbers that are part of the group mass message chat.
Message	The message body text.
Subject	The subject of the message.
Message Received Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was originally meant to be received.
Message Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was created on the device, in both cases where it was either sent or received on the device.
Scheduled Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was scheduled by the local user to be sent.
Group Chat ID	The unique identifier for a group mass message sent by the local user.
Message ID	The message identifier. Some messages will have the same message identifier indicating they are part of the same message.
Message Type	Indicates whether the message is SMS or MMS.
Message Direction	Indicates whether the message was sent or received on the local user's device.
IMSI	The international mobile subscriber identity of the local device's

Attribute	Description
	SIM card.
Read	Indicates whether or not the message has been read by the local user.
Content Type	The content MIME type of the message.
File Name	The name of the file.
File Path	The local file path of the file sent or received.
URL	The URL of the website previewed in the message.
Description	The description of the website previewed in the message.
Title	The title of the website previewed in the message.
Search Query	This is an automatic search query result given when the web preview for a location or URL is sent in the message.
Attachment	The attachment associated with the message.

Additional Information

Samsung Text Message Logs

Description	Text message logs recovered from a Samsung Android device.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where data was recovered from.
Partner	An identifier for the person who communicated with the local user.
Partner Name	The name of the partner, as set by the local user.
Direction	The direction of the message, relative to the local device (Incoming or Outgoing).
Date/Time - UTC (yyyy-mm-dd)	The date and time of the text message.
Message Content	The text message content.
Subject	The subject of the text message. If message type is MMS this field has a value, otherwise is empty.
Message Type	The type of message. This can be 'SMS' or 'MMS'.

Additional Information

Signal Conversations - Android

Description	Signal Conversations contains information about the group or individual conversations that the local user has participated in.
Recovery method	Parsing

Attribute	Description
Partner Phone Number	The phone number of the partner for individual conversation.
Partner Display Name	The display name of the partner for individual conversation.
Group Name	The name of the group for group conversation.
Group Member Phone Number(s)	The list of phone numbers for the group members.
Group Member(s)	The list of display names for the group members.
Group Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the group was created.
Message Count	The number of messages in the conversation.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the last message in the conversation was sent or received, to the nearest second.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The date and time when the conversation was last viewed by the local user.
Snippet	The short preview of the last message in a conversation.
Type	The type of the last message in the conversation.
Pinned	Indicates if the conversation has been pinned by the local user.
Archived	Indicates if the conversation has been archived by the local user.
Group Avatar	The avatar of the group.

Additional Information

Signal Group Members

Description	Signal Group Members specifies the members from each of the Signal groups that the local user is a member of.
Recovery method	Parsing

Attribute	Description
Group Member	The phone number of the group member.
UUID	The unique user ID associated with group member.
Group Name	The name of the group.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the group was created (Empty for Android).
Group Avatar	The avatar of the group.

Additional Information

Signal Groups

Description	Signal Groups contains information about the members of groups
Recovery method	Parsing

Attribute	Description
Group Name	The name of the group.
Group ID	The ID of the group.
Group Member(s)	The user names of the group members.
Group Member Phone Number (s)	The phone numbers of the group members.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the group was created (empty for Android).
Group Avatar	The avatar of the group.

Additional Information

Signal Local User

Description	Signal Local User contains information about the local user account.
Recovery method	Parsing

Attribute	Description
Local User	The name of the local user.
Avatar	The avatar used by the local user account (empty for Android).

Additional Information

Signal Messages - Android

Description	Signal Messages contains information about the messages and calls that are exchanged between the local user and other users.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message.
Recipient	The recipient of the message.
Partner	The partner of the call.
Message	The content of the message. For Group Update type messages, a System Message prefix is attached which tries to imitate a Signal message although the wording might vary.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the the message was first attempted to be sent.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received.
Attachment	The attachment of the message.
File Name	The name of the attachment file.
File Path	The path where the attachment file is located.

Attribute	Description
MIME Type	The MIME type of the attachment.
Type	The type of message.
Direction	The direction of the message.
Read	Indicates whether or not the message has been read by the local user.
Latitude	The latitude of the message.
Longitude	The longitude of the message.

Additional Information
Some Group Update messages might remain encoded. If you notice this issue, contact Magnet Technical Support to request that a new encoding type gets added to this artifact.

Signal Users

Description	Signal Users lists all of the users and profiles present in the application.
Recovery method	Parsing

Attribute	Description
Phone Numbers	The list of phone numbers associated with the user.
UUIDs	The list of unique user IDs (UUIDs) associated with the user.
Type of User	The type of the user, such as local or non-local user. If the local user cannot be determined, the value will be unknown.

Attribute	Description
Full Name	The full name of the user, as stored by the Signal application.
Profile Name	The profile name of the user. This is usually a nickname.
Avatar	The user's avatar.

Additional Information

Skype Accounts

Description	Skype Accounts contains information about the Skype accounts that are recovered, such as user information and when the account was created.
Recovery method	Parsing and carving

Attribute	Description
Skype Name	The Skype name of the account.
Display Name	The display name of the account.
Full Name	The full name of the account.
Email(s)	The email of this account.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date when the profile was created.
Last Online Date/Time - UTC (yyyy-mm-dd)	The last time that the account was online.

Attribute	Description
Birthday (yyyy-mm-dd)	The birthday of the account.
Gender	The gender of the account.
City	The city where the account is located.
State/Province	The state/province where the account is located.
Country	The country where the account is located.
Home Phone	The home phone of this contact.
Office Phone	The office phone of this account.
Mobile Phone	The mobile phone of this account.
Homepage	The homepage of this contact.
About Info	The about info of this contact.
Profile Last Modified On Date/Time - UTC (yyyy-mm-dd)	The date when the profile was last modified.
Mood Text	The text used to express mood.
Last Used On Date/Time - UTC (yyyy-mm-dd)	The last time that the account was used.
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	The time that the avatar was created.
Picture	The avatar for this contact.

Additional Information

Skype Activity

Description	Skype Activity contains interactions that occured between users on Skype. These interactions include messages, group interactions, calls, sent/received files, and SMS. This information is recovered for Skype 8.1 and later.
Recovery method	Parsing and carving

Attribute	Description
Conversation ID	The ID of this conversation.
Profile Name	The local user's profile name.
Sender	The username of the sender/initiator of the interaction.
Sender Email	The sender's email as given in the message (if available).
Recipient(s)	The recipients or targets of the interaction.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the interaction was initiated.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the interaction was last updated (for example, when a call ends).
Message Type	The type of the interaction.
Message	The content of the message or a summary of the interaction.
Emotion Count	The number of reactions to the interaction. Reactions include likes, dislikes, emojis and more.

Attribute	Description
File Name	The name of any attached files associated with the interaction.
File Size (Bytes)	The size in bytes of any attached files.
File	The attachment file (if applicable).
Attachment Data Recovered	Indicates whether the attached file was recovered from the local filesystem.
Thumbnail URL	A URL that directs to the thumbnail picture (if applicable).
Call Duration (Seconds)	The length of the call in seconds (if applicable).
Metadata	The content of the message, if it consisted of interpreted data (XML or JSON data, rather than plain text).
Attachment	The attachment associated with the activity.

Additional Information

Skype Calls

Description	Skype Calls contains information about Skype calls that occur between users.
Recovery method	Parsing and carving

Attribute	Description
Local Username	The user logged into Skype at the time of the call.

Attribute	Description
Call Initiator	The user who started the call.
Initiator Display Name	The display name of the user. This might be different from the user-name.
Recipient Name(s)	The users who accepted a call from the call initiator and participated in the call for a period of time.
Call Participants	The users who accepted and participated in the call from the call ini-tiator for some duration.
Started Date/Time - UTC (yyyy-mm-dd)	The start time of the call.
Duration	The total duration of the Skype call.
Metadata	Additional details about the call extracted in XML format. This includes information on the amount of time that each participant was in the call.

Additional Information

Skype Chat Messages

Description	Skype Chat Messages contains Skype messages sent from one user to another.
Recovery method	Parsing and carving

Attribute	Description
Chat ID	The ID of the chat.
Profile Name	The profile name of the caller.
Author	The author of the message.
Recipient(s)	The recipient(s) of the chat.
From Display Name	The display name of the message sender.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The body of the message or a description of the action taken. For example, adding another participant to a group chat or sharing a file or picture.
Attachment Name	The name of the attachment that was sent. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Attachment Size (bytes)	The size of the attached file, in bytes. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Metadata	Additional details about the action, extracted in its original XML format.
Message Status	The status of the message.
Message Type	The type of message.

Additional Information

Skype Chatsync Messages

Description	Skype Chatsync Messages contains Skype messages that were sent from one user to another, and that are parsed from the chatsync directory.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of this message.
Chat Partner / Group Chat ID	The other part of this message.
Chat Initiator	The initiator of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The content or body of the message.
Message Type	The type of the message.

Additional Information

Skype Contacts

Description	Skype Contacts contains information about Skype contacts that are recovered, which may or may not be added contacts.
Recovery method	Parsing and carving

Attribute	Description
Profile Name	The profile name of the user.
Skype Name	The Skype name of the contact.
Full Name	The full Name of this account
Display Name	The display name of this account.
Email(s)	The email of this account.
Last Online Date/Time - UTC (yyyy-mm-dd)	The last time that the account was online.
Is Blocked	Indicates whether the contact is blocked.
Contact Added	Specifies whether the contact is an added contact or just cached into the database (1 if the contact was added, 0 otherwise). Contacts can be cached into the database for a variety of reasons (for example, as a suggested contact).
Birthday (yyyy-mm-dd)	The birthday of this account.
Gender	The gender of this account.
City	The city where this account is located.
State / Province	The state/province where this account is located.
Country	The country where this account is located.
Home Phone	The home phone of this contact.

Attribute	Description
Office Phone	The office phone of this account.
Mobile Phone	The mobile phone of this account.
PSTN Number	The PSTN number of this contact.
Homepage	The homepage of this contact.
About Info	The about info of this contact.
Profile Loaded Date/Time - UTC (yyyy-mm-dd)	Previously called Profile Created On Date/Time, this attribute represents the date and time when a contact's profile is first created on the user's device. When the profile information is updated by the contact, the date in the database is also updated.
Mood Text	The text used to express mood.
Last Used On Date/Time - UTC (yyyy-mm-dd)	The last time that the account was used.
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	The time that the avatar was created.
Image	The image for this contact.

Additional Information

Skype Emotions

Description	Skype Emotions contains the reactions of users to Skype messages.
Recovery method	Parsing and carving

Attribute	Description
Emotion	The type of emotion that the user reacted to the message with. The emotion is displayed using the shortcut from Skype (for example, cwl represents the emotion Crying With Laughter).
Message Content	The content of the message that the user reacted to. If the content of the message is plain text, this attribute matches the "Message" attribute from the "Skype Activity" artifact. Otherwise, this attribute matches the "Metadata" attribute.
Skype Name	The Skype name of the user who reacted to the message.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the user reacted to the message.

Additional Information

Skype File Transfers

Description	Skype File Transfers contains files that are transferred from one user to another using Skype.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Partner Handle	The username of the file transfer partner.
Partner Display Name	The display name of the file transfer partner.
File Name	The name of the file that was being transferred.
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the file transfer was started.
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date and time when the file transfer was completed.
File Path	The path to the local file.
Transferred File	The file that was transferred.
Type	The type of file that was being transferred.
File Size (Bytes)	The size of the file being transferred.
Bytes Transferred	The number of bytes that were transferred.
Status	The status of the file (for example, transfer, transferring or cancelled).

Additional Information

Skype Group Chat

Description	Skype Group Chat contains information about the Skype group chats that a user is a part of.

Recovery method	Parsing and carving

Attribute	Description
Chat ID	The group chat's unique identifier.
Profile Name	The name of the user.
Participants	The participants of the chat.
Posters	The users that have posted to the chat.
Active Members	The currently active user's of the group.
Started Date/Time - UTC (yyyy-mm-dd)	The date and time that the chat started.
Chat Name	The name of the chat.
Last Changed Date/Time - UTC (yyyy-mm-dd)	The date and time that the chat was modified.

Additional Information

Skype IP Addresses

Description	Skype IP Addresses contains the IP addresses that are associated with a Skype user account.
Recovery method	Parsing and carving

Attribute	Description
Username	The username of Skype accounts.
IP Address	The IP address for the Skype user.
Date/Time - UTC (yyyy-mm-dd)	The date and time.
IP Address Type	The type of IP address (Local or Public).

Additional Information

Skype Notifications

Description	Skype Notifications contains notifications that were shown to users on Skype.
Recovery method	Parsing and carving

Attribute	Description
Read	Indiactes whether the user has read the notification.
Conversation ID	The ID of this conversation.
Profile Name	The local user's profile name.
Sender	The username of the sender/initiator of the interaction.
Recipient(s)	The recipients or targets of the interaction.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the interaction was initiated.

Attribute	Description
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the interaction was last updated (for example, when a call ends).
Message Type	The type of the interaction.
Message	The content of the message or summary of the interaction.
Emotion Count	The number of reactions to the interaction. Reactions include likes, dislikes, emojis, and more.
File Name	The name of any attached files associated with the interaction.
File Size (Bytes)	The size in bytes of any attached files.
File	The attachment file (if applicable).
Attachment Data Recovered	Indicates whether the attached file was recovered from the local filesystem.
Thumbnail URL	A URL that directs to the thumbnail picture (if applicable).
Metadata	The content of the message, if it consisted of interpreted data (XML or JSON data, rather than plain text).

Additional Information

Slack Channel Messages

Description	Slack Channel Messages contains messages sent or received in channels in the user's Slack workspace.
Recovery method	Parsing

Attribute	Description
Workspace ID	The unique identifier for the slack workspace.
Sender	The name or user ID of whoever sent the message.
Channel Name	The name of the channel that the message was sent to.
Message	The message text.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message Status	The delivered status of the message.

Additional Information

Slack Channels

Description	Slack Channels contains information about each of the channels and conversations that exist in a user's Slack workspace.
Recovery method	Parsing

Attribute	Description
Channel Name	The name of a channel or message group.
Channel ID	The ID of a channel or message group.
Workspace ID	The unique identifier for the slack workspace.

Attribute	Description
Created By	The name or user ID of whoever created the channel.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the channel was created.
Topic	The topic text for the channel.
Topic Author	The name or user ID of whoever last wrote the topic text.
Channel Type	The type of channel (Public, Private, General, Single User DM, Multi User DM.)
Last Read Date/Time - UTC (yyyy-mm-dd)	The date and time when the channel was last read.
Member	Represents whether or not the local user is a member of the channel.
Starred	Represents whether or not the local user has starred the channel.

Additional Information

Slack Direct Messages

Description	Slack Direct Messages contains information about direct messages sent or received in 1:1 chats or group chats.
Recovery method	Parsing

Attribute	Description
Workspace ID	The unique identifier for the slack workspace.
Sender	The name or user ID of whoever sent the message.
Recipient(s)	The names or user IDs of the message recipients.
Message	The message text.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message Status	The delivered status of the message.

Additional Information

Slack Files

Description	Slack Files contains information about any files that have saved to the Slack workspace. Files may or may not have been shared with other users.
Recovery method	Parsing

Attribute	Description
Workspace ID	The unique identifier for the slack workspace
Title	The title given to the file.
File Name	The name of the file.

Attribute	Description
Created By	The name or user ID of whoever created the file.
Permanent Link	A permalink to the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was uploaded
FileSize	The size of the file
Deleted	Represents whether or not the file has been deleted.

Additional Information

Slack Users

Description	Slack Users contains information about each user in the Slack workspace.
Recovery method	Parsing

Attribute	Description
Workspace ID	The unique identifier for the slack workspace.
Full Name	The full name of the user.
First Name	The first name of the user.
Last Name	The last name of the user.

Attribute	Description
User Name	The unique user name of the user.
Display Name	The slack display name of the user.
Email	The user email.
Phone Number	The user phone number.
Member ID	The user ID.
Title	The user title.
Status Message	The status message for the user
Account Type	The type of account the user has.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the user was last updated.
Timezone	The timezone that the user is in.

Additional Information

Slack Workspaces

Description	Slack Workspaces contains information about each of the workspaces that the local user is apart of.
Recovery method	Parsing

Attribute	Description
ID	The unique identifier for the slack workspace.
Name	The name of the slack workspace.
Domain	The domain of the slack workspace.
Local User ID	The unique identifier of the local user.
Local User	The name of the local user.
Local User Display Name	The display name of the local user.
Local Email Address	The email address of the local user.
Password/Token	The local user password/token.

Additional Information

Snapchat Chat Messages

Description	Snapchat Chat Messages contains the chat messages sent between users.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the message.
Recipient(s)	The recipient(s) of the message.

Attribute	Description
Message ID	The ID of the message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the chat message.
Message	The content of the message.
Type	The type of the message. This value can be one of the following: Snap, Text, Media, Voice, Emoji, Call/Deleted message/Mini/Game (Snapchat removed Mini/Game feature in early 2023), Screenshot, Unsuccessful voice call, Unsuccessful video call, or Spotlight.
Saved By Sender	Whether the message was saved by the sender (Yes or No).
Saved By Recipient	Whether the message was saved by the recipient (Yes or No).
Released By Recipient	Whether the recipient let the chat message be deleted (Yes or No).
Message Status	The status of the message.
Skin Tone Percentage	The percentage of the image that is skin tone.
MD5 Hash	The MD5 hash of the image.
SHA1 Hash	The SHA1 hash of the image.
Attachment	The attachment associated with the chat message. The attachment recovery might depend on if the user saved the media to the chat.

Additional Information

Snapchat Group Members

Description	Snapchat Group Members contains information about participants of the groups that the local user is a member of.
Recovery method	Parsing and carving

Attribute	Description
Group Chat ID	The ID of the group.
Group Name	The name of the group.
Group Member	The ID of the participant of the group.
Added Date/Time - UTC	The date and time that the participant joined the group.
Deleted	Whether the participant left the group (Yes or No)

Additional Information

Snapchat Memories

Description	Snapchat Memories contains pictures and videos that the Snapchat user saves as a memory.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The ID of the memory.
User ID	The ID of the user.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the snap was originally taken.
Timezone	The time zone of the device when the original snap was taken, or when the media was moved from the device's gallery to the My Eyes Only section of the application.
Type	Indicates whether the memory is saved as a regular snap or My Eyes Only, the latter being password protected.
Media Type	The media type, either a picture or video.
Duration (Seconds)	The duration of time before the snap expires.
Attachment URL	The url of the memory.
Attachment	The attachment for the memory, if it's not a picture.
Latitude	The latitude of the location where the snap was originally taken.
Longitude	The longitude of the location where the snap was originally taken.
Size (Bytes)	The encrypted size of the snap media. Any overlay that was added to the snap is not included when determining the size of the snap media.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.

Attribute	Description
Attachment Path	The file path of the media attachment on the device.
Skin Tone Percentage	The percentage of the picture that appears to be skin tone. Any overlay that was added to the snap is not included when calculating the skin tone.
MD5 Hash	The MD5 hash of the decrypted media. Any overlay that was added to the snap is not included when creating the hash signature.
SHA1 Hash	The SHA1 hash of the decrypted media. Any overlay that was added to the snap is not included when creating the hash signature.
PhotoDNA Hash	The PhotoDNA hash of the image.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

Snapchat Received Videos

Description	Snapchat Received Videos contains the videos sent to the user.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file.
File Extension	The extension of the file.
Image	A generated thumbnail of the video.
Created Date/Time - UTC (yyyy-mm-	The date and time that the video file was created.

Attribute	Description
dd)	
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the video file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the video was last written to.
Skin Tone Percentage	The amount of skin tone found in the video.
File Size (Bytes)	The size of the video in bytes.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Additional Information

TamTam Messenger Channels - Android

Description	TamTam Messenger Channels contains messages that belong to channel conversations recovered from the local device (the channel type must be User Channel or Default Channel).
Recovery method	Parsing

Attribute	Description
Sender	The name of the channel in which the message originated.
Sender ID	The TamTam ID of the channel in which the message originated.
Recipient	The display name of the owner contact that received the message.
Recipient ID	The TamTam ID of the owner contact that received the message
Message	The content of the message. If the messages is a contact share, this attribute displays the text from the VCard.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the message.
Status	The delivery status of the message: Sent or Received.
Channel Type	The classification of the Channel. Channels created by TamTam users are displayed as 'User Channel' whereas 'Default Channel' describes channels that are created and managed by Tamtam. TamTam user are automatically signed up to some of these channels upon application download.
Message Type	The type of message content (Text, Picture, Audio, Video, File, Call, Geo Location or Contact Share). If the message is not in one of these formats, this attribute is empty.
Latitude	The latitude coordinate, if the message type is Geo location.
Longitude	The longitude coordinate, if the message type is Geo location.
Attachment URL	A URL for any attachments that are sent or received. Attachments can be downloaded from this URL. However, to recover pictures properly, you

Attribute	Description
	must append '&fn=w_1440' manually to the end of the URL.
Attachment	The locally stored attachment, if the attachment was sent by the local user.

Additional Information
In TamTam Messenger 3.0.0, video attachments aren't always available. To learn more, see Reviewing video files from TamTam Messenger v3.0.0.

TamTam Messenger Contacts

Description	TamTam Messenger Contacts displays information about the TamTam contacts associated with the local user's account (including the local user).
Recovery method	Parsing

Attribute	Description
Contact ID	A unique ID for the contact.
Profile Name	The profile name of the contact.
Website URL	The contact's TamTam website URL, if one exists.
About Info	Information that the user has provided about their self.
Avatar URL	A URL to the user's profile picture. A termination '&fn=w_1440' should be manually added to the URL to properly display the picture.
Updated Date/Time -	The last time that the contact was updated on the local device. If the contact was not added by the local user, this does not display a value. Some con-

Attribute	Description
UTC (yyyy-mm-dd)	tacts might be stored on the local user's device and may have not been added to their contact list. For example, this might occur when the local user belongs to a group but does not have all of the group participants as contacts. In these cases, TamTam adds the group contacts to the application database but they won't automatically be updated.

Additional Information

TamTam Messenger Conversations - Android

Description	TamTam Messenger Conversations contains information about all the chats recovered from the local device (includes individual, group, and channel messages).
Recovery method	Parsing

Attribute	Description
Chat Type	The type of conversation (Individual, Group, User Channel and Default Channel). Individual indicates one-to-one conversations, while Group indicates many-to-many conversations. User Channel indicates a one-to-many conversation created by a TamTam user. Default Channels are one-to-many conversations created and managed by TamTam.
Chat ID	A unique ID for the conversation.
Participants	A list of the participants that belong to the conversation. User Channels only display the local user as a participant whereas Default Channels do

Attribute	Description
	not display any participants.
Chat Name	The name of the conversation (only available in Groups and Channels).
Description	The description of the conversation (only available in Groups and Channels)
Address URL	The URL for the channel's webpage. Users can sign up to the channel using this page if the channel is public.

Additional Information

TamTam Messenger Groups - Android

Description	TamTam Messenger Groups contains all messages that belong to group conversations recovered from the local device.
Recovery method	Parsing

Attribute	Description
Sender	The display name of the contact who sent the message.
Sender ID	The TamTam ID of the contact who sent the message. If the contact ID is not recovered, this attribute displays the chat ID of the conversation that the message belongs to.
Recipient	The name of the owner user who received the message.

Attribute	Description
Recipient ID	The TamTam ID of the owner user who received the message.
Message	The content of the message. If the messages is a contact share, this attribute displays the text from the VCard.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the message.
Status	The delivery status of the message: Sent or Received.
Message Type	The type of message content (Text, Picture, Audio, Video, File, Call, Geo Location or Contact Share). If the message is not in one of these formats, this attribute is empty.
Latitude	The latitude coordinate, if the message type is Geo location.
Longitude	The longitude coordinate, if the message type is Geo location.
Attachment URL	A URL for any attachments that are sent or received. Attachments can be downloaded from this URL. However, to recover pictures properly, you must append '&fn=w_1440' manually to the end of the URL.
Attachment	The locally stored attachment, if the attachment was sent by the local user.

Additional Information

In TamTam Messenger 3.0.0, video attachments aren't always available. To learn more, see Reviewing video files from TamTam Messenger v3.0.0.

TamTam Messenger Messages - Android

Description	TamTam Messenger Messages contains all individual messages (one-to-one) recovered from the local device.
Recovery method	Parsing

Attribute	Description
Sender	The display name of the contact who sent the message.
Sender ID	The TamTam ID of the contact who sent the message. If the contact ID is not recovered this attribute displays the chat ID of the conversation that the message belongs to.
Recipient	The display name of the contact, group or channel that received the message.
Recipient ID	The TamTam ID of the contact, group or channel that received tha message.
Message	The content of the message. If the messages is a contact share, this attribute displays the text from the VCard.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the message.
Status	The delivery status of the message: Sent or Received.
Message Type	The type of message content (Text, Picture, Audio, Video, File, Call, Geo Location or Contact Share). If the message is not in one of these

Attribute	Description
	formats, this attribute is empty.
Latitude	The latitude coordinate, if the message type is Geo location.
Longitude	The longitude coordinate, if the message type is Geo location.
Attachment URL	A URL for any attachments that are sent or received. Attachments can be downloaded from this URL. However, to recover pictures properly, you must append '&fn=w_1440' manually to the end of the URL.
Attachment	The locally stored attachment, if the attachment was sent by the local user.

Additional Information
In TamTam Messenger 3.0.0, video attachments aren't always available. To learn more, see Reviewing video files from TamTam Messenger v3.0.0.

Textfree Attachments

Description	Textfree Attachments contains Attachments from the Android Textfree application.
Recovery method	Parsing and carving

Attribute	Description
Message ID	The ID of the message.
Media URL	The URL from where the media could originaly be downloaded.

Attribute	Description
Type	The type of media (including picture, voicemail and video).
Preview	The binary data of the attachment. If the attachment is a video, the preview is a frame from the video.
Metadata	Any metadata associated with the attachment. An example of this is VoicemailDuration.
Media ID	The internal ID used by the application. This value may point to other places where the attachment is used and/or contained.

Additional Information
The Metadata column is always empty for the Android version of the application.

Textfree Contacts

Description	Textfree Contacts contains contacts from the Android Textfree application.
Recovery method	Parsing and carving

Attribute	Description
First Name	The first name of the contact.
Last Name	The last name of the contact.
Company Name	The company name of the contact.
Phone Numbers	All phone numbers associated with the contact.

Attribute	Description
Email(s)	All emails associated with the contact.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the contact was modified.
Contact ID	The internal ID used by the application. This value may point to other places where the attachment is used and/or contained.

Additional Information
Company Name, Email(s), Last Modified Date/Time will always be empty for the Android version of the application.

Textfree Groups

Description	Textfree Groups contains information about group chats from the Android Textfree application.
Recovery method	Parsing

Attribute	Description
Group	The group number.
Group Name	The name of the group.
Group Phone Number	The phone number of the group.
Group Member Name(s)	The names of all of the group participants.
Group Member Phone Number(s)	The phone numbers of all of the group participants.

Additional Information
The Group Name column will always be empty for the Android version of the application.

Textfree Messages / Calls

Description	Messages from the Android Textfree application.
Recovery method	Parsing and carving

Attribute	Description
Message Partner	The name of the message partner.
Message Partner ID	The ID of the messaging partner. This value may contain the contact's phone number.
Sender Name	The name of the sender.
Sender ID	The ID of the sender.
Message ID	The ID of the message. This value can be used to find related attachments in the TextFree Attachments table.
Message Body	The content of the message.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that is associated with the message.
Attachment Type	The type of media file (for example: jpeg, png, wav).
Media URL	The URL from where the media could originally be downloaded.
Media ID	The internal ID used by the application. This value may point to other places where the attachment is used or contained, or both.

Attribute	Description
Preview	The preview of the media file.
Message Type	The type of the message.
Chat Type	The type of the chat.
Direction	The direction of the message.
Read	The read status of the message.
Call Duration (Seconds)	The call duration in seconds, if the message is a call.

Additional Information
The Sender ID column is always left empty for Android.

TextMe Calls

Description	TextMe Calls contains information about the calls that the suspect participates in using the TextMe application.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the call.
Sender Phone Number	The phone number of the sender.

Attribute	Description
Recipient	The recipient of the call.
Recipient Phone Number	The phone number of the recipient.
Display Name	The chosen display name for the call participant.
Call Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the call was initiated.
Call End Date/Time - UTC (yyyy-mm-dd)	The date and time when the call ended.
Direction	The direction of the call, either incoming or outgoing.
Status	Whether the call was unanswered, answered, or if the caller left a voicemail.
Call Type	Indicating if the call was an audio call or video call. In later versions of TextMe, this indicates whether the call was 'in', 'out' or 'missed'.
Voicemail	The associated voicemail message.

Additional Information

In some versions of TextMe, call logging does not behave as expected. If a suspect sends or receives a call, a database entry is created as normal. If another call occurs with the same user, without there being any messages in between, the timestamps from the first call are overwritten in the database with the timestamps from the second call. This behavior makes it seem as if the first call never occurred. The timestamps are repeatedly overwritten for each call until a message is sent, at which point a new database entry can be created for the next new call.
For Android TextMe Calls, it is not possible to determine the display name of the recipient, so the 'Display Name' column will always be empty.

TextMe Messages

Description	TextMe Messages contains individual chat messages that are sent and received using the TextMe application.
Recovery method	Parsing and carving

Attribute	Description
Conversation Partner	The name of the other participant or recipient in the conversation. In some cases, when the owner of the device cannot be retrieved, this value is returned as "[sender], [recipient]".
Recipient Phone Number	The phone number of the recipient.
Sender	The sender of the message.
Sender Phone Number	The phone number of the sender.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent, regardless of whether the message was sent or received.
Message	The body of the message.
Direction	Whether the message was sent or received.
Status	Whether the message was unsent, sent, delivered, or read.
Attachment Name	The name of the attachment, if one exists (can be pictures, videos, or URL links).

Attribute	Description
Attachment Path	The file path of the attachment, if one exists.
Attachment Type	The file type of the attachment, if one exists.
Attachment	The attachment data.
Group Name	The display name of the group.

Additional Information

TextPlus Activity

Description	TextPlus Activity contains information about messages and calls from TextPlus on an Android device.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the activity.
Recipient	The recipient of the activity.
Date/Time	The date and time when the activity happened.
Activity Type	The type of the activity, which is either Message or Call.
Message Body	If the activity type is Message, the text of the message is displayed.
Call Duration	If the activity type is Call, the duration of the call in seconds is displayed.

Attribute	Description
(Seconds)	
Attachment URL	The URL associated with the attachment sent in the activity, if one exists. For some activities, access this URL in the browser to visualize the attachment content.

Additional Information

TextPlus Calls

Description	TextPlus Calls contains call information from TextPlus data on an Android device.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username of the TextPlus account.
User	The identifier for the recipient of the call. This could be a GUID or phone number depending on the TextPlus version.
Display Name	The display name of the TextPlus account.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the call was made.
Duration (Units Unknown)	The duration of the call (can be in milliseconds or seconds). To determine which unit of duration is being used, human inspection is required.

Additional Information

TextPlus Logged In Account

Description	TextPlus Logged In Account contains information about the user currently logged into TextPlus on an Android device.
Recovery method	Parsing

Attribute	Description
User Name	The name of the logged in user.
Display Name	The display name of the logged in user.
Phone Number	The phone number of the logged in user.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the logged in account was created.
Gender	The gender of the logged in user.
Last Known Location Latitude	The latitude of the last known location the app was used.
Last Known Location Longitude	The longitude of the last known location the app was used.
Last Known Location Date/Time - UTC (yyyy-mm-dd)	The date and time of the last known usage of the app.

Additional Information

TextPlus Messages

Description	TextPlus Messages contains message information from TextPlus data on an Android device.
Recovery method	Parsing and carving

Attribute	Description
Sender Name	The sender of the message.
Sender	The identifier for the sender of the message. This could be a GUID or phone number depending on the TextPlus version.
Recipient Name	The recipient of the message.
Recipient	The identifier for the recipient of the message. This could be a GUID or phone number depending on the TextPlus version.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent or received.
Message Body	The text contents of the message.
Message Type	Indicates if the message is incoming, outgoing, or an unknown message type.
Status	Indicates if the message was read ('Read'), unread ('Unread') or has an unknown status.

Additional Information

Touch Experiences

Description	Touch Experiences contains experiences in the Android Touch application. Similar to photo albums on Facebook except more private, users can post media to an experience and share it with friends, who can comment on the posted media and share media of their own.
Recovery method	Parsing

Attribute	Description
Experience Name	The name of the experience.
Experience Members	All of the members in the experience.
Experience Owner	The user who created the experience.
Author	The author of the post.
Experience Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the experience was created.
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the post was sent/received.
Comment	A comment on the content of the experience. This comment can be seen by other users viewing the experience.
Media URL	The URL of a media item posted to the experience.
Downloaded Image	The raw content of the media in the post, downloaded from the URL specified in 'Media URL'.

Attribute	Description
Status	The status of the post. Describes whether it was sent or received, and whether or not it was viewed/downloaded by the local user.

Additional Information

Touch Friends

Description	Touch Friends contains contact information for friends of the local user in the Android Touch application.
Recovery method	Parsing

Attribute	Description
Touch ID	The friend's unique Touch ID.
First Name	The friend's first name.
Last Name	The friend's last name.
Avatar URL	The URL of the friend's avatar.
Downloaded Image	The raw content of the friend's avatar, downloaded from the URL specified in 'Avatar URL'.

Additional Information

Touch Local User

Description	Touch Local User contains contact information for the local user in the Android Touch application.
Recovery method	Parsing

Attribute	Description
Touch ID	The local user's unique Touch ID.
First Name	The local user's first name.
Last Name	The local user's last name.
Email	The local user's email.
Phone Number	The local user's phone number.
Avatar URL	The URL of the local user's avatar.
Downloaded Image	The raw content of the local user's avatar, downloaded from the URL specified in 'Avatar URL'.
Country Code	The country code of the local user.

Additional Information

Touch Messages

Description	Touch Messages contain messages that were sent and received in the Android Touch application.

Recovery method	Parsing

Attribute	Description
Sender	The sender of the message.
Recipients	The recipient(s) of the message. In a group conversation, recipients will be in a comma-delimited list.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The content of the message.
Message Type	A phrase describing the content of the message. The possible values are 'Text', 'Image', 'Audio', 'Video', and 'Profile Picture Changed'.
Message Status	The status of the message. This value describes whether the message was sent or received by the local user, and describes the interactions that the user has had with it: whether or not it was viewed, or, in the case of media, whether or not it was downloaded.
Media URL	The URL of the media in the message, if it contains video, audio or an image.
Downloaded Image	The raw content of the media in the message, downloaded from the URL specified in 'Media URL'.
Local Media Path	The path to the content of the media in the message on the local phone.

Additional Information

Verizon Messages Messages

Description	Verizon Messages contains information about the messages sent or received by the local user.
Recovery method	Parsing

Attribute	Description
Sender	The phone number of the device that sent the message.
Recipient(s)	The phone numbers of the devices that received the message.
Message Direction	Indicates whether the message was incoming or outgoing. If the direction is not recognized, the value will be an integer.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The text for the message.
Attachment Name	The attachment file name.

Additional Information

Viber Messages

Description	Viber Messages contains details about sent/received Android Viber messages.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the message.
Sender Name	The name of the person who sent the message.
Recipient(s)	The recipient(s) of the message. In a group chat, the recipients will be shown as a comma-delimited list.
Recipient Screen Name (s)	The screen name(s) of the person(s) who received the message.
Participant	The contact name of one of the participants of the record. It is up to the investigator to determine if this is the local user, or that of the chat partner.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message that was sent. If the message type was a call this will identify if the call was outgoing, incoming or a missed call. For locations the message is a google maps link to the sent location. For images the message can be empty or a blurb of text.
Chat Type	The type of conversation where the message originates from (Group chat or One-to-one).
Type	The type of message that was sent. Possible values include Text, Sticker, Call, Video, Location, Notification, and Image.
Message Status	The status of the message. This can be one of the following: 'Sent / Failed', 'Sent / Not Delivered', 'Sent / Delivered', or 'Received'.
Attachment	The attachment file name, as stored in the application.

Attribute	Description
Name	
File Attachment	The attachment file name, as named by the user.
File Size (Bytes)	The size of the file.
State	The state of the attachment. This can be one of the following: Complete / Pending, Downloading, or Incomplete Upload / Incomplete Download.
Secret Chat	Indicates whether a message is sent in a secret chat (Yes if true).
Expiration (dd hh:mm:ss)	If the message is a secret chat message, this value represents the time limit that the message can be visible for before it disappears. The value is converted from seconds and reported as a timestamp in dd:hh:mm:ss format.
Repeat Count	If the message was a call, the number of times that the call was repeated.
File Path	If the message included an attachment, the path to the attachment on the local phone, in the form of a URL.
Location Address	The address for the location that was sent.
Latitude	The map latitude location information.
Longitude	The map longitude location information.
Nearby Locations	The locations that are geographically close to the user when they use the Share Location feature within the application (these locations are cached even if a location is not actually shared).
Attachment	The attachment, as stored in the application.

Additional Information

WeChat Friends

Description	WeChat Friends contains stored contact information for the WeChat application on Android.
Recovery method	Parsing

Attribute	Description
Username	The unique username of the friend.
Nickname	The nickname of the friend.
Gender	The friend's gender.
Phone Number	The friend's phone number.
Email	The friend's email address.
Full Name	The friend's full name.
Participants	A list of the participants that belong to the chat room.
Original Location	The geolocation that is configured from a list of countries and cities when the user creates their account. This is not a real-time location.
Profile Picture URL	The profile picture URL of the friend.

Additional Information

WeChat Messages

Description	WeChat Messages contains stored messages for the WeChat application on Android.
Recovery method	Parsing and carving

Attribute	Description
Sender User Name	The user name or ID of the sender, as assigned by the application.
Sender Nick-name	The display name of the sender, as defined by the user.
Recipient User Name	The user name of the person receiving the message.
Recipient Nick-name	The nickname of the person receiving the message.
Group Chat Name	The name of the group chat, if the message is sent in a group chat.
Group Chat ID	The unique ID of the group chat, if the message is sent in a group chat.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was created on the device.
Message	The content of the message. For Location, Notice, and Pay messages, this content will be extracted from XML data. Contact Card messages will dis-

Attribute	Description
	play the XML data for the contact.
XML Data	The raw XML data for Picture, Location, Notice, and Pay messages.
Call Duration (Seconds)	The duration of voice and/or video call in seconds.
Type	The type of the message (Text, Picture, Audio, Friend Request, Contact Card, Video, Animated Emoticon, Location Data, Shared Information, Voice/Video Call, Sight Video, Group Voice/Video Call, Notice, Pay Message, or Location Sharing).
Account	The user name of the account that was used to send the message.
Latitude	The latitude of the location data sent within the message.
Longitude	The longitude of the location data sent within the message.
Attachment	The attachment (such as audio, video) associated with the message.
Attachment Data Recovered	Indicates whether attachment data was recovered (Yes or Null).
Attachment Path	The absolute path to recovered message attachments.
Content Format	The content format of successfully recovered audio file attachments. AXIOM Process will attempt to decode audio from SILK V3 to WAV. Successfully converted attachments are saved and playable in AXIOM Examine. Unconverted attachments are saved in their original format and can be manually decoded using another tool or method.

Additional Information

Wickr Me Conversations

Description	Wickr Me Conversations contains details about all the Individual, Group, and Room conversations the local user is a part of.
Recovery method	Parsing

Attribute	Description
Conversation ID	The unique identifier for the conversation.
Participants	The names of all participants in the conversation.
Type	The type of conversation. Individual is used for 1-on-1 or group conversations, and Room is used for room conversations.
Name	The name of the Room. Only populated if the conversation is in a room.
Description	The description of the Room. Only populated if the conversation is in a room.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the last message in this conversation was sent.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the conversation was last synced on the device.

Additional Information

To learn more about Wickr Me, see Artifact profile: Wickr Me.

Wickr Me Messages

Description	Wickr Me Messages contains decrypted and decoded messages sent or received by a Wickr Me user on Android. These messages can include text messages, call logs, transmitted locations, attachments such as pictures and videos, voice messages, and more.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender's Wickr username.
Recipient(s)	The recipient's Wickr username.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when this message was sent.
Message	The message content.
Message Type	The message type. This value is interpreted from the ZPRIMARYTYPE. This value can be: Text, Call, Attachment, Location, Key Verification, System Message, or Control (Group Conversation Events).
Chat Type	The type of the chat. This value can be Individual, or Room.
Room Name	The name of the chat room.
Direction	Indicates whether the message was incoming or outgoing.
Read	Indicates whether or not the message was read.

Attribute	Description
Call Duration (Seconds)	The duration of the call in seconds.
Call Status	The status of the call, if applicable. This value can be: Started, Completed, Missed, or Cancelled.
Attachment Name	The file name of the attachment included in the message, if applicable.
Attachment Path	The original file path of the encrypted attachment, if applicable.
Attachment	The decrypted attachment file, if applicable (can include photos, video, or voice messages).
Latitude	The latitude of the coordinates (for transmitted locations only).
Longitude	The longitude of the coordinates (for transmitted locations only).

Additional Information

To learn more about Wickr Me, see Artifact profile: Wickr Me.

Wickr Me Users

Description	Wickr Me Users contains details about the users the local user has interacted with in the app.
Recovery method	Parsing

Attribute	Description
User Name	The name of the user.
User ID	The ID of the user.
Starred	Dictates whether the user has been starred or not.
Hidden	Dictates whether the user is hidden or not.
Blocked	Dictates whether the user is blocked or not.
Bot Account	Dictates whether the user is a bot.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The date and time when the user was last active.
Profile Image	The profile image of the user.

Additional Information
To learn more about Wickr Me, see Artifact profile: Wickr Me.

Zalo Contacts

Description	Zalo Contacts contains the user's Zalo contacts.
Recovery method	Parsing

Attribute	Description
User Name	The contact's username.
User ID	The contact's unique user ID.

Attribute	Description
Profile Picture URL	The contact's profile picture URL.
Gender	The contact's gender.
Phone Number	The contact's phone number.
Birthday (yyyy-mm-dd)	The contact's birthday.
Status	The contact's status message.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact was last active.
Is Friend	If the contact is friends with the user.
Type	The contact's type of account.

Additional Information

Zalo Groups

Description	Zalo Groups contains Zalo groups that the user participates in.
Recovery method	Parsing

Attribute	Description
Name	The name of the group.
ID	The unique ID of the chat group.
Created By	The username of the person who created the chat room.

Attribute	Description
Group Member(s)	The usernames of all of the members in the group.
Number of Participants	The number of participants in the group.

Additional Information

Zalo Messages

Description	Zalo Messages contains messages or calls sent or received using Zalo.
Recovery method	Parsing

Attribute	Description
Sender User Name	The username of the person sending the message.
Recipient User Name	The username of the person receiving the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent on the device.
Direction	The direction that the message was sent.
Message	The content of the message.
Picture	Any picture attachments in the message.
Attachment	Any non-picture attachments in the message, including audio and video.

Attribute	Description
Duration (Seconds)	The duration of calls.
Status	The status of calls. The status of some calls is ambiguous as it's not possible to distinguish whether calls are accepted or ended by the user receiving the call.
Message Type	The type of message. The different message types include text, audio, video and more.
Latitude	The latitude data sent within a message.
Longitude	The longitude data sent within a message.
Media URL	The URL of additional media attachments.
Attachment Path	The absolute path to recovered attachments in a message.

Additional Information

Zalo Profiles

Description	Zalo Profiles contains profile information of the local Zalo user.
Recovery method	Parsing

Attribute	Description
User Name	The user's username.

Attribute	Description
User ID	The user's unique user ID.
Profile Picture URL	The user's profile picture URL.
Gender	The user's gender.
Birthday (yyyy-mm-dd)	The user's birthday.
Phone Number	The user's phone number.
Status	The user's status message.

Additional Information

Zello Messages

Description	Zello Messages provides information about the various messages the user has sent and received on the app.
Recovery method	Parsing

Attribute	Description
Sender	The display name of the user who sent the message (Local User if it was the local user).
Recipient	The display name of the user who received the message (Local User if it was the local user).
Message	The content of the message.

Attribute	Description
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Direction	Indicates whether the message was incoming or outgoing.
Message Type	The type of message. This can include Alert, Audio Message, Location, Message, Picture, or the actual value with "not parsed" indicated in brackets.
Read	Indicates whether or not the message has been read.
Attachment	The recovered picture attachment.
Latitude	The latitude portion of the location data that is sent with the message.
Longitude	The longitude portion of the location data that is sent with the message.

Additional Information

Zello Profiles

Description	Zello Profiles provides information about the various profiles and channels the user has interacted with on the app.
Recovery method	Parsing

Attribute	Description
User Name	The user name for the profile, this will be empty for chan-

Attribute	Description
	nel profiles.
Name	The display name for the profile, this will be empty for channel profiles.
Created Date/Time - UTC (yyyy-mm-dd)	The data and time when the profile was created.
Channel Name	The name of the channel, this will be empty if the profile is not a channel.
Channel Type	The type of the channel, this will be empty if the profile is not a channel.
Location Name	The name of the profile location.
Website	The website field for the profile.
About	The about field for the profile
Profile Picture URL	A URL corresponding to the profile image for the profile.

Additional Information

Zoom Channels

Description	Zoom Channels contains information about the channels that the local user participates in.
Recovery method	Parsing

Attribute	Description
Channel ID	The ID of the channel.
Channel Name	The display name of the channel.
Owner ID	The ID of the Zoom user that created the channel.
Participant IDs	The IDs of the participants of the channel.
Participants User Names	The names of the participants of the channel.
Description	A description of the channel, as provided by the creator of the channel.

Additional Information

Zoom Chat Messages

Description	Zoom Chat Messages contains details about Zoom chat messages sent outside of a meeting.
Recovery method	Parsing and carving

Attribute	Description
Sender Name	The name of the person who sent the message.
Sender ID	The ID of the person who sent the message.
Buddy ID	The ID of the person or group that the message was sent to.

Attribute	Description
Recipient Name	The name of the person who received the message.
Recipient ID	The ID of the person who received the message.
Group Chat ID	The ID of the group this message was sent in.
Message ID	The GUID of the message.
Message	The body of the message.
Message Date/Time - UTC (yyyy-mm-dd)	A timestamp that indicates when the message was sent or received, depending on whether the local user was the sender or receiver.
Sender	Whether the message was sent by the local user or a remote user.
Read	Specifies whether the message has been read. The displayed value is either 'Yes' or 'No'.
Message Type	The type of message that was sent. The message types are 'Message', 'Picture', 'File', or 'Notification'.
Attachment Name	The name of the attachment that was sent.
Attachment Local File Path	The local path where the attachment was saved. This is empty if the attachment was not saved.
Attachment	The contents of the attachment if it can be recovered.

Additional Information

The Attachment Name column is always empty on Android.

Zoom Contacts

Description	Zoom Contacts contains information about a user's Zoom contacts.
Recovery method	Parsing and carving

Attribute	Description
Buddy ID	The user ID of the contact.
Email	The email address of the contact.
Display Name	The display name of the contact.
Description	A description of the contact, as provided by that user.
Personal Meeting ID	An ID that can be used to start up a meeting with the contact.
Region	The default country or region where the contact is located.

Additional Information

Zoom Meeting Messages

Description	Zoom Meeting Messages contains details about Zoom chat messages sent during a meeting.
Recovery method	Parsing and carving

Attribute	Description
Message ID	The GUID of the message.
Sender Name	The name of the person who sent the message.
Sender ID	The ID of the person who sent the message.
Receiver Name	The name of the person who received the message. If blank, the message was sent to everyone in the meeting.
Receiver ID	The ID of the person who received the message. If zero, the message was sent to everyone in the meeting.
Message	The body of the message.
Message Date/Time - UTC (yyyy-mm-dd)	A timestamp that indicates when the message was sent or received, depending on whether the local user was the sender or receiver.
Read	Specifies whether the message has been read. The displayed value is either 'Yes' or 'No'.
Message Type	The type of message that was sent.
Conference ID	The ID for the meeting the message was sent in.

Additional Information

Zoom User Accounts

Description	Zoom User Accounts contains details about the local user's zoom account.
Recovery method	Parsing and carving

Attribute	Description
User ID	The unique identifier for the user.
User Name	The username of the account.
Email	The email address associated with the account.
First Name	The first name of the user.
Last Name	The last name of the user.
Phone Number	The phone number of the user.
Profile Image URL	The URL to the profile picture of the user.
Downloaded Profile Image	The data for the profile picture.

Additional Information

Connected Devices

Latent Wireless Geolocated WiFi Hotspots

Description	Latent Wireless Geolocated WiFi Hotspots contains information about WiFi hotspots that were discovered using a Latent Wireless device. Latent Wireless stores information about the hotspots in a database that Magnet AXIOM can parse for details about each hotspot.
Recovery method	Parsing

Attribute	Description
MAC Address	The MAC address of the detected WiFi hotspot.
First Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was first discovered.
Last Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was last seen.
Strongest Seen Date/Time - UTC (yyyy-mm-dd)	Indicates when the WiFi hotspot was detected at its highest strength.
Network Name (SSID)	The SSID of the WiFi hotspot.
Channel	The WiFi hotspot channel.
RSSI	The received signal strength indicator for the WiFi hotspot.
Latitude	The latitude where the WiFi hotspot was detected.
Longitude	The longitude where the WiFi hotspot was detected.
Secure	Indicates whether the WiFi hotspot is secure.

Additional Information

LogMeIn Activity

Description	LogMeIn Activity records connection events that occur using the LogMeIn remote desktop client. These records can include remote sessions and file sharing events.
Recovery method	Parsing

Attribute	Description
Date/Time Local Time	The time in local time when the log line was recorded.
Activity Type	The type of the activity that was recorded. Session type indicates that the event is a remote session. SessionDateReport indicates that the recorded event is a session summary. FileShare type indicates that the recorded event was a file being shared with other users.
Connection Type	The type of connection that was used.
Status	Indicates the status of the file sharing event (only applies to FileShare activities).
Remote IP Address	The public IP address of the client server.
Local IP Address	The public IP address of the host server.
Connection State	The login or logout state of the connection.
OS Version	The OS version of the host.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Remote Desktop Protocol

Description	The Remote Desktop Protocol artifact can indicate whether a device accesses external network devices, or was accessed by external network devices. The data collected by this artifact is recovered from the Windows Event Log, as well as the Windows Registry.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID from the Windows Event Log.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the Registry Key associated with the Remote Desktop Protocol (RDP) connection was modified.
Direction	The direction (outgoing or incoming) of the RDP connection.
Event Description Summary	The description of the event recovered.
Origin Service Name	The windows service or local account that initiated the RDP connection.
Origin Domain Name	The local domain name of the service or user that initiated the RDP connection.
Origin IP Address	The IP address of the device that initiated the RDP connection.

Attribute	Description
Origin Port	The IP Port of the device that initiated the RDP connection.
Destination User Name	The username of the account that was remotely connected to.
Destination Domain Name	The user domain of the account that was remotely connected to.
Destination IP Address	The IP address of the device that was remotely connected to.
Destination Port	The IP Port of the device that was remotely connected to.
Event Data	The raw Windows Event Log data for the RDP connection.

Additional Information

Remote Desktop Protocol Bitmap Cache

Description	Remote Desktop Protocol Bitmap Cache provides a reconstruction of the RDP Bitmap Cache, which gives an indication of what may have been on screen during an RDP session.
Recovery method	Parsing

Attribute	Description
Preview	A reconstructed image of the contents of the Remote Desktop Protocol bitmap cache. The image is produced by concatenating the individual cache bitmap tiles in the order that we find them, so the image is expected to look fragmented.

Additional Information

TeamViewer Activity

Description	TeamViewer Activity contains information about incoming and outgoing remote connections using TeamViewer remote desktop software.
Recovery method	Parsing

Attribute	Description
Computer Name	The name of the local computer.
TeamViewer ID	The TeamViewer ID of the local computer.
Local User	The local computer user that was logged in during the connection.
Direction	The direction (incoming or outgoing) of the connection that the activity was part of.
Remote Computer Name	The name of the remote computer associated with the connection.
Remote TeamViewer ID	The TeamViewer ID of the remote computer associated with the connection.
Session Type	The type of connection (remote control or file transfer).
Date/Time - UTC (yyyy-mm-dd)	The date and time of the activity.
Activity	The TeamViewer activity being reported.

Additional Information

Your Phone Contacts

Description	Your Phone Contacts contains information about contacts synced from a mobile device to a computer using Your Phone. The Your Phone application can sync data from Android and iOS devices to computers running Windows 10.
Recovery method	Parsing

Attribute	Description
Display Name	The contact's display name.
Nickname	The contact's nickname.
Phone Number	The contact's phone number.
Type	The type of phone number associated with the contact, for example Home, Mobile, or Business.
Last Time Contacted Date/Time - UTC (yyyy-mm-dd)	The last time that this contact either sent a message to, or received a message from the synced device or local user since the Your Phone application was installed.
Number of Times Contacted	The number of times the synced device or local user either sent a message to, or received a message from the contact since the Your Phone application was installed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that this contact's details were modified.

Additional Information

Your Phone Devices

Description	Your Phone Devices contains information about the devices that are synced to the user's computer by using the Your Phone application.
Recovery method	Parsing

Attribute	Description
Application Version	The version of Your Phone running on the computer.
Last Run Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was last run on the computer.
Device Application Version	The version of the Your Phone companion application running on the device.
Device ID	A GUID identifier generated to uniquely identify devices within the Your Phone application.
Device Name	The name provided by the device and displayed in the user interface when referring to it.
Device Platform	The device's platform (Android or iOS).
Device Messages Synced Date	The date and time when the device last synchronized its messages data with Your Phone.
Computer Messages Synced Date	The date and time when the computer last synchronized its messages data with Your Phone.

Attribute	Description
Device Contacts Synced Date	The date and time when the device last synchronized its contacts data with Your Phone.
Computer Contacts Synced Date	The date and time when the computer last synchronized its contacts data with Your Phone.
Device Photos Synced Date	The date and time when the device last synchronized its picture data with Your Phone.
Computer Photos Synced Date	The date and time when the computer last synchronized its picture data with Your Phone.

Additional Information

Your Phone Pictures

Description	Your Phone Pictures contains information about pictures synced from a mobile device to a computer using Your Phone. The Your Phone application syncs the 25 most recently taken photos from Android and iOS devices to computers running Windows 10.
Recovery method	Not applicable

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.

Attribute	Description
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Device ID	A GUID identifier generated to uniquely identify devices synced using the Your Phone application.
Device Name	The name of the device (as provided by the device) which is displayed in the user interface for Your Phone.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.

Attribute	Description
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial	The serial number of the lens (extracted from Exif data).

Attribute	Description
Number	
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS Latitude (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicates whether the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.
Exif Data	A searchable field for all raw exif properties.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Your Phone SMS/MMS

Description	Your Phone SMS/MMS contains information about messages synced from a mobile device to a computer using Your Phone. The Your Phone application can sync data from Android and iOS devices to computers running Windows 10.
Recovery method	Parsing and carving

Attribute	Description
Sender	The phone number that sent the message.
Recipient(s)	The phone number(s) the message was sent to.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message content.
Message Direction	Indicates whether the message was sent or received by the synced device or local user.
Message Type	Indicates whether the message is SMS or MMS.
Message Status	Indicates whether the message has been read.
Attachment Name	The name of the attached file, if applicable (MMS only).

Additional Information

Custom

File Signature Mismatch (Audio)

Description	File Signature Mismatch (Audio) contains identified mismatches between a known file signature header and the extension (or lack thereof) for an audio file. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.
Attachment	The mismatched file.

Additional Information

File Signature Mismatch (Container)

Description	File Signature Mismatch (Container) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a container. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mismatch.
File Path	The path to the mismatched file.
Attachment	The mismatched file.

Additional Information

File Signature Mismatch (Document)

Description	File Signature Mismatch (Document) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a document. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type, we return a mis-match.
File Path	The path to the mismatched file.
Attachment	The mismatched file.

Additional Information

File Signature Mismatch (Picture)

Description	File Signature Mismatch (Picture) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a picture. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file. If the mime type is unknown, this defaults to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file. If the mime type is unknown, this defaults to application/octet-stream. If there is no file extension, but the mime type is known, a mismatch is is returned.
File Path	The path to the mismatched file.
Attachment	The mismatched file.

Additional Information

File Signature Mismatch (Video)

Description	File Signature Mismatch (Video) contains identified mismatches between a

	known file signature header and the extension (or lack thereof) for a video. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified mime type of the header of the file, if we don't know what the mime type is we default to application/octet-stream.
File Extension Type	The identified mime type of the extension of the file, if we don't know what the mime type is we default to application/octet-stream. If there is no file extension, but we identify a known header mime type we return a mis-match.
File Path	The path to the mismatched file.
Attachment	The mismatched file.

Additional Information

Documents

CSV Documents

Description	CSV Documents contains CSV documents (.csv) that are located on the system.
Recovery method	Parsing

Attribute	Description
File Name	The name of the CSV document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last modified.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was created.
File Content	The content of the CSV document.
Size (Bytes)	The size of the CSV document in bytes.
SHA1 Hash	The SHA1 hash of the contents of the document.
MD5 Hash	he MD5 hash of the contents of the document.

Additional Information
For information about supported formats, see Supported media and file types.

Evernote Accounts

Description	Evernote Accounts contains information about the user accounts that have been used to log in on the device.
Recovery method	Parsing

Attribute	Description
User Name	The display name of the user's account
User ID	The user ID of the account.
Email	The email address associated with the account.
Full Name	The full name associated with the account.
Active Account	Indicates which account was active at the time of acquisition.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the account was created.
Login Date/Time - UTC (yyyy-mm-dd)	The date and time that the account was initially logged in on the device.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the account was last updated.

Additional Information

Evernote Contacts

Description	Evernote Contacts contains information about users that have communicated with the local user account.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the contact.
Contact ID	The contact ID of the contact.
Account Name	The account name of the contact.

Additional Information

Evernote Notes

Description	Evernote Notes contains any notes associated with the local user, including notes shared from other users to the local user.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the note.
Content	The content of the note.

Attribute	Description
Type	The type of note.
File Name	The name of the attachment that was included with the note.
File	The attachment that was included in the note.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was created.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was updated.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was deleted.
Owner	The owner of the note. If a note is shared from one user to another, the owner is the user that shared the note.
Shared With	The accounts that the note was shared with.
Last Modifier Name	The username of the last modifier of the note.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time of the starting time for the reminder of the note.
End Date/Time - UTC (yyyy-mm-dd)	The date and time of the end time for the reminder of the note.
Locale	The location where the note was taken.
Latitude	The latitude of the location where the note was taken.
Longitude	The longitude of the location where the note was taken.
Notebook Name	The name of the notebook where the note was saved.

Additional Information

Evernote Work Chat

Description	Evernote Work Chat contains messages sent and received by the local user.
Recovery method	Parsing and carving

Attribute	Description
Sender ID	The unique ID of the sender.
Sender Name	The name of the sender.
Sent Date/Time	The date and time when the message was sent.
Message Body	The body of the message.
Participants	The participants of the chat.
Participant IDs	The IDs of the participants of the chat.

Additional Information

Google Docs

Description	Google Docs is a word processing suite available to all Google account holders.

Recovery method	Carving

Attribute	Description
File Name	The name of the file that was backed up.
Owner Email	The email address of the author of the file.
Owner Name	The name of the author of the file.
Last Edited Date/Time - UTC (yyyy-mm-dd)	The last date and time when the file was edited.
Last Modified By Local User Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was edited locally.
File Size	The size of the file.
Last Collaborator Name	The name of the last collaborator of the file.
Last Collaborator Email	The email address of the last collaborator of the file.

Additional Information

Hangul Word Processor

Description	Hangul Word Processor specifies information about files that were created using Hangul Word Processor.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the found file.
Password Required	Indicates whether the file requires a password to be opened.
Application Version	The version of the software used to create the file.
Preview Text	A preview of the file content that contains the first 1024 symbols.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was modified on the filesytem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was accessed on the filesytem.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was created on the filesytem.
Title	The title field of the document.
Subject	The subject field of the document.
Author	The author field of the document.
Date String	The date field of the document.
Keyword	The keyword field of the document.
Additional Information	Any additional information that the author provided for the document. Appears as 'Other' field in the software.

Attribute	Description
Last Saved By	The username of the last user that saved the file.
Document Created Date/Time - Local Time (yyyy-mm-dd)	The date and time when the file was originally created.
Preview Image	An image preview of the title page of the file.
File	The contents of the Hangul Word document.
MD5 Hash	A MD5 hash of the Hangul Word document.
SHA1 Hash	A SHA1 hash of the Hangul Word document.

Additional Information

For information about supported formats, see Supported media and file types.
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Microsoft Excel Documents

Description	Microsoft Excel is a spreadsheet processor developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File	The actual file.
File System Last Modified	The date and time when the file was last modified on the

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
Size (Bytes)	The size of the document.
Title	The title metadata.
Saved Size (Bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
Subject	The subject metadata.
Authors	The authors of the document.
Keywords	The keywords in the metadata of the document.
Comment	The comments metadata.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.

Attribute	Description
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information
For information about supported formats, see Supported media and file types.

Microsoft Office Backstage Items

Description	Microsoft Office Backstage Items are items that can be found in the Backstage View of Microsoft Office applications.
Recovery method	Parsing

Attribute	Description
Item Name	The name of the file or folder.
Item Type	The type of the item (e.g. File, Folder)
File Extension	The file extension
Path	The location at which the original file or folder can be found within.
Author	The author of the file or folder
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file or folder was last modified (extracted from metadata within the file or folder).

Attribute	Description
Last Read Date/Time - UTC (yyyy-mm-dd)	The date and time when the file or folder was last read from (extracted from the metadata within the parent directory).
Resource ID	The position of the resource in relation to other resources.
Sharing Scope	The scope in which the file or folder has been shared.
Note	Indicates whether the file or folder is a OneNote item.
Remote Address	Indicates whether the file or folder is a remote item.

Additional Information

Microsoft PowerPoint Documents

Description	Microsoft PowerPoint is a presentation creator developed by Microsoft. This table captures documents created with PowerPoint, extracted from the filesystem and carved from unallocated space.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File	The actual file.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.

Attribute	Description
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
Size (Bytes)	The size of the document.
Title	The title of the file.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Comment	The comments in the metadata of the file.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

Microsoft Word Documents

Description	Microsoft Word is a word processor developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File	The actual file.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
Size (Bytes)	The size of the document.
Title	The title of the file.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Subject	The subject of the file.
Authors	The authors of the file.

Attribute	Description
Keywords	The keywords in the metadata of the file.
Comment	The comments in the metadata of the file.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

OpenOffice Calc Documents

Description	OpenOffice Calc Documents are spreadsheets similar to Microsoft Excel spreadsheets, but are created using OpenOffice Calc.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the document.
Created Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the file was created. This data is recovered from the <meta:creation-date> tag found in meta.xml.
Modified Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the file was modified. This data is recovered from the <dc:date> tag found in meta.xml.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was modified. This data is recovered from the local ZIP file header for meta.xml.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Recovered Size (Bytes)	The recovered size of the document in bytes.
Password Required	Indicates whether the document is password protected.
Title	The title meta-data as set by the creator. This data is recovered from the <dc:title> tag found in meta.xml. Note that this value can be different from the name of the document.

Attribute	Description
Authors	The authors of the document. This data is recovered from the <meta:initial-creator> tag found in meta.xml.
Subject	The subject of the document as set by the creator. This data is recovered from the <dc:subject> tag found in meta.xml.
Keywords	The keywords metadata in the document. This data is recovered from the <meta:keyword> tag found in meta.xml.
Comment	The comments metadata. This data is recovered from the <dc:-description> tag found in meta.xml.
Editing Cycle	The number of times that the document has been edited. This data is recovered from the <meta:editing-cycles> tag found in meta.xml.
File	The actual file stored as an attachment.

Additional Information

For information about supported formats, see Supported media and file types.
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

OpenOffice Impress Documents

Description	OpenOffice Impress Documents are slide presentations similar to Microsoft PowerPoint presentations, but created using OpenOffice Impress.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the document.
Created Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the file was created. This data is recovered from the <meta:creation-date> tag found in meta.xml.
Modified Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the file was modified. This data is recovered from the <dc:date> tag found in meta.xml.
Modified Date/Time - UTC (yyyy-mm-dd)	The UTC date and time when the file was modified. This data is recovered from the local ZIP file header for meta.xml.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Recovered Size (Bytes)	The recovered size of the document in bytes.
Password Required	Indicates whether the document is password protected.
Title	The title metadata as set by the creator. This data is recovered from the <dc:title> tag found in meta.xml. Note that this value can be different from the File Name value.

Attribute	Description
Authors	The authors of the document. This data is recovered from the <meta:initial-creator> tag found in meta.xml.
Subject	The subject of the document as set by the creator. This data is recovered from the <dc:subject> tag found in meta.xml.
Keywords	The keywords metadata in the document. This data is recovered from the <meta:keyword> tag found in meta.xml.
Comment	The comments metadata. This data is recovered from the <dc:-description> tag found in meta.xml.
Editing Cycle	The number of times that the document has been edited. This data is recovered from the <meta:editing-cycles> tag found in meta.xml.
File	The actual file stored as an attachment.

Additional Information

For information about supported formats, see Supported media and file types.
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

OpenOffice Writer Documents

Description	OpenOffice Writer Documents are documents similar to Microsoft Word documents, but are created using OpenOffice Writer.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the document.
Created Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the file was created. This data is recovered from the <meta:creation-date> tag found in meta.xml.
Modified Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the file was modified. This data is recovered from the <dc:date> tag found in meta.xml.
Modified Date/Time - UTC (yyyy-mm-dd)	The UTC date and time when the file was modified. This data is recovered from the local ZIP file header for meta.xml.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Recovered Size (Bytes)	The recovered size of the document in bytes.
Password Required	Indicates if the document is password protected.
Title	The title metadata as set by the creator. This data is recovered from the <dc:title> tag found in meta.xml. Note that this can be different from the File Name value.

Attribute	Description
Authors	The authors of the document. This data is recovered from the <meta:initial-creator> tag found in meta.xml.
Subject	The subject of the document as set by the creator. This data is recovered from the <dc:subject> tag found in meta.xml.
Keywords	The keywords metadata in the document. This data is recovered from the <meta:keyword> tag found in meta.xml.
Comment	The comments metadata. This data is recovered from the <dc:-description> tag found in meta.xml.
Editing Cycle	The number of times that the document has been edited. This data is recovered from the <meta:editing-cycles> tag found in meta.xml.
File	The actual file stored as an attachment.

Additional Information

For information about supported formats, see Supported media and file types. Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

PDF Documents

Description	Portable Document Format (PDF) is a file format used to present documents in a manner independent of application software, hardware, and operating systems. This table captures documents in this file format, extracted from the filesystem and carved from unallocated space.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
Title	The title of the file.
Authors	The authors of the file.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Subject	The subject of the file.
Keywords	The keywords in the metadata of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
MD5 Hash	An MD5 hash of the PDF content.
SHA1 Hash	A SHA1 hash of the PDF content.
File	The PDF file.

Additional Information
For information about supported formats, see Supported media and file types.

RTF Documents

Description	RTF Documents contains information for each RTF document that was recovered from the search.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the RTF document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was created.
File Content	The contents of the RTF document.
File Size (Bytes)	The size of the RTF document.
MD5 Hash	A MD5 hash of the RTF content.
SHA1 Hash	A SHA1 hash of the RTF content.

Additional Information
For information about supported formats, see Supported media and file types.

Text Documents

Description	Text documents (.txt) that are located on the system.
Recovery method	Parsing

Attribute	Description
Filename	The name of the text document.
Size (Bytes)	The size of the text document in bytes.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was created.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.
File Content	The content of the text document.

Additional Information

For information about supported formats, see Supported media and file types.

Thinkfree Office Viewer Files

Description	Thinkfree Office Viewer Files contains information about the files that the

	user has opened using Thinkfree Office Viewer. Even if the user has deleted the file from the device, this artifact can still recover information about the file if they opened it in the viewer.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file that was opened in Thinkfree Office Viewer.
File Size (Bytes)	The size of the file.
File System Created Date/Time	The date and time when the file was created on the filesystem.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last viewed.
Favorited	Indicates whether the file has been made a favorite.
File Path	The path to the local file.

Additional Information

Email and Calendar

Android Emails

Description	Android Emails contains the email fragments that were recovered from an

	Android device.
Recovery method	Parsing and carving

Attribute	Description
Sender	Who sent the email.
Recipients	Who the email was sent to.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the email.
Subject	The subject of the email.
Email Body	The body of the email
BCC	Who was BCC'd on the email.
CC	Who was CC'd on the email.
Sync Server Date/Time - UTC (yyyy-mm-dd)	The date and time that the server synchronized the email.
Status	Identifies if the email was read or unread.
Attachments	The attachments in the email.

Additional Information

Android Gmail Conversations

Description	Android Gmail Conversations contains information about email conversations between the local user and others, as recovered from an

	Android device.
Recovery method	Parsing and carving

Attribute	Description
Conversation Date/Time - UTC (yyyy-mm-dd)	The date and time when the first message in the conversation was sent.
Subject	The subject of the conversation.
Snippet	A snippet of text from the first message in the conversation.
Attachments	Any attachments that were sent during the conversation.
Permanent Link	A URL to the conversation.

Additional Information

Android Yahoo Mail Attachments

Description	Android Yahoo Mail Attachments contains attachments from emails stored by the Android Yahoo Mail application.
Recovery method	Parsing and carving

Attribute	Description
Message ID	The database key for the message. This key can be used to match up an attachment with an email found in Android Yahoo Mail Emails.
Attachment Name	The file name of the attachment.
Download URL	The URL of the original image attachment, if applicable.
Thumbnail URL	The URL of the thumbnail of the image attachment, if applicable.
Original Saved Location	The path at which this attachment was first saved, if any.
Attachment Size (bytes)	The size of the attached file.
Download State	The displayed value is either 'Complete' or 'Incomplete'.
MIME Type	The file type in MIME format.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the attachment was received or sent. The date and time should match the corresponding entry in Android Yahoo Mail Emails.
Sender	The name of the sender
Attachment Type	The location specified when the attachment is recovered. Downloaded: Recovered from the Download folder indicating it was downloaded by the local user. Sent Locally: Recovered from the autosaved_attachment folder indicating it was sent locally. Cached/Thumbnail: The original or thumbnail

Attribute	Description
	of an image recovered from the cache folder.
Attachment	The attachment.

Additional Information

Android Yahoo Mail Emails

Description	Android Yahoo Mail Emails contains carved and non-carved emails stored by the Android Yahoo Mail application.
Recovery method	Parsing and carving

Attribute	Description
Message ID	The database key for the message. This key can be used to match up an email with attachments found in Android Yahoo Mail Attachments.
From	The email address of the sender.
Recipients	A list of email addresses and labels for the intended recipients in the 'To' field of the email.
Subject	The subject line of the email.
Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was received or sent.
Sent Date/Time -	The date and time that the email was sent.

Attribute	Description
UTC (yyyy-mm-dd)	
Received Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was received.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was last viewed on the local device.
Body	The body of the email in plain text.
Folder ID	The name of the folder that the email was stored in.
Reply To	The email address to which replies to this email will be sent.
Cc	A list of email addresses and labels for the intended recipients in the 'Cc' field of the email.
Bcc	A list of email addresses and labels for the intended recipients in the 'Bcc' field of the email.
Snippet	A short preview of the text of the email body.
Favorited	Whether the email has been favorited locally. The displayed value is either 'Yes' or 'No'.
Replied	Whether the local user has replied to the email. The displayed value is either 'Yes' or 'No'.
Read Status	Whether the email has been opened locally. The displayed value is either 'Read' or 'Unread'.
Has Attachment	Whether the email has an attachment. The displayed value is either 'Yes' or 'No'.

Additional Information

Android Yahoo Mail User Accounts

Description	Android Yahoo Mail User Accounts contains local user accounts from the Android Yahoo Mail application.
Recovery method	Parsing and carving

Attribute	Description
User Name	The user ID of the account.
First Name	The first name of the person associated with the account.
Last Name	The last name of the person associated with the account.
Preferred Name	The user's custom preferred name.
Email Address	The account's email address.

Additional Information

Calendar Events

Description	The Android Calendar application is a default application on Android.
Recovery method	Parsing and carving

Attribute	Description
Summary	A summary of the calendar appointment.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the appointment starts.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the appointment ends.
Event Location	The location of the calendar appointment.
Notes	Notes about the calendar appointment.
Calendar	The name of the calendar from which the event was generated.
Attendees	The attendees of the event.
Timezone	The timezone the appointment is in.
URL	A URL associated with the event.

Additional Information

Calendar Events (UFED Agent)

Description	Calendar Events (UFED Agent) contains details about a user's calendar events on Android. These messages are recovered from <calendar> tag found in a UFED Report.xml
Recovery method	Parsing

Attribute	Description
Subject	The subject of the scheduled event. This data is retrieved from the <subject> tag within the calendar element in a UFED Report.xml.
Event Location	The location of the scheduled event. This data is retrieved from the <location> tag within the calendar element in a UFED Report.xml.
Notes	Notes about the scheduled event. This attribute is referred to as the <Description> in the evidence acquired from the UFED and is retrieved from the <description> tag within the calendar element in a UFED Report.xml.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the scheduled event. This data is retrieved from the <start> tag wihin the calendar element in a UFED Report.xml.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the scheduled event. This data is retrieved from the <end> tag within the calendar element in a UFED Report.xml.
Repeat Until Date/Time - UTC (yyyy-mm-dd)	The date and time when this recurring scheduled event expires. This data is retrieved from the <repeat_until> tag within the calendar element in a UFED Report.xml.
Repeat Interval	Describes the type of recurring event. This data is retrieved from the <repeat_type> tag within the calendar element in a UFED Report.xml.
Repeat Every	Describes the frequency of the recurring event. This data is retrieved from the <repeat_every> tag within the calendar element in a UFED Report.xml.
Repeat On	Indicates the specific day of occurrence of the recurring event. This data is retrieved from the <repeat_position> tag within the calendar element in a UFED Report.xml.

Additional Information

Gmail Emails

Description	Gmail Emails contains the Gmail email fragments that were recovered from an Android device.
Recovery method	Parsing and carving

Attribute	Description
To Address(es)	The recipient(s) of the email.
From Address	The sender of the email.
Thread ID	The ID of the conversation the email is from. Emails with the same Thread ID belong to the same conversation.
Subject	The subject of the email.
Sent Date/Time - UTC (yyyy-mm-dd)	The date that the email was sent.
Received Date/Time - UTC (yyyy-mm-dd)	The time that the email was received.
Email Body	The body of the email.
Email Snippet	A snippet of the email.
cc Address(es)	The recipients of the email that were CC'd.
bcc Address(es)	The recipients of the email that were BCC'd.

Attribute	Description
Reply Address(es)	The reply-to address for the email.
Attachment Data Recovered	Indicates whether attachments for the email were recovered.
Attachments	The file names of any attachments for the email.
Saved Attachments	The file paths of any attachments for the email which were saved locally.

Additional Information

Google Calendar Calendars

Description	Google Calendar Calendars contains a list of all the calendars the user has synced to their Google account.
Recovery method	Parsing

Attribute	Description
Account ID	The account ID assigned by Google
Calendar Display Name	The name of the calendar.
Description	The description of the calendar.
Timezone	The timezone of the calendar.
Created Date/Time - UTC	The date and time the calendar was created.

Attribute	Description
(yyyy-mm-dd)	
Visibility	Indicates if the calendar is visible or hidden on the phone.
Access	The level of permissions the user has for the calendar (Owner Access or Read Only).
Calendar ID	A unique ID for the calendar.

Additional Information

Google Calendar Events

Description	Google Calendar Events contains information about a user's calendar events on the Google Calendar application.
Recovery method	Parsing

Attribute	Description
Event Name	The name of the event.
Description	The description of the event.
Event Date/Time - UTC (yyyy-mm-dd)	The date and time of the event.
Event End Date/Time - UTC (yyyy-mm-dd)	The date and time of the end of the event.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time of when the event was created.
Invitees	The email addresses of those invited to the event.
Event ID	The unique ID of the event.
Account ID	The unique identifier of the owner of the account.
Owner Email	The email address of the owner of the event.
Owner Name	The name of the owner of the event.
Calendar ID	The unique ID of this calendar.
Calendar Display Name	The display name of the calendar to which the event belongs.
Event Location	The location of the event.
Latitude	The latitude of the event.
Longitude	The longitude of the event.
Location URL	The unique location URL for the event's location.
Recurrence	The recurrence of the event.
Event URL	The unique URL of the event.

Additional Information

Outlook Accounts

Description	Outlook Accounts contains information about the user accounts that have been logged in to on the device.
Recovery method	Parsing

Attribute	Description
Email Address	The email address associated with the account.
Description	A description of the account, as set by the user.
Display Name	The display name for the user.
Birthday	The user's birthday in yyyy-mm-dd format.

Additional Information

Outlook Appointments

Description	Microsoft Outlook is a personal information manager and email client. Outlook Appointments captures information related to appointments scheduled in Outlook.
Recovery method	Parsing

Attribute	Description
Sender Name	The person who requested the appointment.
Sender Exchange Account	The sender's Exchange account name.
Recipients	The recipients of the appointment invitation.
Subject	The subject of the appointment.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the appointment starts.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the appointment ends.
Body	The body of the appointment description.
CC	The CC'd recipients of the appointment invitation.
BCC	The BCC'd recipients of the appointment invitation.
Companies	The companies involved in the appointment.
Attachments	The attachments for the appointment.
Locale	The location of the appointment.
Is All-day Event	Indicates if the appointment is an all-day event.
Is Recurring	Indicates if the appointment is recurring.
Recurrence Pattern Description	Describes the recurrence pattern of the appointment, if applicable.
Sensitivity	Indicates if the appointment is sensitive.
Is Hidden	Indicates if the appointment is hidden.

Attribute	Description
Is Private	Indicates if the appointment is private.
Priority	The priority of the appointment.
Importance	The appointment importance setting.
MD5 Hash	The MD5 hash of the appointment.
SHA1 Hash	The SHA1 hash of the appointment.

Additional Information

Outlook Contacts

Description	Microsoft Outlook is a personal information manager and email client. Outlook Contacts captures information related to contacts stored in Outlook.
Recovery method	Parsing

Attribute	Description
Display Name	The contact's display name.
Customer ID	The customer ID of the contact.
Email Address 1	The contact's primary email address.
Email Display As 1	The display string of the contact's primary email address.

Attribute	Description
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the contact details were last modified.
Company Name	The contact's company name.
Department Name	The contact's department name.
Title	The contact's job title.
Profession	The contact's profession.
Manager Name	The name of the contact's manager.
Office Location	The contact's office location.
Business Address	The physical address of the business.
Business Phone	The contact's business phone number.
Business Phone 2	The contact's secondary business phone number.
Business Fax	The contact's business fax number.
Business Homepage	The website of the contact's business.
Email Display Name 1	The display name of the contact's primary email address.
Email Address 2	The contact's secondary email address.
Email Display As 2	The display string of the contact's secondary email address.
Email Display Name 2	The display name of the contact's secondary email address.
Email Address 3	The contact's tertiary email address.

Attribute	Description
Email Display As 3	The display string of the contact's tertiary email address.
Email Display Name 3	The display name of the contact's tertiary email address.
Cellular Phone	The contact's mobile phone number.
Home Address	The contact's home address.
Home Phone	The contact's home phone number.
Home Phone 2	The contact's secondary home phone number.
Home Fax	The contact's home fax number.
FTP Site	The contact's FTP site.
Body	More information about the contact.
Attachments	Any attachments to the contact entry.
Last Modifier Name	The name of the person who last modified the contact details.
MD5 Hash	The MD5 hash of the contact.
SHA1 Hash	The SHA1 hash of the contact.

Additional Information

Outlook Messages

Description	Microsoft Outlook is a personal information manager and email client. Outlook Messages captures information related to emails sent and received in Outlook.
Recovery method	Parsing

Attribute	Description
Sender Name	The sender of the email.
Sender Email	The email address of the sender.
Recipients	The recipients of the email.
Subject	The subject of the email.
Sender Exchange Account	The sender's Exchange account name.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was created.
Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the email synced with the HxStore platform.
Submitted	The date and time that the email was submitted.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Delivered Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was delivered.
Body	The body of the email. For HxStore data sources that include email bodies deleted when an account was removed, the displayed value is the path where the email body was located on the file system.
Folder Name	The name of the folder where the email is stored.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Attachments	The list of attachments on the email.
Headers	The raw email headers.
Priority	The priority of the email.
Importance	The importance of the email.
Sensitivity	The sensitivity of the email.
MD5 Hash	The MD5 hash of the email.
SHA1 Hash	The SHA1 hash of the email.

Additional Information

Samsung Email Logs

Description	Samsung Email Logs contains the email logs that were recovered from a Samsung device.
Recovery method	Parsing

Attribute	Description
Name	The name of the person/business the email is with.
Email Address	The email address of person/business the email is with.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the email.
Message Content	The email message content.
Subject	The subject of the email.

Additional Information

Encryption and Credentials

Android KeyStore

Description	Android KeyStore contains passwords and tokens for websites and other internet services that are recovered from Android KeyStore.
Recovery method	Parsing

Attribute	Description
Account	The user account that the keystore entry applies to.
File Name	The name of the keystore data file.
Type	The type of the keystore data.
Key	The private key found in the keystore data.
Value	The blob value.
Flags	The flags byte.
Blob Info	The info byte.
Initialization Vector	The initialization vector.
AEAD Authentication Tag	The tag used for authentication encryption with associated data (used by KeyStore 3).
MD5 Hash	The MD5 hash used for encryption (used by KeyStore 2).

Additional Information

Android KeyStore - GrayKey

Description	Android KeyStore - GrayKey contains passwords and tokens from the Android GrayKey image, reading the 'android_keystore' file generated by the GrayKey tool.
Recovery method	Parsing

Attribute	Description
Package Name	The package name of the application.
Description	The description of the data provided by the application for the keystore.
Encrypted Data	The encrypted hexidecimal bytes of the keystore data.
Decrypted Data	The decrypted hexidecimal bytes of the keystore data.

Additional Information

Encrypted Files

Description	Encrypted Files contains information about any files that have been recovered on the system that are encrypted. This artifact is not available in Magnet IEF.
Recovery method	Parsing

Attribute	Description
File Name	The name of the encrypted file.
File Size (Bytes)	The size of the encrypted file in bytes.
Detected File Type	The detected type of the encrypted file.
File Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the encrypted file was created on the filesystem.
File Modified Date/Time - UTC	The date and time when the encrypted file was last mod-

Attribute	Description
(yyyy-mm-dd)	ified on the filesystem.
File Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the encrypted file was last accessed on the filesystem.
MD5 Hash	The MD5 hash of the file.
SHA1 Hash	The SHA1 hash of the file.

Additional Information
To learn more, see Search for encrypted files in Magnet AXIOM.

Live System

Logged on Users - Live System

Description	Logged on Users Live System contains the information for each logged on user on the live system.
Recovery method	Parsing

Attribute	Description
Account Type	The type of the user account and the MSDN information about that account type.
Description	The user generated description of the user account.
Account Disabled	Indicates whether the user account is disabled (Yes or No).

Attribute	Description
Domain	The domain that the user account belongs to.
Full Name	The full name of the user.
Installed Date/Time - UTC (yyyy-mm-dd)	Indicates when the user account was installed or created.
Local Account	Indicates whether the user account is a local account (Yes or No).
Locked Out	Indicates whether the user account is locked out (Yes or No).
Name	The name of the user account under the current domain.
Last Used Date/Time - UTC (yyyy-mm-dd)	The last date and time that the user account was used.
Last Login Date/Time - UTC (yyyy-mm-dd)	The last date and time that the user account was logged into.
Logon Type	Indicates how the user account was last logged into and the MSDN information about that logon type.
Password Changeable	Indicates whether the user's account password is changeable (Yes or No).
Will Password Expire	Indicates whether the user's account password will expire (Yes or No).
Password Required	Indicates whether the password is required to log in to the user's account (Yes or No).
Security Identifier	The security identifier of the account.
IP Address	The IP address that has logged in to the account. This value is

Attribute	Description
	either a valid IPv4 address or Local Host.
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the user's information was captured.

Additional Information

Running Processes - Live System

Description	Running Processes Live System contains the information for each process on the live system.
Recovery method	Parsing

Attribute	Description
Name	The name of the process, referred to as the 'Image Name' in task manager.
Description	The description of the executable file, can be blank and still be valid.
Full Path	The full path to the executable of the process.
Process ID	The ID of the process.
Parent Process ID	The process ID of the immediate parent of the process.
User Name	The owner of the process.

Attribute	Description
CPU Time (HH:mm:ss)	Indicates the amount of time that the process required of the CPU.
Elapsed Time (HH:mm:ss)	Indicates how long the process has lived for.
I/O Read Bytes	Indicates how many bytes have been read by the process.
I/O Write Bytes	Indicates how many bytes have been written by the process.
I/O Other Bytes	The number of bytes transferred in input and output operations generated by a process that are neither reads nor writes, including file, network, and device inputs and outputs.
Memory (Private Working Set) Bytes	The number of bytes that have been allocated for the process.
Command Line Call	The call to the command line that will start the process.
Start Date/Time - UTC (yyyy-mm-dd)	Indicates when the process was first started.
Capture Date/Time - UTC (yyyy-mm-dd)	The date and time that the process information was captured.

Additional Information

Location and Travel

Android Google Maps

Description	Android Google Maps contains information about the locations that a user searches for using Google Maps.
Recovery method	Parsing and carving

Attribute	Description
Search Query	The location that the user searched for
Latitude	The latitude associated with the search.
Longitude	The longitude associated with the search.
URL	The URL that contains the search query.
CID	A unique ID - also known as ludocid - that Google assigns to a specific business location in order to identify it within its systems.
FID	A unique ID that relates to reviews that Google holds about a specific business.

Additional Information

Android Wi-Fi Profiles

Description	Wi-Fi Profiles contains a list of the saved Wi-Fi Profiles on a mobile device.
Recovery method	Parsing and carving

Attribute	Description
Network Name (SSID)	The name of the network.
Security Mode	The security mode of the network.
Network Password	The password used to log onto the network.
User Name	The username that was used to log onto the network.
WEP Key	The WEP key used to log onto the network
MAC Address	The MAC Address of the network.
Network ID	An integer used to identify the network. As networks are added to the device, this value gets incremented (the first network added has an ID of 0, the second has an ID of 1, and so on). If a network is deleted and re-added at a later date, it receives the next new ID available instead of reassuming its original ID.
Profile Created Date/Time - Local Time	The date and time that the Wi-Fi profile was created.

Attribute	Description
(yyyy-mm-dd)	
Last Connected Date/Time - Local Time (yyyy-mm-dd)	The date and time of the last network connection.
Connection Count	The number of times that the network was connected to by the device.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Google Maps

Description	Google Maps is a free web service that allows users to get directions.
Recovery method	Carving

Attribute	Description
Search Query	The term that was searched for.
Starting Location	The starting location for navigation/directions.
Center of Map	Indicates where the map was centered.
Business Latitude and Longitude	The latitude and longitude of the business location.

Attribute	Description
Source Address	The source physical address.
Destination Address	The user's desired destination.
Route Type	Indicates how the user will travel (e.g. Car, bus, or bike).
Additional Address	Any additional addresses within the navigation.
Street View Latitude/Longitude	The latitude and longitude information in street view.

Additional Information

Google Maps Directions

Description	Google Maps Directions contains information about directions queries requested by the user using Google Maps.
Recovery method	Carving

Attribute	Description
Origin Address	The address where the direction starts from. This value can be an address, a business description or latitude/longitude coordinates.
Origin Latitude	The latitude associated with the origin address.
Origin Longitude	The longitude associated with the origin address.

Attribute	Description
Destination Address	The destination address where the direction goes to. Several destinations can be added to a direction but only the last one is displayed.
Destination Latitude	The latitude associated with the destination address.
Destination Longitude	The longitude associated with the destination address.
Number of Stops	The number of stops (if any) between origin and destination addresses.
URL	The URL associated with the direction query. Directions can be viewed in a browser by appending the URL to the end of 'www.google.com/maps'.

Additional Information

Google Maps Tiles

Description	Google maps is a free web service that allows users to get directions.
Recovery method	Parsing and carving

Attribute	Description
Image	The actual picture content.
X Coordinate	The X coordinate value that Google uses to download the right tile.
Y Coordinate	The Y coordinate value that Google uses to download the right tile.
Zoom Level	The level that the user was zoomed in to the map. This value is the Z coordinate value that Google uses to download the right tile.

Additional Information

Last Known Locations

Description	Last Known Locations contains a list of the last known locations of the Android device, as tracked by the GPS receiver and recovered using dumpsys.
Recovery method	Parsing

Attribute	Description
Serial Number	The serial number of the Android device.
Type	The type of receiver.
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Altitude (meters)	The altitude of the location.

Additional Information

OnStar RemoteLink Accounts

Description	Contains information about all the OnStar RemoteLink accounts found on the device.
Recovery method	Parsing

Attribute	Description
Account Number	The OnStar account number of the suspect.
Account Key	A secondary identifier for the account on the device.
Created Date/Time	The date and time the account was created on the device.
Updated Date/Time	The date and time the account was updated on the device.
Country Code	The country code associated with the user account.
First Name	The first name of the account holder.
Last Name	The last name of the account holder.
Selected VIN	The VIN of the vehicle that was selected by the app at the time of extraction.

Additional Information

OnStar RemoteLink Hotspot Info

Description	Information about the vehicle Wi-Fi hotspots associated with an OnStar account.
Recovery method	Parsing

Attribute	Description
Network Name (SSID)	The name of the vehicle's hotspot.
Network Password	The password of the vehicle's hotspot.
Created Date/Time	The date and time the hotspot was created.
Updated Date/Time	The date and time the hotspot was updated.
VIN	The Vehicle Identification Number that the hotspot is associated with.

Additional Information

OnStar RemoteLink Recent Location Searches

Description	OnStar RemoteLink Recent Location Searches contains the location searches and commands performed on the results of the searches.
Recovery method	Parsing

Attribute	Description
Destination Address	The addresses searched for by the suspect.
Timestamp Date/Time	The date and time that the search was completed.

Attribute	Description
Created Date/Time	The date and time the entry was created on the device.
Updated Date/Time	The date and time the entry was updated on the device.
Command	The command used to send the address to the vehicle.
Command Status	The status of the command.
Destination Name	The name of the destination address if one was assigned.
VIN	The Vehicle Identification Number of the vehicle to which the command was sent.

Additional Information

OnStar RemoteLink Remote Commands

Description	OnStar RemoteLink Remote Commands contains information about commands sent from the device.
Recovery method	Parsing

Attribute	Description
Requested Command	The command requested by the user.
Request State	The state of the request.

Attribute	Description
Sent Date/Time	The date and time that the command was sent to the vehicle.
Completion Date/Time	The date and time that the command was completed.
Command Description	The description of the command that was sent, if one is available.
VIN	The Vehicle Identification Number of the vehicle that the command was sent to.
Request ID	The ID of the request that was sent, if available.

Additional Information

OnStar RemoteLink Saved Places Of Interest

Description	OnStar RemoteLink Saved Places Of Interest contains addresses for places of interest saved in the OnStar RemoteLink application.
Recovery method	Parsing and carving

Attribute	Description
Address	The full address stored in the application.
State/Province	The state/province of the address.
Country	The country of the address.

Attribute	Description
Latitude	The latitude of the address to map on the world map.
Longitude	The longitude of the address to map on the world map.
Address URL	The URL of the address as stored by OnStar.
Created Date/Time	The date and time that the saved entry was created on the device.
Updated Date/Time	The date and time that the saved entry was updated on the device.
Name	The name of the saved address.

Additional Information

OnStar RemoteLink Saved Wireless Carrier

Description	OnStar RemoteLink Saved Wireless Carrier contains information about the wireless accounts associated with a vehicle.
Recovery method	Parsing

Attribute	Description
Carrier Account ID	The account identifier of the carrier account.
Carrier Type Code	The code that represents the account type.
Carrier Type Description	The carrier associated with the account.
Created	The date and time that the account entry was created on the device.

Attribute	Description
Date/Time	
Updated Date/Time	The date and time that the account entry was updated on the device.
Account Type	The type of wireless account.
Account Description	The description of the account type.
VIN	The Vehicle Identification Number of the vehicle that the wireless account is associated with.

Additional Information

OnStar RemoteLink Vehicle Diagnostics

Description	OnStar RemoteLink Vehicle Diagnostics contains information about the diagnostic values that were retrieved from the vehicle.
Recovery method	Parsing

Attribute	Description
Diagnostic Name	The name of the diagnostic test that was retrieved.
Unit	The unit of measurement associated with the diagnostic test.
Value	The value associated with the diagnostic test.

Attribute	Description
Created Date/Time	The date and time that the diagnostic value was retrieved.
Updated Date/Time	The date and time that the diagnostic value was updated.
Completion Date/Time	The date and time that the server retrieved the diagnostic value from the vehicle.
VIN	The Vehicle Identification Number of the vehicle that the diagnostic value was retrieved from.

Additional Information

OnStar RemoteLink Vehicle Info

Description	OnStar RemoteLink Vehicle Info contains information about the vehicle associated with the account.
Recovery method	Parsing

Attribute	Description
VIN	The Vehicle Identification Number of the vehicle associated with the account.
Vehicle Make	The make of the vehicle.
Vehicle Model	The model of the vehicle.

Attribute	Description
Year	The year of production of the vehicle.
Created Date/Time	The date and time that the vehicle information was added to the device.
Updated Date/Time	The date and time that the vehicle information was updated on the device.
Phone Number	The phone number associated with the vehicle.
Account Number	The OnStar account number that the vehicle is associated with.

Additional Information

Uber Accounts

Description	Uber Accounts contains account information for riders, as recovered from the Uber application (passenger only).
Recovery method	Parsing

Attribute	Description
First Name	The first name of the account holder.
Last Name	The last name of the account holder.
Mobile Phone	The mobile phone number associated with the acount.
Email	The email associated with the account.

Attribute	Description
Share Code	A unique share code associated with the rider.
User ID	The user ID uniquely identifying the account.
Latitude (On App Startup)	The latitude of the user when the application was last opened.
Longitude (On App Startup)	The longitude of the user when the application was last opened.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the user last opened the application.
Last Payment Profile ID	The ID of the payment profile that was last used by the user.
Profile Image URL	The URL of the profile image for the account.
Downloaded Profile Image	

Additional Information

Uber Cached Locations

Description	Uber Cached Locations contains information about locations that Uber caches, such as the initial location on the application's startup, or locations from a trip (passenger only).
Recovery method	Parsing

Attribute	Description
Address	The address of the cached location.
Name	The name of the cached location.
Latitude	The GPS latitude of the cached location.
Longitude	The GPS longitude of the cached location.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the location was cached.
Tag	The tags assigned to the location by the user. These tags are user generated.
Categories	The categories assigned to the location by Uber.

Additional Information

Uber Payments

Description	Uber Payments contains payment information associated with a user's rides, as recovered from the Uber application (passenger only).
Recovery method	Parsing and carving

Attribute	Description
Rider Name	The name of the passenger/rider.
Share Code	A unique share code associated with the rider.

Attribute	Description
Cost	The cost of the trip.
Currency	The currency used to measure the cost of the trip.
Duration (Seconds)	The duration of the trip.
Distance (Kilometers)	The distance of the trip.
Payment Method	The method of payment.
Card Display Name	The payment card display name.

Additional Information

Uber Profiles

Description	Uber Profiles contains information about a user's Uber profiles, as recovered from the Uber application (passenger only).
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the profile.
Profile Email	The email associated with the profile.
Profile User ID	The unique user ID (UUID) associated with the profile.
Profile Payment User ID	The unique user ID that is the payment method for this profile.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the profile was created.

Additional Information

Uber Trips

Description	Uber Trips contains information about a user's Uber rides, as recovered from the Uber application (passenger only).
Recovery method	Parsing

Attribute	Description
Booking Date/Time UTC (yyyy-mm-dd)	The date and time when the trip was booked.
Origin Address	The address of the original start location.
Destination Address	The address of the final destination.
Arrival Date/Time UTC (yyyy-mm-dd)	The date and time when the vehicle arrived at the destination address.
Duration (Seconds)	The duration of the trip.
Distance	The distance of the trip, units unknown.
Driver Name	The first name of the driver.

Attribute	Description
Vehicle Make	The make of the driver's vehicle.
Vehicle Model	The model of the driver's vehicle.
Vehicle Type	The type of Uber car service.
Driver Rating	The driver's rating.
Driver Picture URL	The URL to the driver's profile picture.
Cost	The cost of the trip.
Currency	The currency used to measure the cost of the trip.
Status	The status of the trip.
Route Map URL	The URL to the route taken in the trip.

Additional Information

Waze Events

Description	Waze Events can contain information about upcoming trips that a user has planned.
Recovery method	Parsing

Attribute	Description
Name	The name of the place.

Attribute	Description
Address	The house number and street name of the place.
City	The city of the address.
State	The state/province of the address.
Country	The country of the address.
Start Date/Time	The start date and time that was recommended for the planned drive.
End Date/Time	The date and time that the user planned to arrive at the destination.
Created Date/Time	The date and time when the event was created.
Is All-day Event	Indicates if the planned drive is an all-day event.
Latitude	The GPS latitude coordinates of the place.
Longitude	The GPS longitude coordinates of the place.

Additional Information

Waze Favorites

Description	Waze Favorites contains information about locations that a user has book-marked as a favorite.
Recovery method	Parsing

Attribute	Description
Name	The name of the place bookmarked as a favorite
Address	The house number and street name of the place.
City	The city of the address.
State	The state/province of the address.
Country	The country of the address.
Created Date/Time	The date and time that the address was added as a favorite.
Modified Date/Time	The date and time that the favorite location was last modified by the user.
Accessed Date/Time	The date and time that the favorite location was last accessed in Waze.
Latitude	The GPS latitude coordinates of the place.
Longitude	The GPS longitude coordinates of the place.

Additional Information

Waze Places

Description	Waze Places contains all of the places that the user has searched using Waze.
Recovery method	Parsing

Attribute	Description
Name	The name of the place.
Address	The house number and street name of the place.
City	The city of the address.
State	The state/province of the address.
Country	The country of the address.
Created Date/Time	The date and time when the address was entered in Waze.
Accessed Date/Time	The last date and time when the address was accessed in Waze.
Latitude	The GPS latitude coordinates of the place.
Longitude	The GPS longitude coordinates of the place.

Additional Information

Media

AMR Files

Description	AMR Files contains voicemail messages or memos for both iOS and Android.
Recovery method	Carving

Attribute	Description
File Name	The name of the file the AMR was recovered from.
Size (Bytes)	The size of the AMR content.
MD5 Hash	An MD5 hash of the AMR content.
SHA1 Hash	A SHA1 hash of the AMR content.
Audio	The contents of an AMR file.
Media Duration (Seconds)	The duration of the audio clip in seconds.

Additional Information

For information about supported formats, see Supported media and file types. Media duration is calculated from the number of speech frames carved from the AMR data, where each speech frame has a duration of 20ms, as AMR files do not contain metadata for duration.

Audio

Description	Audio contains Audio files that are recovered and use .mp3 or .wav formats.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file.
File Extension	The extension of the file.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was created.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was last modified.
File Size (Bytes)	The size of the audio file.
MD5 Hash	An MD5 hash of the audio content.
SHA1 Hash	A SHA1 hash of the audio content.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the audio clip in seconds (extracted from Exif data).
Exif Created	The date and time when the audio clip was first recorded (extracted from Exif

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	data).
Exif Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio clip was edited (extracted from Exif data).
Timezone	The timezone setting on the recorder at the time when the audio clip was recorded (extracted from Exif data).
Software	The software used to record or modify the audio clip. This could either be the OS version of the phone used to record the audio clip or the name of the software used to edit the audio clip in post-production (extracted from Exif data).
Latitude	The GPS latitude coordinates of where the audio clip was recorded (extracted from Exif data).
Longitude	The GPS longitude coordinates of where the audio clip was recorded (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of where the audio clip was recorded (extracted from Exif data).
Exif Data	A searchable field for all raw Exif properties.

Additional Information

For information about supported formats, see Supported media and file types.
To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Calc Vault Browser Bookmarks

Description	Calc Vault Browser Bookmarks contains the webpages a user has saved while using Calc Vault.
Recovery method	Parsing

Attribute	Description
Name	The name of the bookmark.
URL	The URL of the bookmark.
User Added	Indicates whether the user added the bookmark (Yes if the user added the bookmark, or No if it is a default bookmark).

Additional Information

Calc Vault Browser History

Description	Calc Vault Browser History contains information about the webpages a user has visited using Calc Vault.
Recovery method	Parsing

Attribute	Description
Name	The name of the webpage visited.
URL	The URL of the webpage visited.

Additional Information

Camera History

Description	Camera History contains a list of the instances where applications have accessed the camera functionality on a device. This artifact can show when an application package accesses camera functionality, which can help the investigator determine when a suspect may have been using their device's camera.
Recovery method	Parsing

Attribute	Description
Date/Time - Local Time (yyyy-mm-dd)	The local date and time of the event.
Action	The action that describes the event.
Camera ID	An ID that can indicate the location of the camera on the phone. The location of the camera can be front, rear, or other.
Package Name	The package name for the application that's accessing the camera.
Process ID	The ID of the process accessing the camera.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Carved Video

Description	Carved Video contains videos that are recovered using carving. Supported formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. Other container formats can also be recovered provided that their underlying packets are the same as one of the supported formats.
Recovery method	Parsing

Attribute	Description
Content Format	The format of the video.
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
File Size (Bytes)	The size of the container and file.
Container Format	The format of the video container.
Saved Video Size (Bytes)	The size of the video that was saved to the database.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Additional Information

As of February 20 2020, this artifact will no longer be included under Videos. Carved Video functionality will be included in the 'Videos' artifact instead.

Google Photos Albums

Description	Google Photos Albums contains information about the albums recovered from the device.
Recovery method	Parsing

Attribute	Description
Title	The name of the album.
Owner	The owner of the album.
User ID	The unique user ID of the owner of the album.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the album was created.
Shared With	A list of the user IDs the album is shared with.
Shared	Indicates if the album is shared with another user.
Album Cover URL	The url of the cover photo for the album.
Album URL	The url of the album.

Additional Information

Google Photos Comments

Description	Google Photos Comments contains information about comments left on an album or individual media by users.
Recovery method	Parsing

Attribute	Description
Author	The author of the album comment.
User ID	The unique user ID of the author of the album comment.
Comment	The content of the comment. Comments include likes when the user clicks a heart-shaped like button.
Item Name	The name of the item that the comment belongs to. The user can comment on albums or individual media.
Type	The type of the item that the comment belongs to. The type can be Album or Media.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the comment was created.

Additional Information

Google Photos Media

Description	Google Photos Media contains information about media items added to Google Photos.

Recovery method	Parsing

Attribute	Description
File Name	The file name of the media item.
Album	The album that the media item belongs to.
Owner	The owner of the media item.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the media item was created.
Size	The size of the media item in bytes.
Duration	The duration of the media item if it is a video.
Caption	The caption of the media item.
Latitude	The latitude of the media item.
Longitude	The longitude of the media item.
Deleted	Indicates whether or not the media item has been deleted. This data is unavailable in Android.
Picture URL	The url of the media item.
Profile Picture URL	The profile picture url of the owner of the media item.

Additional Information

Motion Photos

Description	Motion Photos contains an image and embedded mp4 that has been carved.
Recovery method	Parsing

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.

Attribute	Description
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture, or the name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Latitude	The latitude coordinate in decimal degrees.

Attribute	Description
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS latitude (extracted from Exif data).
Longitude	The longitude coordinate in decimal degrees.
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the picture was taken (extracted from Exif data).
Exif Data	A searchable field for all raw exif properties.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.

Additional Information

If you're having issues previewing this artifact in your cases or exports, see Videos for Motion Photos and Live Photos do not play correctly

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Pictures

Description	Pictures contains pictures that were retrieved using either carving or parsing techniques. The supported picture formats are JPEG (.jpeg, .jpg, .jpe), PNG (.png), Bitmaps (.bmp), Graphics Interchange Format (.gif), Icons (.ico), and Tagged Image File Format (.tif, .tiff).
Recovery method	Parsing and carving

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the that file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file that the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-	The last modified date and time of the picture in the file system.

Attribute	Description
mm-dd)	
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).

Attribute	Description
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The latitude coordinate in decimal degrees.
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS latitude (extracted from Exif data).
Longitude	The longitude coordinate in decimal degrees.
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
Exif Data	A searchable field for all raw exif properties.

Attribute	Description
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicates whether the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

For information about supported formats, see Supported media and file types.
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.
To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Private Photo Vault Albums

Description	Private Photo Vault Albums contains information about the albums a user creates to organize their media in the Private Photo Vault application. The album information can be useful intelligence for how a user might have organized encrypted media.
Recovery method	Parsing

Attribute	Description
Album Title	The name of the album.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the album was created on the device.
Last Modified Date/Time - UTC (yyyy-mm-dd)	Not available on Android.
Decoy	Indicates whether the album is hidden (accessible with a different passcode) or not.
Password	The password protecting the album, if any. Does not affect encryption.
PIN	The value used to generate the encryption key. It can be either a numeric PIN (4 digits) or a sequence of values (2 to 9) of an unlock pattern.

Additional Information

Private Photo Vault Media

Description	Private Photo Vault Media contains information about encrypted media files that the user stores in the Private Photo Vault application. If decryption is successful, the decrypted media content is made available in this artifact. Metadata about the encrypted media files, such as timestamps, are always available. Users will often resort to encrypted media applications for storing illicit material. Being able to decrypt this media can be crucial to a case.
Recovery method	Parsing

Attribute	Description
File Path	The path to the encrypted media file.
Media Type	The type of media (photo or video).
Album Title	The associated album title.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the media was created on the device.
Last Modified Date/Time - UTC (yyyy-mm-dd)	Not available on Android.
Thumbnail Path	Not utilized on Android - see the 'Private Photo Vault Thumbnails - Android' artifact instead.
Picture	The encrypted media.
Thumbnail File	The thumbnail of the encrypted media.

Additional Information

Private Photo Vault Thumbnails - Android

Description	On Android, Private Photo Vault does not explicitly reference thumbnails in the database. Further, multiple resolutions can exist. This artifact will decrypt all of the thumbnails found in the thumbnails directory.
Recovery method	Parsing

Attribute	Description
File Name	The path to the encrypted thumbnail.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the media was created or imported into Private Photo Vault.
Thumbnail File	The thumbnail of the encrypted media.

Additional Information
This artifact may be useful in situations where the original media or database rows have been deleted but thumbnail files remain. It is possible for the same encrypted media to have multiple thumbnails (different resolutions).

RealPlayer Library Assets

Description	RealPlayer Library Assets contains information about the items that have been added to the library. This artifact can reveal information about the user's interaction with the application.
Recovery method	Parsing

Attribute	Description
Type	The type of asset, such as video, photo, or folder.
Path	The path to the asset.
Title	The asset's title.
Original Created Date/Time -	The date and time that the imported asset was original

Attribute	Description
UTC (yyyy-mm-dd)	created.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the asset was added to the library.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the asset was last accessed.
Exif Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the imported asset was created according to its file metadata.
Private	Indicates whether the asset is marked private.
Hidden	Indicates whether the asset is hidden.
Artist	The artist name associated with the asset, if applicable.
File Size (Bytes)	The size of the file in bytes.
Audio Format	The format of the asset's audio content (media files only).
Video Format	The format of the asset's video content (video files only).

Additional Information

RealPlayer Video History

Description	RealPlayer Video History contains information about the media files that were played using RealPlayer. This artifact can reveal information about the user's interaction with the application.
Recovery method	Parsing

Attribute	Description
Video URL	The URL of the video that was played, if streamed.
File Path	Th file path of the video, if it was played from the local filesystem.
File Name	The file name of the video, if it was played from the local filesystem.
Last Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time that the video was last viewed.
First Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time that the video was first viewed.

Additional Information

Thumbcache Pictures

Description	Thumbcache Pictures contains thumbnails and picture previews recovered from thumbcache_xx.db files. The artifact also contains metadata that is cross-referenced from the Windows Search Service database (Windows.edb) where possible.
Recovery method	Parsing

Attribute	Description
Thumbnail File	The name of the thumbnail picture as stored in the thumbcache_xx.db file.

Attribute	Description
Size (Bytes)	The size of the thumbnail picture in bytes.
Picture	The thumbnail picture data that was recovered.
File Name	The name of the file or folder that the thumbnail picture represents.
MIME Type	The MIME type of the file that the thumbnail picture represents. If the thumbnail did not come from a file, this value will be blank.
File Path	The path to the file or folder that the thumbnail picture represents.
File Extension	The extension of the file that the thumbnail picture represents. If the thumbnail did not come from a file, this value will be blank.
Original Width	The original width of the picture file that the thumbnail picture represents. If the thumbnail did not come from a file, this value will be blank.
Original Height	The original height of the picture file that the thumbnail picture represents. If the thumbnail did not come from a file, this value will be blank.
Skin Tone Percentage	The calculated percentage of skin tone in the thumbnail picture.
MD5 Hash	An MD5 hash of the thumbnail picture content.
SHA1 Hash	A SHA1 hash of the thumbnail picture content.
PhotoDNA Hash	The hash of the thumbnail picture content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

Videos

Description	Videos contains videos that are recovered using parsing or carving. Supported formats for parsing include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. Supported carving formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. For more information about supported video formats, see Supported media and file types.
Recovery method	Parsing

Attribute	Description
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
File Name	The name of the file.
File Extension	The extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was last accessed.
Last Modified Date/Time - UTC (yyyy-	The date and time when the video was last modified.

Attribute	Description
mm-dd)	
File Size (Bytes)	The size of the video.
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. "Complete" indicates that a full Exif extraction was performed, including potential metadata located at the end of the video. "Partial" indicates that only Exif information in the header section of the video file was recovered, which should only occur with very large videos (in excess of the limit set in the options screen). "Failed" indicates that the information may have been corrupted and could not be recovered. "Skipped" indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The resolution of the video (extracted from Exif data).
Original Height	The resolution of the video (extracted from Exif data).
Created Date/Time - Local Time	The local date and time when the video was first recorded (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the video was edited (extracted from Exif data).

Attribute	Description
Timezone	The timezone setting on the camera at the time of the video being recored (extracted from Exif data).
Software	The software used to record or modify the video. This could either be the OS version of the phone used to record the video or name of the software used to edit the video in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to record the video (extracted from Exif data).
Model	The model of the camera used to record the video (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to record the video (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS latitude coordinates of the camera where the video was recorded (extracted from Exif data).
Longitude	The GPS longitude coordinates of the camera where the video was recorded (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the video was recorded (extracted from Exif data).
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Attribute	Description
Content Format	The format of the carved video.
Container Format	The format of the carved video container.
Saved Video Size (Bytes)	The size of the carved video that was saved to the database.
Exif Data	A searchable field for all raw exif properties.

Additional Information

If AXIOM Process is configured to save a set amount of data from carved videos, any generated MD5 and SHA1 hashes are based on the saved data, not the full video. This behavior might cause issues when searching for known video hashes, as the hash for a carved video will differ from the actual video if it exceeds the size limit set in AXIOM Process.
To learn more about Exif data for videos, see Extracting Exif data from videos.
To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

VLC Recently Played Files

Description	VLC Recently Played Files contains information about the media files that are played using the VLC Media Player. This artifact can reveal information on the user's interaction with the application.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file that was played in the player.
File Path	The file path to the recently played file.
Resume Time (seconds)	The number of seconds played before the media file is paused or stopped. A value of -1 indicates that the file was watched completely. If the duration is less than 10 seconds, the Media Player will always set the value to 0.

Additional Information

Web Video Fragments

Description	This search recovers two distinct types of web-based video. Fragments of Flash video can be left behind by many video streaming sites, such as YouTube. RTMP Frame Fragments are frames left behind by streaming sites using the RTMP protocol (widely used by webcam chat sites, including Chatroulette and Camstumble). In this case, a thumbnail from a recovered video is displayed, as well as any relevant metadata. Videos can be exported to .FLV format to be played. Due to the nature of the data recovered, some video players will have issues playing the exported files. We recommend trying FFmpeg, VLC, and the GOM player.
Recovery method	Carving

Attribute	Description
Preview	A thumbnail preview of the video.

Attribute	Description
Content Recovered	The raw bytes that were recovered.
Metadata	Any metadata about the video.
Recovered Duration	The length of the video that was recovered.

Additional Information

Operating System

.DS_Store Records

Description	.DS_Store Records contains all the records extracted from .DS_Store files found on the computer. Each record represents a property of a file or a folder. The significance of this artifact is an indicator of high likelihood that the user of the computer was aware of these files and folders with a possibility of attributing a date to that awareness.
Recovery method	Parsing

Attribute	Description
Record Name	The name of the file or folder as stored in the .DS_Store file.
Record Type	The type of the record, or property, that is being logged in the .DS_Store file for a particular file or folder.
Record Value	The value of the property for the given file or folder.

Attribute	Description
Record Date/Time - UTC (yyyy-mm-dd)	The date and time that the record was modified.
Record Path	The full path to the file or folder
.DS_Store Created Date/Time - UTC (yyyy-mm-dd)	The created date of the .DS_Store file from which the record was extracted.
.DS_Store Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date of the .DS_Store file from which the record was extracted.
.DS_Store Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date of the .DS_Store file from which the record was extracted.

Additional Information

In the Apple macOS operating system, .DS_Store (Desktop Services Store) is a hidden file that stores the display information of its containing folder, similar to the file desktop.ini in Microsoft Windows. The file tracks information such as icon positions, view settings, cached file size, cached last modified date, and even the choice of a background image. The .DS_Store is created and maintained by the Finder application in any folder that it accesses, even on remote file systems mounted from servers that share files (for example, via Server Message Block (SMB) protocol or the Apple Filing Protocol (AFP)). .DS_Store files are also included in archives created by macOS users, such as ZIP files, and they are backed up by some cloud file backup services. This means that the presence of .DS_Store Records artifacts on non-Mac evidence such as Windows, Mobile, or Cloud indicates that some of the data may have originated or have been accessed from a macOS computer at some point. For more information on .DS_Store files and their forensic significance see: .DS_Stores: Like Shellbags but for Macs.

Accounts Information

Description	Contains the login information for all accounts on the Android device.
Recovery method	Parsing

Attribute	Description
User Name	The username associated with the account.
Package Name	The name of the application as the device sees it.
Password	The password stored on the device to connect to the account.
Last Login Date/Time - UTC (yyyy-mm-dd)	The date and time of the last successful login.

Additional Information

Anacron Jobs

Description	Anacron jobs are used to execute tasks at a certain frequency on machines that may be powered off.
Recovery method	Parsing

Attribute	Description
Username	The username associated with the task.

Attribute	Description
Frequency	A description of how often the task is triggered.
Identifier	A specific job ID that is used when logging messages for the task.
Command	The command that will be performed when the task is triggered.
Command Shell	The path to the shell file that is used when the task is triggered.
Paths	An environment variable that specifies the paths of the directories used when the task is triggered.

Additional Information

Android Downloads

Description	Android Downloads contains file download information from a recovered Android device.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified.
Save Location	The absolute path on the device to the file downloaded.

Attribute	Description
Notification Package	The Android package name that the download was initiated in.
Bytes Downloaded	The bytes that were downloaded.
Total Bytes	The total bytes of the file.

Additional Information

Bash / ZSH Sessions

Description	Bash / ZSH Sessions contains information about terminal/Bash on a Linux computer, and the commands that are run during each session.
Recovery method	Parsing

Attribute	Description
Session ID	The ID of the session.
User	The user that started the session.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the session started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the session ended.
Session Command History	The command history of the session.

Additional Information

Chromebook Device Information

Description	Chromebook Device Information contains information about the physical device, such as model information, the software version, region information, and the latest Chrome OS version.
Recovery method	Parsing

Attribute	Description
Version	Last installed Chrome version.
Operating System	Operating system type.
Last Mount Date/Time - UTC (yyyy-mm-dd)	Last volume mount date/time in UTC.
Last Mount Date/Time - Format Unknown	Last volume mount date/time when the format is unknown.
Last Write Date/Time - UTC (yyyy-mm-dd)	Last volume write date/time in UTC.
Last Write Date/Time - Format Unknown	Last volume write date/time when the format is unknown.
Mount Count	Volume mount count.
MLB Serial Number	Main Logic Board Serial Number.
Serial Number	Device serial number.
Region	Device region.
Model Name	Model name of the device.
Device First Activity Time	Date and Time the device was first active.

Additional Information

ChromeOS Downloads

Description	Chromebook Downloads contains file download information from a recovered Chromebook device.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file that was downloaded.
File Type	The file extension type of the file that was downloaded.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified.
File Size Bytes	The file size in bytes that were downloaded.
Preview	The image if the file type is an image. Otherwise, this column is empty.
File Content	The file contents if the file type is not an image. Otherwise, this column is empty.

Additional Information

ChromeOS Offline Storage

Description	ChromeOS Offline Storage are files that primarily exist online, but have also been saved to local storage on the Chromebook device for offline use.
Recovery method	Parsing

Attribute	Description
Original File Name	The original state of the file name.
File Name	The name of the file as it currently appears on the file system.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was modified.
File Size (Bytes)	The size of the file in bytes.
Preview	The image if the file type is an image. Otherwise, this column is empty.
File Content	The file contents if the file type is not an image. Otherwise, this column is empty.

Additional Information

Cron Jobs

Description	Cron jobs are used to execute tasks at a certain frequency on continuously running machines.
Recovery method	Parsing

Attribute	Description
Username	The username associated with the task.
Frequency	A description of how often the task is triggered.
Cron Frequency	The cron expression used to specify the task's frequency.
Command	The command that will be performed when the task is triggered.
Command Shell	The path to the shell file that is used when the task is triggered.
Paths	An environment variable that specifies the paths of the directories used when the task is triggered.

Additional Information

CUPS Print Jobs

Description	CUPS Print Jobs contains records of print jobs that were created by the Common Unix Printing System (CUPS).

Recovery method	Parsing

Attribute	Description
Job ID	The ID of the print job.
Job Name	The name of the print job.
Job UUID	The UUID of the print job.
Owner	The owner of the print job.
Application	The application that triggered the print job.
Cached File Name	The name of the cached file to print.
Document Format	The format of the document for the print job.
Copies	The number of copes that the user selected for printing.
Sheets Printed	The actual number of sheets that were printed.
Origin Host Name	The origin host name of the print job request.
Destination Printer	The printer used for the print job.
Printer URI	The URI of the printer used for the print job.
State	The state of the print job.
Printer State Message	The printer state message.
Printer State Reason	The printer state reason.
Created Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the print job was created.

Attribute	Description
Processed Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the print job was processed.
Completed Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the print job was completed.
Attachment	The cached document that was sent for printing, if it's available.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

File System Information

Description	File System Information contains all of the relevant information about the hard drives in use by the operating system.
Recovery method	Parsing

Attribute	Description
ID	The identifier of the hard drive.
Volume Serial Number	This field only applies to FAT and NTFS file systems. This is a 32-bit unsigned int value that is stored in Bios Paramter Block (BPB) and is showed in a special hex format â€“ XXXX-XXXX e.g. EABB-6573. For other file systems, the value of this field should show "n/a".

Attribute	Description
Full Volume Serial Number	This field is a 64-bit volume serial number that is only present in BPB of NTFS file system, for example AABBCCDDEEFF0011. For non-NTFS file systems, "n/a" is displayed for this field.
File System	The type of the file system (e.g "Microsoft NTFS").
Sectors per cluster	The number of sectors in a file system cluster.
Bytes per sector	The number of bytes per sector.
Starting Sector	The starting sector for this partition.
Ending Sector	The ending sector for this partition.
Total Sectors	Encase shows different values for this field based on how a volume is added to the case. For example, if you add just a volume (e.g. your local C:\ drive), it shows 123410271 for the number of sectors, but if you add your local physical drive 0 to the case and then select your C:\ volume in the "Entries" tree (note: your C drive would most likely have another letter in this tree, e.g. E:), then total number of sectors would be one more that the other value, i.e. 123410272. the value show for this field is taken from BPB, which matches the first value. The other value is shown when the parent physical drive is present probably comes from the partition table, and it counts VBR as well.
Total Clusters	The number of clusters comprising the file system.
Free Clusters	The number of unallocated clusters in the file system.
Total Capacity (Bytes)	This value is calculated by (Total Clusters) x (Cluster Size), which shows the capacity of the file system and not the volume containing it. The size of

Attribute	Description
	the volume would be higher than this value.
Unallocated Area (Bytes)	The number of unallocated bytes on the file system, which is calculated by (Number of free clusters) x (cluster size).
Allocated Area (Bytes)	This value is calculated by (Number of allocated clusters) x (cluster size).
Volume Name	The volume label stored in Volume Boot Record (VBR).
Volume Offset (Bytes)	The offset (in bytes) of the volume containing this file system from beginning of the disk. "0" is displayed if the image and/or drive being searched is the image of one volume. Encase shows the number of sectors for this field instead of the number of bytes.
Drive Type	The type of the hard drive.

Additional Information

Google Accounts

Description	Google Accounts contains the Google accounts that are currently signed in on any Google application on the device.
Recovery method	Parsing

Attribute	Description
Account Name	The account name of the user.

Attribute	Description
Display Name	The display name of the user.
Profile ID	The GAIA ID.
Profile Image URL	The URL for the user's profile image.

Additional Information

Network Interfaces - Linux

Description	Network Interfaces lists all network interfaces and their DHCP leases assigned by the local DHCP server.
Recovery method	Parsing

Attribute	Description
Adapter Name	The name of the network adapter.
IPv4 Address	The IPv4 address of the interface.
IPv4 Subnet Mask	The IPv4 subnet mask of the interface
DNS Server(s)	The DNS server associated with this interface.
DHCP Server	The DHCP server associated with this interface.
Domain	The DNS domain of this interface.
Lease Obtained Date/Time - UTC (yyyy-mm-dd)	The date and time that the lease was obtained on this interface.

Attribute	Description
Lease Expires Date/Time - UTC (yyyy-mm-dd)	The date and time that the lease will expire on this interface.

Additional Information

Operating System Information - Linux

Description	This table contains information about the Linux installation.
Recovery method	Parsing

Attribute	Description
Operating System	The name of the operating system.
Operating System Version	The version of the operating system.
Local Hostname	The local hostname of the computer.
DHCP DNS Server(s)	A comma separated list of the DHCP assigned DNS servers. This fragment represents the Domain Name Server(s) (DNS) provided from the DHCP service.
IP	The local network IP address assigned to this computer.
Timezone	The current timezone of the computer.

Additional Information

Recent Files - Linux

Description	The Recent Files - Linux artifact contains information about the files that are accessed by a user. Most Linux distros store this information in XML format in the following location: ($home/.local/share/recently-used.xbel).
Recovery method	Parsing

Attribute	Description
File Path	The path to the file that was accessed.
MIME Type	The MIME type of the file that was accessed.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created.
Application Name	The name of the application that was used to access the file.
Command	The shell command used to access or execute the file, if applicable.
Application Run Count	The number of times the user has accessed the file.

Additional Information

Recent Tasks

Description	Recent Tasks lists recent OS tasks recovered from a Chromebook extraction. Each task is stored in it's own xml file at extracted.tgz\decrypted\mount\root\android-data\data\system_ce\0
Recovery method	Parsing

Attribute	Description
ID	ID of the task.
Task Name	Name of the task.
Origin Activity	Name of the application which originated the task, if applicable.
Application	Name of the application or package context which created the task.
Suspended	Value that represents the activity suspension status.
User ID	ID of the user that created the task.
Associated Application Name	Name of the application which called the process which originated the task.
Task Category	Category value of the task.
First Active Date/Time - UTC (yyyy-mm-dd)	Timestamp of the first recorded task activity.
Last Active Date/Time - UTC (yyyy-mm-dd)	Timestamp of the last recorded task activity.

Attribute	Description
Updated Date/Time - UTC (yyyy-mm-dd)	Timestamp of the last time the task was moved or updated.

Additional Information

SSH Authorized Keys

Description	SSH Authorized keys are pre-configured keys used for logging into user accounts.
Recovery method	Parsing

Attribute	Description
Options	The list of options for the authorized key. This may be empty.
Encryption	The type of encryption used for the public key.
Public Key	The encrypted public key.
Comment	The comment added by the user for the authorized key. This may be empty.

Additional Information

SSH Keys

Description	SSH Keys are used to perform secure activities over the internet.
Recovery method	Parsing

Attribute	Description
File Name	The name of the SSH Keys file.
Type	The type of the SSH Key, either Public or Private.
Encryption	The type of encryption used on the SSH Key.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the file system.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the file system.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the file system.
File Content	The contents of the SSH Key file.

Additional Information

SSH Known Hosts

Description	SSH Known Hosts are public keys used to verify the identity of remote hosts. These are often automatically populated when the user connects to a host for the first time, but they can also be added manually.
Recovery method	Parsing

Attribute	Description
Host Names	The name or names of the specified host.
Marker	An optional tag used to indicate whether the host is a certificate authority.
Encryption	The type of encryption used for the public key.
Public Key	The encrypted public key.
Comment	The comment added by the user for the known host. This may be empty.

Additional Information

Startup Items - Linux

Description	Startup Items contains the configured auto-run scripts for the system at startup.
Recovery method	Parsing

Attribute	Description
Name	The name of the startup script file.
File Path	The path to the startup script file.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the script file was created.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the script file was last accessed.

Attribute	Description
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the script file was last modified.
File Content	The contents of the script file.

Additional Information

System Logs - Linux

Description	System Logs contains the operating system-generated logs stored on the machine.
Recovery method	Parsing

Attribute	Description
File Path	The path to the system log file.
Log Date/Time - Local Time	The date and time that the log entry was written.
User Name	The user name of the user the logging application ran under.
Process Name	The name of the process that generated the log entry.
Process ID	The id of the process that generated the log entry.
Message	The log message.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

System Services - Linux

Description	The System Services artifact lists the current services that exist on the system.
Recovery method	Parsing

Attribute	Description
Name	The service name.
File Path	The path to the service definition file.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the service file was created.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the service file was last accessed.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the service file was last modified.
File Content	The contents of the service definition file.

Additional Information

Trash Items

Description	Trash Items contains information about the items that a user has sent to the trash. This artifact recovers both deleted files and deleted directories.
Recovery method	Parsing

Attribute	Description
Item Name	The name of the file or directory that has been deleted.
Item Type	The type of the deleted item. This can be Folder, File, or Item not found.
File Type	The extension of the file. This attribute is not populated for directories and files with no extensions.
File Size (Bytes)	The size of the file in bytes.
Original Path	The original path of a file or directory recovered from the .trashinfo file. This path is used for restoring files to their original location. Note that the original path of a folder is used as a starting point to which the relative path of each item found inside is appended.
Deleted Date/Time - Local Time (yyyy-mm-dd)	The date and time that a file or directory was added to the trash bin. This is recovered from the .trashinfo file.
Deleted Date/Time - Local Time	The date and time that a file or directory was added to the trash bin. This is recovered from the .trashinfo file.

Attribute	Description
(Format Unknown)	
Data	The preview card.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

User Accounts - Linux

Description	User Accounts contains user accounts information pulled from Linux system files.
Recovery method	Parsing

Attribute	Description
User Name	The username of the account.
Password Hash	A hash of the user's password.
Password Hash Algorithm	The algorithm used to generate the user's password hash.
Last Password Change Date/Time - UTC (yyyy-mm-dd)	The date and time that the user last changed their password.
User ID	The user's ID.

Attribute	Description
Group ID	The user's security group ID.
Account Description	A description of the account.
Home Directory	The user's home directory.
Command Shell	The base directory for shell commands.

Additional Information

Wi-Fi Logs - Android

Description	Wi-Fi Logs - Android contains information about the Wi-Fi networks that a device has connected to.
Recovery method	Parsing

Attribute	Description
Network Name (SSID)	The name of the saved network.
BSSID	A unique identifier for the specific access point, which is often represented as the MAC address for the access point's wireless adapter.
Date/Time - Local Time (yyyy-mm-dd)	The date and time of the network connection. In instances where the year is missing from the source data, this value is represented as a string instead of a date/time.

Attribute	Description
First Connected Date/Time - Local Time (yyyy-mm-dd)	The date and time of the connection event.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Peer-to-Peer

Torrent Active Transfers

Description	Torrent Active Transfers contains information about the torrents that are active on the user's system.
Recovery method	Parsing

Attribute	Description
Torrent Name	The name of the torrent file.
Potential App Name	The name of the application that the torrent was potentially downloaded with.
Download Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file download was started.
Download Completed Date/Time -	The date and time that the torrent file download was

Attribute	Description
UTC (yyyy-mm-dd)	completed.
Download URL	The URL to download the torrent.
Downloaded Bytes	The total number of bytes that has been downloaded.
Download Location	The location on the disk to where the torrent was downloaded.
Bytes Uploaded	The total number of bytes that the system has uploaded for this torrent.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the active transfer was last modified.

Additional Information

Torrent Feeds

Description	Torrent Feeds contains information about RSS feeds that a user subscribes to that contains torrents available for download.
Recovery method	Parsing

Attribute	Description
Feed Name	The name of RSS subscription feed.
Feed URL	The URL of the RSS subscription feed.

Attribute	Description
Torrent Name	The name of the torrent available for download from the feed.
Download URL	The URL to download the torrent.
Description	A description of the contents of the torrent.
Published Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent feed item was published.
Status	The status of the feed item, either 'Downloaded' or 'Not Downloaded'.

Additional Information

Torrent File Fragments

Description	Torrent File Fragments contains data that is carved or parsed from .torrent files that are used to download torrents from various networks on the Internet.
Recovery method	Carving

Attribute	Description
Name	The name of the torrent file
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file was created.

Attribute	Description
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file was modified.
Torrent Creation Date/Time - UTC (yyyy-mm-dd)	The date and time that the torrent file was originally created.
Torrent Files	The files that are listed in the torrent to be downloaded.

Additional Information

Social Networking

Android Facebook Messages

Description	Android Facebook Messages contains Facebook messages recovered from the Android device.
Recovery method	Parsing and carving

Attribute	Description
Text	The content of the message.
Email	The email of the user sending a message.
Name	The display name of the user sending a message.
User Key	The facebook ID for the user sending a message.

Attribute	Description
Delivery Timestamp Date/Time	The delivery time of the message.
Send Timestamp Date/Time	The time when the message was sent.
Message ID	The unique ID of the message that was sent.
Message Source	Indicates if the message was sent from the web, messenger, chat, or mobile.
Coordinates	A GPS location associated with the message.

Additional Information

Android Facebook Pictures

Description	Android Facebook Pictures contains Facebook pictures that are recovered from the Android device.
Recovery method	Parsing

Attribute	Description
URL	The URL of the Facebook picture.
Filename	The file's absolute path on the device.
Image	The picture that was recovered.

Additional Information

Android Instagram Following

Description	Android Instagram Following contains information about the users that are being followed by the local user.
Recovery method	Parsing

Attribute	Description
ID	The unique identification number of a user.
User Name	The username of the user account.
Full Name	The full name of the user.
Biography	The biography written by the user.
External Access	A URL to an external website, provided by the user.
Blocked	Indicates whether the user being followed is blocked by the local user.
Status	Indicates the follow status of the local user (Following, Requested, and Not following).
Profile Picture URL	The URL to the profile picture of the user.
Account Type	The account status of the user (Private or Public).

Additional Information

Android Instagram Posts

Description	Android Instagram Posts contains the posts that a user has put onto Instagram.
Recovery method	Parsing and carving

Attribute	Description
Post ID	The post ID.
ID	The ID of the user who made the post.
User Name	The username on Instagram.
Full Name	The full name of the user.
Comment Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the comment was created.
Text	The text for the given image.
Profile Picture URL	The URL to the profile picture of the user.
Downloaded Profile Picture	The downloaded profile picture.
Posted Image URL	The URL to the image that was posted.
Downloaded Posted Image	
Type	The type of the post.
Posted Date/Time - UTC (yyyy-mm-dd)	The date that the post was made.
Device Date/Time - UTC (yyyy-mm-dd)	The date that the user viewed the post.

Additional Information

Android Instagram Users

Description	Android Instagram Users contains information on users of Instagram.
Recovery method	Parsing

Attribute	Description
ID	The ID of the user.
User Name	The username of the user on Instagram.
Full Name	The full name of the user.
Profile Picture URL	The URL to the profile picture of the user.
Downloaded Profile Picture	The downloaded profile picture.

Additional Information

Android Meet24 Cache Records

Description	Android Meet24 Cache Records contains items cached by Meet24 to improve performance.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached item.
First Visited Date/Time - UTC (yyyy-mm-dd)	The first date and time that the URL was visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL was visited.
Last Synced Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL cache was synced.
File Type	The type of file that was cached, if a file was cached.
Content Size	The size of the file that was cached, if a file was cached.
Image	The bytes of an image file, if an image file was cached.
Content	The bytes of a non-image file that was cached.

Additional Information

Android Meet24 Cookies

Description	Android Meet24 Cookies contains cookies that Meet24 uses for persistent data.
Recovery method	Parsing

Attribute	Description
Host	The host of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie is supposed to expire.
Path	The path of the cookie.

Additional Information

Android Tinder Accounts

Description	Android Tinder Accounts contains all of the recovered Android Tinder Accounts.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of current account owner.

Attribute	Description
Name	The name of the account user.
Last Activity Date/Time - UTC (yyyy-mm-dd)	The last date and time that the account user was active.
Biography	A brief written biography about the users account.
Birthday (yyyy-mm-dd)	The birthday of the account user.
Distance (Miles)	The distance that the user is searching for matches.
Gender	The gender of the account user.

Additional Information

Android Tinder Matches

Description	Android Tinder Matches contains all of the recovered Android Tinder Matches.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the user whom you are matched with.
User Name	The name of the user whom you are matched with.
Created Date/Time	The creation date of the match entry in UTC.

Attribute	Description
Last Activity Date/Time	The last time that there was activity with the match in UTC.
Created Date/Time - Local Time (yyyy-mm-dd)	The creation date of the match entry.
Last Activity Date/Time - Local Time (yyyy-mm-dd)	The last time that there was activity with the match.
Gender	The gender of the matched user.
Message Count	The number of messages that were exchanged with the matched profile.
Viewed Profile	Whether or not the user has viewed the profile.
Draft Message	The contents of a pending draft message.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Android Tinder Messages

Description	Android Tinder Messages contains all of the recovered Android Tinder Messages.
Recovery method	Parsing and carving

Attribute	Description
Sender ID	The user ID of the user whom is part of this conversation and is sending.
Recipient ID	The user ID of the user whom is part of this conversation and is receiving.
Match ID	The ID of the match who the message is received from.
Message Sent Date/Time - Local Time (yyyy-mm-dd)	The local date and time when the message was sent.
Message Sent Date/Time	The date and time when the message was sent in UTC.
Message Body	The body of the message.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Android Tinder Photos

Description	Android Tinder Photos contains all of the recovered Android Tinder Photos.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the user whom the picture belongs to.
User Name	The name of the user whom this picture belongs to.
Image URL	The URL to the Tinder photo.
Downloaded Image	The downloaded image.

Additional Information

Android Whisper Posts

Description	Android Whisper Posts contains the posts stored by the Whisper application.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username of the person at the time when the post was posted.
Text	The content of the post.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time that the post was posted.
Image URL	The URL to the image of the post.
Downloaded Image	The downloaded image from the post, if the option is turned

Attribute	Description
	on in Report Viewer.
Locale	The location of the user when the post was posted.
Latitude	The latitude of the user when the post was posted.
Longitude	The longitude of the user when the post was posted.
Hearts	The number of hearts the post has received.
Replies	The number of replies to the post.

Additional Information
To learn more about Whisper, see Artifact profile: Whisper.

Bebo Live Chat

Description	Bebo Live Chat contains messages sent or received in Bebo live chat. Information found within these attributes can include the status of the message, the date and time, the sender's username, the target's username, and the message itself.
Recovery method	Carving

Attribute	Description
Status	The sent status of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.

Attribute	Description
Source ID	The account of the source.
Target ID	The account of the target.
Message	The content of the chat message.

Additional Information

Facebook Chat

Description	Facebook Chat contains chat messages sent and received using Facebook Chat.
Recovery method	Carving

Attribute	Description
Profile ID	The Facebook profile ID of the sender.
Message ID	The unique ID for a specific chat message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Sender ID	The Facebook ID of the sender.
Downloaded Sender Image	The profile picture of the sender, downloaded from the Internet based on the Sender ID.
Sender Name	The name of the sender.

Attribute	Description
Receiver ID(s)	The Facebook IDs of all the receivers of the message.
Downloaded Receiver Image	The profile picture of the receiver, downloaded from the Internet based on the Receiver ID.
Receiver Names(s)	The name of the receiver.
Message	The content of the chat message.
Sender Offline	The online status of the sender.

Additional Information

Facebook Contacts

Description	Facebook Contacts contains contact information stored by the Facebook application.
Recovery method	Parsing and carving

Attribute	Description
Profile ID	The Facebook profile ID of the contact.
First Name	The Facebook contact's first name.
Last Name	The Facebook contact's last name.
Display Name	The Facebook contact's display name.

Attribute	Description
Small Picture URL	The URL to the the small picture.
Big Picture URL	The URL to the big picture.
Huge Picture URL	The URL to the huge picture.
Phone Numbers	The contact's phone numbers.

Additional Information

Facebook Email

Description	Facebook Email contains email messages sent using Facebook.
Recovery method	Carving

Attribute	Description
Logged-In User ID	The unique Facebook ID of the user that is currently logged in.
Downloaded Logged-In User Image	The profile picture of the sender, downloaded from the Internet based on the Logged-In User ID value.
Author ID	The unique Facebook ID of the author of the email.
Downloaded Author Image	The profile picture of the sender, downloaded from the Internet based on the Author ID value.
Author Name	The name of the author.

Attribute	Description
Recipient(s)	The names of the recipients.
Subject	The subject of the email.
Time Rendered - Local Time (yyyy-mm-dd)	The time that was rendered in the web browser when the user viewed the email.
Time Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the email was last updated.
Original Author	The first author of the email.
Message	The content of the email message.
Thread ID	The unique ID that represents the email trail.
Mobile	Indicates whether this email was sent from a mobile device.
Attachments	Indicates whether this email has attachments.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Facebook Email Snippets

Description	Facebook Email Snippets contains snippets of email messages sent using Facebook.
Recovery method	Carving

Attribute	Description
Subject	The subject of the email.
Snippet	A text snippet of the body of the email.
Original Author	The author of the email.
Recent Author	The most recent author of the email.
Time Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the email was last updated.
Thread ID	The conversation ID.

Additional Information

Facebook Pages

Description	Facebook Pages contains the content of the Facebook webpages that are cached.
Recovery method	Carving

Attribute	Description
Fragment	An HTML fragment of a Facebook webpage.

Additional Information

Facebook Status Updates/Wall Posts/Comments

Description	Facebook Status Updates/Wall Posts/Comments contains information about Facebook status updates, wall posts, and comments that are cached.
Recovery method	Carving

Attribute	Description
Sender ID	The Facebook ID of the sender.
Downloaded Sender Image	If Downloading Images from Web is enabled, the sender's profile picture can be fetched using the Facebook Graph API.
Sender Name	The name of the sender.
Receiver ID	The Facebook ID of the receiver.
Downloaded Receiver Image	If Downloading Images from Web is enabled, the receiver's profile picture can be fetched using the Facebook Graph API.
Receiver Name	The name of the receiver.
Status Update / Wall Post / Comment	The content of the status update, wall post, or comment.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time of the post.

Additional Information

Facebook User/Friends

Description	Facebook User/Friends contains profile information for the Facebook users and friends recovered from the Android device.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the user/friend.
Friend/User	Indicates if the information is for the user or a friend.
Display Name	The display name of the user/friend.
First Name	The first name of the user/friend.
Last Name	The last name of the user/friend.
Email(s)	The user/friends email address(es).
User Image URL	The URL to the user/friends profile picture.
Image	The profile picture.
Phone Number	The user/friends phone number.
Other	Additional information about user/friend.
Birthday (yyyy-mm-dd)	The user/friends birthday.

Additional Information

Foursquare Check-ins

Description	Foursquare Check-ins contains information about the user's check-ins.
Recovery method	Parsing and carving

Attribute	Description
User ID	The user ID
User First Name	The user's first name.
User Last Name	The user's last name.
User Email	The email address of the account used to check in.
Check-In Date/Time - UTC (yyyy-mm-dd)	The date and time when the user checked-in to the specified locaiton.
Location Name	The name of the location that the user checked into.
Comment	The comment a user left about their check-in for the location.
Address	The address of the check-in location.
Latitude	The latitude of the check-in location.
Longitude	The longitude of the check-in location.
City	The city of the check-in location.
State	The state of the check-in location.
Country	The country of the check-in location.
Been Here Count	The number of times that the user has checked into this

Attribute	Description
	location.
User Gender	The user's gender.

Additional Information

Foursquare Locations

Description	Foursquare Locations contains the location information viewed in Foursquare.
Recovery method	Parsing and carving

Attribute	Description
Location Name	The name of the location.
Address	The address of the location.
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Distance (meters)	The distance the user is from the location.
City	The city of the location.
State	The state of the location.
Country	The country of the location.

Additional Information

Foursquare Searches

Description	Foursquare Searches contains the search terms used in Foursquare.
Recovery method	Parsing and carving

Attribute	Description
Search Term	The search term used within Foursquare.

Additional Information

Google+ Chat

Description	Google+ is a web-based social network that allows users to communicate publicly, share photos and videos and also message privately.
Recovery method	Carving

Attribute	Description
Type	Indicates whether or not the message is a sent or received message.
Email	The email address associated with the message.
Message Sent Date/Time - UTC	The date and time that the message was sent.

Attribute	Description
(yyyy-mm-dd)	
Message	The content of the message.

Additional Information

Grindr Buddies

Description	Grindr Buddies contains the buddies and their details that were extracted from the current user's Android data.
Recovery method	Parsing and carving

Attribute	Description
Public ID	The ID of the user in the buddy list.
Display Name	The display name of the buddy.
Last Seen Date/Time - UTC (yyyy-mm-dd)	The date and time when the buddy was last seen.
Last Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the last message that was sent or received from this buddy.
Description	The description of the buddy.
Age	The age of the buddy.
Height (cm)	The height of the buddy.

Attribute	Description
Weight (kg)	The weight of the buddy.
Ethnicity	The ethnicity of the buddy.
Type of User	The type of user.
Distance	The distance of the buddy from the current user.
Favorited	Indicates whether the buddy is a favorite buddy of the current user.
Facebook Account	The name of the user's linked Facebook account.
Instagram Account	The name of the user's linked Instagram account.
Twitter Account	The name of the user's linked Twitter account.

Additional Information

Grindr Messages

Description	Grindr Messages contains the messages (and their details) that were extracted from a user's Android data.
Recovery method	Parsing and carving

Attribute	Description
Sender ID	The ID of the sender of the message.
Receiver ID	The ID of the receiver of the message.

Attribute	Description
Conversation Partner	The buddy's display name the message was with.
Group ID	The ID of the group the message was sent in.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was received.
Message Body	The body of the message.
Has Attachment	Whether or not the message has an attachment.
Read Status	The status of the message (Read or Unread).
Message Direction	Indicates whether the message was incoming to the device, or outgoing from the device.

Additional Information

GROWLr Chat Messages

Description	GROWLr Chat Messages contains the messages on the device that were sent or received through Growlr.
Recovery method	Parsing

Attribute	Description
Account ID	The ID of the other person that the message is with.

Attribute	Description
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent or received.
Message	The body of the message.
Message Type	Indicates whether the message was incoming or outgoing.
Message Status	The status of the message (Read or Unread).
Image Filename	The path to the image that is associated with the message.
Image	The attached image.
Voice Filename	The filename of the attached voice message.
Voice	The attached voice data.

Additional Information

GROWLr Notes

Description	GROWLr Notes contains the notes on Growlr that the user has made, and when they were last modified.
Recovery method	Parsing

Attribute	Description
Text	The body of the note.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the note was modified.

Additional Information

Instagram Direct Messages

Description	Instagram Direct Messages contains Instagram direct messages that are sent or received by the local user.
Recovery method	Parsing and carving

Attribute	Description
Sender	The username of the sender of the message.
Recipient	The username of the recipient of the message.
Message	The message that was sent.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time of the message.
Direction	The direction of the message, relative to the source of the hit.
Picture	The picture attribute is empty for Android as recovered pictures are located in the Attachment attribute instead.

Attribute	Description
Attachment	The attachment that was sent.
Attachment Path	The path to the attachment that was sent.
Media URL	The URL to the media of the message.
Type	The message type.
Status	The status of the message.
Latitude	The latitude of the message.
Longitude	The longitude of the message.
Caption	The original message of a forwarded post.
Original Author	The original author of a forwarded post.
Original Date/Time - UTC (yyyy-mm-dd)	The original date and time of a forwarded post.
Chat ID	The ID of the chat.

Additional Information
Attachments can only be retrieved when searching a full physical extraction of a device.

Instagram Group Members

Description	Instagram Group Members contains information about the Instagram groups that the local user is a member of.
Recovery method	Parsing

Attribute	Description
Group Member	The username of the group member.
Group Name	The name of the group.

Additional Information

Instagram Media

Description	Instagram Media contains the media files that have been found inside the Insatgram application.
Recovery method	Parsing

Attribute	Description
Picture	The picture of the media, or a storyboard if the media is a video.
MIME Type	The MIME type of the media.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.

Attribute	Description
Size (Bytes)	The size of the media file.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
URL	The URL to the media.
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

Instagram Pictures

Description	Instagram is a social media website where users share pictures.
Recovery method	Parsing

Attribute	Description
Profile Image	The profile picture of the poster.
Downloaded Profile Image	The profile image of the poster, downloaded from the Internet.
User ID	The user ID of the poster.
User Name	The username of the poster.
Instagram Image	The picture that was posted, if found locally.
Downloaded Instagram Image	The picture that was posted, downloaded from the Internet.

Additional Information

Instagram Posts

Description	Instagram is a social media website where users share pictures.
Recovery method	Carving

Attribute	Description
Profile Image	The profile picture of the poster.
Download Profile image	The profile image of the poster, downloaded from the Internet.
Text	The content of the post.
Date Created Date/Time - UTC (yyyy-	The date and time when the post was created.

Attribute	Description
mm-dd)	
User ID	The user ID of the poster.
User Name	The username of the poster.
Posted Image	The picture that was posted, if found locally.
Downloaded Posted Image	The picture that was posted, downloaded from the Internet.

Additional Information

Instagram Profiles

Description	Instagram Profiles contains profile information for the users that the local user has had communications with, or has been referred to through direct message communications.
Recovery method	Parsing

Attribute	Description
User Name	The username of the profile.
Name	The name that is associated with the profile.
User ID	The user ID associated with the profile.
Profile Picture	The profile picture of the user's profile.

Attribute	Description
URL	
Local User	Indicates whether the profile belongs to a user logged into the device.
Is Private	Indicates whether the profile is private or not.
Biography	The biography of the user associated with the account.
Following	Indicates whether the user of the profile is following the local user.
Is Followed By	Indicates whether the local user is following the user profile.
Post Notifications	Indicates whether the local user has turned on post notifications for the user profile. This attribute is only populated if the local user is following this user profile.
Email	The public email address associated with this user profile.
Phone Number	The public phone number associated with the user profile.
Address	The public address associated with the user profile.
City	The city associated with the user profile.
ZIP/Postal Code	The ZIP/postal code associated with the user profile.
Latitude	The latitude of the location associated with the user profile.
Longitude	The longitude of the location associated with the user profile.

Additional Information

For Android devices, the Following attribute will always be empty.

Life360 Circle Members

Description	Life30 Circle Members contains information about the members of a circle. A circle is comprised of a group of individuals, such as a family, that the local user has created or has been added to by another circle member.
Recovery method	Parsing

Attribute	Description
Member ID	The unique member ID of the circle member.
First Name	The first name of the member.
Last Name	The last name of the member.
Email Address	The email address of the member.
Phone Number	The phone number of the member.
Circle Name	The name the circle.
Circle ID	The ID of the circle.

Additional Information

Life360 Local User Account

Description	Life360 Local User Account contains information about local user accounts.
Recovery method	Parsing

Attribute	Description
User ID	The unique ID of the local user.
First Name	The first name of the local user.
Last Name	The last name of the local user.
Email Address	The email address of the local user.
Phone Number	The phone number of the local user.

Additional Information

Life360 Messages

Description	Life360 Messages contains messages sent and received by the local user within a circle that they're a member of.
Recovery method	Parsing

Attribute	Description
Sender ID	The unique ID of the sender.
Sender Name	The name of the sender.
Recipient ID(s)	The ID(s) of the recipient(s).
Recipient Name(s)	The name(s) of the recipient(s).
Message Type	The type of the message.

Attribute	Description
Message	The message content.
Created Date/Time	The date and time when the message was created.
Picture URL	The URL of the picture on the Life360 server, if a picture is included in the message.
Read	The read status of the message.
Latitude	The latitude of the location, if the message is a map location.
Longitude	The longitude of the location, if the message is a map location.
Location Name	The name of the location if the message is a map location.
Location Acquired Date/Time	The date and time when the location was acquired if the message is a map location.

Additional Information

Life360 Places

Description	Life360 Places indicates favorite locations that are saved by the user or the application.
Recovery method	Parsing

Attribute	Description
Place Name	The name of the place. The name can be either user-defined or a default

Attribute	Description
	name defined by the application.
Place Address	The address of the place.
Circle ID	The ID of the circle where the place was found.
Owner ID	The owner ID of the place, if the place was created by user.
Latitude	The latitude of the place.
Longitude	The longitude of the place.

Additional Information

Life360 Trip Locations

Description	Life360 Trip Locations indicates the locations that the user visits (or passes by on the way to a destination). During a trip, the application will log locations at regular intervals along the way.
Recovery method	Parsing

Attribute	Description
Updated Date/Time	The date and time that the trip details were last updated. Updates to the trip can be triggered by the user or the application.
Circle ID	The circle ID of the user who created this trip.

Attribute	Description
User ID	The unique ID of the user who created this trip.
Start Date	The date that the trip happened (days begin at 12:00 AM local time).
Latitude	The latitude of the location.
Longitude	The longitude of the location.
Start Date/Time	The date and time when the user arrived at the location.
End Date/Time	The date and time when the user left the location.
Location Name	The name of the location if it is a user created place.
Location Address	The address of the location.

Additional Information

LinkedIn Connections

Description	LinkedIn Connections contains information about LinkedIn users that have communicated with the local user account.
Recovery method	Parsing

Attribute	Description
Public ID	The public ID of the LinkedIn connection.
First Name	The first name of the LinkedIn connection.
Last Name	The last name of the LinkedIn connection.
Occupation	The occupation of the LinkedIn connection.

Additional Information

LinkedIn Emails

Description	LinkedIn Emails contains carved emails that have been sent or received on LinkedIn. These email fragments can include sender and recipient names, subject, date and time, and the full message. Please note that, depending on the browser, these emails might be compressed and are decompressed as they are viewed.
Recovery method	Carving

Attribute	Description
Fragment	An HTML fragment of the email.

Additional Information

LinkedIn Messages

Description	LinkedIn Messages contains messages sent and received by the local user.
Recovery method	Parsing

Attribute	Description
Sender Name	The name of the sender.
Recipient Name(s)	The name(s) of the recipient(s).
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The body of the message.
Attachment Name	The name of attachment to the message.
Attachment URL	The URL of attachment to the message.
Attachment Type	The type of the attachment to the message.
File	The attachment file to the message.

Additional Information

LinkedIn Profile

Description	LinkedIn Profile contains information about the user accounts that the local user has used to log in on the device.

Recovery method	Parsing

Attribute	Description
UserName	The username of local user.
First Name	The first name of the local user.
Last Name	The last name of the local user.
Full Name	The full name of the local user.
Summary	A summary of the local user. This information is provided by the user and can indicate a number of different things, including the user's position or status.

Additional Information

LinkedIn Searches

Description	LinkedIn Searches contains information about the searches that a LinkedIn user has made on the local device.
Recovery method	Parsing

Attribute	Description
Search Key-word	The keyword used by the user as a search term.

Attribute	Description
Date/Time	The date and time when the search occurred.
Search Type	The type of the search. This fragment is only populated if the user has specified the type of search to execute.

Additional Information

Musical.ly Local Users

Description	Musical.ly Local Users contains all of the users that have logged in to Musical.ly on the local device.
Recovery method	Parsing

Attribute	Description
User Name	The user's login name.
User Nickname	The user's chosen nickname.
User ID	The ID of the user in Musical.ly systems.
Account Description	The description that the user has given themself.
Image URL	The URL of the user's profile picture.
Instagram Account	The user's Instagram account.

Attribute	Description
Google Account	The user's Google account.
YouTube Channel	The user's YouTube Channel.
IP Address	The public IP address of the device that the user logged in with.
Is Private	Indicates whether the user prevents others from discovering their profile (Yes or No).
Hide Location	Indicates whether the user keeps their geolocation inforomation hidden on their profile page (Yes or No).
Messaging Availability	Indicates who is able to message the user, as specified by the user (Public or Friends Only).
Country Code	The country code of the country that the user has set for themself.
Language	The language code of the language that the user has set for themself.

Additional Information
The country code and language of the local user cannot be retrieved on Android devices.

Musical.ly Messages

Description	Musical.ly Messages contains messages sent or received in Musical.ly.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the message.
Recipient	The recipient of the message.
Message	The body of the message. This value is empty if a picture message was sent.
Direction	The direction of the message, relative to the source database.
Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was either received or sent on the local device.
Picture	The picture that was sent or received. This value is empty if a text message has been sent.
Read	Indicates whether or not the message has been read by the local device (Yes or No).
Message Status	The status of the message (Delivered or Pending Internet Connection).

Additional Information

The read status for messages cannot be retrieved from Android devices.

Musical.ly Posts

Description	Musical.ly Posts contains posts that Musical.ly has retrieved from the web.
Recovery method	Parsing

Attribute	Description
User Name	The username of the poster.
User Nickname	The nickname of the poster.
User ID	The ID of the poster.
Caption	The caption the user wrote for their post.
Picture	The locally cached post's preview picture.
Cached Video Size (Bytes)	The size of the locally cached post's video.
Video URL	The URL of the post's video.
Picture URL	The URL of the post's preview picture.

Additional Information
The picture and cached video of posts cannot be retrieved on Android devices.

Musical.ly Users

Description	Musical.ly Users contains all of the users that the local user has viewed in Musical.ly.
Recovery method	Parsing

Attribute	Description
User Name	The user's login name.
User Nickname	The user's chosen nickname.

Attribute	Description
User ID	The ID of the user in Musical.ly systems.
Account Description	The description that the user has given themself.
Profile Picture URL	The URL of the user's profile picture.
Instagram Account	The user's Instagram account.
Google Account	The user's Google account.
YouTube Channel	The user's YouTube Channel.
Is Private	Indicates whether the user prevents others from discovering their profile (Yes or No).
Is Friend	Indicates whether the user is a friend of the local user in the source database (Yes or No).
Following	Indicates whether the local user in the source database is following this user (Yes or No).
Post Notifications	Indicates whether the local user wants to receive notifications when this user makes a post (Yes or No).
Hide Location	Indicates whether the user keeps their geolocation information hidden on their profile page (Yes or No).
Messaging Availability	Indicates who is able to message the user, as specified by the user (Public or Friends Only).

Attribute	Description
Country Code	The country code of the country that the user has set for themself.
Language	The language code of the language that the user has set for themself.

Additional Information
The country code and language of the user cannot be retrieved on Android devices.

MySpace Chat - Messages

Description	MySpace Chat Messages contains messages sent or received in MySpace live chat. Information found within these attributes can include the status of the message, the date and time, the sender ID, the target ID, and the message itself. Some user info is also recoverable, such as the real name or username associated to a MySpace ID, image URL, and other information. This information is saved to a User Info report. This has been discontinued as of 2010.
Recovery method	Carving

Attribute	Description
Source ID	The account of the source.
Target ID	The account of the target.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The contents of the chat message.
Status	The sent status of the message.

Additional Information

MySpace Chat - User Info

Description	MySpace is a social networking website popular with music lovers.
Recovery method	Carving

Attribute	Description
User ID	The MySpace user ID.
UserName	The username used on MySpace.
Group	The group that the user is associated to (if applicable).
Image	The user's display picture.

Additional Information

MySpace Inbox Messages

Description	MySpace Inbox Messages contains sessages sent or received in MySpace live chat. Information found within these attributes can include the status of the message, the date and time, the sender ID, the target ID, and the message itself. Some user info is also recoverable, such as the real name or username associated to a MySpace ID, image URL, and other information. This information is saved to a User Info report. This has been discontinued as of 2010.

Recovery method	Carving

Attribute	Description
Sender	The sender of the message.
Subject	The subject of the message.
Message	The contents of the chat message.

Additional Information

Parler Activity - Android

Description	Parler Activity contains information about the posts and comments that the local user makes.
Recovery method	Parsing

Attribute	Description
Type	The type of activity (Post, Comment or Echo).
Post ID	The unique identifier associated with the post.
Comment ID	The unique identifier associated with the comment.
Creator ID	The unique identifier associated with the user who did the activity.

Attribute	Description
Body	The body of the post or comment.
Content Link	The URL of the post or comment.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the post or comment was created.
Parent ID	The unique identifier for the post or comment that this activity is a response to.
Comments Count	The number of comments on the post.
Deleted	Indicates whether the activity was deleted
Reposts Count	The number of times the activity has been reposted
Upvotes	The number of upvotes the activity has
Downvotes	The number of downvotes the activity has

Additional Information

Parler Users - Android

Description	Parler Users contains information about the local user account and any other users they've interacted with.
Recovery method	Parsing

Attribute	Description
ID	The unique identifier associated with the user.
User Name	The user name of the user.
Name	The name of the user.
Biography	The biography of the user.
Local Account	Indicates whether or not the user is the local user.
Joined Date/Time - UTC (yyyy-mm-dd)	The date and time the user joined Parler.
Verified	Indicates whether or not the user is verified on Parler.
Private	Indicates whether or not the user's account is private.
Followers	The number of followers the user has.
Following	The number of accounts the user is following.
Blocked	Indicates whether or not this user was blocked by the local user.
Posts Count	The number of posts the user has.
Likes Count	The number of likes the user has.

Additional Information

Pinterest Accounts

Description	Pinterest Accounts contains information about the accounts that the local

	user has logged in with on the device.
Recovery method	Parsing

Attribute	Description
User ID	The user ID of the local user.
Full Name	The full name of the local user.
Email	The email address of the local user.
Created Date/Time	The created date and time of the local user.
Gender	The gender of the local user.
Country	The country of the local user.
Locale	The location of the local user.
Profile Image URL	The profile image URL of the local user.
Active	The current status of the local user indicates whether the account is coming from an active database.

Additional Information

Pinterest Boards

Description	Pinterest Boards contains information about the boards that were created

	by local user.
Recovery method	Parsing

Attribute	Description
ID	The ID of the board.
Name	The name of the board.
Type	The category type of the board.
Description	The description of the board.
Created Date/Time	The created date and time of the board.
Website URL	The URL of the board.
Owner ID	The owner ID of the board.
Active Account	Active Account indicates whether the board is from the account that's currently logged in on the device.

Additional Information

Pinterest Following

Description	Pinterest Following contains information about the people or boards that local user follows.
Recovery method	Parsing

Attribute	Description
Type	Type indicates what is being followed (People or Board).
ID	The ID of the following.
Name	The name of the following.
Description	The description of the following.
Email	The email address of the following.
Created Date/Time	The created date and time of the following.
Country	The country of the following.
Locale	The location of the following.
Profile Image URL	The profile image URL of the following.
Website URL	The website URL of the following.
Active Account	Active Account indicates whether the following user is of the account that's currently logged in on the device.

Additional Information

Pinterest Messages

Description	Pinterest Messages contains messages or pins sent and received by the local user.
Recovery method	Parsing

Attribute	Description
Sender ID	The ID of the sender.
Sender Name	The name of the sender.
Recipient ID(s)	The user ID(s) of the recipient(s).
Recipient Name(s)	The name(s) of the recipient(s).
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The content of the message.
Pin Title	The title of the pin.
Pin Picture URL	The picture URL associated with the pin.
Attachment Name	The file name of the picture cache associated with the pin.
Attachment	The attachment associated with the pin.
Active Account	Active Account indicates whether the following user is of the account that's currently logged in on the device.

Additional Information

Pinterest Pins

Description	Pinterest Pins contains information about the items that the local user has pinned to their own board.
Recovery method	Parsing

Attribute	Description
Title	The title of the pin.
Description	The description of the pin.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the pin.
Website URL	The URL of the website associated with the pin.
Posted Image URL	The posted image URL associated with the pin.
Attachment Name	The name of the attachment associated with the pin.
Attachment	The attachment associated with the pin.
Pinner ID	The pinner ID of the pin.
Active Account	Active Account indicates whether the following user is of the account that's currently logged in on the device.

Additional Information

Reddit Accounts

Description	Reddit Accounts contains information about the user accounts that are used to log in to the Reddit application on the device.
Recovery method	Parsing

Attribute	Description
User ID	The Reddit user ID.
Account ID	The unique account ID for the user.
Email Address	The email address of the user.
Icon URL	The URL to the user's account icon.
Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time of the Reddit account.

Additional Information

Reddit Posts

Description	Reddit Posts contains information about the posts recovered from the device. These posts might be ones the user has read or created on their device.
Recovery method	Parsing

Attribute	Description
Title	The title of the Reddit post.
Subreddit Name	The subreddit name where the post was posted.
Author	The author of the post.
Over 18	Indicates whether or not the post was flagged as mature content.
Content Link	The URL to content from the post if applicable, or the URL to the

Attribute	Description
	post if there is no external content.
URL	The URL of the post.
Saved	Indicates whether or not the post was saved by the user.
Read Date/Time - UTC (yyyy-mm-dd)	The date and time that the user read the post.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the post was created.

Additional Information

Reddit Recently Visited Subreddits

Description	Reddit Recently Visited Subreddits contains information about the subreddits that a user has recently visited while on their device.
Recovery method	Parsing

Attribute	Description
Subreddit Name	The name of the subreddit.
Sort Order	The order in which posts were sorted within the subreddit (e.g. New, Hot, Top, Controversial).
Sort Time Frame	The time frame in which posts were sorted within the subreddit (e.g. Day, Week, Month, Year).

Attribute	Description
Description	The public facing description of the subreddit.
User Name	The user who visited the subreddit.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the user last visited the subreddit.
Created Date/Time - UTC (yyyy-mm-dd)	The creation date and time of the subreddit.

Additional Information

Sina Weibo Carved Searches

Description	Sina Weibo is a Chinese microblogging (weibo) website. Akin to a hybrid of Twitter and Facebook, it is one of the most popular websites in China. This table carves for a user's searches.
Recovery method	Parsing and carving

Attribute	Description
Search Term	The term that was searched.

Additional Information

Sina Weibo Microblogs

Description	Sina Weibo is a Chinese microblogging (weibo) website. Akin to a hybrid of Twitter and Facebook, it is one of the most popular websites in China. This table captures microblogging information.
Recovery method	Carving

Attribute	Description
Nickname	The blogger's nickname.
User ID	The user ID of the blogger.
Downloaded Profile Picture	The profile picture of the user, downloaded from the Internet based on the user ID.
Microblog Text	The content of the blog.
Posted From URL	The URL from which the blog was posted.

Additional Information

Sina Weibo Posts

Description	Sina Weibo Posts contains Sina Weibo posts that are recovered from a device.
Recovery method	Parsing and carving

Attribute	Description
User ID	The unique identifier for the user posting.
User Nickname	The user's nickname.
Post Date/Time - UTC (yyyy-mm-dd)	The date and time that the content was posted.
Post	The content of the post.
Profile Image URL	The URL for the profile image of the user.
Downloaded Profile Image	The raw content of the user's profile image, downloaded from the URL shown in the Profile Image URL column.
Post Image URL	The URL of the image in the post, if applicable.
Downloaded Post Image	The raw content of the image in the post, if applicable, and is downloaded from the URL shown in the Post Image URL column.
Posted Source	Information that describes the device from where the post was made.
Latitude	The latitude of the post's source device when the post was made.
Longitude	The longitude of the post's source device when the post was made.

Additional Information

Sina Weibo Private Messages

Description	Sina Weibo Private Messages contains Sina Weibo messages that are recovered from a device.
Recovery method	Parsing and carving

Attribute	Description
Conversation Partner ID	The unique ID of the conversation partner.
Conversation Partner	The name of the conversation partner.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent/received.
Message	The actual private message content.
Profile Image URL	The URL for the profile image of the user.
Downloaded Profile Image	The raw content of the user's profile image, downloaded from the URL shown in the Profile Image URL column.
Attachment Type	The type of attachment associated with the message.
Attachment Local File Path	The local path to the file attachment.

Additional Information

Sina Weibo Search History

Description	Sina Weibo is a Chinese microblogging (weibo) website. Akin to a hybrid of Twitter and Facebook, it is one of the most popular websites in China. This table captures a user's searches that have been parsed from the filesystem.
Recovery method	Parsing and carving

Attribute	Description
Search Term	The term that was searched.

Additional Information

TikTok Contacts

Description	TikTok Contacts contains information about a user's contacts in TikTok.
Recovery method	Parsing and carving

Attribute	Description
User Name	The username of the contact.
Nickname	The nickname of the contact.
ID	The unique ID of the contact.
Profile Picture URL	The URL of the profile picture of the contact.

Additional Information

TikTok Messages

Description	TikTok Messages contains information about the messages that a user sends or receives using TikTok.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the message.
Recipient	The recipient of the message.
Message	The content of the message.
Message Type	The type of the message.
Media URL	The URL of any media attached to the message.
Created Date/Time	The time that the message was sent.
Read	Whether the recipient has read the message.
Deleted	Whether the message has been deleted.

Additional Information

TikTok Videos

Description	TikTok Videos contains videos that were either viewed or created by the user.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
File Extension	The extension of the file.

Attribute	Description
Image	A generated thumbnail of the video.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video file was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the video file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was last written to.
Type	The type of the video.
Skin Tone Percentage	The amount of skin tone found in the video.
File Size (Bytes)	The size of the video.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Additional Information

Tumblr Blogs

Description	Tumblr Blogs contains information about the blogs that the user has interacted with. These blogs can include both followed and blocked blogs, though it's not currently possible to distinguish between the two.
Recovery method	Parsing

Attribute	Description
Blog Title	The title of the blog.
Description	The description of the blog.
Creator Name	The name of the blog's creator.
URL	The URL to the blog.

Additional Information

Tumblr Chat Messages

Description	Tumblr Chat Messages contains messages that were sent and received using Tumblr.
Recovery method	Parsing

Attribute	Description
Sender	The display name of the user who sent the message.
Recipient	The display name of the user who received the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The body of the message.
Media URL	The URL of any media attached to the message.

Attribute	Description
Entry ID	The database ID of the request or response from the Tumblr application.

Additional Information

Tumblr Tags

Description	Tumblr Tags contains information about the subject tags that the local user has selected. Selecting a tags expresses the user's interest in a subject so they can see more content of that type.
Recovery method	Parsing

Attribute	Description
Tag	The tag that the local user selected.

Additional Information

Twitter

Description	Twitter is a social networking website that allows users to share status messages, known as tweets.
Recovery method	Carving

Attribute	Description
Name	The full name of the user.
Screen Name	The Twitter handle of the user (e.g. @username).
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the tweet was created.
Tweet Text	The content of the tweet.
In Reply To	Indicates whether the tweet was a reply to another user.
Status ID	The unique identifier for the tweet.
Tweet Source	The type of device or application that was used to create the tweet.
Geo	The geo-location of the user when they posted the tweet.
Retweeted	This identifies whether the tweet was a retweet.
Profile Img URL	The URL link to the profile picture of the user.

Additional Information

Twitter Direct Messages

Description	Twitter Direct Messages contains carved and noncarved direct messages from the Twitter application. Note: Carving will not retrieve the names and screen names of the sender and receiver. Also, carving may be unable to retrieve the message direction on newer versions of Twitter.
Recovery method	Parsing and carving

Attribute	Description
Text	The text of the direct message.
Sender ID	The Twitter ID of the sender.
Recipient ID(s)	The Twitter ID for the recipient(s).
Sent/Received Date/Time - UTC (yyyy-mm-dd)	The date and time that the direct message was sent or received.
Direction	Whether the message was sent or received.
Sender Name	The name of the person sending the direct message.
Sender Screen Name	The screen name or Twitter handle of the person sending the direct message.
Recipient Name(s)	The name(s) of the person(s) receiving the direct message.
Recipient Screen Name(s)	The screen name(s) or Twitter handle(s) of the person(s) receiving the direct message.
Attachments	The attachments associated with the direct message.

Additional Information

Twitter Tweets

Description	Twitter Tweets contains carved and noncarved tweets from the Twitter application.
Recovery method	Parsing and carving

Attribute	Description
Author ID	The numeric ID of the account that posted the tweet.
Status ID	The unique ID of the tweet.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the tweet was created.
Tweet	The text content of the tweet.
Favorited	Whether the tweet has been favorited.
Latitude	The latitude of the location from which the tweet was posted.
Longitude	The longitude of the location from which the tweet was posted.
Retweet Count	The number of times that the tweet has been retweeted.
Tweet Source	The interface that was used to post the tweet.

Additional Information

Twitter Users

Description	Twitter Users contains information about users that were cached on the local user's device.
Recovery method	Parsing and carving

Attribute	Description
User ID	The user's Twitter user ID.
User Name	The user's Twitter username.
Full Name	The user's full name.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the user's Twitter profile was created.
Description	The short profile description that the user writes for themself.
Web URL	The user's website URL.
Following	'Yes' if the local user is following this account, 'No' otherwise. If this attribute is empty, it's undetermined whether the local user is following this account.
Locale	The location the user is from.
Protected	Whether or not the user's account was protected.
Followers	The number of followers that the user has.
Friends	The number of friends that the user has.
Statuses	The number of different statuses that the user has had.
Image URL	The URL to the user's profile picture.
Friend Metadata Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the user's meta information was last updated.
Header URL	The URL to the user's profile banner picture.

Additional Information

VK Messages

Description	VK Messages contains VK messages (either private or group messages) as well as the details about pictures, video, and audio that may have been sent.
Recovery method	Parsing and carving

Attribute	Description
Sender ID	The user ID of the message sender.
Receiver ID(s)	The user ID of the message recipient. This column can contain multiple user IDs if the message is from a group conversation.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent/received.
Message Text	The message text that was sent/received.
Type	The type of message sent. The possible types are 'Private Message' for one-to-one conversations or 'Group Message' for one-to-many conversations.
Message Deleted	The deletion state of the message is unsupported in VK Android and will therefore be empty.
Read State	The read state of the message is unsupported in VK Android and will there-

Attribute	Description
	fore be empty.
Forwarded Message Content	This column contains the original time that a message was sent, the user ID that originally sent the message, and the content (for example, text, video, or audio).
VK Attachment	This column contains details of the attachment that was sent. For picture attachments, a URL to a scaled picture is provided for downloading. When a video is sent, a thumbnail is provided with details of the video (title, date/-time, duration and description). When audio is sent, a URL to the audio is provided as well as the title, artist, and duration.
Latitude	The latitude in VK Android will be contained within VK Attachment or Forwarded Message Content and this column will be empty.
Longitude	The longitude in VK Android will be contained within VK Attachment or Forwarded Message Content and this column will be empty.
Attachment	The attachment that was sent.

Additional Information

The latitude and longitude attributes of this artifact typically only include data if the message has a Geo Location attachment. VK for Android stores location data as an attachment within a BLOB column, and if there are multiple attachments, one VK Messages item could include more than one latitude and longitude. To avoid confusion or displaying incorrect information, the location information typically appears in the attachment or forwarded message content.

VK Users

Description	VK Users contains the various users the data owner has been in com-

	munication with, as well as the users own profile.
Recovery method	Parsing and carving

Attribute	Description
User ID	The user ID of the user.
Gender	Identifies whether the user is a male or female.
Birthdate (yyyy-mm-dd)	The birthdate of the user.
First Name	The first name/given name of the user.
Last Name	The last name/surname of the user.
Profile Image	The URL to the users profile image.
Downloaded Profile Image	

Additional Information

VK Wall Posts

Description	VK Wall Posts contains the wall postings on social networking site VK.-com.
Recovery method	Carving

Attribute	Description
Author	The author of the wall post.
Wall Text	The content of the wall text.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message Relative Timestamp	A relative timestamp for the VK wall post.

Additional Information

VK Web Messages

Description	VK Web Messages contains a combination of both VK instance messages and sent and received messages.
Recovery method	Carving

Attribute	Description
Message Sender	The sender of the message.
Message	The content of the message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message Relative Timestamp	A relative timestamp for the VK message.

Additional Information

Whisper Messages

Description	Whisper Messages contains the messages that were sent and received between the local user and others.
Recovery method	Parsing and carving

Attribute	Description
Partner Name	The username of the person the chat was with.
Message Text	The content of the message.
Sent Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Status	The status of the message (Received or Sent).
Read	Whether or not the message was read by its recipient.
Image	The image that was sent or received.

Additional Information
To learn more about Whisper, see Artifact profile: Whisper.

Web Related

360 Safe Browser Archived Keyword Search Terms

Description	360 Safe Browser is a web browser developed by Qihoo.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword that was searched.
URL	The URL that was invoked because of the search.

Additional Information

360 Safe Browser Archived Web History

Description	360 Safe Browser Archived Web History contains all of the websites the user has gone to, along with when they last visited the site, and how often they have visited the site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the website the user visited.
Title	The title of the website that the user visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the user last visited the website.
Visit Count	The number of times that the user has visited the web-site.
Typed Count	The number of times that the user has manually typed the website's URL.
ID	The 360 Safe Browser identifier of the website.

Additional Information

360 Safe Browser Autofill

Description	360 Safe Browser Autofill contains all of the values that the user has saved to fill in fields at a later date and time.
Recovery method	Parsing

Attribute	Description
Name	The name of the field to fill in.
Value	The value to perform the fill in with.
Count	The number of times that the autofill has been used.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was first created.

Additional Information

360 Safe Browser Autofill Profiles

Description	360 Safe Browser Autofill Profiles contains all of the profiles that are used to represent a person.
Recovery method	Parsing

Attribute	Description
Name	The name that the person goes by or uses.
Email	The email address to use to contact the person.
Number	The telephone number to use to contact the person.
Company	The company the person works at.
Address Line 1	The first line of the person's address (e.g. 123 Fake Street, Fake Town, Fake Country).
Address Line 2	The second line of the person's address (e.g. Suite 123 or Apt. 123).
City	The city that the person lives in.
State	The state or province that the person lives in.
Zipcode	The ZIP Code that the person lives in.
Country	The country that the person lives in.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the person modified the profile.

Additional Information

360 Safe Browser Bookmarks

Description	360 Safe Browser Bookmarks contains all of the websites the user has bookmarked.
Recovery method	Parsing

Attribute	Description
Title	The title of the website.
URL	The URL of the website.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was last modified.
Is Folder	Indicates whether the bookmark is a folder. The possible value for this field are Yes, No, or Invalid.
Parent Folder	The parent folder of the bookmark.

Additional Information

360 Safe Browser Cache Records

Description	360 Safe Browser Cache Records contains all of the files and their information that has been cached by the browser.
Recovery method	Parsing

Attribute	Description
URL	The URL that the file was downloaded from.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.

Attribute	Description
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was first visited.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The last time that the local cache was synced with the web-server.
File Type	The type of cache file.
Content Size (Bytes)	The size of the cache file.
Image	If the content file is an image, it will be displayed here.
Content	If the file is not an image, such as a JavaScript file, the raw bytes will be stored here.

Additional Information

360 Safe Browser Cookies

Description	360 Safe Browser Cookies contains all of the cookies saved to the browser.
Recovery method	Parsing

Attribute	Description
Host	The host that created the cookie.
Name	The name of the cookie.

Attribute	Description
Value	The cookie value.
Accessed Date/Time - UTC(yyyy-mm-dd)	The date and time that the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was created.
Expiration Date/Time - UTC(yyyy-mm-dd)	The date and time that the cookie expires.

Additional Information

360 Safe Browser Current Downloads

Description	360 Safe Browser Current Downloads contains all of the files currently being downloaded.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file being downloaded.
Download Source	The source URL where the file was downloaded.
Saved To	The local file location.
State	The current state of the download.

Attribute	Description
Opened By User	Indicates whether the downloaded file was opened by the user.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Bytes Downloaded	The number of bytes download.
File Size (Bytes)	The size of the file being downloaded, in bytes.

Additional Information

360 Safe Browser Current Session

Description	360 Safe Browser Current Session contains all of the sessions that are currently in use by the browser.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - (UTC)(yyyy-mm-dd)	The date and time that the URL was last visited.

Attribute	Description
Visit Count	The number of times the user accessed the URL.

Additional Information

360 Safe Browser Current Tabs

Description	360 Safe Browser Current Tabs contains all of the open tabs in the browser.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - (UTC)(yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.

Additional Information

360 Safe Browser FavIcons

Description	360 Safe Browser FavIcons contains all of the icons that belong to common webpages the user goes to.
Recovery method	Parsing

Attribute	Description
Page URL	The URL of the webpage.
Icon URL	The URL to the icon image.
Last Updated Date/Time - UTC(yyyy-mm-dd)	The last date and time when the icon was updated.
State	The current state of the download.
Opened By User	Indicates whether the downloaded file was opened by the user.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Bytes Downloaded	The number of downloaded bytes.
File Size (Bytes)	The size of the file being downloaded, in bytes.

Additional Information

360 Safe Browser History Index

Description	360 Safe Browser History Index contains the browsing history of the user.
Recovery method	Parsing

Attribute	Description
Page URL	The webpage URL.
Title	The title of the webpage.
Visited on Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Body	The HTML body of the webpage.

Additional Information

360 Safe Browser Last Session

Description	360 Safe Browser Last Session contains all of the sessions that were last open.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.

Attribute	Description
Title	The title of the webpage.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time that the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

360 Safe Browser Last Tabs

Description	360 Safe Browser Last Tabs contains all of the tabs that were last open.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time that the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

360 Safe Browser Logins

Description	360 Safe Browser Logins contains all of the logins for websites the user has saved.
Recovery method	Parsing

Attribute	Description
User Name	The username for the webpage.
Password	The password for the login of the webpage.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the login information was created.
URL	The URL to the webpage.

Additional Information

360 Safe Browser Saved Credit Cards

Description	360 Safe Browser Saved Credit Cards contains all of the credit card information the user has saved.
Recovery method	Parsing

Attribute	Description
GUID	The identifier of the credit card.
Name On Card	The name on the credit card.
Expiry Date	The date the credit card is supposed to expire in format 'month-year'.
Card Number	The number of the credit card.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the credit card information was last modified.

Additional Information

360 Safe Browser Shortcuts

Description	360 Safe Browser Shortcuts contains all of the shortcuts used by 360 Safe Browser for user entered URLs.
Recovery method	Parsing

Attribute	Description
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.

Attribute	Description
Last Access Date/Time - (UTC) (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the webpage.
Times Used	The number of times that the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (Typed URL or Bookmark).

Additional Information

360 Safe Browser Top Sites

Description	360 Safe Browser Top Sites contains all of the websites the user goes to most often.
Recovery method	Parsing

Attribute	Description
URL	The URL to the webpage.
Title	The title of the webpage.
Last Updated Date/Time - (UTC)	The last time that the information for the top site

Attribute	Description
(yyyy-mm-dd)	was updated.
Thumbnail	The thumbnail of the webpage.

Additional Information

360 Safe Browser Web History

Description	360 Safe Browser Web History contains all of the websites the user has gone to.
Recovery method	Parsing and carving

Attribute	Description
Date Visited Date/Time - (UTC) (dd/MM/yy)	The date and time that the URL was first visited.
URL	The URL that was accessed by the user.
Title	The title of the webpage.
Visit Count	The number of times the user accessed the URL.
Typed Count	The number of times the user has navigated to this page by typing in the address.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition

Attribute	Description
	type is 'link'.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time that the URL was last visited.

Additional Information

360 Safe Browser Web Visits

Description	360 Safe Browser Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Title	The title of the webpage that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a

Attribute	Description
	user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

Aloha Browser Autofill

Description	Aloha Autofill contains records of the autofill values that Aloha saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill was last used.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Aloha Browser Bookmarks

Description	Aloha Bookmarks contains the webpages that a user has bookmarked.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Title	The name of the bookmark.
Parent	The name of the parent folder of the bookmark
Is Folder	Indicates whether the bookmark entry is a folder.

Additional Information

Aloha Browser Downloads

Description	Aloha Browser Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download URL	The URL of the file that was downloaded.

Attribute	Description
File Path	The absolute path on the device to the file downloaded.
URL	The URL of the site in which the file was downloaded.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was downloaded.

Additional Information

Aloha Browser History

Description	Aloha Browser History contains information about the websites that the user visits.
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the user first visited the webpage.
Title	The title of the webpage.
Visit Count	The number of times the user has visited that webpage.

Additional Information

Android Browser Bookmarks

Description	Android Browser Bookmarks contians the webpages that a user has bookmarked.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Name	The name of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date/time when the bookmark was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date/time when the bookmark was last modified.
Is Folder	Indicates whether the bookmark entry is a folder.

Additional Information

Android Browser Search Terms

Description	Android Browser Search Terms contains information about the keyword search terms a user has provided in the browser.

Recovery method	Parsing

Attribute	Description
Search Term	The search term that the user entered.
Search Date/Time - UTC (yyyy-mm-dd)	The date/time when the search was entered.

Additional Information

Android Browser Web History

Description	Android Browser Web History contains information about the websites that the user has visited.
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Title	The title of the webpage that was visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date/time when the webpage was last visited.
Visit Count	The number of times the webpage was visited.

Additional Information

Android Firefox Bookmarks

Description	Android Firefox Bookmarks contains bookmarks from the Firefox web browser on an Android device.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the bookmark.
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was last modified.
Keyword	Any keywords that have been associated with the bookmark. These keywords are user generated.
Description	A description of the bookmark.
Bookmark Data	Any tags that have been associated with the bookmarks. These tags are user generated.
Deleted	Indicates whether the bookmark was deleted (Yes or No).

Additional Information

Android Firefox Web History

Description	Android Firefox Web History contains the webpage history from the Firefox web browser on an Android device.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the webpage.
URL	The URL of the webpage.
First Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the person first visited the webpage.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage history was last modified.
Visit Count	The number of times that the user has visited that webpage.
Deleted	Indicates whether the webpage history was deleted (Yes or No).

Additional Information

Ashley Madison/Backpage Ads/Craigslist Ads/Plenty of Fish

Description	Ashley Madison/Backpage Ads/Craigslist Ads/Plenty of Fish contains recovered webpages from pagefile.sys.

Recovery method	Carving

Attribute	Description
Fragment	The fragment that was extracted.
Source	The location where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Baidu Searches

Description	Baidu Searches Contains information about the search history using the Baidu application.
Recovery method	Parsing

Attribute	Description
Search Term	The term that was searched.
Picture Path	The path to the picture that was searched.

Attribute	Description
Picture URL	The URL of the picture that was searched.
Search Type	The type of search. The options are Text or Picture.
Search Date/Time	The date/time of the search.
File	The file associated with the search.

Additional Information

Baidu Web Visits

Description	Baidu Web Visits contains a history of the websites that the user visited using the Baidu application.
Recovery method	Parsing

Attribute	Description
URL	The URL of the website.
Web Page Title	The title of the webpage.
Visited Date/Time	The date/time when the URL was visited

Additional Information

Bing Toolbar - Map History

Description	Bing Toolbar Map History contains information about maps and locations that were searched for using the Bing Toolbar.
Recovery method	Parsing

Attribute	Description
Location History	The previous location of the map.
Default Location	The default location of the map.
Default lat/long	The default latitude and longitude of the default location.
Show Traffic	Indicates whether the Show Traffic feature was turned on (True or False).
Default Zoom Level	The default zoom level for the map.
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Bing Toolbar - Search History

Description	Bing Toolbar Search History contains information about the search history for the Bing Toolbar.
Recovery method	Parsing

Attribute	Description
Search Term	The keyword that was searched for.
Search Date/Time - UTC (yyyy-mm-dd)	The date and time that the keyword search was conducted.
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Brave Autofill

Description	Brave Autofill contains records of the autofill values that Brave saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The autofill count.

Additional Information

Brave Bookmarks

Description	Brave Bookmarks contain bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was last visited.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Brave Cookies

Description	Brave Cookies contain cookies that Brave downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	The domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Brave Downloads

Description	Brave Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Saved To	The absolute path on the device to the downloaded file.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Brave FavIcons

Description	Brave Favicons contains the favicons that Brave displays in the address bar when visiting a website. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Brave Keyword Search Terms

Description	Information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user

Attribute	Description
	entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Brave Tab History - Android

Description	A history of websites the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the web page (for example, the referrer source might be from Google or another third-party application).

Attribute	Description
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Search Term	The value the user entered into a search.

Additional Information

Brave Top Sites

Description	A list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Additional Information

Brave Web History

Description	A history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Brave Web Visits

Description	A history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

Chrome Archived Keyword Search Terms

Description	Chrome Archived Keyword Search Terms contains keyword search terms that were archived by the browser.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user

Attribute	Description
	entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Chrome Archived Web History

Description	Android Archived Web History contains an archived history of old webpage visits.
Recovery method	Parsing

Attribute	Description
URL	The URL where the archived web history is located.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.
Title	The title of the archived web history.
Visit Count	The total number of visits to the URL.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
ID	The ID for the web history archive.

Additional Information

Chrome Autofill

Description	Chrome Autofill contains records of the autofill values that Chrome saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was last used.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Chrome Autofill Profiles

Description	Android Chrome Autofill Profiles contains profiles that Chrome uses to fill in forms with saved values.

Recovery method	Parsing

Attribute	Description
Name	The name for the autofill profile.
Email	The email used in the the autofill profile.
Number	The phone number used in the autofill profile.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the profile was last modified.
Company	The company name used in the autofill profile.
Address Line 1	The address Line 1 used in the autofill profile.
Address Line 2	The address Line 2 used in the autofill profile.
City	The city used in the autofill profile.
State	The state used in the autofill profile.
Zipcode	The ZIP code used in the autofill profile.
Country	The country used in the autofill profile.

Additional Information

Chrome Bookmarks

Description	Chrome Bookmarks contains browser bookmarks that reference saved webpages.

Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Chrome Cache Records

Description	Chrome Cache Records contains content that Chrome downloads and caches to speed up rendering times. Cached content can include pictures, text, HTML, javascript, and more.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached item.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was first visited.

Attribute	Description
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Last Synced Date/Time - UTC (yyyy-mm-dd)	The date and time when the cache was last synced with the cloud.
File Type	The type of file that was cached.
Content Size (Bytes)	The size of the cached file.
Image	The cached image if the file type is an image. If the file type is not an image, this column is empty.
Content	The cached file contents if the file type is not an image. If the file type is an image, this column is empty.
File Name	The file name of the cached item.
MD5 Hash	An MD5 hash of the cached item if it is a picture. Otherwise, this column is empty.
SHA1 Hash	A SHA1 hash of the cached item if it is a picture. Otherwise, this column is empty.
PhotoDNA Hash	The hash of the cached item for PhotoDNA if it is a picture. Otherwise, this column is empty.

Additional Information

Chrome Cookies

Description	Chrome Cookies contains cookies that Chrome downloads from the Inter-

	net. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	The domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Chrome Current Session

Description	Chrome Current Session contains information about the browser session that's currently underway.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Current Tabs

Description	Chrome Current Tabs contains information about the tabs that are open in the current browser session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.

Additional Information

Chrome Downloads

Description	Android Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the file that was downloaded.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the download began.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the download ended.
Saved To	The local path where the file was downloaded.
State	The state of the downloaded file.
Opened	Whether or not the download was opened by the user.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Chrome Extensions

Description	Chrome Extensions contains information about the extensions that a user has installed on their computer.
Recovery method	Parsing

Attribute	Description
Application Name	The name of the Chrome plugin or extension.
Version	The version number of the plugin or extension.
Description	The description of the plugin or extension.
Install Date/Time - UTC (yyyy-mm-dd)	The install time in the Chrome/Webkit time.
State	The state of the plugin or extension on the google account (Enabled or Disabled).
Permissions	The list of permissions that the plugin or extension has, as recorded in the 'manifest.json' file.
Active Permissions	The list of active permissions that the plugin or extension has, as recorded in the 'Preferences' file.
Granted Permissions	The list of all granted permissions that the plugin or extension has, as recorded in the 'Preferences' file.
Withholding Permissions	States whether the permissions are being withheld, as recorded in the 'Preferences' file.
Installed by OEM	States whether the plugin or extension is installed by OEM (True

Attribute	Description
	or False).
Installed by Default	States whether the plugin or extension is installed by default (True or False).
From Bookmark	States whether the plugin or extension was installed from a bookmark (True or False).
From Webstore	States whether the plugin or extension was installed from the chrome webstore (True or False).
Author	The author.
Homepage	The homepage.

Additional Information

Chrome FavIcons

Description	Chrome FavIcons contains the favicons that Chrome displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite or bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Icon URL	The icon URL of the favicon.

Attribute	Description
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.
Icon	A preview of the favicon.

Additional Information

Chrome History Index

Description	Chrome History Index contains an index of the webpages the user has visited in the past.
Recovery method	Parsing

Attribute	Description
Page URL	The URL of the webpage.
Title	The title of the webpage.
Visited On Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was visited.
Body	A snippet of the webpage.

Additional Information

Chrome Keyword Search Terms

Description	Chrome Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Chrome Last Session

Description	Chrome Last Session contains information about the previous browser session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Last Tabs

Description	Chrome Last Tabs contains information about the tabs that were open during the previous session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.

Attribute	Description
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Chrome Logins

Description	Android Chrome Logins contains login information that a user provides in Chrome. Passwords are often encrypted, so you might not be able to recover them unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username of the login.
Password	The password of the login.
GUID	The GUID of the login found in the keychain.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the login was created.
Last Login Date/Time - UTC	The date and time when the login was last used successfully. If the login is unsuccessful for the page or account, this date and time will

Attribute	Description
(yyyy-mm-dd)	not be updated.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the login was last modified.
URL	The URL of the login page.

Additional Information

Chrome Media History

Description	Chrome Media History contains information about media that a user viewed.
Recovery method	Parsing

Attribute	Description
URL	The URL of the media page.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the media.
Played Seconds	The duration of the media file that has been played, in seconds.

Attribute	Description
Media Duration	The full duration of the media file, in seconds.
Current Position	The position in the video when the user stopped watching, in seconds.
Origin Link	The root URL of the media that was viewed.
Thumbnail URL	The thumbnail URL of the media that was viewed.

Additional Information

Chrome Saved Credit Cards

Description	Android Chrome Saved Credit Cards contains the credit card information saved by the user.
Recovery method	Parsing

Attribute	Description
Name On Card	The name of the person on the credit card.
Card Number	The number on the credit card.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the information was last modified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the card was last used.

Attribute	Description
GUID	The GUID of the user.
Expiry Date	The date the credit card is supposed to expire in month-year format.

Additional Information

Chrome Shortcuts

Description	Chrome Shortcuts contains all of the shortcuts used by Google Chrome for user entered URLs.
Recovery method	Parsing

Attribute	Description
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - UTC (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the webpage.

Attribute	Description
Times Used	The number of times that the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is link.
Type	The type of shortcut, such as typed url or bookmark.

Additional Information
To learn more about the Transition Type fragment, sign in to the Support Portal to read the article Google Chrome transition types.

Chrome Sync Accounts

Description	Chrome Sync Accounts contains information about the Chrome accounts that a user has logged in with. Chrome syncs data to the cloud so that a user can log in on multiple devices.
Recovery method	Parsing

Attribute	Description
Sync Id	The unique ID for the account that's used to sync data to the cloud.
Account Name	The name of the sync account.
Google Account	The GAIA ID of the sync account.

Attribute	Description
Last Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the sync account was synced.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the sync account was created.
Profile Picture URL	The profile picture URL of the sync account.
Active	Indicates whether or not the sync account is active.

Additional Information

Chrome Sync Data

Description	Chrome Sync Data contains information about the data that Chrome has synced to a user's account in the cloud.
Recovery method	Parsing and carving

Attribute	Description
Name	The name of the sync key.
Local Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the local system.
Server Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the server.
Local Created Date/Time - UTC	The created time of the value on the local system.

Attribute	Description
(yyyy-mm-dd)	
Server Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the server.
Type	The type of data that is synced (bookmark, favicon, type URL, and so on).
Parsed Content	The type of parsed data.
Favicon Image	The actual favicon image.

Additional Information

Chrome Tab History

Description	Chrome Tab History contains a history of websites that the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.

Attribute	Description
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the webpage (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Search Term	The value that the user entered into a search.

Additional Information

Chrome Top Sites

Description	Android Chrome Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the site.
Last Updated	The date and time when the site was last updated.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	
Title	The title of the site.
Rank	The rank of the website, where the rank is based on how frequently the website was visited. A value of 1 indicates the most frequent and values increment to 8 as frequency decreases. A value of -1 indicates a site that the user manually added to the list of top sites.
Thumbnail	The thumbnail of the site.

Additional Information

Chrome Web History

Description	Chrome Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.

Attribute	Description
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Chrome Web Visits

Description	Android Chrome Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition

Attribute	Description
	type is link.
Visit Source	The source of the visit.

Additional Information
To learn more about the Transition Type fragment, sign in to the Support Portal to read the article Google Chrome transition types.

Dolphin Browser Bookmarks

Description	Dolphin Browser Bookmarks contains bookmarks from the Dolphin web browser on an Android device.
Recovery method	Parsing

Attribute	Description
Title	The title of the bookmark.
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was modified.
Visits	The number of times that the user visited this bookmark.

Additional Information

The Modified Date/Time field is always empty for Android.

Dolphin Browser History

Description	Dolphin Browser History contains the webpage history from the Dolphin web browser on an Android device.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the webpage.
URL	The URL of the webpage.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the user first visited the webpage.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the user last visited the webpage.
Visits	The number of times that the user has visited the webpage.

Additional Information

DuckDuckGo Bookmarks

Description	DuckDuckGo Bookmarks contains information about the webpages that a user has bookmarked.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Name	The name of the bookmark.
Favorite	Indicates whether the link was added as a favorite. This value is not currently populated for Android.

Additional Information

DuckDuckGo Cookies

Description	DuckDuckGo Cookies contains cookies that DuckDuckGo downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

DuckDuckGo Current Tabs

Description	DuckDuckGo Current Tabs contains information about the tabs that are open in the current browser session.
Recovery method	Parsing

Attribute	Description
URL	The URL of the webpage.

Attribute	Description
Title	The title of the webpage.
Was Viewed	Whether the tab was viewed on the local device or not.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that URL was accessed.
Attachment Path	If a snapshot was saved for that tab, this fragment stores the path of the snapshot image file.
Attachment	If a snapshot was saved for that tab, this is the attachment.

Additional Information

DuckDuckGo Whitelisted Websites

Description	DuckDuckGo Whitelisted Websites contains information about domains that are trusted or protected from deletion by the user.
Recovery method	Parsing

Attribute	Description
Domain	The domain of the website.
Status	Whether the domain was whitelisted or fire proofed. Whitelisted indicates to DuckDuckGo that the domain should always be trusted. Fire proofed domains will keep the navigation data even if the user clicks the option 'Clear All Tabs and Data'.

Additional Information

Ecosia Autofill

Description	Ecosia Autofill contains records of the autofill values that Ecosia saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The count of the autofill.

Additional Information

Ecosia Bookmarks

Description	Ecosia Bookmarks contain browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Ecosia Cookies

Description	Ecosia Cookies contains cookies that Ecosia downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	The domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-	The date and time when the cookie was created.

Attribute	Description
dd)	
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Ecosia Downloads

Description	Ecosia Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Saved To	The absolute path on the device to the downloaded file.

Attribute	Description
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Ecosia FavIcons

Description	Ecosia Favicons contains the favicons that Ecosia displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time when the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Ecosia Keyword Search Terms

Description	Ecosia Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Additional Information

Ecosia Logins

Description	Ecosia Logins contains login information that a user provides in Ecosia. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the data was created.
URL	The URL of the login page.

Additional Information

Ecosia Tab History

Description	Ecosia Tab History contains a history of websites that the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the webpage (for example, the referrer source might be from Google or

Attribute	Description
	another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Search Term	The value that the user entered into a search.

Additional Information

Ecosia Top Sites

Description	Ecosia Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the site.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Additional Information

Ecosia Web History

Description	Ecosia Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Ecosia Web Visits

Description	Ecosia Web Visits contains a history of the websites that the user visits (includes all visits).

Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

Edge Archived Keyword Search Terms

Description	Edge Archived Keyword Search Terms contains keyword search terms that were archived by the browser.
Recovery method	Parsing and carving

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Edge Cache Data

Description	Edge Cache Data contains information about cached data that was saved during browsing.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
URL	The URL of the cached data source.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when cached data was saved on the machine.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when cached data was modified on the source side.

Attribute	Description
File Type	The file type.
Visit Count	The number of times that the current cached file was accessed.
Content Size (Bytes)	The size of the cached file in bytes.
Image	The content of the file as an image, if the file is a supported image type.
File	The content of the file in raw bytes.
Original Path	The original absolute path to the cached file stored in the database.
Relative Path	A relative path to the file based on the location of the WebCache database. Doesn't exist is displayed if the file is not found.

Additional Information

This artifact allows an investigator to see the content a user views, it's origin, and how often the content is reused by the browser. By clearing the cache, the user can effectively delete these records. In some cases, records do not get deleted from the database, but in cases where the files are deleted, the original files cannot be restored.

Edge Chromium Bookmarks

Description	Browser bookmarks that reference saved webpages.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Edge Chromium FavIcons

Description	Contains the favicons that Chrome displays in the address bar for the web-site that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing and carving

Attribute	Description
Page URL	The page URL of the favicon.
Updated Date/Time - UTC (yyyy-mm-dd)	The last time the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Edge Chromium Keyword Search Terms

Description	Information about the keyword search terms that a user enters.
Recovery method	Parsing and carving

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Edge Chromium Tab History

Description	A history of websites the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing and carving

Attribute	Description
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.

Attribute	Description
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the web page (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Search Term	The value the user entered into a search.

Additional Information

Edge Chromium Web History

Description	A history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.

Attribute	Description
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Edge Chromium Web Visits

Description	A history of the websites that the user visits (includes all visits).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

Edge Extensions

Description	Edge Extensions contains information about the extensions or plugins installed in the user's Edge browser.
Recovery method	Parsing and carving

Attribute	Description
Package Name	The package name for the extension.
Application Name	The name of the extension.
Version Number	The most recent version number of the extension.
Created Date/Time - UTC (yyyy-mm-dd)	The time when this extension was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent time that the AppxManifest file for the extension was accessed (most likely the same as created time).
Last Modified Date/Time - UTC (yyyy-mm-dd)	The most recent time when the extension was updated.

Additional Information

Deleted and removed extensions can't be acquired, as all of this data is fully deleted from the browser when the user deletes an extension.

Edge Favorites

Description	Edge Favorites contains information about the websites a user favorites while browsing.
Recovery method	Parsing and carving

Attribute	Description
Favorite Name	The name given to the favorite.
Is Folder	Indicates whether the item is a folder or a URL for a website. This value is Yes if the item is a folder, and No if the item is a URL.
URL	The URL of the favorite.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the favorite was last modified.
Favicon URL	The URL of the favicon for the website.

Additional Information

This artifact allows an investigator to see the content a user views, it's origin, and how often the content is reused by the browser. By clearing the cache, the user can effectively delete these records. In some cases, records do not get deleted from the database, but in cases where the files are deleted, the original files cannot be restored.

Edge Keyword Search Terms

Description	Edge Keyword Search Terms contains information about the keyword

	search terms that a user enters.
Recovery method	Parsing and carving

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Edge Last Session

Description	Edge Last Session contains information about the last snapshot Edge took of the user's browsing session.
Recovery method	Parsing and carving

Attribute	Description
Page URL	The URL of the webpage.
Page Title	The title of the webpage.

Attribute	Description
Image	The browser generated snapshot of the page.
Body	The HTML body that was saved from the page.

Additional Information
At certain time intervals, Edge takes a snapshot of the user's browsing session. Using this artifact, an investigator is able to see exactly what the user was looking at, at the time of snapshot. The time interval between snapshots is unknown. Due to the interval, it's possible for a tab to be opened and closed quick enough that the tab isn't included in a snapshot.

Edge Reading Lists

Description	Edge Reading Lists contains collections of websites that the user has saved for offline viewing.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the Reading List page.
URL	The URL of the Reading List page.
Source Address	Other source information for the Reading List page.
Picture Path	A file path to pictures associated with the Reading List page.
Deleted	Indicates whether the user has deleted the Reading

Attribute	Description
	List page.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the Reading List page was added.
Last Access Date/Time - UTC (yyyy-mm-dd)	The date and time when the Reading List page was last accessed.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the Reading List page was updated.

Additional Information

Edge Top Sites

Description	Edge Top Sites lists the websites that the user visits frequently in the Edge browser. Top Sites can also be removed or added by the user.
Recovery method	Parsing and carving

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the page was added as a top site.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the top site was updated.
Favicon URL	The URL of the favicon for the top site.

Attribute	Description
Title	The title of the top site.
URL	The URL of the top site.

Additional Information

Edge/Internet Explorer 10-11 Content

Description	Edge/Internet Explorer 10-11 Content contains content that the browser caches, including webpages, pictures, and other resources.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
URL	The URL of the cache record.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.
Last Modified by Web Server Date/Time - UTC (yyyy-mm-dd)	The last time that the content was modified on the web server. This time is reflective of when the website created the content on the page and can be before the system being examined was built.
Creation Date/Time	The date and time that the content was created on the local system.

Attribute	Description
- UTC (yyyy-mm-dd)	
Access Count	The number of times that the content was accessed through the web browser.
Filename	The filename of the cached content.
File Size (Bytes)	The size of the cache file.
Image	If the content is an image, it will be displayed here.
Content	If the file is not an image, such as a javascript file, the raw bytes will be stored here.

Additional Information

Edge/Internet Explorer 10-11 Cookies

Description	Edge/Internet Explorer 10-11 Cookies contains site usage information that websites send to the browser when a user visits their sites.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
User	The local user on the system.
URL	The URL that the cookie is for.

Attribute	Description
Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.
Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time that the cookie was updated by the website at the URL visited.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Access Count	The number of times that the cookie was accessed.
Filename	The filename of the cookie.
File Size (Bytes)	The size of the cookie.

Additional Information

Edge/Internet Explorer 10-11 Daily/Weekly History

Description	Edge/Internet Explorer 10-11 Daily/Weekly History contains websites that a user visits using Internet Explorer, which are recovered from the daily/weekly history.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
URL	The URL that was accessed by the user.

Attribute	Description
User	The local user on the system.
Accessed Date/Time - Local (yyyy-mm-dd)	The most recent visit to the URL.
Access Count	The number of times that the website was accessed.
Browser Source	The directory of the browser from where the history is extracted from.

Additional Information
At the end of the week, all the daily .dat records are bundled into a weekly history and a new daily .dat file is created. This table represents a good secondary source for evidence if the main history is missing details or records.

Edge/Internet Explorer 10-11 Dependency Entries

Description	Edge/Internet Explorer 10-11 Dependency Entries contains a history of the websites that the browser is required to load in order to render a page.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
URL	The URL visited by the user.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.

Additional Information

Records for this artifact are similar to the main history, the difference being that this artifact also includes dependencies for viewed websites (for example, if a viewed website contains pictures stored on another website).

Edge/Internet Explorer 10-11 Downloads

Description	Edge/Internet Explorer 10-11 Downloads contains information about the files that a user downloads using the browser.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
URL	The URL of the downloaded file.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last time that the user accessed the downloaded URL.
Redirect URL	The previous URL that led the user to the downloaded URL.
Download Location	The local path where the file was saved.
Temporary Download Location	The local path where the file was saved temporarily (usually while downloading).

Additional Information

Internet Explorer 9 introduced a new integrated download manager which stores the details of downloaded files in a new download INDEX.DAT file. This file has a different structure to the standard INDEX.DAT files.

Edge/Internet Explorer 10-11 Main History

Description	Edge/Internet Explorer 10-11 Main History contain records of the websites that a user visits using Internet Explorer, which are recovered from the main history.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
URL	The URL that was accessed by the user.
User	The local user on the system.
Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.
Page Title	The title of the webpage.
Access Count	The number of times that the website was accessed.
Browser Source	The directory of the browser from where the history is extracted from.

Additional Information

The access count does not always accurately represent the real access count. These values should only be used as an estimate.

Firefox Add-ons

Description	Firefox Add-ons contains the add-ons from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
Name	The name of the add-on.
Version	The version the add-on.
Install Date/Time - UTC (yyyy-mm-dd)	The date and time when the add-on was installed.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the add-on was updated.
Extension Enabled	Indicates whether the add-on is enabled by the user.
Description	The description of the add-on.

Additional Information

Firefox Bookmarks

Description	Firefox Bookmarks contains the bookmarks from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
URL	The URL of the website that was bookmarked.
Added Date/Time - UTC (yyyy-MM-dd)	The date and time that the bookmark was created.
Last Modified Date/Time - UTC (yyyy-MM-dd)	The date and time that the field was last modified.
Title	The title of the bookmark.
Bookmark Type	The type of bookmark (Bookmark Item or Bookmark Folder).

Additional Information

Firefox Cache Records

Description	Firefox Cache Records contains the files that the Firefox web browser has cached on a device.
Recovery method	Parsing

Attribute	Description
URL	The URL of file that was cached.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cache file was created.
MIME Type	The MIME type of the file.
Content Size (Bytes)	The size of the cached file.
Image	A preview of the cached file, if the cached file is anything but a picture.
Content	The content of the cached file.

Additional Information

Firefox Cookies

Description	Firefox Cookies contains the cookies from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
Host	The host domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.

Attribute	Description
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie will expire, if it is set to expire.
Path	The path to the cookie.

Additional Information

Firefox Downloads

Description	Firefox Downloads contains the downloads from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file being downloaded.
Download Source	The URL of the file being downloaded.
Start Date/Time - UTC (yyyy-MM-dd)	The date and time when the download was started.
End Date/Time -	The date and time when the download was ended.

Attribute	Description
UTC (yyyy-MM-dd)	
Saved To	The path to where the file was downloaded to.
Temp Path	The path to where the file was saved during downloading.
State	The state of the download can be Download In Progress, Download Complete, Download Stopped, or Download Paused.
Referrer	If the webpage used a mirror for downloading, this value is the path to the original download URL.

Additional Information

Firefox FavIcons

Description	Firefox FavIcons contains the favicons from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
URL	The URL of the icon.

Additional Information

Firefox FormHistory

Description	Firefox FormHistory contains the form history from the Firefox web browser on a device.
Recovery method	Parsing and carving

Attribute	Description
Field Name	The name of the field.
Value	The value of the field.
First Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the field was first used.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the field was last used.
Times Used	The number of times that the field was used.
ID	The unique ID of the field.

Additional Information

Firefox Input History

Description	Firefox Input History contains the input to forms from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
URL	The URL that the input was given to.
Input	The value that was given.
Use Count	The number of times that the input has been used.
ID	The unique ID of the input.

Additional Information

Firefox Logins

Description	Firefox Logins contains login information for websites that a user logs in to using the browser.
Recovery method	Parsing

Attribute	Description
URL	The URL of the login page.
Username	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the data was created.

Additional Information

Firefox Private Browsing History

Description	Firefox Private Browsing History contains the URLs that were loaded during a Private Browsing session from the Firefox web browser on a device.
Recovery method	Carving

Attribute	Description
URL	The URL.

Additional Information

Firefox SessionStore Artifacts

Description	Firefox SessionStore Artifacts contains the webpages from the last active session from the Firefox web browser on a device.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the webpage.
URL	The URL of the webpage.
Referrer URL	The URL of the webpage, if the webpage was a redirect.

Additional Information

Firefox Web History

Description	Firefox Web History contains the webpages from the last active session from the Firefox web browser on a device.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage.
Visit Count	The number of times that the webpage has been visited.
Typed	Indicates whether the user typed the URL (Yes or No).

Additional Information

Firefox Web Visits

Description	Firefox Web Visits contains all of the non-archived URL visits for Firefox.
Recovery method	Parsing

Attribute	Description
URL	The URL that was visited.
Title	The title of the page that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the page was visited.
Typed	Indicates whether the user typed the URL (Yes or No).
Transition Type	Identifies how the transition to the page happened.

Additional Information

Flash Cookies

Description	This artifact has been deprecated and is no longer supported in AXIOM. Flash cookies are Internet browser cookies that are saved when a user watches a flash video (e.g. YouTube).
Recovery method	Carving

Attribute	Description
Cookie Name	The name of the cookie.
Content	The flash content of the cookie. This content is essentially serialized

Attribute	Description
	ActionScript code. Primitive values such as integers and strings are shown, as well as more complicated data structures such as objects and arrays. A complex data structure's value is shown only once, along with an "object ID" that gets generated. For all subsequent references to that structure in the content, it's referred to by the generated object ID.
Domain	The domain or host that created the cookie.
Source	The location of where the artifact was found
Located At	The File Offset/Physical Offset/Table name of where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Google Analytics First Visit Cookies

Description	Google Analytics First Visit Cookies contains information about Google Analytics first-visit cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Host	Contains the domain of the URL.

Attribute	Description
Creation DateTime	The date and time when the site was first visited.
Most Recent Visit Date/Time	The date and time of most recent session.
2nd Most Recent Visit Date/Time	The date and time of previous session.
Hits	The number of visits.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics First Visit Cookies Carved

Description	Google Analytics First Visit Cookies Carved contains information about Google Analytics first-visit cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	Contains the domain of the URL.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Most Recent Visit Date/Time - UTC (yyyy-mm-dd)	The date and time of the most recent session.

Attribute	Description
2nd Most Recent Visit Date/Time - UTC (yyyy-mm-dd)	The date and time of the second most recent session.
Hits	The number of visits.

Additional Information

Google Analytics Referral Cookies

Description	Google Analytics Referral Cookies contains information about Google Analytics referral cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Cookie Source	The source URL used to reach the site.
Host	Contains the domain of the URL.
Update Date/Time	The last time the cookie was updated.
Campaign	The method of referral.
Access Method	Indicates whether the site was accessed organically or was referred.
Keyword	The keywords used to arrive at the site.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics Referral Cookies Carved

Description	Google Analytics Referral Cookies Carved contains information about Google Analytics referral cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	Contains the domain of the URL.
Last Update Date/Time - UTC (yyyy-mm-dd)	The last time the cookie was updated.
Cookie Source	The source URL used to reach the site.
Access Method	Indicates whether the site was accessed organically or was referred.
Campaign	The method of referral.
Keyword	The keywords used to arrive at the site.
Path to Page	

Additional Information

Google Analytics Session Cookies

Description	Google Analytics Session Cookies contains information about Google Analytics session cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Host	Contains the domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start time of the current sesion.
Outbound Link Events Left	
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics Session Cookies Carved

Description	Google Analytics Session Cookies Carved contains information about Google Analytics session cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	Contains the domain of the URL.
Start Current Session Date/Time	The start date and time of the current sesion.
Page Views	The number of visits to this page from the user.
Outbound Link Events Left	

Additional Information

Google Analytics URLs

Description	Google Analytics URLs contains URLs that are discovered in other artifacts that are related to Google Analytics.
Recovery method	Carving

Attribute	Description
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	Contains the domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.

Attribute	Description
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics URLs Carved

Description	Google Analytics URLs Carved contains information about Google Analytics URLs that are recovered using carving.
Recovery method	Carving

Attribute	Description
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all of the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	Contains the domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.

Attribute	Description
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.

Additional Information

Google Toolbar

Description	The Google toolbar is a browser add-on where a user can perform Google searches. While there are many different features to the Google Toolbar, search history is the focus. Search history can be either typed or done by autocomplete. It's also possible to determine where the user's search comes from, whether it is Google Search, YouTube, Google Maps, Google News, etc.
Recovery method	Parsing

Attribute	Description
Search	The keyword that was searched for.
Search Type	The type of Google search that the user completed (pictures, web, etc.).

Additional Information

Internet Explorer Cache Records

Description	Internet Explorer Cache Records contains temporary Internet files that are written locally when the user views pages from the Internet.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the cache record.
User	The local user.
Last Modified by Web Server Date/Time - UTC (yyyy-mm-dd)	The last time that the content was modified on the web server. This time is reflective of when the website created the content on the page, and this can be from before the system being examined was built.
Last Checked by Local Host Date/Time - UTC (yyyy-mm-dd)	The date and time that the content was checked for recency on the local system.
Cache Retrieval Count	The number of times that the cache record was requested by the browser.
Filename	The name of the file.
File Type	The filename of the cached content.
Content Size (Bytes)	The size of the cached file.

Attribute	Description
Image	If the content file is an image, it will be displayed here.
Content	If the file is not an image, such as a JavaScript file, the raw bytes will be stored here.

Additional Information

Internet Explorer Cookie Records

Description	Internet Explorer Cookie Records contains site usage information that web-sites send to the browser when a user visits their sites.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that created the cookie.
User	The user of the system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL was accessed.
Last Modified by Web Server Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL record was modified.
Visit Count	The number of times that the URL was vis-ited.
Web Page Title	The title of the webpage.
File Name	The name of the cookie file.

Additional Information

Internet Explorer Cookies

Description	Internet Explorer Cookies contains site usage information that websites send to the browser when a user visits their sites.
Recovery method	Parsing

Attribute	Description
Host	The host that created the cookie.
Name	The name of the cookie.
Value	The cookie value.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Flags	The flags associated with the cookie.

Additional Information

Internet Explorer Downloads

Description	Internet Explorer Downloads contains information about the files that a

	user downloads using the browser.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL for the file download.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was downloaded.
Status	The download status.
Saved To	The local path where the file was saved.
Referrer URL	The previous URL that led the user to the download URL.
File Size (Bytes)	The size of the file in bytes.
Source IP	The IP address of the download URL.

Additional Information

Internet Explorer Favorites

Description	Internet Explorer Favorites contains webpages that the user has set as a favorite.
Recovery method	Parsing and carving

Attribute	Description
Favorite Name	The name of the favorite as it shows up in Internet Explorer.
URL	The URL of the favorite.
Modified Date/Time - UTC (yyyy-mm-dd)	The last time that the user modified the favorite.
User	The user to whom the favourite belongs.
Favorites Root Location	The local path that is the root storage point for the favorite.
Folder Structure	The folder structure under which the favorite will show up in Internet Explorer.
Icon URL	The URL of the icon for the favorite if an icon does exist.

Additional Information

Internet Explorer InPrivate/Recovery URLs

Description	Internet Explorer InPrivate/Recovery URLs contains URLs visited during InPrivate browsing that are saved in Internet Explorer recovery files (used to recover tabs in the event of a crash).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that was visited.
File Create Date/Time - UTC (yyyy-mm-dd)	The date and time that the Internet record was created.
Description	The title of the website.
Local MAC address	The MAC address of the local machine.

Additional Information

Internet Explorer Leak Records

Description	Internet Explorer Leak Records contains browser history records that are scheduled for deletion.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL visited.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL record was modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL was accessed.
Visit Count	The number of times that the URL was visited.

Additional Information

LEAK artifacts are created when an error occurs while the system attempts to delete a record and the Temporary Internet File is unavailable for some reason.

Internet Explorer Main History

Description	Internet Explorer Main History contains websites that a user visits using Internet Explorer, which are recovered from the main history.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that was visited.
User	The local user.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Last visited (2nd Timestamp) Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Web Page Title	The webpage title.

Additional Information

Internet Explorer PrivacIE Records

Description	Internet Explorer PrivacIE Records contains websites that a user visits while having the privacy settings turned on.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL visited.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL record was modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last date and time that the URL was accessed.
Visit Count	The number of times that the URL was visited.

Additional Information

Internet Explorer Typed URLs

Description	Internet Explorer Typed URLs contains URLs that the user types directly into the address bar for Internet Explorer.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that was typed into the address bar.
Last Entered Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last typed.

Additional Information
This includes data that a user pastes into the address bar, as well as instances when a user starts typing in the address bar and clicks on a suggestion from the browser. You may also see local paths and network locations here when the user types a location in Windows Explorer.

Internet Explorer Weekly History

Description	Internet Explorer Weekly History contains websites that a user visits using Internet Explorer, which are recovered from the weekly history.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that was visited.
User	The local user.
Last Visited Date/Time (local time) (yyyy-mm-dd)	The date and time that the URL was last visited. This date is local to the machine that visited the website.
Weekly History File Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the weekly history file was created.

Attribute	Description
Visit Count	The number of times that the user accessed the URL.
Web Page Title	The webpage title.

Additional Information
At the end of the week, all the daily .dat records are bundled into a weekly history and a new daily .dat file is created. This table represents a good secondary source for evidence if the main history is missing details or records.

Iron Browser Autofill

Description	Iron Browser Autofill contains records of the autofill values that Iron Browser saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Iron Browser Bookmarks

Description	Iron Browser Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Iron Browser Cookies

Description	Iron Browser Cookies contains cookies that Iron Browser downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Iron Browser Downloads

Description	Iron Browser Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.

Attribute	Description
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the downloaded was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the downloaded finished.
Saved To	The absolute path on the device to the file downloaded.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Iron Browser FavIcons

Description	Iron Browser Favicons contains the favicons that Iron Browser displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Iron Browser Keyword Search Terms

Description	Iron Browser Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Additional Information

Iron Browser Logins

Description	Iron Browser Logins contains login information that a user provides in Iron Browser. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the data was created.
URL	The URL of the login page.

Additional Information

Iron Browser Tab History

Description	Iron Browser Tab History contains a history of websites that the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the webpage (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Search Term	The value that the user entered into a search.

Additional Information

Iron Browser Top Sites

Description	Iron Browser Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Additional Information

Iron Browser Web History

Description	Iron Browser Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Iron Browser Web Visits

Description	Iron Browser Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

Kiwi Browser Autofill

Description	Kiwi Browser Autofill contains records of the autofill values that Kiwi Browser saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Kiwi Browser Bookmarks

Description	Kiwi Browser Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Kiwi Browser Cookies

Description	Kiwi Browser Cookies contains cookies that Kiwi Browser downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Kiwi Browser Downloads

Description	Kiwi Browser Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the downloaded was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the downloaded finished.
Saved To	The absolute path on the device to the file down-

Attribute	Description
	loaded.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Kiwi Browser FavIcons

Description	Kiwi Browser Favicons contains the favicons that the Kiwi Browser displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Kiwi Browser Keyword Search Terms

Description	Kiwi Browser Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Additional Information

Kiwi Browser Tab History

Description	Kiwi Browser Tab History a history of websites the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the web page (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Search Term	The value the user entered into a search.

Additional Information

Kiwi Browser Top Sites

Description	Kiwi Browser Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Additional Information

Kiwi Browser Web History

Description	Kiwi Browser Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Kiwi Browser Web Visits

Description	Kiwi Browser Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

Lunascape Autofill

Description	Lunascape Autofill contains records of the autofill values that Lunascape saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was last used.
Value	The saved autofill value for this type of field.
Count	The number of times that the autofill has been applied.

Additional Information

Lunascape Bookmarks

Description	Lunascape Bookmarks contains the webpages that a user has bookmarked.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Title	The name of the bookmark.

Additional Information

Lunascape Cookies

Description	Lunascape Cookies contains information about the cookies that the browser downloaded from the websites that the user has visited.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.

Attribute	Description
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Lunascape History

Description	Lunascape History contains information about the websites that the user visits.
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.

Additional Information

Magnet Web Page Saver Captured HTML

Description	This table contains information on the HTML of a webpage captured by Magnet Web Page Saver.
Recovery method	Parsing

Attribute	Description
URL	The URL of the captured webpage.
Web Page Title	The title of the webpage.
Captured Date/Time	The date and time when the webpage was captured.
MD5 Hash	The MD5 hash of the captured HTML body.
HTML Source	The HTML source of the captured webpage.

Additional Information

Magnet Web Page Saver Captured Media

Description	This table contains information on the media of a webpage captured by Magnet Web Page Saver.
Recovery method	Parsing

Attribute	Description
URL	The URL of the captured webpage.
Resource URL	The URL of the captured media.
Captured Date/Time	The date and time when the webpage was captured.
MD5 Hash	The MD5 hash of the captured media.

Additional Information

Magnet Web Page Saver Captured Webpage

Description	This table contains information on the screenshots of a webpage collected by Magnet Web Page Saver.
Recovery method	Parsing

Attribute	Description
URL	The URL of the captured webpage.
Web Page Title	The title of the webpage.
Captured Date/Time	The date and time when the webpage was captured.
MD5 Hash	The MD5 hash of the screenshot of the captured webpage.

Additional Information

Malware/Phishing URLs

Description	Malware/Phishing URLs contains records that are believed to be either malware or phishing related URLs.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the website.
URL	The URL of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time this is associated with the artifact.
Artifact	The name of the artifact that the URL belongs to.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Mi Browser Autofill

Description	Mi Browser Autofill contains records of the autofill values that Mi Browser saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Mi Browser Bookmarks

Description	Mi Browser Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was created.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Mi Browser Cookies

Description	Mi Browser Cookies contains cookies that Mi Browser downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	The domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Mi Browser Downloads

Description	Mi Browser Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the file that was downloaded.
Downloaded Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was downloaded.
Saved To	The absolute path on the device to the downloaded file.
File Size (Bytes)	The file size of the download.

Additional Information

Mi Browser History

Description	Mi Browser History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.

Additional Information

Mint Browser Bookmarks

Description	Mint Browser Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was created.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Mint Browser Cookies

Description	Mint Browser Cookies contains cookies that Mint Browser downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	The domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Mint Browser Downloads

Description	Mint Browser Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the file that was downloaded.
Downloaded Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was downloaded.
Saved To	The absolute path on the device to the downloaded file.
File Size (Bytes)	The file size of the download.

Additional Information

Mint Browser History

Description	Mint Browser History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.

Additional Information

Naver Web History

Description	Naver Web History contains a record of all the websites a user has visited using the Naver browser. This artifact tracks the first instance and last instance that a user has visited a site.
Recovery method	Parsing

Attribute	Description
Title	The title of the website that the user visited.
URL	The URL of the website that the user visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the user last visited the website.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the user first visited the website.

Additional Information

Opera Archived Keyword Search Terms

Description	Opera is a web browser developed by Opera Software, and opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Keyword Search Term	The keyword that was searched.
URL	The URL that was invoked by the search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Opera Archived Web History

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was first visited.
URL	The URL that was accessed by the user.
Title	The title of the webpage.
Visit Count	The number of times that the user accessed the URL.
Typed Count	The number of times the user has navigated to this page by typing in the address.
Transition Type	Describes how the browser navigated to a particular URL on a particular visit. For example, if a user visits a page by clicking a link on another page, the transition type is "Link".
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.

Additional Information

Opera Autofill

Description	Opera Autofill contains records of the autofill values that Opera saves for different types of text fields.
Recovery method	Parsing and carving

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Opera Autofill Profiles

Description	Opera is a web browser developed by Opera Software, and uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Name	The name of the user.
Email	The user's email.
Number	The user's phone number.
Company	The user's company.
Address Line 1	The user's address.

Attribute	Description
Address Line 2	The user's address.
City	The user's city.
State	The user's state.
Zipcode	The user's ZIP Code.
Country	The user's country.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the autofill profile was last modified.

Additional Information

Opera Bookmarks

Description	Opera Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Opera Cache Records

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that the file was downloaded from.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was first visited.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The last time that the local cache was synced with the web-server.
File Type	The type of cache file.
Content Size (Bytes)	The size of the cache file.
Image	If the content file is an image, it will be displayed here.
Content	If the file is not an image (e.g. a javascript file), the raw bytes will be stored here.

Additional Information

Opera Cookies

Description	Opera Cookies contain cookies that Opera downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing and carving

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie expires.
Path	The path of the cookie value.

Additional Information

Opera Current Session

Description	Opera is a web browser developed by Opera Software, and Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating

	systems.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect, if applicable.

Additional Information

Opera Current Tabs

Description	Opera is a web browser developed by Opera Software, and Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect, if applicable.

Additional Information

Opera Downloads

Description	Opera Downloads includes information about the files that a user downloads from the Internet.
Recovery method	Parsing and carving

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the downloaded was started.

Attribute	Description
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time that the downloaded finished.
Saved To	The absolute path on the device to the file downloaded.
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Opera FavIcons

Description	Opera Favicons contains the favicons that Opera displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing and carving

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.

Attribute	Description
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Opera History Index

Description	Opera is a web browser developed by Opera Software, and uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Page URL	The webpage URL.
Title	The title of the webpage.
Visited On Date/Time - UTC (yyyy-mm-dd)	The date and time tha the URL was last visited.
Body	The HTML body of the webpage.

Additional Information

Opera Keyword Search Terms

Description	Opera Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing and carving

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Opera Last Session

Description	Opera is a web browser developed by Opera Software, and uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect, if applicable.

Additional Information

Opera Last Tabs

Description	Opera is a web browser developed by Opera Software, and uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.

Attribute	Description
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL used to redirect, if applicable.

Additional Information

Opera Logins

Description	Opera is a web browser developed by Opera Software, and uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL the autofill was extracted from.
User Name	The username to be auto-populated.
Password	The password that was remembered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the autofill was saved.

Additional Information

Opera Media History

Description	Opera Media History contains information about media that a user viewed.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the media page.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the media.
Played Seconds	The duration of the media file that has been played, in seconds.
Media Duration	The full duration of the media file, in seconds.
Current Position	The position in the video that the user stopped watching, in seconds.
Origin Link	The root URL of the media that was viewed.
Thumbnail URL	The thumbnail URL of the media that was viewed.

Additional Information

Opera Saved Credit Cards

Description	Opera is a web browser developed by Opera Software, and uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
GUID	A unique identifier for the credit card.
Name On Card	The name on the credit card.
Expiry Date	The date the credit card is supposed to expire in format 'month-year'.
Card Number	The credit card number.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that the credit card information was modified.

Additional Information

Opera Search Field History

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Search Entries	The term that was searched for.

Additional Information

Opera Shortcuts

Description	Opera Shortcuts contains all of the shortcuts used by Opera for user entered URLs.
Recovery method	Parsing and carving

Attribute	Description
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - (UTC) (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the webpage.
Times Used	The number of times that the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition

Attribute	Description
	type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

Additional Information

Opera Top Sites

Description	Opera Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Additional Information

Opera Typed History

Description	Opera is a web browser developed by Opera Software. Web history are recently visited webpages. Opera stores a user's browsing history so that he or she can view it later. This search carves and parses web history from the Opera web browser, including the typed history (i.e. URLs or search terms entered by the user). The entire history file is not required; single records can be carved from live RAM captures and unallocated clusters, and so on.
Recovery method	Parsing and carving

Attribute	Description
Last Typed Date/Time - UTC (yyyy-mm-dd)	The last date and time that the content was typed.
Typed URL/Data	The content that was typed. This could be a URL or other data.
Type	The type of content that was typed (e.g. URL).

Additional Information

Opera Web History

Description	Opera Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Opera Web Visits

Description	Opera Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the webpage was last visited.

Attribute	Description
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Indicates how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is link.
Visit Source	The source of the visit.

Additional Information

Pornography URLs

Description	Pornography URLs contains records of what are believed to be pornography related URLs.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the website.
URL	The URL of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact that the URL belongs to.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

You can find a list of the domains that are supported by this refined result at Pornography URLs.

Potential Browser Activity

Description	The Browser Activity artifact will recover browser-related URLs. This includes Chrome Incognito and Firefox Private Browsing URLs, HTTP request artifacts from multiple browsers, and regular web browsing artifacts. This does not include metadata such as the Windows username, dates/times, and so on. Note that some recovered URLs can be from background browser processes related to certificate authorities, etc.
Recovery method	Carving

Attribute	Description
URL	The URL that the request was sent to.
User Agent	The string that represents the browser that sent the request.

Additional Information

Puffin Browser Bookmarks

Description	Contains bookmarks from the Puffin Browser for Android.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the bookmark.
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was added.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the user last visited the web page.
Visits	The number of times the user visited this bookmark.

Additional Information

Puffin Browser History

Description	Contains the web history for the Puffin Browser for Android.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the web page.
URL	The URL of the web page.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time the user last visited the web page.
Last Accessed Date/Time - Local Time (yyyy-mm-dd)	The date and time the user last visited the web page.

Attribute	Description
Visits	The number of times the user has visited that web page.

Additional Information
Last Accessed Date/Time - Local Time is always empty for Android Puffin Browser History Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Rebuilt Webpages

Description	Rebuilt Webpages contains the data that allows for the reconstruction of webpages.
Recovery method	Not applicable

Attribute	Description
Page Title	The title.
URL	The URL.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the original record was created.
Domain	The domain.
Cache Table	The table that the data to re-construct the page came from.
Cache RowID	The row ID in the table that constructed the rebuilt webpage.

Additional Information

Safari Bookmarks

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to webpages that have been bookmarked.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the bookmarked webpage.
Title	The title of the bookmarked webpage.
Type	The type of bookmark (for example, Bookmark, Favorite, and Folder)
Read	No data is populated for this fragment on Windows.
Added Date/Time - UTC (yyyy-mm-dd)	Indicates the date and time that the bookmark was added.
Last Visited Date/Time - UTC (yyyy-mm-dd)	No data is populated for this fragment on Windows.
Modified Date/Time - UTC (yyyy-mm-dd)	Indicates the date and time that the bookmark was modified.

Attribute	Description
Locally Added	Indicates whether the bookmark was created on the local device or a synced device with the same Apple ID. This data is not always available for every bookmark on Windows.

Additional Information

Safari Cache Records

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to webpages that have been cached on the local system.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL from which the file was downloaded.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cache file was created.
File Type	The type of the cached file.
Content Size	The size of the cached file.
Image	If the content file is an image, it will be displayed in this column.
Content	If the file is not an image (e.g. if it is a javascript file), the raw file content will be stored here.

Additional Information

Safari Downloads

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to files that have been downloaded from Safari.
Recovery method	Parsing and carving

Attribute	Description
Download URL	The URL of the downloaded file.
Saved to Path	The local path where the download was saved.
Download Identifier	The unique identifier for the download.
Amount Downloaded (Bytes)	The number of bytes downloaded.
Size of Download (Bytes)	The size of the download in bytes.

Additional Information

Safari History

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures history entries which have been parsed from the filesystem.

Recovery method	Parsing and carving

Attribute	Description
URL	The URL of a visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Redirect URL	The URL that the user was redirected to.
Title	The title of the webpage.
Visit Count	The number of times that the URL was visited.
Visit Source	Indicates whether the website was viewed on the local device or on a synced device.

Additional Information

Safari iCloud Devices

Description	Safari iCloud Devices contains information about the devices that are synced to an iCloud account. Each device can access any browser tabs that are synced to the account.
Recovery method	Parsing and carving

Attribute	Description
Unique Device Identifier	A unique ID for the device that is accessing the tab.
Device Name	The name of the device that is linked to the iCloud account.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the device first synced to the iCloud account.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the device last synced with the iCloud account.

Additional Information

Safari iCloud Tabs

Description	Safari iCloud Tabs contains information about tabs that have been opened in the browser and synced to an iCloud account. Synchronized tabs are available to any device that logs in to the iCloud account.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the tab.
URL	The URL address of the tab.
Unique Device Identifier	A unique ID for the device that is accessing the tab.

Attribute	Description
Device Name	The name of the device that is accessing the tab.
Tab ID	The unique ID of the tab.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was last modified.
Modified By	The name of the device that last modified the tab.
Close Requested	Indicates whether a close request has been opened for the tab.
Close Request Date/Time - UTC (yyyy-mm-dd)	The date and time when the close request was created.

Additional Information

Safari Last Session

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to the user's last session with Safari.
Recovery method	Parsing and carving

Attribute	Description
Tab URL	The webpage URL.
Tab Title	The title of the webpage.

Additional Information

Safari Top Sites

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows. This table captures information related to the user's top sites.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Feed Last Update Time	The date and time that the top site content was last updated.
Feed URL	The URL of the RSS feed.

Additional Information

Samsung Browser Archived Keyword Search Terms

Description	Keyword search terms that were archived by the browser.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Samsung Browser Archived Web History

Description	Samsung Browser Archived Web History contains an archived history of old webpage visits.
Recovery method	Parsing

Attribute	Description
URL	The URL where the archived web history is located.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was visited.

Attribute	Description
Title	The title of the archived web history.
Visit Count	Total visits to this URL.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
ID	The ID for the web history archive.

Additional Information

Samsung Browser Autofill

Description	Samsung Browser Autofill contains a collection of saved values that were used to fill in forms and fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Value	The value.
Count	The count of the autofill.

Additional Information

Samsung Browser Autofill Profiles

Description	Samsung Browser Autofill Profiles contains the profiles that Samsung Browser uses to fill in forms with saved values.
Recovery method	Parsing

Attribute	Description
Name	The name for the autofill profile.
Email	The email used in the the autofill profile.
Number	The phone number used in the autofill profile.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the profile was last modified.
Company	The company name used in the autofill profile.
Address Line 1	The address Line 1 used in the autofill profile.
Address Line 2	The address Line 2 used in the autofill profile.
City	The city used in the autofill profile.
State	The state used in the autofill profile.
Zipcode	The Zip Code used in the autofill profile.
Country	The country used in the autofill profile.

Additional Information

Samsung Browser Bookmarks

Description	Samsung Browser Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Name	The title of the bookmarked page.
Account Name	The user account that created the bookmark.
Device ID	The ID of the device the bookmark was created on.
Device Name	The name of the device the bookmark was created on.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time whne the bookmark was last modified.
Deleted	Whether the bookmark has been deleted.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark (URL or Folder).

Additional Information

Samsung Browser Cache Records

Description	Content that Samsung Browser downloads and caches to speed up rendering times. Cached content can include pictures, text, html, javascript, and more.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached item.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was first visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Last Synced Date/Time - UTC (yyyy-mm-dd)	The date and time the cache was last synced with the cloud.
File Type	The type of file that was cached.
Content Size (Bytes)	The size of the cached file.
Image	The cached image if the file type is an image. Otherwise, this column is empty.
Content	The cached file contents if the file type is not an image. Otherwise, this column is empty.

Additional Information

Samsung Browser Cached Thumbnails

Description	Samsung Browser Cached Thumbnails contains thumbnail previews of the web pages that a user visits while using the browser.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cached item.
Thumbnail	A partial screenshot of the web page which is used as a thumbnail.
Preview Image	A full screenshot of the cached web page.

Additional Information

Samsung Browser Cookies

Description	Samsung Browser Cookies contains cookies that Samsung Browser downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.

Attribute	Description
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Samsung Browser Current Session

Description	Information about the browser session that's currently underway.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Title	The title of the web page.

Attribute	Description
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Samsung Browser Current Tabs

Description	Information about the tabs that are open in the current browser session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Title	The title of the web page.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Samsung Browser Downloads

Description	Information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The file name of the download.
Start Time Date/Time - UTC (yyyy-mm-dd)	The download start time.
End Time Date/Time - UTC (yyyy-mm-dd)	The download end time.
Saved To	The location that the download was saved to.
State	The state of the download.
Opened By User	Whether the download is opened by the user.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	File size of the download.

Additional Information

Samsung Browser FavIcons

Description	Contains the favicons that Samsung Browser displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.

Recovery method	Parsing

Attribute	Description
Page URL	Page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	Last time the favicon was updated.
Icon URL	Icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Samsung Browser History Index

Description	An index of the webpages the user has visited in the past.
Recovery method	Parsing

Attribute	Description
Page URL	The URL of the webpage.
Visited On Date/Time - UTC (yyyy-mm-dd)	When the webpage was visited.
Title	The title of the webpage.
Body	A snippet of the webpage.

Additional Information

Samsung Browser Keyword Search Terms

Description	Information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Samsung Browser Last Session

Description	Information about the previous browser session.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.

Attribute	Description
Title	The title of the web page.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Samsung Browser Last Tabs

Description	Information about the tabs that were open during the previous session.
Recovery method	Parsing

Attribute	Description
URL	The web page URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Title	The title of the web page.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

Samsung Browser Logins

Description	Login information that a user provides in Samsung Browser. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the data was created.
URL	The URL of the login page.

Additional Information

Samsung Browser Media History

Description	Samsung Browser Media History contains information about the media files (audio and video) that the user views in the browser.
Recovery method	Parsing

Attribute	Description
Page URL	The URL of the page that contains the media file.
Video URL	The URL of the media file.
Title	The media title.
Thumbnail	The media thumbnail.
Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the user visited the page containing the media file.
Played (Seconds)	The duration of the media file that has been played, in seconds.
Duration (Seconds)	The full duration of the media file, in seconds.

Additional Information

Samsung Browser Saved Credit Cards

Description	Samsung Browser Saved Credit Cards contains information about the credit cards that a user has saved to their device.
Recovery method	Parsing

Attribute	Description
Name On Card	The name of the person on the credit card.
Card Number	The number on the credit card.

Attribute	Description
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the information was last modified.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time the credit card autofill information was last used.
GUID	An ID for the credit card.
Expiry Date	The date the credit card is supposed to expire in format 'month-year'.

Additional Information

Samsung Browser Saved Pages

Description	Samsung Browser Saved Pages contains information about web pages that were saved for offline viewing by the user. This includes basic page data, preview icon, user and device info. In addition, an .mhtml backup of the page is recovered, if it wasn't deleted.
Recovery method	Parsing

Attribute	Description
URL	The URL of the saved webpage.
Title	The title of the saved webpage.
Description	The brief description of the saved webpage.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the page was saved.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when saved page was last modified.
Icon	The preview icon for the saved page.
Deleted	Indicates whether saved page backup was deleted.
Account Name	The email account of the user that saved the page.
Device ID	The device ID.
Device Name	The device name.
Page Saved	The HTML content of the saved page. Uses .mhtml format instead of .html, which can affect display in various browsers.

Additional Information

Samsung Browser Shortcuts

Description	Contains all of the shortcuts used by Google Samsung Browser for user entered URLs.
Recovery method	Parsing

Attribute	Description
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - UTC (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the web page.
Times Used	The number of times the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

Additional Information

Samsung Browser Tab History

Description	A history of websites the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the web page (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Search Term	The value the user entered into a search.

Additional Information

Samsung Browser Tabs

Description	Samsung Browser Tabs contains information about the tabs that the user has opened in the browser (not including private browsing). This artifact can also recover tabs that were opened but deleted.
Recovery method	Parsing

Attribute	Description
Tab ID	The ID of the tab. This value can be used to identify specific tab files.
Tab URL	The URL of the website open in the tab.
Tab Title	The title of the website that's open in the tab.
Deleted	Indicates whether the tab has been deleted in the browser.
Account Name	The email account of the user that opened the tab.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the tab was last modified.
Sync Date/Time - UTC (yyyy-mm-dd)	Indicates the date and time that the tab was last synced, if the browser on the local device is synced with another device.
Device Name	The device name.
Device ID	The device ID.

Additional Information

Samsung Browser Top Sites

Description	A list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the site was last updated.
Title	Title of the site.
Thumbnail	Thumbnail of the site

Additional Information

Samsung Browser Web History

Description	A history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times the webpage was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Samsung Browser Web Visits

Description	A history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

SharePoint Discussions

Description	This table captures information related to discussions held on SharePoint.

Recovery method	Carving

Attribute	Description
Subject	The subject of the discussion.
Discussion Link	A link to the discussion.
Fragment	A fragment of the discussion.
Modified Date/Time - Local Time	The date and time when the content was last modified.
Created By	The user who created the content.
Creator Link	A link to the user that created the content.
Reply Count	The number of replies in the discussion.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

SharePoint Recycle Bin

Description	This table captures information about content in a SharePoint recycle bin.
Recovery method	Carving

Attribute	Description
Name	The name of the file in the recycle bin.
Type	The type of the file in the recycle bin.
Original Location	The file's original location.
Creator Name	The user who created the file.
Creator Email Address	The email address of the user who created the file.
Deleted Date/Time - Local Time	The date and time that the file was deleted.
Size	The size of the file.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

SharePoint Shared Documents

Description	This table captures information related to shared documents stored on SharePoint.
Recovery method	Carving

Attribute	Description
Content Type	The type of the content.
Content Name	The name of the conten.t

Attribute	Description
Content Link	A link to the content.
Modified Date/Time - Local Time	The date and time when the content was last modified.
Modified By	The user that modified the content.
Modified By Link	A link to the user who modified the content.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Sleipnir Autofill

Description	Sleipnir Autofill contains records of the autofill values that Sleipnir saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was last used.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Sleipnir Bookmarks

Description	Sleipnir Bookmarks contains the webpages that a user has bookmarked.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was added.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the bookmark was last updated.
Name	The name of the bookmark.
Type	The type of bookmark.
Parent Folder	The name of the parent folder of the bookmark.

Additional Information

Sleipnir Cookies

Description	Sleipnir Cookies contains information about the cookies that the browser

	downloaded from the websites that were visted by the user.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time that the cookie expires.
Path	The path of the cookie value.

Additional Information

Sleipnir Search Terms

Description	Sleipnir Search Terms contains information about the keyword search terms that a user has provided in the browser.
Recovery method	Parsing

Attribute	Description
Search Term	The search term that the user entered.
URL	The URL of the keyword search.
Search Date/Time - UTC (yyyy-mm-dd)	The date and time when the keyword search took place.
Count	The number of times that the search occured.

Additional Information

Sleipnir Web History

Description	Sleipnir Web History contains information about the websites that the user visited.
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.

Additional Information

UC Browser Bookmarks

Description	UC Browser Bookmarks contains the webpages that a user has bookmarked.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Title	The title of the bookmark.
Is Folder	Indicates if the bookmark entry is a folder.

Additional Information

UC Browser Cookies

Description	UC Browser Cookies contains information about the cookies that the browser downloaded from the website that the user has visited.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

UC Browser Downloads

Description	UC Browser Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
File Name	The name of the downloaded file.

Attribute	Description
Saved To	The absolute path on the device to the file downloaded.
Download URL	The URL of the file that was downloaded.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the downloaded finished.
File Size (Bytes)	The file size of the download.

Additional Information

UC Browser History

Description	UC Browser History contains information about the websites that the user visits.
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.

Additional Information

WebKit Browser Session/Tabs (Carved)

Description	WebKit Browser Sessions/Tabs contains information about the browser sessions and tabs that the user has open, while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers, such as Firefox and Safari, aren't likely to appear under this artifact.
Recovery method	Carving

Attribute	Description
URL	The URL of the webpage.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

WebKit Browser Web History (Carved)

Description	WebKit Browser Web History contains information about the websites that a user visits while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers aren't likely to appear under this artifact, however, some URLs found by other browsers may also be found by this artifact.
Recovery method	Carving

Attribute	Description
URL	The URL of the visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited
Title	The title of the visited webpage.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the webpage was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Whale Autofill

Description	Whale Autofill contains records of the autofill values that Whale saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Whale Bookmarks

Description	Whale Bookmarks contans browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Whale Cookies

Description	Whale Cookies contains cookies that Whale downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-	The date and time when the cookie was created.

Attribute	Description
dd)	
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Whale Downloads

Description	Whale Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was finished.
Saved To	The absolute path on the device to the downloaded file.

Attribute	Description
State	The completion state of the download.
Opened By User	Indicates whether the user has opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Whale FavIcons

Description	Whale Favicons contains the favicons that Whale displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last time that the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Whale Keyword Search Terms

Description	Whale Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.

Additional Information

Whale Logins

Description	Whale Logins contains login information that a user provides in Whale. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username entered.
Password	The password entered.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the data was created.
URL	The URL of the login page.

Additional Information

Whale Tab History

Description	Whale Tab History contains a history of websites that the user has opened on each tab within the application. Each tab contains its own timeline of activity generated by the user.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the tab file.
Tab ID	The unique ID of a tab entry in a tab file.
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Referrer URL	A URL for the application or source that makes the request to open the webpage (for example, the referrer source might be from Google or another third-party application).
Originating URL	The URL of the webpage that led the user to the current URL.

Attribute	Description
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Search Term	The value that the user entered into a search.

Additional Information

Whale Top Sites

Description	Whale Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the site.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Additional Information

Whale Web History

Description	Whale Web History contains a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Whale Web Visits

Description	Whale Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

XBox 360 Internet Explorer Cache Records

Description	Internet explorer is a Windows-based desktop application for browsing the internet. All Windows computers are pre-loaded with this web-browser as the default internet browser.
Recovery method	Carving

Attribute	Description
URL	The URL of the cache record.
User	The local user.
Last Modified by Web Server Date/Time - UTC (yyyy-mm-dd)	The last time that the content was modified on the web server. This time is reflective of when the website created the content on the page and can be before the system being examined was built.
Last Checked by Local Host Date/Time - UTC (yyyy-mm-dd)	The date and time that the content was checked for recency on the local system.
Cache Retrieval Count	The number of times that the item was retrieved from the cache.
Filename	The name of the file.
File Type	The filename of the cached content.
Content Size (Bytes)	The size of the cache file.
Image	If the content file is an image, it will be displayed here.
Content	If the file is not an image, as in the case of a JavaScript file for example, the raw bytes will be stored here.

Additional Information

XBox 360 Internet Explorer Daily History

Description	Internet explorer is a Windows-based desktop application for browsing the Internet. All Windows computers are pre-loaded with this web-browser as the default Internet browser.
Recovery method	Carving

Attribute	Description
URL	The URL that was visited.
User	The local user.
Last Visited Date/Time (local time) (yyyy-mm-dd)	The local date and time that the URL was last visited.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time that the URL was last visited.
Visit Count	The number of times that the URL was visted.
Web Page Title	The webpage title.

Additional Information

XBox 360 Internet Explorer Favorites/Recent/Featured Items

Description	Internet explorer is a Windows-based desktop application for browsing the Internet. All Windows computers are pre-loaded with this web-browser as the default Internet browser.

Recovery method	Carving

Attribute	Description
URL	The URL of the item.
Display Name	The name of the item.

Additional Information

XBox 360 Internet Explorer Weekly History

Description	Internet explorer is a Windows-based desktop application for browsing the Internet. All Windows computers are pre-loaded with this web-browser as the default Internet browser.
Recovery method	Carving

Attribute	Description
URL	The URL that was visited.
User	The local user.
Last Visited Date/Time (local time) (yyyy-mm-dd)	The local date and time that the URL was last visited.
Weekly History File Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the weekly history file was created.

Attribute	Description
Visit Count	The number of times that the URL was visited.
Web Page Title	The webpage title.

Additional Information

XBox Internet Explorer Main History

Description	Internet explorer is a Windows-based desktop application for browsing the Internet. All Windows computers are pre-loaded with this web-browser as the default Internet browser.
Recovery method	Carving

Attribute	Description
URL	The URL that was visited.
User	The local user.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time that the URL was last visited.
Last Visited (2nd Timestamp) Date/Time - (UTC) (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the URL was visted.
Web Page Title	The webpage title.

Additional Information

Yandex Autofill

Description	Yandex Autofill contains records of the autofill values that Yandex saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Value	The saved autofill value for this type of field.
Count	The count of this autofill.

Additional Information

Yandex Bookmarks

Description	Yandex Bookmarks contains browser bookmarks that reference saved webpages.
Recovery method	Parsing

Attribute	Description
URL	The URL of the bookmark.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time whne the bookmark was added.
Name	The name of the bookmark.
Parent	The name of the parent folder of the bookmark.
Type	The type of bookmark.

Additional Information

Yandex Cookies

Description	Yandex Cookies contains the cookies that Yandex downloads from the Internet. These cookies contain information about the websites that a user visits.
Recovery method	Parsing

Attribute	Description
Host	Contains the domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path of the cookie value.

Additional Information

Yandex Downloads

Description	Yandex Downloads contains information about the files that a user downloads from the Internet.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
File Name	The name of the downloaded file.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Saved To	The absolute path on the device to the downloaded

Attribute	Description
	file.
State	The completion state of the download.
Opened By User	Indicates whether the user opened the downloaded file or not.
Bytes Downloaded	The bytes that were downloaded.
File Size (Bytes)	The file size of the download.

Additional Information

Yandex FavIcons

Description	Yandex Favicons contains the favicons that Yandex displays in the address bar for the website that's currently displayed. These icons are sometimes downloaded when you favorite/bookmark a website.
Recovery method	Parsing

Attribute	Description
Page URL	The page URL of the favicon.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time when the favicon was updated.
Icon URL	The icon URL of the favicon.
Icon	A preview of the favicon.

Additional Information

Yandex Keyword Search Terms

Description	Yandex Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Yandex Logins

Description	Yandex Logins contains login information that a user provides in Yandex. Passwords are often encrypted, so you might not be able to recover those unless you're examining a live system.
Recovery method	Parsing

Attribute	Description
User Name	The username entered.
Password	The password entered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the data was created.
URL	The URL of the login page.

Additional Information

Yandex Shortcuts

Description	Yandex Shortcuts contains all of the shortcuts used by Yandex for user entered URLs.
Recovery method	Parsing

Attribute	Description
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - UTC (yyyy-mm-dd)	The last access time of the shortcut.

Attribute	Description
Web Page Title	The title of the webpage.
Times Used	The number of times that the shortcut was used.
Transition Type	Describes how the browser navigated to the URL of the shortcut. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

Additional Information

Yandex Sync Data

Description	Yandex Sync Data contains information about the data that Yandex has synced to a user's account in the cloud.
Recovery method	Parsing

Attribute	Description
Name	The name of the sync key.
Local Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the local system.
Server Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified time of the value on the server.
Local Created Date/Time - UTC	The created time of the value on the local system.

Attribute	Description
(yyyy-mm-dd)	
Server Created Date/Time - UTC (yyyy-mm-dd)	The created time of the value on the server.
Type	The type of data that is synced (bookmark, favicon, type URL, and more).
Parsed Content	The type of parsed data.
Favicon Image	The actual favicon image.

Additional Information

Yandex Top Sites

Description	Yandex Top Sites contains a list of the websites that are the most popular to the user. Top sites are displayed on the browser home page which allows the user to quickly click on a frequently visited site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the site.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the site was last updated.
Title	The title of the site.
Thumbnail	The thumbnail of the site.

Additional Information

Yandex Web History

Description	Yandex Web History a history of the websites that the user visits (includes unique visits only).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the visited page.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

Yandex Web Visits

Description	Yandex Web Visits contains a history of the websites that the user visits (includes all visits).

Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the webpage was last visited.
Title	The title of the webpage that was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

YARA Rules

YARA Rule Matches

Description	The YARA artifact contains information about files and processes that matched with conditions specified in a YARA rule.

Recovery method	Parsing

Attribute	Description
File Name	The name and extension of the file whose content matched with the condition(s) from the YARA rule. The value is blank if the match came from a process (executable/application that was loaded into memory at the time of the memory dump) during memory analysis using the Comae plugin option.
File size (bytes)	The size of the file in bytes. The value is blank if the match came from a Process.
Process Name	The name of the process that matched with the condition(s) from the YARA rule. The value is blank if the match came from a file.
Process ID	The ID of the process (PID). The value is blank if the match came from a File.
Matched rule set(s)	List of the paths and respective YARA rule sets that had a match.
Matched rule	The YARA rule name that a match was found for.
Matching conditions	List of conditions for the YARA rule that had a match.

Additional Information

iVe

Location and Travel

Attached Devices - iVe

Description	Attached Devices - iVe contains information about all the instances of a device that have been attached to the various vehicles exported by iVe. The data for this artifact is recovered using iVe and exported as IVO files for Magnet AXIOM.
Recovery method	Parsing

Attribute	Description
Device Name	The name of the attached device.
Device Type	The type of the attached device.
Unique Identifier	The unique number identifying the attached device.
Identifier Type	The type of unique identifier used for the attached device.
Manufacturer	The manufacturer of the attached device.
Model	The model of the attached device.
Interface Type	The interface connection type for the attached device.
Vehicle Make	The make of the vehicle the device was connected to.
Description	The description of the infotainment system of the vehicle.

Additional Information

Call Logs - iVe

Description	Call Logs - iVe contains information about phone calls that were made by a user in the vehicle. The data for this artifact is recovered using iVe and exported as IVO files for Magnet AXIOM.
Recovery method	Parsing

Attribute	Description
Contact Name	The name of the contact.
Phone Number	The phone number of the contact.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the call in UTC time.
Start Date/Time - Local (yyyy-mm-dd)	The start date and time of the call in Local time.
Direction	The direction of the call (Incoming or Outgoing).
Device ID	The identifier of the device that was connected to the vehicle.
Device Name	The name or names of the device that were connected to the vehicle.
Device Type	The manufacturer of the device connected to the vehicle.

Attribute	Description
Device Model	The model of the device connected to the vehicle.
Vehicle Make	The make of the vehicle the device was connected to.
Description	The description of the infotainment system of the vehicle.

Additional Information

Contacts - iVe

Description	Contacts - iVe contains information about contacts saved by the user. The data for this artifact is recovered using iVe and exported as IVO files for Magnet AXIOM.
Recovery method	Parsing

Attribute	Description
First Name	The first name of the contact.
Last Name	The last name of the contact.
Company	The company or place of work of the contact.
Phone Number(s)	The list of phone numbers of the contact.
Email Address	The email address of the contact.
URL	The URL or web address of the contact.

Attribute	Description
Photo URL	The URL of a photo of the contact.
Picture	The profile picture of the contact.
Device ID	The unique identifier of the contact's device.
Device Name	The name of the contact's device.
Device Type	The contact's type of device.
Device Model	The model of the contact's device.
Vehicle Make	The make of the contact's vehicle.
Description	The model of the contact's vehicle.

Additional Information

Device Info - iVe

Description	Device Info - iVe contains information about the vehicle and the infotainment system used. The data for this artifact is recovered using iVe and exported as IVO files for Magnet AXIOM.
Recovery method	Parsing

Attribute	Description
Device Type	The type of the infotainment system for the vehicle.

Attribute	Description
Vehicle Make	The make of the vehicle.
Description	The description of the infotainment system of the vehicle.
Interface Type	The type of interface for the vehicle.
Unique Identifier	A unique number identifying the vehicle.
Identifier Type	The type of the unique identifier for the vehicle (i.e. Serial Number, VIN, etc.).

Additional Information

Events - iVe

Description	Events - iVe contains information about events between the device, the user, and/or the vehicle. The data for this artifact is recovered using iVe and exported as IVO files for Magnet AXIOM.
Recovery method	Parsing

Attribute	Description
Event	Description of the event that was initiated by the device, the user, or the vehicle.
Event Type	The type of the event.
Action	The action taken by the device, the user, or the vehicle tied to the

Attribute	Description
	event.
Event Date/Time - UTC (yyyy-mm-dd)	The event date and time in UTC time. Note: The Event Date/Time may be reported with an invalid date but valid time.
Event Date/Time - Local Time (yyyy-mm-dd)	The event date and time in Local time. Note: The Event Date/Time may be reported with an invalid date but valid time.
Latitude	The latitude of the event.
Longitude	The longitude of the event.
Track Name	The name of the set of data tracked by iVe (usually corresponds to one trip in the vehicle).
Geohash	The geohash of the event.
Vehicle Make	The make of the vehicle the device was connected to.
Description	The description of the infotainment system of the vehicle.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Files - iVe

Description	Files - iVe contains information about files that the vehicle and the infotainment system have stored or read from the device. The data for this artifact is recovered using iVe and exported as IVO files for Magnet AXIOM.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file.
File Path	The path to the file.
Original Path	The original path to the file.
Device ID	The identifier of the device that was connected to the vehicle.
Device Name	The name or names of the device that was connected to the vehicle.
Device Type	The manufacturer of the device connected to the vehicle.
Device Model	The model of the device connected to the vehicle.
Vehicle Make	The make of the vehicle the device was connected to.
Description	The description of the infotainment system of the vehicle.

Additional Information

Metadata - iVe

Description	Metadata - iVe contains information about the application and vehicle. The data for this artifact is recovered using iVe and exported as IVO files for Magnet AXIOM.
Recovery method	Parsing

Attribute	Description
Name	The name of the metadata item.
Group	The group the metadata item belongs to.
Value	The value of the metadata item.
Vehicle Make	The make of the vehicle the device was connected to.
Description	The description of the infotainment system of the vehicle.

Additional Information

Routes - iVe

Description	Routes - iVe contains information about the routes created by the user. The data for this artifact is recovered using iVe and exported as IVO files for Magnet AXIOM.
Recovery method	Parsing

Attribute	Description
Name	The name of the route.
Date/Time - UTC (yyyy-mm-dd)	The date and time the route was completed in UTC time.
Date/Time - Local Time (yyyy-mm-dd)	The date and time the route was completed in Local time.

Attribute	Description
Vehicle Make	The make of the vehicle the device was connected to.
Description	The description of the infotainment system of the vehicle.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

SMS - iVe

Description	SMS - iVe contains information about SMS messages that were sent and received by users in the vehicle. The data for this artifact is recovered using iVe and exported as IVO files for Magnet AXIOM.
Recovery method	Parsing

Attribute	Description
Sender	The phone number of the sender.
Recipient	The phone number of the recipient.
Sent Date/Time - UTC (yyyy-mm-dd)	The sent date and time of the call in UTC time.
Sent Date/Time - Local Time (yyyy-mm-dd)	The sent date and time of the call in Local time.

Attribute	Description
Message	The content of the message.
Message Status	The status of the message (read or unread).
Device ID	The identifier of the device that was connected to the vehicle.
Device Name	The name or names of the device that were connected to the vehicle.
Device Type	The manufacturer of the device connected to the vehicle.
Device Model	The model of the device connected to the vehicle.
Vehicle Make	The make of the vehicle the device was connected to.
Description	The description of the infotainment system of the vehicle.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Trackpoints - iVe

Description	Trackpoints - iVe contains information about trackpoints created by the user. The data for this artifact is recovered using iVe and exported as IVO files for Magnet AXIOM.
Recovery method	Parsing

Attribute	Description
Track Name	The name of the set of data tracked by iVe (usually corresponds to one trip in the vehicle).
Date/Time - UTC (yyyy-mm-dd)	The date and time the vehicle was at that trackpoint in UTC time.
Date/Time - Local (yyyy-mm-dd)	The date and time the vehicle was at that trackpoint in local time.
Latitude	The latitude of the trackpoint.
Longitude	The longitude of the trackpoint.
Geohash	The geohash of the trackpoint location.
Velocity	The velocity of the vehicle at a point in time.
Vehicle Make	The make of the vehicle.
Description	The description of the infotainment system of the vehicle.

Additional Information

Velocity Points - iVe

Description	Velocity Points - iVe contains information about the velocity of the vehicle at different times in a trip. The data for this artifact is recovered using iVe and exported as IVO files for Magnet AXIOM.
Recovery method	Parsing

Attribute	Description
Track Name	The name of the set of data tracked by iVe (usually corresponds to one trip in the vehicle).
Point Number	The number identifying the point that iVe uses to group velocity values.
Date/Time - UTC (yyyy-mm-dd)	The date and time the vehicle was at that velocity in UTC time.
Date/Time - Local (yyyy-mm-dd)	The date and time the vehicle was at that velocity in local time.
Velocity	The velocity of the vehicle.
Vehicle Make	The make of the vehicle.
Description	The description of the infotainment system of the vehicle.

Additional Information

Waypoints - iVe

Description	Waypoints - iVe contains information about waypoints created by the user. The data for this artifact is recovered using iVe and exported as IVO files for Magnet AXIOM.
Recovery method	Parsing

Attribute	Description
Name	The name of the waypoint.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the waypoint in UTC time.
Date/Time - Local (yyyy-mm-dd)	The date and time of the waypoint in Local time.
Latitude	The latitude of the waypoint.
Longitude	The longitude of the waypoint.
Street	The street address of the waypoint.
State	The state of the waypoint.
ZIP/Postal Code	The ZIP code or postal code of the waypoint.
City	The city the waypoint is located in.
Country	The country the waypoint is located in.
Geohash	The geohash of the waypoint location.
Vehicle Make	The make of the vehicle the device was connected to.
Description	The description of the infotainment system of the vehicle.

Additional Information

Windows Phone

Advanced Search Tools

Dynamic Application Finder

Description	Artifacts found using the Dynamic Application Finder vary depending on your case's evidence. To learn more, see Processing details > Find more artifacts in the AXIOM User Guide.
Recovery method	Parsing

Attribute	Description

Additional Information

Communication

IP Addresses - Audio/Video Calls

Description	IP Addresses of web audio/video calls show who a user was communicating with. Each instance of this artifact represents a single hop in the communication chain. By showing the relationship between multiple hops, you can determine where a call originated from and what the final destination was.
Recovery method	Carving

Attribute	Description
Call ID	The ID of the call.
Message ID	The ID of the message.
Domain	The domain used for the call.
Connection Type	The type of connection.
Origin IP Address	The originating IP address for this hop in the call.
Origin Port	The originating port for this hop in the call.
Destination IP Address	The destination IP address for this hop in the call.
Destination Port	The destination port address for this hop in the call.
Date/Time - UTC (yyyy-mm-dd)	The timestamp associated with this hop in the call.
Remote User ID	The unique ID of the remote user.
Communication Protocol	The communication protocol for this call (either UDP or TCP).
Metadata	Any additional details about the call.

Additional Information

Lync / OC Calls

Description	Lync/OC is a business grade communication application created by Microsoft.
Recovery method	Carving

Attribute	Description
Remote Participant Email	The email of the remote participant.
Remote Participant Display Name	The display name of the remote participant.
Call Started Date/Time - Local Time (yyyy-mm-dd)	The date and time when the call was started, local to the system.
Call Ended Date/Time - Local Time (yyyy-mm-dd)	The date and time when the call ended, local to the system.
Duration (Seconds)	The duration of the call in seconds.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Lync / OC File Transfers

Description	Lync/OC is a business grade communication application created by Microsoft.
Recovery method	Carving

Attribute	Description
Type	The type of file.
Sender	The sender of the file.
Recipient	The recipient of the file.

Attribute	Description
File	The file name or path.
File Size (Bytes)	The size of the file.
Transfer Event Date/Time - Local Time (yyyy-mm-dd)	The start and end date time of the transfer.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Lync / OC Fragments

Description	Lync/OC is a business grade communication application created by Microsoft.
Recovery method	Carving

Attribute	Description
HTML Fragment	The HTML fragment of the conversation.

Additional Information

Lync / OC Messages

Description	Lync/OC is a business grade communication application created by Microsoft.
Recovery method	Carving

Attribute	Description
Sender Email	The email address of the sender.
Sender Display Name	The display name of the sender.
Body	The body of the message.
Sent Date/Time - Local Time (yyyy-mm-dd)	The date and time when the message was sent, local to the system.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Skype Accounts

Description	Skype Accounts contains information about the Skype accounts that are recovered, such as user information and when the account was created.
Recovery method	Parsing

Attribute	Description
Skype Name	The Skype name of the account.
Display Name	The display name of the account.
Full Name	The full name of the account.
Email(s)	The email of this account.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date when the profile was created.
Last Online Date/Time - UTC (yyyy-mm-dd)	The last time that the account was online.
Birthday (yyyy-mm-dd)	The birthday of the account.
Gender	The gender of the account.
City	The city where the account is located.
State/Province	The state/province where the account is located.
Country	The country where the account is located.
Home Phone	The home phone of this contact.
Office Phone	The office phone of this account.
Mobile Phone	The mobile phone of this account.
Homepage	The homepage of this contact.
About Info	The about info of this contact.
Profile Last Modified On Date/Time - UTC (yyyy-mm-dd)	The date when the profile was last modified.
Mood Text	The text used to express mood.

Attribute	Description
Last Used On Date/Time - UTC (yyyy-mm-dd)	The last time that the account was used.
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	The time that the avatar was created.
Picture	The avatar for this contact.

Additional Information

Skype Calls

Description	Skype Calls contains information about Skype calls that occured between users.
Recovery method	Parsing and carving

Attribute	Description
Local Username	The user logged into Skype at the time of the call.
Call Initiator	The user who started the call.
Initiator Display Name	The display name of the user. This might be different from the user-name.
Recipient(s)	The users who accepted a call from the call initiator and participated in the call for a period of time.
Call Participants	The users who accepted and participated in the call from the call ini-tiator for some duration.

Attribute	Description
Started Date/Time - UTC (yyyy-mm-dd)	The start time of the call.
Duration	The total duration of the Skype call.
Metadata	Additional details about the call extracted in XML format. This includes the amount of time that each participant was in the call.

Additional Information

Skype Chat Messages

Description	Skype Chat Messages contains Skype messages sent from one user to another.
Recovery method	Parsing and carving

Attribute	Description
Profile Name	The profile name of the caller.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Author	The author of the message.
From Display Name	The display name of message's sender.

Attribute	Description
Message	The body of the message or a description of the action taken. For example, adding another participant to a group chat or sharing a file or picture.
Attachment Name	The name of the attachment that was sent. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Attachment Size (Bytes)	The size of the attached file, in bytes. This attribute is populated when the Message Type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Metadata	Additional details about the action, extracted in its original XML format.
Message Status	The status of the message.
Message Type	The type of message.
Chat ID	The ID of this chat.
Recipient	The recipient of the chat.

Additional Information

Skype Chatsync Messages

Description	Skype Chatsync Messages contains Skype messages sent from one user to another that are parsed from the chatsync directory.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local Skype user.
Chat Initiator	The user that started the conversation.
Chat Partner/Group Chat ID	The other user in the chat, or a group chat identifier.
Message Type	Indicates whether the message was sent or received.
Message	The content or body of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.

Additional Information

Skype Chatsync Messages Carved

Description	Skype Chatsync Messages Carved contains Skype messages sent from one user to another, and that are carved from the Chatsync directory.
Recovery method	Parsing

Attribute	Description
Message Type	Indicates whether the message was sent or received.

Attribute	Description
Message	The content or body of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.

Additional Information

Skype Contacts

Description	Skype Contacts contains information about Skype contacts that are recovered, which may or may not be added contacts.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the contact.
Skype Name	The Skype name of the contact.
Display Name	The contact's display name.
Is Blocked	Indicates whether or not the contact is blocked.
Contact Added	Specifies whether the contact is an added contact or just cached into the database (1 if the contact was added, 0 otherwise). Contacts can be cached into the database for a variety of reasons (for example, as a 'suggested contact').
Full Name	The contact's full name.

Attribute	Description
Birthday (yyyy-mm-dd)	The contact's birthday.
Gender	The contact's gender.
City	The city where the contact is from.
State / Province	The state or province that the contact is from.
Country	The country that the contact is from.
Home Phone	The contact's home phone number.
Office Phone	The contact's office phone number.
PSTN Number	The contact's public switched telephone network.
Email(s)	The email address(es) of the contact.
Homepage	The contact's homepage.
About Info	Information about the contact.
Profile Loaded Date/Time - UTC (yyyy-mm-dd)	This fragment was previously called Profile Created On Date/Time. The value in this field represent the date and time when a contact's profile is first created on the user's device. When the profile information is updated by the contact, the date in the database is also updated.
Profile Last Modified Date/Time - UTC (yyyy-	The date and time when the contact last modified their profile.

Attribute	Description
mm-dd)	
Mood Text	The contact's mood.
Last Online Date/Time - UTC (yyyy-mm-dd)	The last date and time that the contact was seen online.
Last Used Date/Time - UTC (yyyy-mm-dd)	The last date and time the contact accessed contacts.
Avatar Timestamp Date/Time - UTC (yyyy-mm-dd)	The last date and time when the contact updated their avatar.

Additional Information

Skype File Transfers

Description	Skype File Transfers contains files that are transferred from one user to another using Skype.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Partner Handle	The username of the file transfer partner.
Partner Display Name	The display name of the file transfer partner.
File Name	The file name being transferred.
Type	The type of file being transferred.
File Path	The path to the local file.
Transferred File	The file that was transferred.
File Size (Bytes)	The size of the file being transferred.
Bytes Transferred	The number of bytes that were transferred.
Transfer Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the file transfer was started.
Transfer Finish Date/Time - UTC (yyyy-mm-dd)	The date and time when the file transfer completed.
Status	The status of the file, such as transfer, transferring or cancelled.

Additional Information

Skype Group Chat

Description	Skype Group Chat contains information about the Skype group chats that a user is a part of.

Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Chat ID	The group chat's unique identifier.
Participants	The participants of the chat.
Posters	The users that have posted to the chat.
Active Members	The currently active user's of the group.
Chat name	The name of the chat.
Started Date/Time - UTC (yyyy-mm-dd)	The date and time when the chat started.
Last Changed Date/Time - UTC (yyyy-mm-dd)	The date and time when the chat was modified.

Additional Information

Skype IP Addresses

Description	Skype IP Addresses contains IP addresses that are associated with a Skype user account.
Recovery method	Parsing and carving

Attribute	Description
Username	The Skype username.
IP Address	The IP address of that user.
IP Address Type	The IP address type.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the IP address log.

Additional Information

Skype SMS

Description	Skype SMS contains SMS messages that a user sends or recieves using Skype.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Author	The author of the message.
Message	The message content.
Target Number(s)	The phone numbers of the recipients.

Attribute	Description
Status	The status of the message.
Reply-to Number	A phone number that the recipients can reply to.

Additional Information

Skype Voicemails

Description	Skype Voicemails contains voicemails that a user sends or recieves using Skype.
Recovery method	Parsing

Attribute	Description
Profile Name	The name of the user.
Partner Handle	The username of the conversation partner.
Partner Display Name	The display name of the conversation partner.
Subject	Identifies the subject of the voicemail.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Duration	The length of the voicemail.
Allowed Duration	The maximum length allowed for the voicemail.

Attribute	Description
Size	The size of the recording.
Path	The file path of the voicemail.
Type	Identifies whether the voicemail was received or sent.
Status	The status of the voicemail, recording or played for example.

Additional Information

Windows Phone Call Logs

Description	Windows Phone Call Logs contains the call logs on a Windows Phone 8 device.
Recovery method	Parsing and carving

Attribute	Description
Phone Number	The phone number of the other device the phone call was with.
Partner Name	The name of the other person the phone call was with.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time that the call was started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time that the call was ended.

Attribute	Description
Call Status	The status of the call. This value can be Outgoing Call, Incoming Call, or Missed Call.

Additional Information

Windows Phone Contacts

Description	Windows Phone Contacts contains the contacts on a Windows Phone 8 device.
Recovery method	Parsing

Attribute	Description
Contact Name	The name of the contact.
Phone Number	The phone number of the contact.
Email Address	The email address of the contact.
Address	The street address of the contact.
City	The city of the contact.
State/Province	The state or province of the contact.
Country	The country of the contact.
Zip/Postal Code	The ZIP postal code of the contact.

Attribute	Description
Occupation	The occupation of the contact.
Employer	The employer of the contact.
Profile Image URL	The URL of the profile image associated with the contact.

Additional Information

Windows Phone Contacts Carved Fragments

Description	Windows Phone Contacts Carved Fragments contains the carved contacts fragments from a Windows Phone 8 device.
Recovery method	Carving

Attribute	Description
Fragment	The carved contact fragment. This information is presented as-is and is not formatted or separated.

Additional Information

Windows Phone SMS/MMS

Description	Windows Phone SMS/MMS contains the call logs on a Windows Phone 8 device.

Recovery method	Parsing and carving

Attribute	Description
Type	The type of the message, either SMS or MMS.
Direction	The direction of the message (Incoming or Outgoing).
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the message.
Conversation Partner	The number or identifier of the conversation partner.
Status	The status of the message (Read, Sent, or Unknown).
Message	The message content of the SMS or MMS.

Additional Information

Connected Devices

SIM Card ICCID

Description	SIM Card ICCID contains the ICCID number that identifies the device's SIM card.

Recovery method	Parsing

Attribute	Description
ICCID	The integrated circuit card identifier.

Additional Information

SIM Card IMSI

Description	SIM Card IMSI contains IMSI numbers used to identify the mobile subscriber, as recovered from the SIM card.
Recovery method	Parsing

Attribute	Description
IMSI	The international mobile subscriber identity.

Additional Information

SIM Card Phone Numbers

Description	SIM Card Phone Numbers contains records of all the phone numbers saved to the device SIM card. The type of number is indicated by the record type.

Recovery method	Parsing

Attribute	Description
Phone Number	The phone number for the specific record type.
Record Type	Identifies the type of record that the phone number is. This value can be Abbreviated dialing numbers(ADN), Emergency call codes (ECC), Last number dialed (LND), MSISDN, Service dialing numbers (SDN), or Fixed dialing numbers (FDN).

Additional Information

SIM Card Service Providers

Description	SIM Card Service Providers contains the names of mobile service providers that the device has connected with, and which are recovered from the SIM card.
Recovery method	Parsing

Attribute	Description
Service Provider Name	The identity of the mobile phone service provider.

Additional Information

SIM Card SMS Messages

Description	SIM Card SMS Messages contains messages sent or received by the local user which were saved to the SIM card.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the SMS message.
Recipient	The recipient of the SMS message.
Message Date/Time	For incoming messages, this timestamp indicates when the message was received by the mobile service center. For outgoing messages, there is no data available for this field.
Message	The message body of the SMS message.
Deleted	Identifies whether the message has been deleted (Yes or No).
Message Status	Identifies whether the message has been read, unread, drafted or sent.
SMSC	The short message service center number.

Additional Information

USB Devices

Description	USB Devices contains a history of all USB devices that have been con-

	nected to the system.
Recovery method	Parsing

Attribute	Description
Device Class ID	The class ID of the USB device.
Serial Number	The USB device serial number.
Class	The class of the device (USB or USBSTOR).
Last Written Date/Time - UTC (yyyy-mm-dd)	The date and time when the device was last written to.
Device Description	The description of the device.
Friendly Name	The friendly name of the device.
Manufacturer	The manufacturer of the device.
Last Assigned Drive Letter	The last drive letter that was assigned to the device by Windows.
Volume GUID	The GUID of the volume.
VSN Decimal	The volume serial number in decimal notation.
VSN Hex	The volume serial number in hexadecimal notation.
Associated User Accounts	Any user accounts that have used the device.
First Connected Date/Time - UTC (yyyy-mm-dd)	The date and time when the device was first connected.

Additional Information

To learn more about USB Devices, see Artifact profile: USB Devices.

Your Phone Contacts

Description	Your Phone Contacts contains information about contacts synced from a mobile device to a computer using Your Phone. The Your Phone application can sync data from Android and iOS devices to computers running Windows 10.
Recovery method	Parsing

Attribute	Description
Display Name	The contact's display name.
Nickname	The contact's nickname.
Phone Number	The contact's phone number.
Type	The type of phone number associated with the contact, for example Home, Mobile, or Business.
Last Time Contacted Date/Time - UTC (yyyy-mm-dd)	The last time that this contact either sent a message to, or received a message from the synced device or local user since the Your Phone application was installed.
Number of Times Contacted	The number of times the synced device or local user either sent a message to, or received a message from the contact since the Your Phone application was installed.
Last Modified	The last date and time that this contact's details were modified.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	

Additional Information

Your Phone Devices

Description	Your Phone Devices contains information about the devices that are synced to the user's computer by using the Your Phone application.
Recovery method	Parsing

Attribute	Description
Application Version	The version of Your Phone running on the computer.
Last Run Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was last run on the computer.
Device Application Version	The version of the Your Phone companion application running on the device.
Device ID	A GUID identifier generated to uniquely identify devices within the Your Phone application.
Device Name	The name provided by the device and displayed in the user interface when referring to it.
Device Platform	The device's platform (Android or iOS).

Attribute	Description
Device Messages Synced Date	The date and time when the device last synchronized its messages data with Your Phone.
Computer Messages Synced Date	The date and time when the computer last synchronized its messages data with Your Phone.
Device Contacts Synced Date	The date and time when the device last synchronized its contacts data with Your Phone.
Computer Contacts Synced Date	The date and time when the computer last synchronized its contacts data with Your Phone.
Device Photos Synced Date	The date and time when the device last synchronized its picture data with Your Phone.
Computer Photos Synced Date	The date and time when the computer last synchronized its picture data with Your Phone.

Additional Information

Your Phone Pictures

Description	Your Phone Pictures contains information about pictures synced from a mobile device to a computer using Your Phone. The Your Phone application syncs the 25 most recently taken photos from Android and iOS devices to computers running Windows 10.
Recovery method	Not applicable

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Device ID	A GUID identifier generated to uniquely identify devices synced using the Your Phone application.
Device Name	The name of the device (as provided by the device) which is displayed in the user interface for Your Phone.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.

Attribute	Description
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial	The serial number of the camera (extracted from Exif data).

Attribute	Description
Number	
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS Latitude (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the picture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the picture content.
SHA1 Hash	A SHA1 hash of the picture content.
PhotoDNA Hash	The hash of the picture content for PhotoDNA.
Potential Original Media	Indicates whether the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.
Exif Data	A searchable field for all raw exif properties.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Your Phone SMS/MMS

Description	Your Phone SMS/MMS contains information about messages synced from a mobile device to a computer using Your Phone. The Your Phone application can sync data from Android and iOS devices to computers running Windows 10.
Recovery method	Parsing and carving

Attribute	Description
Sender	The phone number that sent the message.
Recipient(s)	The phone number(s) the message was sent to.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message content.
Message Direction	Indicates whether the message was sent or received by the synced device or local user.
Message Type	Indicates whether the message is SMS or MMS.
Message Status	Indicates whether the message has been read.
Attachment Name	The name of the attached file, if applicable (MMS only).

Additional Information

Custom

File Signature Mismatch (Audio)

Description	File Signature Mismatch (Audio) contains identified mismatches between a known file signature header and the extension (or lack thereof) for an audio file. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file. If we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file. If we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Container)

Description	File Signature Mismatch (Container) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a container. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file. If we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Document)

Description	File Signature Mismatch (Document) contains identified mismatches

	between a known file signature header and the extension (or lack thereof) for a document. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file. If we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file. If we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Picture)

Description	File Signature Mismatch (Picture) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a picture. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.

Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file. If the MIME type is unknown, this defaults to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file. If the MIME type is unknown, this defaults to application/octet-stream. If there is no file extension, but the MIME type is known, a mismatch is is returned.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Video)

Description	File Signature Mismatch (Video) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a video. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file. If we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file. If we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

Documents

CSV Documents

Description	CSV Documents contains CSV documents (.csv) that are located on the system.
Recovery method	Parsing

Attribute	Description
File Name	The name of the CSV document.

Attribute	Description
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last modified.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was created.
File Content	The content of the CSV document.
Size (Bytes)	The size of the CSV document in bytes.
SHA1 Hash	The SHA1 hash of the contents of the document.
MD5 Hash	he MD5 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

Microsoft Excel Documents

Description	Microsoft Excel is a spreadsheet processor developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created	The date and time when the file was created on the filesys-

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	tem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Size (Bytes)	The size of the document in bytes.
Saved Size (Bytes)	The size of the document (in bytes) that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title metadata.
Subject	The subject metadata.
Authors	The authors of the document.
Keywords	The keywords metadata in the document.
Comments	The comments metadata.
Last Author	The last author to edit the document.
Last printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

Microsoft PowerPoint Documents

Description	Microsoft PowerPoint is a presentation creator developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.

Attribute	Description
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title metadata.
Subject	The subject metadata.
Authors	The authors of the document.
Keywords	The keywords metadata in the document.
Comments	The comments metadata.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

Microsoft Word Documents

Description	Microsoft Word is a word processor developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Size (bytes)	The size of the document.
Saved Size (bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title metadata.
Subject	The subject metadata.
Authors	The authors of the document.
Keywords	The keywords metadata in the document.
Comments	The comments metadata.

Attribute	Description
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

PDF Documents

Description	Portable Document Format (PDF) is a file format used to present documents in a manner independent of application software, hardware, and operating systems. This table captures documents in this file format, extracted from the filesystem and carved from unallocated space.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time whne the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
File	The PDF file.

Additional Information

For information about supported formats, see Supported media and file types.

RTF Documents

Description	RTF Documents contains the information for each RTF document that was recovered from the search.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the RTF document.
File Size (Bytes)	The size of the RTF document in bytes.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the RTF document was last modified.
File Content	The contents of the RTF document.
MD5 Hash	A MD5 hash of the RTF content.
SHA1 Hash	A SHA1 hash of the RTF content.

Additional Information

For information about supported formats, see Supported media and file types.

Text Documents

Description	Text documents (.txt) that are located on the system.
Recovery method	Parsing

Attribute	Description
Filename	The name of the text document.
Size (Bytes)	The size of the text document in bytes.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was created.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.
File Content	The content of the text document.

Additional Information

For information about supported formats, see Supported media and file types.

Email and Calendar

Gmail Email Fragments

Description	Gmail Email Fragments contains the Gmail email fragments that were recovered from a Windows Phone device.
Recovery method	Parsing

Attribute	Description
HTML Fragment	The HTML fragment of the email.

Additional Information

Gmail Webmail

Description	Gmail Webmail contains the Gmail email that was recovered from a Windows Phone device.
Recovery method	Carving

Attribute	Description
Email(s)	The email addresses involved with the email.
Status	The status of the email.

Attribute	Description
Subject	The subject of the email.
Snippet	A snippet of the email.
Attachments	The name of any attachments.
Sent Date/Time - Local Time	The local date and time of when the email was sent. This value is saved in the database as a string, so attempts to sort or filter the column may not behave as expected. Instead of sorting by date, the column sorts alphabetically.
Last Modified or Viewed Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was last modified.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Hotmail Webmail

Description	Hotmail is a web-based email client that allows users to send and receive emails. Hotmail was replaced by Outlook.com in 2012.
Recovery method	Carving

Attribute	Description
Type	The type of fragment found. This value can be one of Contacts, Message, Folder view, Inbox Message, Edit Message, Plaintext Message Fragment, or Welcome Page.
HTML Fragment	The HTML fragment that was found.

Additional Information

Hushmail® Webmail

Description	Hushmail® Webmail contains carved fragments of messages that are sent or recieved using Hushmail. This artifact uses inbox listings to recover the emails that were received by a user.
Recovery method	Carving

Attribute	Description
Sender	The sender of the email.
Receiver	The receiver of the email.
Subject	The subject of the email.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the email was received.

Additional Information

Mailinator Inbox Access

Description	Mailinator Inbox Access contains instances when a user accesess their Mailinator inbox. Mailinator is webmail service that allows users to send and receive emails anonymously.
Recovery method	Carving

Attribute	Description
Inbox	The inbox that was accessed.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the inbox was accessed.

Additional Information

Mailinator Snippets

Description	Mailinator Snippets contains snippets of email messages that are sent using Mailinator. Mailinator is webmail service that allows users to send and receive emails anonymously.
Recovery method	Carving

Attribute	Description
Sender Name	The sender of the email.

Attribute	Description
Sender Address	The sender's email address.
Sender Mailserver IP	The sender's mailserver IP address.
Recipient Address	The receiver of the email.
Subject	The subject of the email.
Boddy Snippet	A snippet of the email body.
Received Date/Time - UTC (yyyy-mm-dd)	The date and time when the email was received.

Additional Information

Offline Gmail webmail

Description	Gmail is a web-based email website that allows users to send and receive emails.
Recovery method	Parsing

Attribute	Description
From Address	The sender of the email.
To Address(es)	The recipients of the email.
cc Address(es)	The recipients of the email that were CC'd.
bcc Address(es)	The recipients of the email that were BCC'd.

Attribute	Description
Subject	The subject of the email.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the email was sent or received.
Status	The sent status of the email.
Email Body	The body of the email.

Additional Information

Outlook Appointments

Description	Microsoft Outlook is a personal information manager and email client from Microsoft.
Recovery method	Parsing

Attribute	Description
Sender Name	The sender name.
Recipients	The recipients of the appointment.
Recipients CC	The CC'd recipients of the appointment.
Recipients BCC	The BCC'd recipients of the appointment.
Companies	The companies involved.
Subject	The subject of the appointment.

Attribute	Description
Body	The body of the appointment.
Attachments	If there are any attachments on the appointment.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the appointment starts.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the appointment ends.
Locale	The location of the appointment.
Is All-day Event	Indicates whether the appointment is a full date event.
Is Recurring	Indicates whether the appointment is recurring.
Recurrence Pattern Description	The recurring pattern, if applicable.
Sensitivity	Indicates whether the appointment is sensitive.
Is Hidden	Indicates whether the appointment is hidden.
Is Private	Indicates whehther the appointment is private.
Sender Exchange Account	The senders Exchange Account name.
Priority	The priority of the appointment.
Importance	The appointment importance setting.
MD5 Hash	An MD5 hash of the appointment.
SHA1 Hash	A SHA1 hash of the appointment.

Additional Information

Outlook Contacts

Description	Microsoft Outlook is a personal information manager and email client from Microsoft.
Recovery method	Parsing

Attribute	Description
Display Name	The contact's display name.
Company Name	The contact's company name.
Department Name	The contact's department name.
Title	The contact's job title.
Profession	The contact's profession.
Manager Name	The name of the contact's manager.
Office Location	The contact's office location.
Business Phone	The contact's business phone number.
Business Phone 2	The contact's business phone number.
Business Fax	The contact's business fax number.
Business Homepage	The contact's business' website.
Email Address 1	The contact's email address.
Email Display As 1	Indicates how the contact's email should be displayed.

Attribute	Description
Email Display Name 1	The contact's email display name.
Email Address 2	The contact's email address.
Email Display As 2	Indicates the contact's email should be displayed.
Email Display Name 2	The contact's email display name.
Email Address 3	The contact's email address.
Email Display As 3	Indicates how the contact's email should be displayed.
Email Display Name 3	The contact's email display name.
Cellular Phone	The contact's mobile phone number.
Home Address	The contact's address.
Home Phone	The contact's home phone number.
Home Phone 2	The contact's home phone number.
Home Fax	The contact's home fax number.
FTP Site	The contact's FTP site.
Body	More information about the contact.
Attachments	Any attachments on the contact entry.
Customer ID	The customer ID of the contact.
Last Modifier Name	The person that last modified the contact details.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the contact was last modified.

Additional Information

Outlook Emails

Description	Microsoft Outlook is a personal information manager and email client from Microsoft.
Recovery method	Parsing

Attribute	Description
Sender Name	The sender of the email.
Sender Email	The email address of the sender.
Recipients	The recipients of the email.
Subject	The subject of the email.
Sender Exchange Account	The sender's Exchange account name.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was created.
Sync Date/Time - UTC (yyyy-mm-dd)	The date and time when the email synced with the HxStore platform.

Attribute	Description
Submitted Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was submitted.
Delivered Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was delivered.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the email was last modified.
Body	The body of the email. For HxStore data sources that include email bodies deleted when an account was removed, the displayed value is the path where the email body was located on the file system.
Folder Name	The name of the folder where the email is stored.
CC	The recipients of the email that were CC'd.
BCC	The recipients of the email that were BCC'd.
Attachments	The list of attachments on the email.
Headers	The raw email headers.
Priority	The priority of the email.
Importance	The importance of the email.
Sensitivity	The sensitivity of the email.

Attribute	Description
Read	Indicates whether the email was opened and therefore marked as Read. Note that Outlook users can also manually mark emails as either Read or Unread.
MD5 Hash	The MD5 hash of the email.
SHA1 Hash	The SHA1 hash of the email.

Additional Information

Outlook Journals

Description	Microsoft Outlook is a personal information manager and email client from Microsoft.
Recovery method	Parsing

Attribute	Description
Type Description	The type of journal entry.
Subject	The subject of the journal.
Start Date/Time - UTC (yyyy-mm-dd)	The start date and time of the journal.
End Date/Time - UTC (yyyy-mm-dd)	The end date and time of the journal.
Duration (minutes)	The length of the journal entry in minutes.
Body	The body of the journal.

Attribute	Description
Attachments	The list of attachments on the journal.
Creator Name	The journal creators name.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the journal was created.
Last Modifier Name	The user that last modified the journal.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the journal was last modified.
MD5 Hash	An MD5 hash of the appointment.
SHA1 Hash	A SHA1 hash of the appointment.

Additional Information

Outlook Notes

Description	Microsoft Outlook is a personal information manager and email client from Microsoft.
Recovery method	Parsing

Attribute	Description
Body	The body of the note.
Creator Name	The creator's name of the note.

Attribute	Description
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was created.
Last Modifier Name	The user who last modified the note.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the note was last modified.
MD5 Hash	An MD5 hash of the appointment.
SHA1 Hash	A SHA1 hash of the appointment.

Additional Information

Outlook Tasks

Description	Microsoft Outlook is a personal information manager and email client from Microsoft.
Recovery method	Parsing

Attribute	Description
Subject	The subject of the task.
Due Date (yyyy-mm-dd)	The due date of the task.
Status	The status of the task.
Percent Complete	The percent the task is complete.

Attribute	Description
Owner	The owner of the task.
Body	The content of the task body.
Attachments	Any attachments that are attached to the task.
Recipients	The recipients of the task.
Start Date (yyyy-mm-dd)	The date the task was started.
Completed Date (yyyy-mm-dd)	The date the task was completed.
Is Complete	Indicates whether the task is complete.
Actual Work (Minutes)	The actual amount of time that it took to finish the task.
Total Work (Minutes)	The number of working minutes it took to finish the task.
Mileage	The mileage that was travelled for the task.
Billing Information	Any billing information for the task.
Delegator	The person who delegated this task to the user.
Delegation State	Indicates whether the task was delegated.
Creator Name	The creator of the task.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time when the task was created.
Last Modifier Name	The user who last modified the task.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the task was last modified.

Attribute	Description
Is Hidden	Indicates whether the task is hidden.
Is Private	Indicates whether the task is private.
Is Read-Only	Indicates whether the task is read-only.
Sensitivity	Indicates whether the task is sensitive.
Is Team Task	Indicates whether the task is for a team.
Is Recurring	Indicates whether the task is recurring.
Recurrence Pattern Description	The recurring pattern, if applicable.
Is Reminder Set	Indicates whether the task has a reminder.
Reminder Date/Time - UTC (yyyy-mm-dd)	The date and time of the task reminder.
Priority	The priority of the task.
MD5 Hash	An MD5 hash of the appointment.
SHA1 Hash	A SHA1 hash of the appointment.

Additional Information

Outlook Web App Email Fragments

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to emails sent and received from Outlook's web application.
Recovery method	Carving

Attribute	Description
Sender	The sender of the email.
Recipients	The recipient(s) of the email.
Subject	The subject of the email.
Server Timestamp	The timestamp of the email on the server.
Is Draft	Indicates whether the email is a draft.
Fragment	The recovered raw email fragment.

Additional Information

Outlook Web App Inbox

Description	Microsoft Outlook is a personal information manager and email client. This table captures information related to the inbox viewed from Outlook's web application.
Recovery method	Carving

Attribute	Description
Participants	The participants of the email.
Subject	The subject of the email.
Server Timestamp	The timestamp of the email on the server.

Additional Information

Outlook Webmail Inbox

Description	Outlook.com (formerly hotmail.com) is a webmail website that allows users to send and receive emails.
Recovery method	Carving

Attribute	Description
Sender	The sender of the email.
Date/Time - UTC (yyyy-mm-dd)	The date and time when the email was sent or received.
Displayed Date/Time - Local (yyyy-mm-dd)	The date and/or time when the user was shown on the webpage.
Subject	The subject of the message.
Status	The sent status of the email.

Additional Information

Windows Phone Emails

Description	Windows Phone Emails contains the emails that were recovered from a Windows Phone device.
Recovery method	Parsing and carving

Attribute	Description
Sender	The sender of the email. This value includes the name and the email address.
Subject	The subject of the email.
Snippet	The snippet of the email body.
Email Timestamp Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the email.

Additional Information

Yahoo! Webmail

Description	Yahoo Mail is a web-based email client that allows users to send and receive emails.
Recovery method	Carving

Attribute	Description
Type	The email type. Folder Listing means that the email was recovered from the Inbox view, Message means that the user was looking at an individual email, and Compose means that the user was composing a message.
Sender Name	The name of the sender.
Sender	The email of the sender.

Attribute	Description
Email	
Receiver Name	The name of the receiver.
Receiver Email	The email of the receiver.
Subject	The email subject.
HTML Fragment	An HTML fragment of the email.

Additional Information

Location and Travel

Google Maps

Description	Google maps is a free web service that allows users to get directions.
Recovery method	Carving

Attribute	Description
Search Query	The term that was searched for.
Starting Location	The starting location for navigation or directions.
Center of Map	Indicates where the map was centered.

Attribute	Description
Business Latitude and Longitude	The latitude and longitude of the business location.
Source Address	The source physical address.
Destination Address	The user's desired destination.
Route Type	Indicates how the user will travel (e.g. car, bus, bike).
Additional Address	Any additional addresses within the navigation.
Street View Latitude/Longitude	The latitude and longitude information in street view.

Additional Information

Google Maps Tiles

Description	Google maps is a free web service that allows users to get directions.
Recovery method	Parsing and carving

Attribute	Description
Image	The actual picture content.
X Coordinate	The X coordinate value that Google uses to download the right tile.
Y Coordinate	The Y coordinate value that Google uses to download the right tile.
Zoom Level	The level that the user was zoomed in to the map. This value can be understood as the Z coordinate value that Google uses to download the right tile.

Additional Information

Media

AMR Files

Description	AMR Files contains voicemail messages or memos for both iOS and Android.
Recovery method	Carving

Attribute	Description
File Name	The name of the file the AMR was recovered from.
Size (Bytes)	The size of the AMR content.
MD5 Hash	An MD5 hash of the AMR content.
SHA1 Hash	A SHA1 hash of the AMR content.
Audio	The contents of an AMR file.
Media Duration (Seconds)	The duration of the audio clip in seconds.

Additional Information

For information about supported formats, see Supported media and file types. Media duration is calculated from the number of speech frames carved from the AMR data, where each speech frame has a duration of 20ms, as AMR files do not contain metadata for duration.

Audio

Description	Audio contains audio files that are recovered that use the .mp3 or .wav formats.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file.
File Extension	The extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was created.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was last modified.
File Size (Bytes)	The size of the audio file.

Attribute	Description
MD5 Hash	An MD5 hash of the audio content.
SHA1 Hash	A SHA1 hash of the audio content.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the audio clip in seconds (extracted from Exif data).
Exif Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio clip was first recorded (extracted from Exif data).
Exif Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio clip was edited (extracted from Exif data).
Timezone	The timezone setting on the recorder at the time when the audio clip was recorded (extracted from Exif data).
Software	The software used to record or modify the audio clip. This could either be the OS version of the phone used to record the audio clip or the name of the software used to edit the audio clip in post-production (extracted from Exif data).
Latitude	The GPS latitude coordinates of where the audio clip was recorded (extracted from Exif data).

Attribute	Description
Longitude	The GPS longitude coordinates of where the audio clip was recorded (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of where the audio clip was recorded (extracted from Exif data).
Exif Data	A searchable field for all raw Exif properties.

Additional Information
For information about supported formats, see Supported media and file types. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Carved Video

Description	Carved Video contains videos that are recovered using carving. Supported formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. Other container formats can also be recovered provided that their underlying packets are the same as one of the supported formats.
Recovery method	Parsing

Attribute	Description
Content Format	The format of the video.
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).

Attribute	Description
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
File Size (Bytes)	The size of the container and file.
Container Format	The format of the video container.
Saved Video Size (Bytes)	The size of the video that was saved to the database.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Additional Information

As of February 20 2020, this artifact will no longer be included under Videos. Carved Video functionality will be included in the Videos artifact instead.

Pictures

Description	Pictures contains pictures retrieved using either carving or parsing techniques. The supported formats are as follows: JPEG (.jpeg, .jpg, .jpe), PNG (.png), Bitmaps (.bmp), Graphics Interchange Format (.gif), Icons (.ico), and Tagged Image File Format (.tif, .tiff).
Recovery method	Parsing and carving

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction	The Exif extraction status indicates the level of Exif extraction that was per-

Attribute	Description
Status	formed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).

Attribute	Description
Latitude	The latitude coordinate in decimal degrees.
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS latitude (extracted from Exif data).
Longitude	The longitude coordinate in decimal degrees.
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
Altitude (meters)	The GPS coordinates of the camera where the picture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicating if the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.
Exif Data	A searchable field for all raw exif properties.

Additional Information

For information about supported formats, see Supported media and file types.
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.
To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Videos

Description	Videos contains videos that are recovered using parsing or carving. Supported formats for parsing include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. Supported carving formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. For more information about supported video formats, see Supported media and file types.
Recovery method	Parsing

Attribute	Description
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
File Name	The name of the file.
File Extension	The extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was created.

Attribute	Description
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was last modified.
File Size (Bytes)	The size of the video.
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed, including potential metadata located at the end of the video. Partial indicates that only Exif information in the header section of the video file was recovered, which should only occur with very large videos (in excess of the limit set in the options screen). Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the video in seconds (extracted from Exif data).
Original Width	The resolution of the video (extracted from Exif data).
Original	The resolution of the video (extracted from Exif data).

Attribute	Description
Height	
Exif Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was first recorded (extracted from Exif data).
Exif Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the video being recored (extracted from Exif data).
Software	The software used to record or modify the video. This could either be the OS version of the phone used to record the video or name of the software used to edit the video in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to record the video (extracted from Exif data).
Model	The model of the camera used to record the video (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to record the video (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS latitude coordinates of the camera where the video was recorded

Attribute	Description
	(extracted from Exif data).
Longitude	The GPS longitude coordinates of the camera where the video was recorded (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the video was recorded (extracted from Exif data).
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.
Content Format	The format of the carved video.
Container Format	The format of the carved video container.
Saved Video Size (Bytes)	The size of the carved video that was saved to the database.
Exif Data	A searchable field for all raw exif properties.

Additional Information

Supported formats include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. For more information about supported video formats, see Supported media and file types.

To learn more about Exif data for videos, see Extracting Exif data from videos.

To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Web Video Fragments

Description	This search recovers two distinct types of web-based video. Fragments of flash video can be left behind by many video streaming sites, such as YouTube. RTMP Frame Fragments are frames left behind by streaming sites using the RTMP protocol (widely used by webcam chat sites, including Chatroulette and Camstumble). While viewing the case, a thumbnail from a recovered video is displayed, as well as any relevant metadata. Videos can be exported to .FLV format to be played. Due to the nature of the data recovered, some video players will have issues playing the exported files. In these cases, you should try FFmpeg, VLC, and the GOM player.
Recovery method	Carving

Attribute	Description
Preview	A thumbnail preview of the video.
Content Recovered	The raw bytes that were recovered.
Metadata	Any metadata about the video.
Recovered Duration	The length of the video that was recovered.

Additional Information

Operating System

.DS_Store Records

Description	.DS_Store Records contains all the records extracted from .DS_Store files found on the computer. Each record represents a property of a file or a folder. The significance of this artifact is an indicator of high likelihood that the user of the computer was aware of these files and folders with a possibility of attributing a date to that awareness.
Recovery method	Parsing

Attribute	Description
Record Name	The name of the file or folder as stored in the .DS_Store file.
Record Type	The type of the record, or property, that is being logged in the .DS_Store file for a particular file or folder.
Record Value	The value of the property for the given file or folder.
Record Path	The full path to the file or folder.
.DS_Store Created Date/Time - UTC (yyyy-mm-dd)	The created date of the .DS_Store file from which the record was extracted.
.DS_Store Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date of the .DS_Store file from which the record was extracted.
.DS_Store Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date of the .DS_Store file from which the record was extracted.

Additional Information

In the Apple macOS operating system, .DS_Store (Desktop Services Store) is a hidden file that stores the display information of its containing folder, similar to the file desktop.ini in Microsoft Windows. The file tracks information such as icon positions, view settings, cached file size, cached last modified date, and even the choice of a background image. The .DS_Store is created and maintained by the Finder application in any folder that it accesses, even on remote file systems mounted from servers that share files (for example, via Server Message Block (SMB) protocol or the Apple Filing Protocol (AFP)). .DS_Store files are also included in archives created by macOS users, such as ZIP files, and they are backed up by some cloud file backup services. This means that the presence of .DS_Store Records artifacts on non-Mac evidence such as Windows, Mobile, or Cloud indicates that some of the data may have originated or have been accessed from a macOS computer at some point. For more information on .DS_Store files and their forensic significance see: .DS_Stores: Like Shellbags but for Macs.

Autorun Items

Description	The Autorun Items artifact describes the programs that are configured to run automatically when a certain system event occurs.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the program.
File Path	The file path to the program.
Command	The command executed when the trigger condition is met. For run items, this is the raw registry value.

Attribute	Description
Type	The type of autorun item.
Trigger Condition	The system event condition that triggers the autorun command.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the registry key containing the autorun item was last modified.
Metadata	Additional information about the autorun items.

Additional Information

File Associations

Description	File Associations contais information about application associations for files. Users or applications can set associations for file types so that when a file of a specified file type is opened, a command gets triggered by Windows.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the program that is run when a file of the specified file type is opened.
File Path	A path to the program that is run when a file of the specified file type is opened.

Attribute	Description
Command	The command that is executed when a file of the specified file type is opened.
File Type	The file type that triggers the associated command to be executed.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the registry key that contains the file association information was last modified.

Additional Information

Jump List Dest List Entries

Description	Jump lists are quick lists of recent applications or files that a user launched. The Dest List entries correspond to a list of shortcuts that are generated on a per application basis.
Recovery method	Parsing

Attribute	Description
App ID	The unique application identifier generated by Windows based on install location.
Potential App Name	A potential application name from a list of common applications and install locations.

Attribute	Description
Entry ID	The entry ID.
Data	Other data within the shortcut entry.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last time that the shortcut entry was accessed.
Pin Status	Inidcates whether the shortcut was pinned in the dest list.
Birth Volume MAC Address	The MAC address of the volume that the shortcut was created on.
New Volume MAC Address	The MAC address of the volume that the shortcut is on.
NetBios Name	The machine name on the network.
Access Count	The number of times a file is accessed through a Jump List.

Additional Information

Jump List Shortcut Entries

Description	Jump lists are quick lists of recent applications or files that a user can use.
Recovery method	Parsing

Attribute	Description
App ID	The unique application identifier generated by Windows based on install location.
Potential App Name	A potential application name from a list of common applications and install locations.
Jump List Type	The type of jump list (Automatic or Custom).
Linked Path	The path to the target file
Arguments	Any commands being passed to the target file.
Target File Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the shortcut target file was created.
Target File Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the shortcut target file was last modified.
Target File Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the shortcut target file was last accessed.
Target Attributes	Any file attributes of the target file.
Drive Type	The type of drive for the shortcut.
Serial Number	The serial number of the drive.
Volume Name	The name of the volume where the shortcut resides.
Net Bios Name	The machine name on the network.
MAC Address	The MAC address of the volume that the shortcut is on.
Target File Size (Bytes)	The size of the shortcut file.

Additional Information

LNK Files

Description	LNK files are Windows shortcut files to other files on the system.
Recovery method	Parsing and carving

Attribute	Description
Linked Path	The path to the target file.
Arguments	Any commands being passed to the target file.
Target File Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the shortcut target file was created.
Target File Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the shortcut target file was last modified.
Target File Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the shortcut target file was last accessed.
Target Attributes	Any file attributes of the target file.
Drive Type	The type of drive for the shortcut.
Serial Number	The serial number of the drive.
Volume Name	The name of the volume where the shortcut resides.

Attribute	Description
Show Command	Indicates how the shortcut should show the target when opened. This value can be SW_SHOWNORMAL, SW_SHOWMAXIMIZED, SW_SHOWMINNOACTIVE, or Unknown.
Net Bios Name	The machine name on the network.
MAC Address	The MAC address of the volume that the shortcut is on.
Target File Size (Bytes)	The size of the shortcut file.

Additional Information

Network Share Information

Description	Network Share Information contains information about mapped network drives on Windows.
Recovery method	Parsing

Attribute	Description
Network Name	The network share name.
Mapped Drive Letter	The drive letter assigned to the share.
Connection Type	The type of connection to the share.
Provider Name	The share provider.

Attribute	Description
Account	The account associated with the network share.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the share mapping was last modified.

Additional Information

Operating System Information

Description	This table provides information about the Windows installation.
Recovery method	Parsing

Attribute	Description
Operating System	The operating system.
Version Number	The version number of the operating system.
Install Date/Time - UTC (yyyy-mm-dd)	The date and time that the operating system was installed.
Product Key	The product key used to license the operating system.
Owner	The owner of the operating system license.
Displayed Com-	The computer name that is displayed to the user of the system. This value

Attribute	Description
puter Name	is updated every time the system is restarted.
Computer Name	The name of the computer. This value can be can be different than the Displayed Computer Name if the user has changed their computer's name and not updated the system.
DHCP DNS Server(s)	A comma separated list of the DHCP assigned DNS servers. This fragment represents the Domain Name Server(s) (DNS) provided from the DHCP service. This is stored in the registry as DhcpNameServer.
Operating System Version	The version of the operating system.
Build Number	The build number of the operating system.
Product ID	The product ID of the operating system.
Last Service Pack	The last service pack that was installed.
Organization	The owner of the operating license organization.
Last Shutdown Date/Time - UTC (yyyy-mm-dd)	The date and time that the operating system was last shut down.
System Root	The path to the system root.
Path	The path.
Last Access Time Enabled	Indicates whether or not last accessed times are updated on this computer. If they are, this will be Yes, otherwise this will be No.

Additional Information

Prefetch Files - Windows 8/10

Description	Prefetch files are used to speed up launching of frequently used executables. This table is for Windows 8 and 10.
Recovery method	Parsing and carving

Attribute	Description
Application Name	The application that was run.
Application Run Count	The number of times the application was run. On some versions of Windows this count can be zero, while still having run date and time data.
File Created Date/Time - UTC (yyyy-mm-dd)	The date and time when prefetch file was created.
Last Run Date/Time - UTC (yyyy-mm-dd)	The last date and time that the application was run.
File Hash	A hash of the file name and path, which is included in the file name for the prefetch file.
2nd Last Run Date/Time - UTC (yyyy-mm-dd)	The 2nd last date and time that the application was run.
3rd Last Run Date/Time - UTC (yyyy-mm-dd)	The 3rd last date and time that the application was run.

Attribute	Description
4th Last Run Date/Time - UTC (yyyy-mm-dd)	The 4th last date and time that the application was run.
5th Last Run Date/Time - UTC (yyyy-mm-dd)	The 5th last date and time that the application was run.
6th Last Run Date/Time - UTC (yyyy-mm-dd)	The 6th last date and time that the application was run.
7th Last Run Date/Time - UTC (yyyy-mm-dd)	The 7th last date and time that the application was run.
8th Last Run Date/Time - UTC (yyyy-mm-dd)	The 8th last date and time that the application was run.
Volume Name	The name of the first volume.
Volume Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the first volume was created.
Volume 2 Name	The name of the second volume.
Volume 2 Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the second volume was created.

Additional Information

Prefetch Files - Windows XP/Vista/7

Description	Prefetch files are used to speed up launching of frequently used executables. This table is for versions of Windows XP, Vista and 7.
Recovery method	Parsing and carving

Attribute	Description
Application Name	The application that was run.
Application Run Count	The number of times the application was run. On some versions of Windows this count can be zero, while still having run date and time data.
File Created Date/Time - UTC (yyyy-mm-dd)	The date and time when prefetch file was created.
Last Run Date/Time - UTC (yyyy-mm-dd)	The last date and time that the application was run.
File Hash	A hash of the file name and path, which is included in the file name for the prefetch file.
Volume Name	The name of the first volume.
Volume Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the first volume was created.
Volume 2 Name	The name of the second volume.
Volume 2 Created	The date and time when the second volume was created.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	

Additional Information

Shellbags

Description	Windows Shellbags track folder access by keeping logs of the view mode of a folder. If a shellbag record exists for a path, it has been previously viewed.
Recovery method	Parsing

Attribute	Description
Path	The path
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the path view was modified.
Mode	The view mode to which the path is currently set.
Registry Key Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the shellbags registry key was last modified.

Additional Information

Startup Items

Description	Startup Items contains the configured auto-run programs for the system at startup.
Recovery method	Parsing

Attribute	Description
Program Name	The name of the program.
Path	The path to the program.
Type	The type of autorun (Run, RunOnce, RunOnceEx, or Startup).
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the autorun was last modified.

Additional Information

Timezone Information

Description	Timezone Information contains the timezone information that is stored in the Windows registry.
Recovery method	Parsing

Attribute	Description
Current Control Set	The current control set.
Failure Control Set	The last control set with which the system did not boot correctly.
Last Known Good Control Set	The last control set with which the system booted correctly.
Current Timezone Offset (minutes)	The current timezone offset of the system, in minutes.
Standard Timezone Name	The name of the standard timezone for the system.
Standard Timezone Offset (minutes)	The offset of the standard timezone for the system, in minutes.
Standard Timezone Start Date/Time - Local Time (yyyy-mm-dd)	The date and time when the standard timezone of the system comes into effect.
Daylight Timezone Name	The name of the daylight timezone for the system.
Daylight Timezone Offset	The offset of the daylight timezone for the system, in minutes.
Daylight Timezone Start Date/Time - Local Time (yyyy-mm-dd)	The date and time when the daylight timezone of the system comes into effect.
Display	The name and offset of the currently active timezone, in a readable format.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

User Accounts - Windows

Description	User accounts are pulled from the Windows registry.
Recovery method	Parsing

Attribute	Description
User Name	The username of the account.
Full Name	The user's full name.
Type of User	The type of user (Domain User or Built-in).
Security Identifier	The security identifier of the account.
Relative Identifier	The relative identifier of the account.
Internet User Name	The internet user name of the account.
Internet UID	The internet UID of the account.
Profile Path	The path to the profile folder.
Last Local Login Date/Time - UTC (yyyy-mm-dd)	The date and time that the local user last logged in. The login time only applies to local logins, not domain users.
Last Password Change Date/Time - UTC (yyyy-mm-dd)	The date and time that the user last changed their password.
Password Required	Indicates whether the account requires a password.
Password Hint	The user's password hint.
LM Hash	The LM hash for the local account password, if one can be recovered.

Attribute	Description
NTLM Hash	The NTLM hash for the local account password, if one can be recovered.
Account Description	A description of the account.
User Group(s)	Any groups that the user is a part of.
Login Script	Any login scripts that get run when logging in as that user.
Last Incorrect Password Login Date/Time - UTC (yyyy-mm-dd)	The date and time that the user last entered the wrong password.
Local Login Count	The number of times that the local user has logged in.
Account Disabled	Indicates whether the account is disabled.

Additional Information
To learn more about the Password Required field, see Understanding the Password Required field of the User Accounts artifact.

Windows Event Logs

Description	Event logs are logs of events from any Windows application.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Event Type	The event type associated with the log. Event types are determined by the

Attribute	Description
	Event ID and, in some cases, a LoginType property indicated by the Event Data attribute. For example, an RDP event can have a number of different Event IDs, but it must have a LoginType of 10.
Security Identifier	The security user ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the event recovered, if available.
Level	The level of error.
Keywords	The event keywords.
Provider Name	The name of the event provider.
Task category	The category that the event falls under.
Computer	The computer that generated the event.
Event Data	Any event data.

Additional Information

Windows Event Logs - Firewall Events

Description	Event logs related to firewall events.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the event recovered, if available.
Rule ID	The firewall rule ID associated with the event.
Rule Name	The firewall rule name associated with the event.
Modifying User	The modifying user associated with the event, if applicable.
Modifying Application	The modifying application associated with the event, if applicable.
Direction	The direction (Inbound or Outbound) of the firewall event, if applicable.
Event Data	Any event data.

Additional Information

Windows Event Logs - Networking Events

Description	Event logs related to networking and file share setup events.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the event recovered, if available.
Subject User SID	The SID of the user who initiated the networking event.
Subject Username	The Username of the user who initiated the networking event.
Subject Domain Name	The domain name of the user who initiated the networking event.
Subject ID	The logon id of the user who initiated the networking event.
Network Share	The network share associated with the event.
Local File Path	The local file path of the network share associated with the event.
Network Name SSID	The SSID of the wifi network, if any, associated with the networking event.

Attribute	Description
Adapter Name	The local machine's network adapter, associated with the networking event.
Local MAC Address	The mac address of the local machine's network adapter, associated with the networking event.
Unique Device Identifier	The device identifier of the local machine associated with the networking event.
Event Data	Any event data.

Additional Information

Windows Event Logs - Office Alert Events

Description	Event logs related to Microsoft Office alerting events.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the event recovered, if available.

Attribute	Description
Application Name	The name of the Office application sending the alert.
Message	The short description of the alert.
Content	An unknown data value. This is often a number (such as an error code).
Version	The office application version.
Event Data	Any event data.

Additional Information

Windows Event Logs - Scheduled Task Events

Description	Event logs related to scheduled task events that are from any Windows application.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.

Attribute	Description
Event Description Summary	The description of the event recovered, if available.
Task Name	The name of the task associated with this log.
User Name	The username, if any, associated with this log.
Event Data	Any event data.

Additional Information

Windows Event Logs - Script Events

Description	Event logs related to WMI or Powershell events.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the event recovered, if available.
Security User ID	The SID of the user associated with the powershell event.

Attribute	Description
User Name	The username associated with the event.
Computer Name	The computer name associated with the event.
Process ID	The ID of the process, if any, associated with the event.
Command	The command, if any, associated with the event.
Event Data	Any event data.

Additional Information

Windows Event Logs - Service Events

Description	Event logs related to service events that are from any Windows application.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Sum-	The description of the event recovered, if available.

Attribute	Description
mary	
Service Name	The name of the service associated with this log.
Service File Name	The filename associated with the service referenced.
Service Type	The service type associated with this log.
Service Start Type	The startup type referenced in this event.
Service Account	The account corresponding to this service event.
Event Data	Any event data.

Additional Information

Windows Event Logs - Storage Device Events

Description	Event logs related to storage device events for external storage devices.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.

Attribute	Description
Event Description Summary	The description of the event recovered, if available.
Action	The action performed with the storage device, either 'Connected' or 'Disconnected'.
Total Capacity (Bytes)	Total capacity of the attached storage device, in bytes. If this field is 0, this device was disconnected.
Manufacturer	The manufacturer of the attached storage device.
Model	The model of the attached storage device.
Serial Number	The serial number of the attached storage device.
Parent ID	The Parent ID of the attached storage device.
Volume Serial Number	A list of Volume Serial Numbers of the attached storage device.
Event Data	Any event data.

Additional Information

Windows Event Logs - System Events

Description	Event logs related to networking and file share setup events.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the event recovered, if available.
Subject User SID	The SID of the user who initiated the event.
Subject Username	The Username of the user who initiated the event.
Subject Domain Name	The domain name of the user who initiated the event.
Subject ID	The logon id of the user who initiated the event.
Process Name	The name of the process associated with the event.
Process ID	The id of the process associated with the event.
Object ID	The registry object identifier associated with the event.
Object	The registry object value associated with the event.
Event Data	Any event data.

Additional Information

Windows Event Logs - User Events

Description	Event logs related to user events that are from any Windows application.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the event recovered, if available.
Logon Type	The logon type associated with the log.
Subject Username	The subject username.
Subject Domain Name	The subject domain name.
Subject User SID	The subject user security identifier.
Target Username	The target username
Target Domain Name	The target domain name.
Target User SID	The target user security identifier.
Event Data	Any event data.

Additional Information

Windows Event Logs - User PNP Events

Description	Event logs related to user PNP events that are from any Windows application.
Recovery method	Parsing and carving

Attribute	Description
Event ID	The event ID.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the event was created.
Event Record ID	The Event Record ID number that corresponds to the true order of events being created.
Event Description Summary	The description of the recovered event, if available.
Service Name	The name of the service that was added.
Driver Name	The name of the driver that was installed.
Driver Version	The version of the driver that was installed.
Driver Company	The company that produced the driver that was installed.
Driver Type	The description of the device for which the driver was installed.
Event Data	Any event data.

Additional Information

Social Networking

Bebo Live Chat

Description	Bebo Live Chat contains messages sent or received in Bebo live chat. Information found within these attributes can include the status of the message, the date and time, the sender username, the target username, and the message itself.
Recovery method	Carving

Attribute	Description
Status	The sent status of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Source ID	The account of the source.
Target ID	The account of the target.
Message	The content of the chat message.

Additional Information

Facebook

Facebook, being one of the most popular social networking sites in the world, presents numerous opportunities for gathering evidence. You can recover messages that are sent and received,

status updates and wall posts, and pages and pictures that the user views. On mobile devices, you can also recover user profiles and contacts.

Facebook can provide background information about a user, as well as evidence of who they are communicating with or associated with. Status and location updates can provide details about where a user has been and what they've been doing.

Forensic notes

The Facebook Pictures artifact represents cached pictures found on the system that originated from Facebook. When caching pictures, Facebook names the pictures using a particular format which allows forensic tools to know that they come from Facebook. These pictures can be user profile pictures, friends' pictures, or any other picture that gets cached while browsing Facebook.

Artifacts

Related resources

How important are Facebook artifacts?

Recovering Facebook artifacts

Facebook Chat

Description	Facebook Chat contains messages sent and received using Facebook Chat.
Recovery method	Carving

Attribute	Description
Profile ID	The Facebook profile ID of the sender.
Message ID	The unique ID for a specific chat message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Sender ID	The Facebook ID of the sender.
Downloaded Sender Image	The profile picture of the sender, downloaded from the Internet based on the Sender ID.
Sender Name	The name of the sender.
Receiver ID(s)	The Facebook IDs of all the receivers of the message.
Downloaded Receiver Image	The profile picture of the receiver, downloaded from the Internet based on the Receiver ID.
Receiver Names(s)	The name of the receiver.
Message	The content of the chat message.
Sender Offline	The online status of the sender.

Additional Information

Facebook Email Snippets

Description	Facebook Email Snippets contains snippets of email messages sent using Facebook.
Recovery method	Carving

Attribute	Description
Subject	The subject of the email.
Snippet	A text snippet of the body of the email.
Original Author	The author of the email.
Recent Author	The most recent author of the email.
Time Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time when the email was last updated.
Thread ID	The conversation ID.

Additional Information

Facebook Email

Description	Facebook Email contains email messages sent using Facebook.
Recovery method	Carving

Attribute	Description
Logged-In User ID	The unique Facebook ID of the user that is currently logged in.
Downloaded Logged-In User Image	The profile picture of the sender, downloaded from the Internet based on the Logged-In User ID.
Author ID	The unique Facebook ID of the author of the email.
Downloaded Author Image	The profile picture of the sender, downloaded from the

Attribute	Description
	Internet based on the Author ID.
Author Name	The name of the author.
Recipient(s)	The names of the recipients.
Subject	The subject of the email.
Time Rendered - Local Time (yyyy-mm-dd)	The time that was rendered in the web browser when the user viewed the email.
Time Last Updated Date/Time - UTC (yyyy-mm-dd)	The date and time of when the email was last updated.
Original Author	The first author of the email.
Message	The content of the email message.
Thread ID	The unique ID that represents the email trail.
Mobile	Indicates whether this email was sent from a mobile device.
Attachments	Indicates whether this email has attachments.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Facebook Pages

Description	Facebook Pages contains the content of the Facebook webpages that are cached.

Recovery method	Carving

Attribute	Description
Fragment	An HTML fragment of a Facebook webpage.

Additional Information

Facebook Pictures

Description	Facebook Pictures contains any cached pictures that are recovered that originate from Facebook.
Recovery method	Carving

Attribute	Description
File Name	The name and extension of the file the picture came from.
Image	The actual picture content.
Size (Bytes)	The size of the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.

Attribute	Description
Potential Profile ID or Picture ID	The potential Facebook profile ID or picture ID.
Tags	The tags associated with the picture content.
Skin Tone Percentage	The percentage of the image that is skin tone.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the picture was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the picture was last accessed.
MD5 Hash	The MD5 hash of the picture content.
SHA1 Hash	The SHA1 hash of the picture content.
PhotoDNA Hash	The PhotoDNA hash of the picture content.
Category	An integer that indicates the Project VIC category for the picture.

Additional Information

Facebook Status Updates/Wall Posts/Comments

Description	Facebook Status Updates/Wall Posts/Comments contains information about Facebook status updates, wall posts, and comments that are cached.
Recovery method	Carving

Attribute	Description
Sender ID	The Facebook ID of the sender.
Downloaded Sender Image	If Downloading Images from Web is enabled, the sender's profile picture can be fetched using the Facebook Graph API.
Sender Name	The name of the sender.
Receiver ID	The Facebook ID of the receiver.
Downloaded Receiver Image	If Downloading Images from Web is enabled, the receiver's profile picture can be fetched using the Facebook Graph API.
Receiver Name	The name of the receiver.
Status Update / Wall Post / Comment	The content of the status update, wall post, or comment.
Posted Date/Time - UTC (yyyy-mm-dd)	The date and time of the post.

Additional Information

Google+ Chat

Description	Google+ is a web-based social network that allows users to communicate publicly, share photos and videos, and message privately.
Recovery method	Carving

Attribute	Description
Type	Indicates whether or not the message is a sent or received message.
Email	The email address associated with the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The content of the message.

Additional Information

Instagram Pictures

Description	Instagram is a social media website where users share pictures.
Recovery method	Carving

Attribute	Description
Profile Image	The profile picture of the poster.
Downloaded Profile Image	The profile image of the poster, downloaded from the Internet.
User ID	The user ID of the poster.
User Name	The username of the poster.
Instagram Image	The picture that was posted, if found locally.
Downloaded Instagram Image	The picture that was posted, downloaded from the Internet.

Additional Information

Instagram Posts

Description	Instagram is a social media website where users share pictures.
Recovery method	Carving

Attribute	Description
Profile Image	The profile picture of the poster.
Download Profile image	The profile image of the poster, downloaded from the Internet.
Text	The content of the post.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the post was created.
User ID	The user ID of the poster.
User Name	The username of the poster.
Posted Image	The picture that was posted, if found locally.
Downloaded Posted Image	The picture that was posted, downloaded from the Internet.

Additional Information

LinkedIn Emails

Description	LinkedIn Emails contain fragments of emails sent or received using LinkedIn. These email fragments can include the to and from names, subject, date and time, and the full message. Please note that, depending on the browser, these emails will be in a compressed gzipped form which gets decompressed on-the-fly.
Recovery method	Carving

Attribute	Description
Fragment	An HTML fragment of the email.

Additional Information

MySpace Chat - User Info

Description	MySpace is a social networking website popular with music lovers.
Recovery method	Carving

Attribute	Description
User ID	The MySpace user ID.
UserName	The username used on MySpace.
Group	The group that the user is associated with (if applicable).
Image	The user's display picture.

Additional Information

MySpace Live Chat

Description	MySpace Live Chat contains messages sent or received in MySpace live chat. Information found within these attributes can include the status of the message, the date and time, the sender ID, target ID, and the message itself. Some user info is also recoverable, such as the real name or user-name associated with a MySpace ID, image URL, and other information. This information is saved to a User Info report. This has been discontinued as of 2010.
Recovery method	Carving

Attribute	Description
Status	The sent status of the message.
Message Sent Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Source ID	The account of the source.
Target ID	The account of the target.
Message	The contents of the chat message.

Additional Information

Sina Weibo Carved Searches

Description	Sina Weibo is a Chinese microblogging (weibo) website. Akin to a hybrid of Twitter and Facebook, it is one of the most popular websites in China.
Recovery method	Carving

Attribute	Description
Search Term	The keyword that was searched for.

Additional Information

Sina Weibo Microblogs

Description	Sina Weibo is a Chinese microblogging (weibo) website. Akin to a hybrid of Twitter and Facebook, it is one of the most popular websites in China.
Recovery method	Carving

Attribute	Description
Nickname	The nickname.
User ID	The user ID of the blogger.
Downloaded Profile Picture	The profile picture of the user, downloaded from the Internet based on the user ID.

Attribute	Description
Microblog Text	The content of the blog.
Posted From URL	The URL from which the blog was posted.

Additional Information

Sina Weibo Search History

Description	Sina Weibo is a Chinese microblogging (weibo) website. Akin to a hybrid of Twitter and Facebook, it is one of the most popular websites in China.
Recovery method	Parsing

Attribute	Description
Search Term	The keyword that was searched for.

Additional Information

Twitter

Description	Twitter is a social networking website that allows users to share status messages, known as tweets.
Recovery method	Carving

Attribute	Description
Name	The full name of the user.
Screen Name	The Twitter handle of the user (e.g. @username).
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the tweet was created.
Tweet Text	The content of the tweet.
In Reply To	Indicates whether the tweet was a reply to another user.
Status ID	The unique identifier for the tweet.
Tweet Source	The type of device or application that was used to create the tweet.
Geo	The geo-location of the user when they posted the tweet.
Retweeted	Indicates whether the tweet was a retweet.
Profile Img URL	The URL link to the profile picture of the user.

Additional Information

Web Related

360 Safe Browser Archived Keyword Search Terms

Description	360 Safe Browser is a web browser developed by Qihoo.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword that was searched.
URL	The URL that was invoked because of the search.

Additional Information

360 Safe Browser Archived Web History

Description	Contains all of the websites the user has gone to. Along with when they last visited the site, and how often they have visited the site.
Recovery method	Parsing

Attribute	Description
URL	The URL of the website the user visited.
Title	The title of the website the user visited.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the user last visited the website.
Visit Count	The amount of times the user has visited the website.
Typed Count	The amount of times the user has manually types the website's URL.
ID	The 360 Safe Browser identifier of the website.

Additional Information

360 Safe Browser Autofill

Description	Contains all of the values that the user has saved to fill in fields at a later date and time.
Recovery method	Parsing

Attribute	Description
Name	The name of the field to fill in.
Value	The value to perform the fill in with.
Count	The amount of times the autofill has been used.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was first created.

Additional Information

360 Safe Browser Autofill Profiles

Description	Contains all of the profiles that are used to represent a person.
Recovery method	Parsing

Attribute	Description
Name	The name the person goes by or uses.

Attribute	Description
Email	The email address to use to contact the person.
Number	The telephone number to use to contact the person.
Company	The company the person works at.
Address Line 1	The first line of the person's address. E.g. 123 Fake Street, Fake Town, Fake Country.
Address Line 2	The second line of the person's address. E.g. Suite 123 or Apt. 123.
City	The city the person lives in.
State	The state or province the person lives in.
Zipcode	The zip code the person lives in.
Country	The country the person lives in.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the person modified the profile.

Additional Information

360 Safe Browser Bookmarks

Description	Contains all of the websites the user has bookmarked.
Recovery method	Parsing

Attribute	Description
Title	The title of the website.
URL	The URL of the website.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was created.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the bookmark was last modified.
Is Folder	Is the bookmark a folder. Can be 'Yes', 'No' or '-Invalid-'.
Parent Folder	The parent folder of the bookmark.

Additional Information

360 Safe Browser Cache Records

Description	Contains all of the files and their information that has been cached by the browser.
Recovery method	Parsing

Attribute	Description
URL	The URL the file was downloaded from.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.

Attribute	Description
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was first visited.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The last time the local cache was synced with the web-server.
File Type	The type of cache file.
Content Size (Bytes)	The size of the cache file.
Image	If the content file is an image, it will be displayed here.
Content	If the file is not an image, ie. A javascript file, the raw bytes will be stored here.

Additional Information

360 Safe Browser Cookies

Description	Contains all of the cookies saved to the browser.
Recovery method	Parsing

Attribute	Description
Host	The host that created the cookie.
Name	The name of the cookie.
Value	The cookie value.

Attribute	Description
Accessed Date/Time - UTC(yyyy-mm-dd)	The date and time the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was created.
Expiration Date/Time - UTC(yyyy-mm-dd)	The date and time the cookie expires.

Additional Information

360 Safe Browser Current Downloads

Description	Contains all of the files currently being downloaded.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file being downloaded.
Download Source	The source URL where the file was downloaded.
Saved To	The local file location.
State	The current state of the download.
Opened By User	If the downloaded file was opened by the user.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.

Attribute	Description
Bytes Downloaded	The number of bytes download.
File Size (Bytes)	The size of the file being downloaded, in bytes.

Additional Information

360 Safe Browser Current Session

Description	Contains all of the sessions that are currently in use by the browser.
Recovery method	Parsing

Attribute	Description
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - (UTC)(yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.

Additional Information

360 Safe Browser Current Tabs

Description	Contains all of the open tabs in the browser.
Recovery method	Parsing

Attribute	Description
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - (UTC)(yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.

Additional Information

360 Safe Browser FavIcons

Description	Contains all of the icons that are belong to common web pages the user goes to.
Recovery method	Parsing

Attribute	Description
Page URL	The URL of the web page.

Attribute	Description
Icon URL	The URL to the icon image.
Last Updated Date/Time - UTC(yyyy-mm-dd)	The local file location.
State	The current state of the download.
Opened By User	If the downloaded file was opened by the user.
Start Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Time Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.
Bytes Downloaded	The number of bytes download.
File Size (Bytes)	The size of the file being downloaded, in bytes.

Additional Information

360 Safe Browser History Index

Description	Contains the browsing history of the user.
Recovery method	Parsing

Attribute	Description
Page URL	The web page URL.
Title	The title of the web page.

Attribute	Description
Visited on Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Body	The HTML body of the web page.

Additional Information

360 Safe Browser Last Session

Description	Contains all of the sessions that were last open.
Recovery method	Parsing

Attribute	Description
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable

Additional Information

360 Safe Browser Last Tabs

Description	Contains all of the tabs that were last open.
Recovery method	Parsing

Attribute	Description
URL	The web page URL.
Title	The title of the web page.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time the URL was last visited.
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable

Additional Information

360 Safe Browser Logins

Description	Contains all of the logins for web sites the user has saved.
Recovery method	Parsing

Attribute	Description
User Name	The user name for the web page.

Attribute	Description
Password	The password for the login of the web page.
Created Date/Time - UTC (yyyy-mm-dd)	When the login information was created.
URL	The URL to the web page.

Additional Information

360 Safe Browser Saved Credit Cards

Description	Contains all of the credit card information the user has saved.
Recovery method	Parsing

Attribute	Description
GUID	The identifier of the credit card.
Name On Card	The name on the credit card.
Expiry Date	The date the credit card is supposed to expire in format 'month-year'.
Card Number	The number of the credit card.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the credit card information was last modified.

Additional Information

360 Safe Browser Shortcuts

Description	Contains all of the shortcuts used by 360 Safe Browser for user entered URLs.
Recovery method	Parsing

Attribute	Description
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - (UTC) (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the web page.
Times Used	The number of times the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Type	The type of shortcut (for example, 'typed url' or 'bookmark').

Additional Information

360 Safe Browser Top Sites

Description	Contains all of the web sites the user goes to most often.
Recovery method	Parsing

Attribute	Description
URL	The URL to the web page.
Title	The title of the web page.
Last Updated Date/Time - (UTC) (yyyy-mm-dd)	The last time the information for the top site was updated.
Thumbnail	The thumbnail of the web page.

Additional Information

360 Safe Browser Web History

Description	Contains all of the web sites the user has gone to.
Recovery method	Parsing and carving

Attribute	Description
Date Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time the URL was first visited.

Attribute	Description
URL	The URL that was accessed by the user.
Title	The title of the web page.
Visit Count	The number of times the user accessed the URL.
Typed Count	The number of times the user has navigated to this page by typing in the address.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Last Visited Date/Time - (UTC) (yyyy-mm-dd)	The date and time the URL was last visited.

Additional Information

360 Safe Browser Web Visits

Description	A history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Title	The title of the webpage that was visited.

Attribute	Description
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

Bing Toolbar - Search History

Description	Bing toolbar is a toolbar that can be used to search the Internet using Bing.
Recovery method	Parsing

Attribute	Description
Search Term	The keyword that was searched for.
Search Date/Time - UTC (yyyy-mm-dd)	The date and time when the keyword search was conducted.

Attribute	Description
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Chrome

Google Chrome is free web browser developed by Google and is available on all major operating systems, for both mobile and desktop. As of 2016, Chrome usage represents over 70% of the world's total browser traffic.

Analyzing the websites a user visits and the time the visits occur can provide valuable insights about a user. One notable feature that Google Chrome has is that it allows users to sync their bookmarks, browsing history, and more across multiple platforms and devices by using cloud sync accounts.

Forensic notes

Web Visits vs Web History

Chrome has two distinct artifacts that are very similar nature: Chrome Web Visits and Chrome Web History. Both of these artifacts are recovered from the History database. Chrome Web History is parsed from the URLS table and only contains information for the last visited date of a particular website. Chrome Web Visits can contain multiple entries for the same website, giving the examiner a more complete look at browser usage if the user visited a website multiple times. For example, if a user visits www.magnetforensics.com six times, the Chrome Web History artifact

displays only the last time the site is visited, while the Chrome Web Visits artifact potentially displays records for all six instances. Chrome Web Visits was added in a later version of Chrome than Chrome Web History.

Carved web history

The Chrome / 360 Safe Browser / Opera Carved Web History is essentially the same as Chrome Web History except that it's recovered using carving and you may find additional deleted hits with it. The 360 Safe and Opera browsers are included in this artifact because when the data is carved, it's not possible to tell which browser the hit comes from as they're all formatted the same way.

Autofill and profile data

Chrome stores field data that the user has previously input as autofill and profile settings. For example, if you visit magnetforensics.com and login to the customer portal, browsers automatically save your username (and other details) so that you don't have to type it in each time you visit the site. This data is helpful for recovering usernames and other information that your user has filled out on various sites.

Sessions and tabs

When the system has an active session available, Chrome stores the browsing activity as the Chrome Current Session and any tabs that are open as Chrome Current tabs. The previous session and tabs are maintained in Chrome Last Session and Chrome Last Tabs so that the user can restore the last session and tabs if Chrome is closed.

Artifacts

Related resources

Artifact profile: Google Chrome

How does Chrome's 'incognito' mode affect digital forensics?

Forensic email analysis: browser artifacts you may find on a PC or laptop

Chrome Archived Keyword Search Terms

Description	Chrome Archived Keyword Search Terms contains keyword search terms that were archived by the browser.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword that was searched.
URL	The URL that was invoked by the search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Chrome Autofill

Description	Chrome Autofill contains records of the autofill values that Chrome saves for different types of text fields.
Recovery method	Parsing

Attribute	Description
Name	The name of the autofill value.

Attribute	Description
Value	The saved autofill value for this type of field.
Count	The count of this autofill.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill value was created.
Last Used Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill was last used.

Additional Information

Chrome Keyword Search Terms

Description	Chrome Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Chrome Web Visits

Description	Chrome Web Visits contains a history of the websites that the user visits (includes all visits).
Recovery method	Parsing

Attribute	Description
URL	The URL of the visited webpage.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the webpage was last visited.
Typed Count	The number of times the website was accessed by the user typing the URL (as opposed to clicking a link).
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition type is 'link'.
Visit Source	The source of the visit.

Additional Information

To learn more about the Transition Type fragment, sign in to the Support Portal to read the article Google Chrome transition types.

Edge Cache Data

Description	Information about cache data that was saved during browsing.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
URL	The URL of the cache data source.
Creation Date/Time - UTC (yyyy-mm-dd)	Date and Time when cache data was saved on the machine.
Last Modified Date/Time - UTC (yyyy-mm-dd)	Date and Time when cache data was modified on the source side.
File Type	The file type.
Visit Count	Indicates the number of times the current cache file was accessed.
Content Size (Bytes)	Cache file size in bytes.
Image	The content of the file as an image, if the file is a supported image type.
File	The content of the file in raw bytes.
Original Path	Original absolute path to the cache file stored in the database.
Relative Path	A relative path to the file based on the location of the WebCache database, or [Doesn't exist] if the file is not found.

Additional Information

This artifact allows an investigator to see the content a user views, it's origin, and how often the content is reused by the browser. By clearing the cache, the user can effectively delete these records. In some cases, records do not get deleted from the database, but in cases where the files are deleted, the original files cannot be restored.

Edge Extensions

Description	Information about the extensions/plugins installed in the user's Edge browser
Recovery method	Parsing and carving

Attribute	Description
Package Name	The Package name for the extension
Application Name	The name of the extension
Version Number	The most recent version number of the extension
Created Date/Time - UTC (yyyy-mm-dd)	The time when this extension was created
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent time the AppxManifest file for the extension was accessed (most likely the same as created time)
Last Modified Date/Time - UTC (yyyy-mm-dd)	The most recent time when the extension was updated

Additional Information

Deleted and removed extensions can't be acquired, as all of this data is fully deleted from the browser when the user deletes an extension.

Edge Favorites

Description	Edge Favorites contains information about the websites a user favorites while browsing.
Recovery method	Parsing and carving

Attribute	Description
Favorite Name	The name given to the favorite.
Is Folder	Indicates whether the item is a folder or a URL for a website (Yes if the item is a folder, and No if the item is a URL).
URL	The URL of the favorite.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the favorite was last modified.
Favicon URL	The URL of the favicon for the website.

Additional Information

This artifact allows an investigator to see the content a user views, it's origin, and how often the content is reused by the browser. By clearing the cache, the user can effectively delete these records. In some cases, records do not get deleted from the database, but in cases where the files are deleted, the original files cannot be restored.

Edge Last Session

Description	Information about the last snapshot Edge took of the user's browsing session.
Recovery method	Parsing and carving

Attribute	Description
Page URL	The URL of the web page.
Page Title	The title of the web page.
Image	The browser generated snapshot of the page.
Body	The HTML body that was saved from the page.

Additional Information

At certain time intervals, Edge takes a snapshot of the user's browsing session. Using this artifact, an investigator is able to see exactly what the user was looking at, at the time of snapshot. The time interval between snapshots is unknown. Due to the interval, it's possible for a tab to be opened and closed quick enough that the tab isn't included in a snapshot.

Edge Reading Lists

Description	Edge Reading Lists contains collections of websites that the user has saved for offline viewing.
Recovery method	Parsing and carving

Attribute	Description
Title	The title of the Reading List page.
URL	The URL of the Reading List page.
Source Address	Other source information for the Reading List page.
Picture Path	A file path to pictures associated with the Reading List page.
Deleted	Indicates whether the user has deleted the Reading List page.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time the Reading List page was added.
Last Access Date/Time - UTC (yyyy-mm-dd)	The date and time the Reading List page was last accessed.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the Reading List page was updated.

Additional Information

Edge Top Sites

Description	Edge Top Sites lists the websites that the user visits frequently in the Edge browser. Top Sites can also be removed or added by the user.
Recovery method	Parsing and carving

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the page was added as a Top Site.
Updated Date/Time - UTC (yyyy-mm-dd)	The date and time the Top Site was updated.
Favicon URL	The URL of the favicon for the Top Site.
Title	The title of the Top Site.
URL	The URL of the Top Site.

Additional Information

Edge/Internet Explorer 10-11 Content

Description	Content that the browser caches, including web pages, pictures and other resources.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
URL	The URL of the cache record.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.

Attribute	Description
Last Modified by Web Server Date/Time - UTC (yyyy-mm-dd)	The last time the content was modified on the web server. This time is reflective of when the website created the content on the page and can be before the system being examined was built.
Creation Date/Time - UTC (yyyy-mm-dd)	The date and time the content was created on the local system.
Access Count	The number of times the content was accessed through the web browser.
Filename	The filename of the cached content.
File Size (Bytes)	The size of the cache file.
Image	If the content is an image, it will be displayed here.
Content	If the file is not an image, i.e. a javascript file, the raw bytes will be stored here.

Additional Information

Edge/Internet Explorer 10-11 Cookies

Description	Site usage information that websites send to the browser when a user visits their sites.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
User	The local user on the system.
URL	The URL that the cookie is for.
Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.
Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time the cookie was updated by the web-site at the URL visited.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was created.
Access Count	The number of times the cookie was accessed.
Filename	The filename of the cookie.
File Size (Bytes)	The size of the cookie.

Additional Information

Edge/Internet Explorer 10-11 Daily/Weekly History

Description	Websites that a user visits using Internet Explorer, which are recovered from the Daily/Weekly history.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
URL	The URL that was accessed by the user.
User	The local user on the system.
Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.
Access Count	The number of times the website was accessed.
Browser Source	The directory of the browser from where the history is extracted from.

Additional Information
At the end of the week, all the daily .dat records are bundled into a weekly history and a new daily .dat file is created. This table represents a good secondary source for evidence if the main history is missing details or records.

Edge/Internet Explorer 10-11 Dependency Entries

Description	A history of the websites that the browser is required to load in order to render a page.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.

Attribute	Description
URL	The URL visited by the user.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.

Additional Information
Records for this artifact are similar to the main history, the difference being that this artifact also includes dependencies for viewed websites (for example, if a viewed website contains pictures stored on another website).

Edge/Internet Explorer 10-11 Downloads

Description	Information about the files a user downloads using the browser.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
URL	The URL of the file download.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last time the user accessed the download URL.
Redirect URL	The previous URL that led the user to the download URL.
Download Location	The local path where the file was saved.
Temporary Download Location	The local path where the file was saved temporarily (usually while downloading).

Additional Information
Internet Explorer 9 introduced a new integrated download manager which stores the details of downloaded files in a new download INDEX.DAT file. This file has a different structure to the standard INDEX.DAT files.

Edge/Internet Explorer 10-11 Main History

Description	Records of the websites that a user visits using Internet Explorer, which are recovered from the main history.
Recovery method	Parsing and carving

Attribute	Description
Entry ID	The entry ID.
URL	The URL that was accessed by the user.
User	The local user on the system.
Accessed Date/Time - UTC (yyyy-mm-dd)	The most recent visit to the URL.
Page Title	The title of the webpage.
Access Count	The number of times the website was accessed.
Browser Source	The directory of the browser from where the history is extracted from.

Additional Information

The access count does not always accurately represent the real access count. These values should only be used as an estimate.

Firefox Bookmarks

Description	Contains the bookmarks from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
URL	The URL of the website that was bookmarked.
Added Date/Time - UTC (yyyy-MM-dd)	The Date/Time the bookmark was created.
Last Modified Date/Time - UTC (yyyy-MM-dd)	The Date/Time the field was last modified.
Title	The title of the bookmark.
Bookmark Type	The type of bookmark, can be either 'Bookmark Item' or 'Bookmark Folder'.

Additional Information

Firefox Cache Records

Description	Contains all of the cached entries in the Firefox Cache Map.
Recovery method	Parsing

Attribute	Description
URL	The URL of the cache entry.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cache entry was created.
MIME Type	The MIME type of the cache data.
Content Size (Bytes)	The content size of the cached data.
Image	The image, should one be associated with the cache entry.
Content	The content, should any be associated with the cache entry.

Additional Information

Firefox Cookies

Description	Contains the cookies from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
Host	The host domain of the cookie.
Name	The name of the cookie.
Value	The value of the cookie.
Accessed Date/Time - UTC (yyyy-MM-	The Date/Time the cookie was last accessed.

Attribute	Description
dd)	
Created Date/Time - UTC (yyyy-MM-dd)	The Date/Time the cookie was created.
Expiration Date/Time - UTC (yyyy-MM-dd)	The Date/Time the cookie will expire, if it is set to expire.
Path	The path to the cookie.

Additional Information

Firefox Downloads

Description	Contains the downloads from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
File Name	The name of the file being downloaded.
Download Source	The URL of the file being downloaded.
Start Date/Time - UTC (yyyy-MM-dd)	The Date/Time the download was started.
End Date/Time - UTC (yyyy-MM-dd)	The Date/Time the download was ended.
Saved To	The path to where the file was downloaded to.

Attribute	Description
Temp Path	The path to where the file was saved during downloading.
State	The state of the download can be 'Download In Progress', 'Download Complete', 'Download Stopped', or 'Download Paused'.
Referrer	If the web page used a mirror for downloading, the path to the original download URL.

Additional Information

Firefox FavIcons

Description	Contains the fav icons from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
URL	The URL of the icon.

Additional Information

Firefox FormHistory

Description	Contains the form history from the Firefox web browser on a device.
Recovery method	Parsing and carving

Attribute	Description
Field Name	The name of the field.
Value	The value of the field.
First Used Date/Time - UTC (yyyy-MM-dd)	The Date/Time the field was first used.
Last Used Date/Time - UTC (yyyy-MM-dd)	The Date/Time the field was last used.
Times Used	The number of times the field has been used.
ID	The unique ID of the field.

Additional Information

Firefox Input History

Description	Contains the input to forms from the Firefox web browser on a device.
Recovery method	Parsing

Attribute	Description
URL	The URL the input was given to.
Input	The value that was given.
Use Count	The number of times the input has been used.
ID	The unique ID of the input.

Additional Information

Firefox Private Browsing History

Description	Contains the URLs that were loaded during a Private Browsing session from the Firefox web browser on a device.
Recovery method	Carving

Attribute	Description
URL	The URL.

Additional Information

Firefox SessionStore Artifacts

Description	Contains the web pages from the last active session from the Firefox web browser on a device.
Recovery method	Carving

Attribute	Description
Title	The title of the web page.
URL	The URL of the web page.
Referrer URL	The URL of the web page, if the web page was a redirect.

Additional Information

Firefox Web History

Description	Contains the web pages from the last active session from the Firefox web browser on a device.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the web page.
Last Visited Date/Time - UTC (yyyy-MM-dd)	The Date/Time the web page was last visited.
Title	The title of the web page.
Visit Count	The number of times the web page has been visited.
Typed	Did the user type the URL, can be 'Yes' or 'No'.

Additional Information

Firefox Web Visits

Description	Contains all of the non-archived URL visits for Firefox.
Recovery method	Parsing

Attribute	Description
URL	The URL that was visited.
Title	The title of the page that was visited.
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time that the page was visited.
Typed	Did the user type the URL, can be 'Yes' or 'No'.
Transition Type	How the transition to the page happened.

Additional Information

Flash Cookies

Description	This artifact has been deprecated and is no longer supported in AXIOM. Flash cookies are internet browser cookies that are saved when a user watches a flash video (e.g. YouTube)
Recovery method	Carving

Attribute	Description
Cookie Name	The name of the cookie.
Content	The flash content of the cookie. This content is essentially serialized ActionScript code. Primitive values such as integers and strings are shown,

Attribute	Description
	as well as more complicated data structures such as objects and arrays. A complex data structure's value is shown only once, along with an "object ID" that gets generated. For all subsequent references to that structure in the content, it's referred to by the generated object ID.
Domain	The domain or host that created the cookie.
Source	The location of where the artifact was found.
Located At	The File Offset/Physical Offset/Table name where the artifact was found within the source.
Evidence Number	The identifier assigned to the physical evidence that this artifact was recovered from.

Additional Information

Google Analytics First Visit Cookies

Description	Google Analytics First Visit Cookies contains information about Google Analytics first-visit cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Creation DateTime	The date and time when the site was first visited.

Attribute	Description
Most Recent Visit Date/Time	The date and time of the most recent session.
2nd Most Recent Visit Date/Time	The date and time of the previous session.
Hits	The number of visits.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics First Visit Cookies Carved

Description	Google Analytics First Visit Cookies Carved contains information about Google Analytics first-visit cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Creation DateTime	The date and time when the cookie was created.
Most Recent Visit Date/Time	The date and time of the most recent session.
2nd Most Recent Visit Date/Time	The date and time of the previous session.
Hits	The number of visits.

Additional Information

Google Analytics Referral Cookies

Description	Google Analytics Referral Cookies contains information about Google Analytics referral cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Cookie Source	The source URL that was used to reach the site.
Host	The domain of the URL.
Update Date/Time	The last time that the cookie was updated.
Campaign	The method of referral.
Access Method	Indicates whether the site was accessed organically or was referred.
Keyword	The keywords used to arrive at the site.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics Referral Cookies Carved

Description	Google Analytics Referral Cookies Carved contains information about Google Analytics referral cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Cookie Source	The source URL that was used to reach the site.
Host	The domain of the URL.
Update Date/Time	The last time that the cookie was updated.
Campaign	The method of referral.
Access Method	Indicates whether the site was accessed organically or was referred.
Keyword	The keywords used to arrive at the site.

Additional Information

Google Analytics Session Cookies

Description	Google Analytics Session Cookies contains information about Google Analytics session cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start time of the current sesion.
Outbound Link Events Left	
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics Session Cookies Carved

Description	Google Analytics Session Cookies Carved contains information about Google Analytics session cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start date and time of the current sesion.
Outbound Link Events Left	

Additional Information

Google Analytics URLs

Description	Google Analytics URLs contains URLs that are discovered in other artifacts that are related to Google Analytics.
Recovery method	Carving

Attribute	Description
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	The domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics URLs Carved

Description	Google Analytics URLs Carved contains information about Google Analytics URLs that are recovered using carving.
Recovery method	Carving

Attribute	Description
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	The domain of the URL. This value is carved from the source starting after 'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.

Additional Information

Google Toolbar

Description	The Google toolbar is a browser add-on where a user can perform Google searches. While there are many different features to the Google Toolbar,

	search history is the focus. Search history can be either typed or done by autocomplete. It's also possible to determine where the user's search comes from, such as whether it's from Google Search, YouTube, Google Maps, or Google News for example.
Recovery method	Parsing

Attribute	Description
Search	The keyword that was searched for.
Search Type	The type of Google search that the user completed (pictures, web, etc.).

Additional Information

Internet Explorer Cache Records

Description	Temporary Internet files that are written locally when the user views pages from the Internet.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of the cache record.
User	The local user.
Last Modified by	The last time the content was modified on the web server. This time

Attribute	Description
Web Server Date/Time - UTC (yyyy-mm-dd)	is reflective of when the website created the content on the page and can be before the system being examined was built.
Last Checked by Local Host Date/Time - UTC (yyyy-mm-dd)	The date and time the content was checked for recency on the local system.
Cache Retrieval Count	The number of times the cache record was requested by the browser.
Filename	The name of the file.
File Type	The filename of the cached content.
Content Size (Bytes)	The size of the cache file.
Image	If the content file is an image, it will be displayed here.
Content	If the file is not an image, ie. A javascript file, the raw bytes will be stored here.

Additional Information

Internet Explorer Cookie Records

Description	Site usage information that websites send to the browser when a user visits their sites.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that created the cookie.
User	The user of the system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL was accessed.
Last Modified by Web Server Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL record was modified.
Visit Count	The number of times the URL was visited.
Web Page Title	The title of the webpage.
File Name	The name of the cookie file.

Additional Information

Internet Explorer Cookies

Description	Site usage information that websites send to the browser when a user visits their sites.
Recovery method	Parsing

Attribute	Description
Host	The host that created the cookie.

Attribute	Description
Name	The name of the cookie.
Value	The cookie value.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time the cookie expires.
Flags	The flags associated with the cookie.

Additional Information

Internet Explorer Downloads

Description	Information about the files a user downloads using the browser.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL for the file download.
Date/Time - UTC (yyyy-mm-dd)	The date and time the file was downloaded.
Status	The download status.
Saved To	The local path where the file was saved.
Referrer URL	The previous URL that led the user to the download URL.
File Size (Bytes)	The size of the file in bytes.
Source IP	The IP address of the download URL.

Additional Information

Internet Explorer Favorites

Description	Web pages that the user has set as a favorite.
Recovery method	Parsing and carving

Attribute	Description
Favorite Name	The name of the favorite as it shows up in Internet Explorer.
URL	The URL of the favorite.
Modified Date/Time - UTC (yyyy-mm-dd)	The last time the user modified the favorite.
User	The user to whom the favourite belongs.
Favorites Root Location	The local path that is the root storage point for the favorite.
Folder Structure	The folder structure under which the favorite will show up in Internet Explorer.
Icon URL	The url of the icon for the favorite if an icon does exist.

Additional Information

Internet Explorer InPrivate/Recovery URLs

Description	URLs visited during InPrivate browsing that are saved in Internet Explorer recovery files (used to recover tabs in the event of a crash).
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that was visited.
File Create Date/Time - UTC (yyyy-mm-dd)	The date and time that the Internet record was created.
Description	The title of the website.
Local MAC address	The MAC address of the local machine.

Additional Information

Internet Explorer Leak Records

Description	Browser history records that are scheduled for deletion.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL visited.
Last Modified Date/Time - UTC (yyyy-mm-	The last date and time the URL record was mod-

Attribute	Description
dd)	ified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL was accessed.
Visit Count	The number of times the URL was visited.

Additional Information
LEAK artifacts are created when an error occurs while the system attempts to delete a record and the Temporary Internet File is unavailable for some reason.

Internet Explorer Main History

Description	Websites that a user visits using Internet Explorer, which are recovered from the main history.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that was visited.
User	The local user.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Last visited (2nd Timestamp) Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.

Attribute	Description
Visit Count	The number of times the user accessed the URL.
Web Page Title	The webpage title.

Additional Information

Internet Explorer PrivacIE Records

Description	Websites that a user visits while having the privacy settings turned on.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL visited.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL record was modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last date and time the URL was accessed.
Visit Count	The number of times the URL was visited.

Additional Information

Internet Explorer Typed URLs

Description	URLs that the user types directly into the address bar for Internet Explorer.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that was typed into the address bar.
Last Entered Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last typed.

Additional Information

This includes data that a user pastes into the address bar, as well as instances when a user starts typing in the address bar and clicks on a suggestion from the browser. You may also see local paths and network locations here when the user types a location in Windows Explorer.

Internet Explorer Weekly History

Description	Websites that a user visits using Internet Explorer, which are recovered from the weekly history.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that was visited.
User	The local user.
Last Visited Date/Time (local time) (yyyy-mm-dd)	The date and time the URL was last visited. This date is local to the machine that visited the website.
Weekly History File Created Date/Time - UTC (yyyy-mm-dd)	The date and time the weekly history file was created.
Visit Count	The number of times the user accessed the URL.
Web Page Title	The webpage title.

Additional Information
At the end of the week, all the daily .dat records are bundled into a weekly history and a new daily .dat file is created. This table represents a good secondary source for evidence if the main history is missing details or records.

Malware/Phishing URLs

Description	Malware/Phishing URLs contains records that are believed to be either malware or phishing related URLs.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the website.

Attribute	Description
URL	The URL of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact that the URL belongs to.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Opera Archived Keyword Search Terms

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Keyword Search Term	The keyword that was searched.
URL	The URL that was invoked by the search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Opera Archived Web History

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Date Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was first visited.
URL	The URL that was accessed by the user.
Title	The title of the webpage.
Visit Count	The number of times the user accessed the URL.
Typed Count	The number of times the user has navigated to this page by typing in the address.
Transition Type	Describes how the browser navigated to a particular URL on a particular visit. For example, if a user visits a page by clicking a link on another page, the transition type is Link.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.

Additional Information

Opera Autofill Profiles

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Name	The name of the user.
Email	The user's email.
Number	The user's phone number.
Company	The user's company.
Address Line 1	The user's address.
Address Line 2	The user's address.
City	The city where the user is from.
State	The state where the user is from.
Zipcode	The Zip Code of the user.
Country	The user's country.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the autofill profile was last modified.

Additional Information

Opera Bookmarks

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Name	The name of the bookmark.
URL	The URL that was bookmarked.
Added Date/Time - UTC (yyyy-mm-dd)	The date and time when the bookmark was added.
Parent	The parent bookmarks folder (if applicable).
Type	The type of bookmark.

Additional Information

Opera Cache Records

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that the file was downloaded from.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
First Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was first visited.
Last Sync Date/Time - UTC (yyyy-mm-dd)	The last time that the local cache was synced with the web-server.
File Type	The type of cache file.
Content Size (Bytes)	The size of the cache file.
Image	If the content file is an image, it will be displayed here.
Content	If the file is not an image, such as a JavaScript file, the raw bytes will be stored here.

Additional Information

Opera Cookies

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Host	The host that created the cookie.
Name	The name of the cookie.
Value	The cookie value.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie was created.
Expiration Date/Time - UTC (yyyy-mm-dd)	The date and time when the cookie expires.
Path	The path to the cookie.

Additional Information

Opera Current Session

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect, if applicable.

Additional Information

Opera Current Tabs

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.

Attribute	Description
Visit Count	The number of times the user accessed the URL.
Redirect URL	The URL to use to redirect, if applicable.

Additional Information

Opera Downloads

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file being downloaded.
Download Source	The source URL where the file was downloaded.
Saved To	The local file location.
State	The current state of the download.
Opened By User	If the downloaded file was opened by the user.
Start Date/Time - UTC (yyyy-mm-dd)	The date and time when the download was started.
End Date/Time - UTC (yyyy-mm-dd)	The date and time when the download finished.

Attribute	Description
Bytes Downloaded	The number of bytes downloaded.
File Size (Bytes)	The total file size in bytes.

Additional Information

Opera History Index

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Page URL	The webpage URL.
Title	The title of the webpage.
Visited On Date/Time - UTC (yyyy-mm-dd)	The date and time the URL was last visited.
Body	The HTML body of the webpage.

Additional Information

Opera Keyword Search Terms

Description	Opera Keyword Search Terms contains information about the keyword search terms that a user enters.
Recovery method	Parsing and carving

Attribute	Description
Keyword Search Term	The keyword search term that the user entered.
URL	The URL of the keyword search.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was visited.

Additional Information

Opera Last Session

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect, if applicable.

Additional Information

Opera Last Tabs

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.

Attribute	Description
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL used to redirect, if applicable.

Additional Information

Opera Logins

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that the autofill was extracted from.
Username	The username to be auto-populated.
Password	The password that was remembered.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the autofill was saved.

Additional Information

Opera Saved Credit Cards

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
GUID	A unique identifier for the credit card.
Name On Card	The name on the credit card.
Expiry Date	The date the credit card is supposed to expire in format 'month-year'.
Card Number	The credit card number.
Date Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time when the credit card information was modified.

Additional Information

Opera Search Field History

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
Search Entries	The term that was searched for.

Additional Information

Opera Shortcuts

Description	Opera Shortcuts contains all of the shortcuts used by Opera for user entered URLs.
Recovery method	Parsing and carving

Attribute	Description
Search Term	The search term as interpreted by the browser.
URL	The URL of the shortcut.
Original Search Query	The original search query entered by the user.
Last Access Date/Time - (UTC) (yyyy-mm-dd)	The last access time of the shortcut.
Web Page Title	The title of the webpage.
Times Used	The number of times the shortcut has been used.
Transition Type	Describes how the browser navigated to this URL. For example, if a user visits a page by clicking a link on another page, the transition

Attribute	Description
	type is 'link'.
Type	The type of shortcut, such as Typed URL or Bookmark.

Additional Information

Opera Top Sites

Description	Opera is a web browser developed by Opera Software. Opera uses the Blink layout engine. Opera runs on Microsoft Windows and OS X operating systems.
Recovery method	Parsing and carving

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Updated Date/Time - UTC (yyyy-mm-dd)	The last date and time when the top site was updated.
Thumbnail	A thumbnail of the webpage.

Additional Information

Opera Typed History

Description	Opera is a web browser developed by Opera Software. Opera Typed History includes those addresses that have been entered explicitly, as opposed to addresses that were visited via a link. This search will carve and parse web history from the Opera web browser, including carving and parsing the ï¿½typedï¿½ history (URLs or search terms entered by the user). The entire history file is not required and single records can be carved from live RAM captures and unallocated clusters.
Recovery method	Parsing and carving

Attribute	Description
Last Typed Date/Time - UTC (yyyy-mm-dd)	The last date and time that the content was typed.
Typed URL/Data	The content that was typed. This value could be a URL or other data.
Type	The type of content that was typed (e.g. URL).

Additional Information

Opera Web History

Description	Opera is a web browser developed by Opera Software. Web History contains recently visited webpages. Opera stores a user's browsing history so that he or she can view it later. This search will carve and parse web history

	from the Opera web browser, including carving and parsing the ï¿½-typedï¿½ history (URLs or search terms entered by the user). The entire history file is not required and single records can be carved from live RAM captures and unallocated clusters.
Recovery method	Parsing and carving

Attribute	Description
Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the user visited the web-site.
URL	The URL accessed.
Title	The webpage title.

Additional Information

Pornography URLs

Description	Pornography URLs contains records that are believed to be pornography related URLs.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the website.

Attribute	Description
URL	The URL of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact the URL belongs to.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information
You can find a list of the domains that are supported by this refined result at Pornography URLs.

Potential Browser Activity

Description	The Browser Activity artifact will recover browser-related URLs. This includes Chrome Incognito and Firefox Private Browsing URLs, HTTP request artifacts from multiple browsers, and regular web browsing artifacts. This does not include metadata such as the Windows username, dates and times, and so on. Note that some recovered URLs can be from background browser processes related to certificate authorities.
Recovery method	Carving

Attribute	Description
URL	The URL that was accessed either programmatically or by the user.
User Agent	The application that was used to request the URL. This is often the browser type (e.g. Google Chrome).

Additional Information

Rebuilt Webpages

Description	Rebuilt Webpages contains viewable webpages that are rebuilt from data that's been recovered from the cache.
Recovery method	Not applicable

Attribute	Description
Page Title	The title of the page.
URL	The cached URL.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the cache entry was created.
Domain	The domain for the cache entry.
Cache Table	The table that the cache entry originates from.
Cache RowID	The row ID that the cache entry originates from.

Additional Information

Safari Bookmarks

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows.

Recovery method	Parsing and carving

Attribute	Description
Title	The name of the bookmark.
URL	The URL that was bookmarked.

Additional Information

Safari Cache Records

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL that the file was downloaded from.
Date Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the cache file was created.
File Type	The type of the cache file.
Content Size	The size of the cache file.
Image	If the content file is an image, it will be displayed here.

Attribute	Description
Content	If the file is not an image, such as when the file is a JavaScript file, the raw bytes will be stored here.

Additional Information

Safari Downloads

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows.
Recovery method	Parsing and carving

Attribute	Description
Download URL	The URL of the file download.
Saved to Path	The local path where the download was saved.
Download Start Date/Time - UTC (yyyy-mm-dd)	The date and time the download started.
Download End Date/Time - UTC (yyyy-mm-dd)	The date and time the download finished.
Download Identifier	The unique identifier for the download.
Amount Downloaded (Bytes)	The number of bytes downloaded.
Size of Download (Bytes)	The size of the download.

Additional Information

Safari History

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows.
Recovery method	Parsing and carving

Attribute	Description
URL	The URL of a visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Redirect URL	The URL that the user was redirected to.
Title	The title of the webpage.
Visit Count	The number of times when the URL was visited.
Visit Source	Indicates whether the website was viewed on the local device or on a synced device.

Additional Information

Safari Last Session

Description	Safari is a web browser developed by Apple. Safari is installed by default

	on all Mac computers and is available for windows.
Recovery method	Parsing and carving

Attribute	Description
Tab URL	The webpage URL.
Tab Title	The title of the webpage.

Additional Information

Safari Top Sites

Description	Safari is a web browser developed by Apple. Safari is installed by default on all Mac computers and is available for windows.
Recovery method	Parsing

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Feed Last Update Time	The last date and time that the top site content was updated.
Feed URL	The URL of the RSS feed.

Additional Information

WebKit Browser Session/Tabs (Carved)

Description	WebKit Browser Sessions/Tabs contains information about the browser sessions and tabs that the user has open, while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers, such as Firefox and Safari, aren't likely to appear under this artifact.
Recovery method	Carving

Attribute	Description
URL	The webpage URL.
Title	The title of the webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
Visit Count	The number of times that the user accessed the URL.
Redirect URL	The URL to use to redirect if applicable.

Additional Information

WebKit Browser Web History (Carved)

Description	WebKit Browser Web History contains information about the websites that a user visits while using a browser built with WebKit. Some examples of browsers that use WebKit are Chrome, Opera, and 360 Safe Browser. This artifact consolidates the existing Chrome, Safe Browser, and Opera equivalents in a single artifact. Usage of other browsers aren't likely to appear under this artifact, however, some URLs found by other browsers may also be found by this artifact.
Recovery method	Carving

Attribute	Description
URL	The URL of the visited webpage.
Title	The title of the visited webpage.
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when this webpage was last visited.
Visit Count	The number of times that the webpage was visited.
Typed Count	The number of times that the website was accessed by the user typing the URL (as opposed to clicking a link).

Additional Information

YARA Rules

YARA Rule Matches

Description	The YARA artifact contains information about files and processes that matched with conditions specified in a YARA rule.
Recovery method	Parsing

Attribute	Description
File Name	The name and extension of the file whose content matched with the condition(s) from the YARA rule. The value is blank if the match came from a process (executable/application that was loaded into memory at the time of the memory dump) during memory analysis using the Comae plugin option.
File size (bytes)	The size of the file in bytes. The value is blank if the match came from a Process.
Process Name	The name of the process that matched with the condition(s) from the YARA rule. The value is blank if the match came from a file.
Process ID	The ID of the process (PID). The value is blank if the match came from a File.
Matched rule set(s)	List of the paths and respective YARA rule sets that had a match.
Matched rule	The YARA rule name that a match was found for.
Matching conditions	List of conditions for the YARA rule that had a match.

Additional Information

Windows Memory

Memory

Callbacks

Description	The Callbacks artifact contains information about kernel callbacks which can be used to monitor and/or react to events.
Recovery method	Parsing

Attribute	Description
Callback Name	The name of the callback.
Callback Subscriber Symbol	The subscriber symbol for the callback.
Callback Subscriber Address	The subscriber address for the callback.

Additional Information

Drivers

Description	The Drivers artifact contains information about loaded DLLs.
Recovery method	Parsing

Attribute	Description
Driver Name	The filename of the driver DLL.
Object Name	The unique identifying name of the driver.
Base Address	The base address for the driver.
Size	The driver file size in bytes.
File Path	The full path to the driver DLL.

Additional Information

Dynamically Loaded Libraries

Description	The Dynamically Loaded Libraries artifact contains information about DLLs loaded by a process.
Recovery method	Parsing

Attribute	Description
Process Name	The name of the process that loaded the DLL.
Process ID	The ID of the process that loaded the DLL.
File Path	The path of the process that loaded the DLL.
Load Count	The number of child DLLs found for this process.
DLL Path	The file path to the DLL.

Attribute	Description
DLL Name	The name of the DLL.
DLL Load Time	The time when the DLL was loaded.

Additional Information

Executive Object Callbacks

Description	The Windows Kernel Object Manager allows users to define custom objects in addition to the default objects. Each object has callbacks for when that object type is created, deleted, or otherwise modified. Malware can use these callbacks maliciously.
Recovery method	Parsing

Attribute	Description
Object Name	The name of the Windows object.
Close Procedure Name	The symbol name of the Close procedure the callback points to.
Close Procedure Hook	Hook information of the Close procedure if a hook is set.
Close Procedure NT	Indicates whether the Close procedure is inside the Windows kernel image.
Close Procedure Address	The kernel address of the Close procedure.
Delete Procedure Name	The symbol name of the Delete procedure the callback points to.

Attribute	Description
Delete Procedure Hook	Hook information of the Delete procedure if a hook is set.
Delete Procedure NT	Indicates whether the Delete procedure is inside the Windows kernel image.
Delete Procedure Address	The kernel address of the Delete procedure.
Dump Procedure Name	The symbol name of the Dump procedure the callback points to.
Dump Procedure Hook	Hook information of the Dump procedure if a hook is set.
Dump Procedure NT	Indicates whether the Dump procedure is inside the Windows kernel image.
Dump Procedure Address	The kernel address of the Dump procedure.
OkayToClose Procedure Name	The symbol name of the OkayToClose procedure the callback points to.
OkayToClose Procedure Hook	Hook information of the OkayToClose procedure if a hook is set.
OkayToClose Procedure NT	Indicates whether the OkayToClose procedure is inside the Windows kernel image.
OkayToClose Procedure Address	The kernel address of the OkayToClose procedure.
Open Procedure Name	The symbol name of the Open procedure the callback points to.
Open Procedure Hook	Hook information of the Open procedure if a hook is set.
Open Procedure NT	Indicates whether the Open procedure is inside the Windows

Attribute	Description
	kernel image.
Open Procedure Address	The kernel address of the Open procedure.
Parse Procedure Name	The symbol name of the Parse procedure the callback points to.
Parse Procedure Hook	Hook information of the Parse procedure if a hook is set.
Parse Procedure NT	Indicates whether the Parse procedure is inside the Windows kernel image.
Parse Procedure Address	The kernel address of the Parse procedure.
QueryName Procedure Name	The symbol name of the QueryName procedure the callback points to.
QueryName Procedure Hook	Hook information of the QueryName procedure if a hook is set.
QueryName Procedure NT	Indicates whether the QueryName procedure is inside the Windows kernel image.
QueryName Procedure Address	The kernel address of the QueryName procedure.
Security Procedure Name	The symbol name of the Security procedure the callback points to.
Security Procedure Hook	Hook information of the Security procedure if a hook is set.
Security Procedure NT	Indicates whether the Security procedure is inside the Windows kernel image.
Security Procedure	The kernel address of the Security procedure.

Attribute	Description
Address	
Object Type Flags	Flags for the Windows object type.

Additional Information

MFT

Description	The MFT artifact can be used to recover temporary files stored in the Master File Table (MFT).
Recovery method	Parsing

Attribute	Description
Name	The name of the object.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time.
Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time.
Read Date/Time - UTC (yyyy-mm-dd)	The last read date and time.
MFT Record Number	The record number of the object in the MFT.

Additional Information

Network Connections - Memory

Description	The Network Connections - Memory artifact contains information about network connections.
Recovery method	Parsing

Attribute	Description
Protocol	The connection protocol (TCP or UDP).
Local IP Address	The local IP address.
Local Port	The local port number.
Remote IP Address	The remote IP address.
Remote Port	The remote port.
State	The TCP connection state (LISTENING, ESTABLISHED, CLOSED).
Process ID	The ID of the process that owns the connection.
Owner	The ID of the process that owns the connection.
Created Date/Time - UTC (yyyy-mm-dd)	The time when the connection was created.

Additional Information

Open Handles

Description	The Open Handles artifact contains information about open handles owned by a process.
Recovery method	Parsing

Attribute	Description
Process ID	The ID of the process (PID) that owns the open handle.
Handle ID	The ID of the open handle.
Handle Type	The type of the open handle.
Details	The handle name.
Base Address	The base address of the open handle.

Additional Information

Process Security Identifiers

Description	The Process Security Identifiers artifact provides SID details of the process owner.
Recovery method	Parsing

Attribute	Description
Process Name	The name of the process.
Process ID	The ID of the process (PID).
Security Identifier	The security identifer (SID) of the process owner.
Security Identifier Name	The name of the security identifer (SID) of the process owner.

Additional Information

Processes

Description	The Processes artifact contains information about the processes that are loaded into memory.
Recovery method	Parsing

Attribute	Description
Process Name	The name of the process.
Process ID	The process ID (PID).
Parent Process ID	The ID of the parent process (PPID).
Number of Threads	The number of threads that the process contains.
Session ID	The session ID for the process.
WoW64 Process	Indicates whether the process is a WoW64 process (1 if it is a WoW64 process, 0 if not, and blank if no information is available).

Attribute	Description
Process Start Date/Time - UTC (yyyy-mm-dd)	The time when the process started.
Process Exit Date/Time - UTC (yyyy-mm-dd)	The time when the process ended.
Company	The name of the company that owns and/or wrote the process.
Description	A description of the process.
Service	Indicates whether the process is a service (1 if it is a service, 0 if not).

Additional Information

Scheduled Tasks - Memory

Description	The Scheduled Tasks artifact contains information about scheduled tasks.
Recovery method	Parsing

Attribute	Description
Author	The author of the task.
Description	A description of the task.

Attribute	Description
Scheduled Tasks Hash	The hash associated with the task in the registry.
Name	The name of the task.
Path	The path of the task in the Windows Task Scheduler.
User	The user that created the task.
Command	The command for the task.
Scheduled Tasks Parameters	Parameters for the task.

Additional Information

User Sids - Memory

Description	The User Sids artifact can be used to recover the Security Identifiers associated with a user.
Recovery method	Parsing

Attribute	Description
User Profile Path	The path of the user profile.
Security Identifier	The security identifier for the profile.

Additional Information

YARA Rules

YARA Rule Matches

Description	The YARA artifact contains information about files and processes that matched with conditions specified in a YARA rule.
Recovery method	Parsing

Attribute	Description
File Name	The name and extension of the file whose content matched with the condition(s) from the YARA rule. The value is blank if the match came from a process (executable/application that was loaded into memory at the time of the memory dump) during memory analysis using the Comae plugin option.
File size (bytes)	The size of the file in bytes. The value is blank if the match came from a Process.
Process Name	The name of the process that matched with the condition(s) from the YARA rule. The value is blank if the match came from a file.
Process ID	The ID of the process (PID). The value is blank if the match came from a File.
Matched rule set(s)	List of the paths and respective YARA rule sets that had a match.
Matched rule	The YARA rule name that a match was found for.
Matching conditions	List of conditions for the YARA rule that had a match.

Additional Information

Kindle

Advanced Search Tools

Dynamic Application Finder

Description	Artifacts found using the Dynamic Application Finder vary depending on your case's evidence. To learn more, see Processing details > Find more artifacts in the AXIOM User Guide.
Recovery method	Parsing

Attribute	Description

Additional Information

Cloud Storage

Android Dropbox

Description	Android Dropbox contains Dropbox file information recovered from a Kindle device.
Recovery method	Parsing

Attribute	Description
File Path	The path to the file.
Updated File Name	The name of the file or folder being updated.
Local Modified Date/Time - UTC (yyyy-mm-dd)	The local date and time when the file or folder was modified.
Updated Modified Date/Time - UTC (yyyy-mm-dd)	The updated date and time when the file or folder was modified.
Displayed Modified Date/Time	The displayed modified date and time.
Local File Size (Bytes)	The size of the file on the local machine.
Updated File Size (Bytes)	The updated size of the file.
Favorited	Indicates whether or not the file has been favorited.
File Version	The file version.

Additional Information

Android Dropbox Account Info

Description	Android Dropbox Account Info contains Dropbox account information recovered from a Kindle device.
Recovery method	Parsing

Attribute	Description
Display Name	The display name of the Dropbox user account.
User ID	The ID of the Dropbox user account.
Country	The country that the user account is set for.
Email	The email address associated with the account.

Additional Information

Communication

AIM

Description	America Online Instant Messenger (AIM) is a desktop chat application that allows AOL account holders to chat with one another and transfer files.
Recovery method	Parsing

Attribute	Description
Fragment	A HTML fragment of an AIM message.

Additional Information

AIM Chat Messages

Description	AIM Chat Messsages contains chat messages from a user's AIM account.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the AIM chat message.
Recipient	The recipient of the AIM chat message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the message was sent.
Message	The message body.

Additional Information

Android Kik Messenger Attachments

Description	Android Kik Messenger Attachments contains the attachments of messages from Kik Messenger from an Android device.
Recovery method	Parsing

Attribute	Description
Message ID	The ID of the message.

Attribute	Description
Attachment	The attachment.
File Metadata	Any metadata from the file.

Additional Information

Android Kik Messenger Contacts

Description	Android Kik Messenger Contacts contains information about a user's Kik Messenger contacts.
Recovery method	Parsing

Attribute	Description
Contact ID	The ID of the contact.
Display Name	The display name of the contact.
Local Name	The local name of the person on the device.
User Name	The username of the contact.
Photo URL	The URL to the profile photo of the contact.
Photo Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the contact's profile photo.
Group Member	Indicates whether the contact is a member of a group (Yes or No).

Attribute	Description
Is User Blocked	Indicates whether the contact is blocked by the local user.

Additional Information

Android Kik Messenger Messages

Description	Android Kik Messenger Messages contain Kik Messenger messages sent or received by the local user.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of the device where the data was recovered from.
Partner	The person that the local user sent a message to or received a message from.
Message Timestamp Date/Time - UTC (yyyy-mm-dd)	The timestamp of the message.
Message Body	The body of the message.
Message Status	The status of the message. The possible values are: Trying to establish connection, Message has been sent to recipient, Message has been

Attribute	Description
	delivered to recipient, Message has been read by recipient and Unknown message status.
Message Type	The type of message. The possible values are: Message Received, Message Sent, and Unknown Message Type.
Attachment	The attachment sent with the message.

Additional Information

Facebook Messenger Messages

Description	Facebook Messenger Messages contains messages recovered from Facebook Messenger.
Recovery method	Parsing and carving

Attribute	Description
Sender Name	The display name of the person sending the message.
Sender ID	The user ID of the person sending the message.
Receiver Name	The display name of the person receiving the message.
Group Name	The display name of the group receiving the message.
Receiver ID	The user ID of the person receiving the message.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	The date and time when message was sent.
Deleted Date/Time - UTC (yyyy-mm-dd)	The date and time the message was deleted from the application.
Text	The text of the message.
Message Type	The type of message that was sent. If multiple attachments were sent together, this fragment indicates the number of attachments.
Send State	Represents whether the message was sent, received or queued. This field is always empty for Android.
Media Info	The information about the media that is found. This value can be a URL to the media, a file name, or a sticker ID.
Latitude	The latitude portion of the location data that is sent with the message.
Longitude	The longitude portion of the location data that is sent with the message.
Application Name	The name of the application that generated the data (Facebook Messenger or Facebook Messenger Kids).
Thread ID	The thread ID of the message. This is also the Facebook ID of the remote party.
Message ID	The internal unique message ID.
Message Source	The source of the message creation platform.

Attribute	Description
Attachment	The recovered attachment. If the attachment is a video, the video gets segmented into multiple files. Each segment gets collected for playback in Magnet AXIOM, but the actual file size might differ from the size that AXIOM reports due to the segmentation.

Additional Information

IP Addresses - Audio/Video Calls

Description	IP Addresses of web audio/video calls show who a user was communicating with. Each instance of this artifact represents a single hop in the communication chain. By showing the relationship between multiple hops, you can determine where a call originated from and what the final destination was.
Recovery method	Carving

Attribute	Description
Call ID	The ID of the call.
Message ID	The ID of the message.
Domain	The domain used for the call.
Connection Type	The type of connection.
Origin IP Address	The originating IP address for this hop in the call.

Attribute	Description
Origin Port	The originating port for this hop in the call.
Destination IP Address	The destination IP address for this hop in the call.
Destination Port	The destination port address for this hop in the call.
Date/Time - UTC (yyyy-mm-dd)	The timestamp associated with this hop in the call.
Remote User ID	The unique ID of the remote user.
Communication Protocol	The communication protocol for this call (either UDP or TCP).
Metadata	Any additional details about the call.

Additional Information

Skype Accounts

Description	Skype Accounts contains information about the Skype accounts that are recovered, such as user information and when the account was created.
Recovery method	Parsing

Attribute	Description
Skype Name	The Skype name of the account.
Display Name	The display name of the account.

Attribute	Description
Full Name	The full name of the account.
Email(s)	The email of this account.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date when the profile was created.
Last Online Date/Time - UTC (yyyy-mm-dd)	The last time that the account was online.
Birthday (yyyy-mm-dd)	The birthday of the account.
Gender	The gender of the account.
City	The city where the account is located.
State/Province	The state/province where the account is located.
Country	The country where the account is located.
Home Phone	The home phone of this contact.
Office Phone	The office phone of this account.
Mobile Phone	The mobile phone of this account.
Homepage	The homepage of this contact.
About Info	The about info of this contact.
Profile Last Modified On Date/Time - UTC (yyyy-mm-dd)	The date when the profile was last modified.
Mood Text	The text used to express mood.
Last Used On Date/Time - UTC (yyyy-mm-dd)	The last time that the account was used.
Avatar Timestamp Date/Time - UTC (yyyy-mm-	The time that the avatar was created.

Attribute	Description
dd)	
Picture	The avatar for this contact.

Additional Information

Skype Calls

Description	Skype Calls contains information about Skype calls that occur between users.
Recovery method	Parsing and carving

Attribute	Description
Local Username	The user logged into Skype at the time of the call.
Call Initiator	The user who started the call.
Initiator Display Name	The display name of the user. This might be different from the user-name.
Recipient(s)	The users who accepted a call from the call initiator and participated in the call for a period of time.
Call Participants	The users who accepted and participated in the call from the call initiator for some duration.
Started Date/Time - UTC (yyyy-mm-dd)	The start time of the call.

Attribute	Description
Duration	The total duration of the Skype call.
Metadata	Additional details about the call extracted in XML format. This includes the duration of time each participant was in the call.

Additional Information

Skype Chat Messages

Description	Skype Chat Messages contains Skype messages sent from one user to another.
Recovery method	Parsing and carving

Attribute	Description
Profile Name	The profile name of the caller.
Message Sent Date/Time - (UTC) (yyyy-mm-dd)	The date and time when the message was sent.
Author	The author of the message.
From Display Name	The display name of who sent the message.
Message	The body of the message or a description of the action taken. For example, adding another participant to a group chat or sharing a file or

Attribute	Description
	picture.
Attachment Name	The name of the attachment that was sent. This attribute is populated when the message type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Attachment Size (Bytes)	The size of the attached file, in bytes. This attribute is populated when the message type is POSTED_FILE or POSTED_PICTURE. Otherwise, this attribute is empty.
Metadata	Additional details about the action, extracted in its original XML format.
Message Status	The status of the message.
Message Type	The type of message.
Chat ID	The ID of this chat.
Recipient	The recipient of the chat.

Additional Information

Skype Chatsync Messages

Description	Skype Chatsync Messages contains Skype messages sent from one user to another that are parsed from the Chatsync directory.
Recovery method	Parsing and carving

Attribute	Description
Local User	The local user of this message.
Chat Initiator	The initiator of the message.
Chat Partner/Group Chat ID	The other part of this message.
Message Type	The type of the message.
Message Sent Date/Time - (UTC)(yyyy-mm-dd)	The date and time when the message was sent.

Additional Information

Skype Contacts

Description	Skype Contacts contains information about Skype contacts that are recovered, which may or may not be added contacts.
Recovery method	Parsing

Attribute	Description
Profile Name	The profile name of the user.
Skype Name	The Skype name of the contact.
Display Name	The display name of this account.
Is Blocked	Indicates whether this contact is blocked.
Contact Added	Specifies whether the contact is an added contact or just cached into the

Attribute	Description
	database (1 if the contact was added, 0 otherwise). Contacts can be cached into the database for a variety of reasons, such as a suggested contact.
Full Name	The full name of this account.
Birthday	The birthday of this account.
Gender	The gender of this account.
City	The city where this account is located.
State/Province	The state or province where this account is located.
Country	The country where this account is located.
Home Phone	The home phone of this contact.
Office Phone	The office phone of this account.
Mobile Phone	The mobile phone of this account.
PSTN Number	The PSTN number of this contact.
Email(s)	The email of this account.
Homepage	The homepage of this contact.
About Info	The about info of this contact.
Profile Loaded Date/Time - (UTC)(yyyy-mm-dd)	This fragment was previously called Profile Created On Date/Time. This value of this fragment represents the date and time when a contact's profile was first created on the user's device. When the profile information is updated by the contact, the date in the database is also updated.
Mood Text	The text used to express mood.

Attribute	Description
Last Online On Date/Time - (UTC)(yyyy-mm-dd)	The last time that the account was online.
Last used On Date/Time - (UTC)(yyyy-mm-dd)	The last time that the account was used.
Avatar Timestamp Date/Time - (UTC)(yyyy-mm-dd)	The time when the avatar was created.
Image	The image for this contact.

Additional Information

Skype IP Addresses

Description	Skype IP Addresses contains IP addresses that are associated with a Skype user account.
Recovery method	Parsing and carving

Attribute	Description
Username	The username of Skype accounts.
IP Addresses	The IP addresses for the Skype user.
IP Address Type	The type of IP address (Local or Public).
Date/Time - (UTC)(yyyy-mm-dd)	The date and time.

Additional Information

Connected Devices

SIM Card ICCID

Description	SIM Card ICCID contains the ICCID number that identifies the device's SIM card.
Recovery method	Parsing

Attribute	Description
ICCID	The integrated circuit card identifier.

Additional Information

SIM Card IMSI

Description	SIM Card IMSI contains IMSI numbers used to identify the mobile subscriber, as recovered from the SIM card.
Recovery method	Parsing

Attribute	Description
IMSI	The international mobile subscriber identity.

Additional Information

SIM Card Phone Numbers

Description	SIM Card Phone Numbers contains records of all the phone numbers saved to the device SIM card. The type of number is indicated by the record type.
Recovery method	Parsing

Attribute	Description
Phone Number	The phone number for the specific record type.
Record Type	Identifies the type of record the phone number is. This value can be Abbreviated dialing numbers(ADN), Emergency call codes (ECC), Last number

Attribute	Description
	dialed (LND), MSISDN, Service dialing numbers (SDN), or Fixed dialing numbers (FDN).

Additional Information

SIM Card Service Providers

Description	SIM Card Service Providers contains the names of mobile service providers that the device has connected with, and which are recovered from the SIM card.
Recovery method	Parsing

Attribute	Description
Service Provider Name	The identity of the mobile phone service provider.

Additional Information

SIM Card SMS Messages

Description	SIM Card SMS Messages contains messages sent or received by the local user which were saved to the SIM card.
Recovery method	Parsing

Attribute	Description
Sender	The sender of the SMS message.
Recipient	The recipient of the SMS message.
Message Date/Time	For incoming messages, this timestamp indicates when the message was received by the mobile service center. For outgoing messages, there is no data available for this field.
Message	The message body of the SMS message.
Deleted	Identifies whether the message has been deleted (Yes or No).
Message Status	Identifies whether the message has been read, unread, drafted, or sent.
SMSC	The short message service center number.

Additional Information

Your Phone Contacts

Description	Your Phone Contacts contains information about contacts synced from a mobile device to a computer using Your Phone. The Your Phone application can sync data from Android and iOS devices to computers running Windows 10.
Recovery method	Parsing

Attribute	Description
Display Name	The contact's display name.
Nickname	The contact's nickname.
Phone Number	The contact's phone number.
Type	The type of phone number associated with the contact, for example Home, Mobile, or Business.
Last Time Contacted Date/Time - UTC (yyyy-mm-dd)	The last time that this contact either sent a message to, or received a message from the synced device or local user since the Your Phone application was installed.
Number of Times Contacted	The number of times the synced device or local user either sent a message to, or received a message from the contact since the Your Phone application was installed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last date and time that this contact's details were modified.

Additional Information

Your Phone Devices

Description	Your Phone Devices contains information about the devices that are synced to the user's computer by using the Your Phone application.
Recovery method	Parsing

Attribute	Description
Application Version	The version of Your Phone running on the computer.
Last Run Date/Time - UTC (yyyy-mm-dd)	The date and time when the application was last run on the computer.
Device Application Version	The version of the Your Phone companion application running on the device.
Device ID	A GUID identifier generated to uniquely identify devices within the Your Phone application.
Device Name	The name provided by the device and displayed in the user interface when referring to it.
Device Platform	The device's platform (Android or iOS).
Device Messages Synced Date	The date and time when the device last synchronized its messages data with Your Phone.
Computer Messages Synced Date	The date and time when the computer last synchronized its messages data with Your Phone.
Device Contacts Synced Date	The date and time when the device last synchronized its contacts data with Your Phone.
Computer Contacts Synced Date	The date and time when the computer last synchronized its contacts data with Your Phone.
Device Photos Synced Date	The date and time when the device last synchronized its picture data with Your Phone.
Computer Photos Synced Date	The date and time when the computer last synchronized its picture data with Your Phone.

Additional Information

Your Phone Pictures

Description	Your Phone Pictures contains information about pictures synced from a mobile device to a computer using Your Phone. The Your Phone application syncs the 25 most recently taken photos from Android and iOS devices to computers running Windows 10.
Recovery method	Not applicable

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Device ID	A GUID identifier generated to uniquely identify devices synced using the Your Phone application.
Device Name	The name of the device (as provided by the device) which is displayed in the user interface for Your Phone.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-	The last accessed date and time of the picture in the file system.

Attribute	Description
mm-dd)	
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken

Attribute	Description
	(extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture or name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS Latitude (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the pciture was taken (extracted from Exif data).

Attribute	Description
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicates whether the media is likely the original source.
Category	An integer that indicates the Project VIC category for the picture.
Exif Data	A searchable field for all raw exif properties.

Additional Information

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Your Phone SMS/MMS

Description	Your Phone SMS/MMS contains information about messages synced from a mobile device to a computer using Your Phone. The Your Phone application can sync data from Android and iOS devices to computers running Windows 10.
Recovery method	Parsing and carving

Attribute	Description
Sender	The phone number that sent the message.
Recipient(s)	The phone number(s) the message was sent to.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time when the message was sent.
Message	The message content.
Message Direction	Indicates whether the message was sent or received by the synced device or local user.
Message Type	Indicates whether the message is SMS or MMS.
Message Status	Indicates whether the message has been read.
Attachment Name	The name of the attached file, if applicable (MMS only).

Additional Information

Custom

File Signature Mismatch (Audio)

Description	File Signature Mismatch (Audio) contains identified mismatches between a known file signature header and the extension (or lack thereof) for an audio file. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Container)

Description	File Signature Mismatch (Container) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a container. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.

Attribute	Description
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Document)

Description	File Signature Mismatch (Document) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a document. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.

Attribute	Description
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Picture)

Description	File Signature Mismatch (Picture) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a picture. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file. If the MIME type is unknown, this defaults to application/octet-stream.

Attribute	Description
File Extension Type	The identified MIME type of the extension of the file. If the MIME type is unknown, this defaults to application/octet-stream. If there is no file extension, but the MIME type is known, a mismatch is is returned.
File Path	The path to the mismatched file.

Additional Information

File Signature Mismatch (Video)

Description	File Signature Mismatch (Video) contains identified mismatches between a known file signature header and the extension (or lack thereof) for a video. A mismatch might occur when a user changes or removes the extension for a file as a way to avoid detection.
Recovery method	Parsing

Attribute	Description
File Name	The file name of the identified mismatch.
File Extension	The parsed extension of the file.
File Type	The identified MIME type of the header of the file, if we don't know what the MIME type is we default to application/octet-stream.
File Extension Type	The identified MIME type of the extension of the file, if we don't know what the MIME type is we default to application/octet-stream. If there is no file

Attribute	Description
	extension, but we identify a known header MIME type we return a mismatch.
File Path	The path to the mismatched file.

Additional Information

Documents

CSV Documents

Description	CSV Documents contains CSV documents (.csv) that are located on the system.
Recovery method	Parsing

Attribute	Description
File Name	The name of the CSV document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last modified.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the CSV document was created.
File Content	The content of the CSV document.

Attribute	Description
Size (Bytes)	The size of the CSV document in bytes.
SHA1 Hash	The SHA1 hash of the contents of the document.
MD5 Hash	he MD5 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

Microsoft Excel Documents

Description	Microsoft Excel is a spreadsheet processor developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last modified on the filesystem.

Attribute	Description
Size (Bytes)	The size of the document in bytes.
Saved Size (Bytes)	The size of the document (in bytes) that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title metadata.
Subject	The subject metadata.
Authors	The authors of the document.
Keywords	The keywords metadata in the document.
Comments	The comments metadata.
Last Author	The last author to edit the document.
Last printed Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the document was created, extracted from meta-data within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

Microsoft PowerPoint Documents

Description	Microsoft PowerPoint is a presentation creator developed by Microsoft. This table captures documents created with PowerPoint, extracted from the filesystem and carved from unallocated space.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
File	The actual file.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.

Attribute	Description
Keywords	The keywords in the metadata of the file.
Comments	The comments in the metadata of the file.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information

For information about supported formats, see Supported media and file types.

Microsoft Word Documents

Description	Microsoft Word is a word processor developed by Microsoft.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was created on the filesystem.
File System Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last accessed on the filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified on the filesystem.
Size (bytes)	The size of the document.
Saved Size (bytes)	The size of the document that was recovered. Extremely large documents may not be fully recovered.
File	The actual file.
Title	The title metadata.
Subject	The subject metadata.
Authors	The authors of the document.
Keywords	The keywords metadata in the document.
Comments	The comments metadata.
Last Author	The last author to edit the document.
Last Printed Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last printed extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was last modified, extracted from metadata within the document.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the document was created, extracted from metadata within the document.
Company	The company metadata.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.

Additional Information
For information about supported formats, see Supported media and file types.

PDF Documents

Description	Portable Document Format (PDF) is a file format used to present documents in a manner independent of application software, hardware, and operating systems. This table captures documents in this file format, extracted from the filesystem and carved from unallocated space.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the document.
File System Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was created on the filesystem.
File System Last Accessed	The date and time that the file was last accessed on the

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	filesystem.
File System Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the file was last modified on the filesystem.
Size (Bytes)	The size of the document.
Saved Size (Bytes)	The size of the document that was recovered. Large documents may not be fully recovered.
Title	The title of the file.
Subject	The subject of the file.
Authors	The authors of the file.
Keywords	The keywords in the metadata of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time the document was created, extracted from metadata within the document.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time the document was last modified, extracted from metadata within the document.
File	The PDF file.
MD5 Hash	An MD5 hash of the PDF content.
SHA1 Hash	A SHA1 hash of the PDF content.

Additional Information

For information about supported formats, see Supported media and file types.

RTF Documents

Description	RTF Documents contains the information for each RTF document that was recovered from the search.
Recovery method	Parsing and carving

Attribute	Description
Filename	The name of the RTF document.
File Size (Bytes)	The size of the RTF document in bytes.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the RTF document was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the RTF document was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the RTF document was last modified.
File Content	The contents of the RTF document.
MD5 Hash	A MD5 hash of the RTF content.
SHA1 Hash	A SHA1 hash of the RTF content.

Additional Information

For information about supported formats, see Supported media and file types.

Text Documents

Description	Text documents (.txt) that are located on the system.
Recovery method	Parsing

Attribute	Description
Filename	The name of the text document.
Size (Bytes)	The size of the text document in bytes.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was last modified.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was last accessed.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the text document was created.
MD5 Hash	The MD5 hash of the contents of the document.
SHA1 Hash	The SHA1 hash of the contents of the document.
File Content	The content of the text document.

Additional Information

For information about supported formats, see Supported media and file types.

Email and Calendar

Android Emails

Description	Android Emails contains the email attributes that were recovered from a Kindle device.
Recovery method	Parsing and carving

Attribute	Description
Sync Server Date/Time - UTC (yyyy-mm-dd)	The date and time that the server synchronized the email.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the email.
Subject	The subject of the email.
Status	Identifies whether the email was 'read' or 'unread'.
Sender	Who sent the email.
Recipients	Who the email was sent to.
CC	Who was CC'd on the email.
BCC	Who was BCC'd on the email.
Attachments	The attachments in the email.
Email Body	The body of the email.

Additional Information

Android Gmail

Description	Android Gmail contains the Gmail email fragments that were recovered from a Kindle device.
Recovery method	Parsing and carving

Attribute	Description
From Address	The sender of the email.
To Address(es)	The recipient(s) of the email.
cc Address(es)	The recipients of the email that were CC'd.
bcc Address(es)	The recipients of the email that were BCC'd.
Reply Address(es)	The reply-to address for the email.
Sent Date/Time - UTC (yyyy-mm-dd)	The date when the email was sent.
Received Date/Time - UTC (yyyy-mm-dd)	The time when the email was received.
Subject	The subject of the email.
Email Snippet	A snippet of the email.
Email Body	The body of the email.

Additional Information

Samsung Email Logs

Description	Samsung Email Logs contains the email logs that were recovered from a Kindle device.
Recovery method	Parsing

Attribute	Description
Email Address	The email address of person or business that the email is with.
Date/Time - UTC (yyyy-mm-dd)	The date and time of the email.
Name	The name of the person or business that the email is with.
Subject	The subject of the email.
Message Content	The email message content.

Additional Information

Location and Travel

Google Maps

Description	Google Maps is a free web service that allows users to get directions.
Recovery method	Carving

Attribute	Description
Search Query	The term that was searched for.
Starting Location	The starting location for navigation/directions.
Center of Map	Indicates where the map was centered.
Business Latitude and Longitude	The latitude and longitude of the business location.
Source Address	The source physical address.
Destination Address	The user's desired destination.
Route Type	Indicates how the user will travel (eg. car, bus, or bike).
Additional Address	Any additional addresses within the navigation.
Street View Latitude/Longitude	The latitude and longitude information in street view.

Additional Information

Google Maps Tiles

Description	Google Maps is a free web service that allows users to get directions.
Recovery method	Parsing and carving

Attribute	Description
Image	The actual picture content.
X Coordinate	The X coordinate value that Google uses to download the right tile.

Attribute	Description
Y Coordinate	The Y coordinate value that Google uses to download the right tile.
Zoom Level	The level that the user was zoomed in to the map. This is the Z coordinate value that Google uses to download the right tile.

Additional Information

Media

AMR Files

Description	AMR Files contains voicemail messages or memos for both iOS and Android.
Recovery method	Carving

Attribute	Description
File Name	The name of the file the AMR was recovered from.
Size (Bytes)	The size of the AMR content.
MD5 Hash	An MD5 hash of the AMR content.
SHA1 Hash	A SHA1 hash of the AMR content.
Audio	The contents of an AMR file.
Media Duration (Seconds)	The duration of the audio clip in seconds.

Additional Information

For information about supported formats, see Supported media and file types. Media duration is calculated from the number of speech frames carved from the AMR data, where each speech frame has a duration of 20ms, as AMR files do not contain metadata for duration.

Audio

Description	Audio contains audio files that are recovered that use the .mp3 or .wav formats.
Recovery method	Parsing and carving

Attribute	Description
File Name	The name of the file.
File Extension	The extension of the file.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was created.
Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio file was last accessed.
Last Modified Date/Time -	The date and time when the audio file was last modified.

Attribute	Description
UTC (yyyy-mm-dd)	
File Size (Bytes)	The size of the audio file.
MD5 Hash	An MD5 hash of the audio content.
SHA1 Hash	A SHA1 hash of the audio content.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Media Duration (Seconds)	The duration of the audio clip in seconds (extracted from Exif data).
Exif Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio clip was first recorded (extracted from Exif data).
Exif Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the audio clip was edited (extracted from Exif data).
Timezone	The timezone setting on the recorder at the time when the audio clip was recorded (extracted from Exif data).

Attribute	Description
Software	The software used to record or modify the audio clip. This could either be the OS version of the phone used to record the audio clip or the name of the software used to edit the audio clip in post-production (extracted from Exif data).
Latitude	The GPS latitude coordinates of where the audio clip was recorded (extracted from Exif data).
Longitude	The GPS longitude coordinates of where the audio clip was recorded (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of where the audio clip was recorded (extracted from Exif data).
Exif Data	A searchable field for all raw Exif properties.

Additional Information

For information about supported formats, see Supported media and file types.
To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Carved Video

Description	Carved Video contains videos that are recovered using carving. Supported formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. Other container formats can also be recovered provided that their underlying packets are the same as one of the supported formats.
Recovery method	Parsing

Attribute	Description
Content Format	The format of the video.
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
File Size (Bytes)	The size of the container and file.
Container Format	The format of the video container.
Saved Video Size (Bytes)	The size of the video that was saved to the database.
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.

Additional Information

As of February 20 2020, this artifact will no longer be included under Videos. Carved Video functionality will be included in the Videos artifact instead.

Pictures

Description	Pictures contains pictures retrieved using either carving or parsing techniques. The supported formats are as follows: JPEG (.jpeg, .jpg, .jpe), PNG (.png), Bitmaps (.bmp), Graphics Interchange Format (.gif), Icons (.ico), and Tagged Image File Format (.tif, .tiff).

Recovery method	Parsing and carving

Attribute	Description
Image	The image data that was recovered.
File Name	The name and extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
File Extension	The extension of the file the picture came from. If the picture did not come from a file, this value will be blank.
Created Date/Time - UTC (yyyy-mm-dd)	The created date and time of the picture in the file system.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date and time of the picture in the file system.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date and time of the picture in the file system.
Size (Bytes)	The size of the image in bytes.
Skin Tone Percentage	The calculated percentage of skin tone in the picture.
Original Width	The original width of the picture, before any applied resizing.

Attribute	Description
Original Height	The original height of the picture, before any applied resizing.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed. Partial indicates that some of the available metadata may not have been recovered, which only occurs when carving for TIFF pictures. Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Created Date/Time - Local Time	The local date and time when the picture was first taken (extracted from Exif data).
Modified Date/Time - Local Time	The local date and time when the picture was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the picture being taken (extracted from Exif data).
Software	The software used to create or modify the picture. This could either be the OS version of the phone used to take the picture, or the name of the software used to edit the picture in post-production (extracted from Exif data).
Make	The manufacturer of the camera used to take the picture (extracted from Exif data).
Model	The model of the camera used to take the picture (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).

Attribute	Description
Lens Model	The model of the lens used to take the picture (extracted from Exif data).
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The latitude coordinate in decimal degrees.
GPS Latitude	The GPS latitude coordinates of where the picture was taken (extracted from Exif data).
GPS Latitude Reference	The cardinal coordinates of the GPS latitude (extracted from Exif data).
Longitude	The longitude coordinate in decimal degrees.
GPS Longitude	The GPS longitude coordinates of where the picture was taken (extracted from Exif data).
GPS Longitude Reference	The cardinal coordinates of the GPS longitude (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the pciture was taken (extracted from Exif data).
MD5 Hash	An MD5 hash of the image content.
SHA1 Hash	A SHA1 hash of the image content.
PhotoDNA Hash	The hash of the image content for PhotoDNA.
Potential Original Media	Indicates whether the media is likely the original source.

Attribute	Description
Category	An integer that indicates the Project VIC category for the picture.
Exif Data	A searchable field for all raw exif properties.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Videos

Description	Videos contains videos that are recovered using parsing or carving. Supported formats for parsing include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. Supported carving formats include AVI, MP4, DIVX, A3GP, M4A, QT, and WEBM. For more information about supported video formats, see Supported media and file types.
Recovery method	Parsing

Attribute	Description
Image	The thumbnail of the video (this is created by Magnet IEF/Magnet AXIOM).
File Name	The name of the file.
File Extension	The extension of the file.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was last accessed.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was last modified.
File Size (Bytes)	The size of the video.
Skin Tone Percentage	The percentage of the video that contains what appears to be visible skin.
Exif Extraction Status	The Exif extraction status indicates the level of Exif extraction that was performed. Complete indicates that a full Exif extraction was performed, including potential metadata located at the end of the video. Partial indicates that only Exif information in the header section of the video file was recovered, which should only occur with very large videos (in excess of the limit set in the options screen). Failed indicates that the information may have been corrupted and could not be recovered. Skipped indicates that the extraction was skipped.
Media Duration	The duration of the video in seconds (extracted from Exif data).

Attribute	Description
(Seconds)	
Original Width	The resolution of the video (extracted from Exif data).
Original Height	The resolution of the video (extracted from Exif data).
Exif Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was first recorded (extracted from Exif data).
Exif Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the video was edited (extracted from Exif data).
Timezone	The timezone setting on the camera at the time of the video being recored (extracted from Exif data).
Software	The software used to record or modify the video. This could either be the OS version of the phone used to record the video, or the name of the software used to edit the video in post-production (extracted from Exif data).
Make	The manufacturer of the camera that was used to record the video (extracted from Exif data).
Model	The model of the camera that was used to record the video (extracted from Exif data).
Camera Serial Number	The serial number of the camera (extracted from Exif data).
Lens Model	The model of the lens used to record the video (extracted from Exif data).

Attribute	Description
Lens Serial Number	The serial number of the lens (extracted from Exif data).
Latitude	The GPS latitude coordinates of the camera where the video was recorded (extracted from Exif data).
Longitude	The GPS longitude coordinates of the camera where the video was recorded (extracted from Exif data).
Altitude (meters)	The GPS altitude coordinates of the camera where the video was recorded (extracted from Exif data).
MD5 Hash	An MD5 hash of the video content.
SHA1 Hash	A SHA1 hash of the video content.
Category	An integer that indicates the Project VIC category for the video.
Content Format	The format of the carved video.
Container Format	The format of the carved video container.
Saved Video Size (Bytes)	The size of the carved video that was saved to the database.
Exif Data	A searchable field for all raw exif properties.

Additional Information

Supported formats include AVI, MP4, MOV, MPEG, DIVX, A3GP, ASF, WMV, DVR-MS, MKV, VOB, MOD, and WEBM. For information about supported formats, see Supported media and file types.

Additional Information
To learn more about Exif data for videos, see Extracting Exif data from videos. To learn more about the Exif Data fragment, sign in to the Support Portal to read the article Exif data fragment for Exif-enabled artifacts.

Operating System

.DS_Store Records

Description	.DS_Store Records contains all the records extracted from .DS_Store files that were found on the computer. Each record represents a property of a file or a folder. This artifact is a good indicator of whether the user of the computer was aware of these files and folders with a possibility of attributing a date to that awareness.
Recovery method	Parsing

Attribute	Description
Record Name	The name of the file or folder as stored in the .DS_Store file.
Record Type	The type of the record, or property, that is being logged in the .DS_Store file for a particular file or folder.
Record Value	The value of the property for the given file or folder.
Record Path	The full path to the file or folder.
.DS_Store Created Date/Time - UTC (yyyy-mm-dd)	The created date of the .DS_Store file from which the record was extracted.

Attribute	Description
.DS_Store Modified Date/Time - UTC (yyyy-mm-dd)	The last modified date of the .DS_Store file from which the record was extracted.
.DS_Store Accessed Date/Time - UTC (yyyy-mm-dd)	The last accessed date of the .DS_Store file from which the record was extracted.

Additional Information

In the Apple macOS operating system, .DS_Store (Desktop Services Store) is a hidden file that stores the display information of its containing folder, similar to the file desktop.ini in Microsoft Windows. The file tracks information such as icon positions, view settings, cached file size, cached last modified date, and even the choice of a background image. The .DS_Store is created and maintained by the Finder application in any folder that it accesses, even on remote file systems mounted from servers that share files (for example, via Server Message Block protocol or the Apple Filing Protocol). .DS_Store files are also included in archives created by macOS users, such as ZIP files, and they are backed up by some cloud file backup services. This means that the presence of .DS_Store Records artifacts on non-Mac evidence such as Windows, Mobile, or Cloud indicates that some of the data may have originated or have been accessed from a macOS computer at some point. For more information on .DS_Store files and their forensic significance see: .DS_Stores: Like Shellbags but for Macs.

Accounts Information

Description	Accounts Information contains the login information for all accounts on the Android device.
Recovery method	Parsing

Attribute	Description
Username	The username that is associated with the account.
Package Name	The name of the application as the device sees it.
Password	The password stored on the device to connect to the account.
Last Login Date/Time - UTC (yyyy-mm-dd)	The date and time of the last successful login.

Additional Information

Android Downloads

Description	Android Downloads contains file download information from a recovered Android device.
Recovery method	Parsing

Attribute	Description
Download Source	The URL of the file that was downloaded.
Save Location	The absolute path on the device to the downloaded file.
Last Modified Date/Time - UTC (yyyy-mm-dd)	The date and time when the file was last modified.
Notification Package	The Android package name that the download was

Attribute	Description
	initiated in.
Bytes Downloaded	The bytes that were downloaded.
Total Bytes	The total bytes of the file.

Additional Information

File System Information

Description	File System Information contains all of the relevant information about the hard drives in use by the operating system.
Recovery method	Parsing

Attribute	Description
Volume Serial Number	This field only applies to FAT and NTFS file systems. This is a 32-bit unsigned integer value that is stored in Bios Paramter Block (BPB) and is showed in a special hex format â€“ XXXX-XXXX (e.g. EABB-6573). For other file systems, the value of this field should show "n/a".
Full Volume Serial Number	This field is a 64-bit volume serial number that is only present in BPB of NTFS file system, for example AABBCCDDEEFF0011. For non-NTFS file systems, "n/a" is displayed for this field.
File System	The type of the file system (e.g. "Microsoft NTFS").
Sectors per	The number of sectors in a file system cluster (e.g. 8).

Attribute	Description
cluster	
Bytes per sector	The number of bytes per sector.
Starting Sector	The starting sector for this partition.
Ending Sector	The ending sector for this partition.
Total Sectors	Encase shows the different values for this field based on how a volume is added to the case. For example, if you add just a volume (e.g. your local C:\ drive), 123410271 is displayed for the number of sectors. However, if you add your local physical drive 0 to the case and then select your C:\ volume in the "Entries" tree (note: your C drive would most likely have another letter in this tree, e.g. E:), then the total number of sectors would be one more that the other value (i.e. 123410272). The value for this field is taken from BPB, which matches the first value. The other value is shown when the parent physical drive that is present probably comes from the partition table, and it counts VBR as well.
Total Capacity (Bytes)	This value is calculated by the total clusters multiplied by the cluster size, which shows the capacity of the file system and not the volume containing it. The size of the volume would be higher than this value.
Total Clusters	The number of clusters comprising the file system.
Unallocated Area (Bytes)	The number of unallocated bytes on the file system, which is calculated by multiplying the number of free clusters by the cluster size.
Free Clusters	The number of unallocated clusters in the file system.
Allocated Area (Bytes)	This value is determined by multiplying the number of allocated clusters by the cluster size.

Attribute	Description
Volume Name	The volume label stored in Volume Boot Record (VBR).
Volume Offset (Bytes)	The offset (in bytes) of the volume containing this file system from beginning of the disk. "0" is displayed if the image and/or drive being searched is the image of one volume. Encase shows the number of sectors for this field instead of the number of bytes.
ID	The identifier of the hard drive.
Drive Type	The type of the hard drive.

Additional Information

Social Networking

Android Instagram Posts

Description	Android Instagram Posts contains the posts that a user has put onto Instagram.
Recovery method	Parsing and carving

Attribute	Description
ID	The post ID.
Full Name	The full name of the user.
Profile Picture URL	The URL to the profile picture of the user.

Attribute	Description
Downloaded Profile Image	The downloaded profile picture.
User Name	The username on Instagram.
Posted Image URL	The URL to the image that was posted.
Downloaded Posted Image	
Text	The text for the given image.
Created Date/Time - UTC (yyyy-mm-dd)	The date that the image was created.
Taken Date/Time - UTC (yyyy-mm-dd)	The date that the image was taken.
Device Date/Time - UTC (yyyy-mm-dd)	The date that the user viewed the post.

Additional Information

Android Instagram Users

Description	Android Instagram Users contains the posts that a user has put onto Instagram.
Recovery method	Parsing and carving

Attribute	Description
ID	The ID of the user.
Full Name	The full name of the user.

Attribute	Description
Profile Picture URL	The URL to the profile picture of the user.
Downloaded Profile Image	The downloaded profile picture.
User Name	The username on Instagram.

Additional Information

Android Sina Weibo Posts

Description	Android Sina Weibo Posts contains Sina Weibo posts that have been recovered from a device.
Recovery method	Parsing and carving

Attribute	Description
User ID	The Sina Weibo user ID.
User Nickname	The user's Sina Weibo nickname.
Profile Image URL	The URL to the user's profile image.
Downloaded Profile Image	
Post	The text that the user has posted.
Post Date/Time - UTC (yyyy-mm-dd)	The date and time that the user made the post.
Post Image URL	The URL to an image that was posted.

Attribute	Description
Downloaded Post Image	
Posted Source	The source of the post.
Longitude	The longitude of the poster.
Latitude	The latitude of the poster.

Additional Information

Android Sina Weibo Private Messages

Description	Android Sina Weibo Private Messages contains Sina Weibo private messages recovered from a device.
Recovery method	Parsing and carving

Attribute	Description
User ID	The Sina Weibo user ID.
Recipient Nickname	The recipient's Sina Weibo nickname.
Profile Image URL	The URL to the user's profile image.
Downloaded Profile Image	
Message	The text that the user has sent as a message.
Message Date/Time - UTC (yyyy-mm-dd)	The date and time that the user sent the message.

Attribute	Description
Attachment Type	The MIME type of the attachment.
Attachment Local File Path	The path to the attachment on the device.

Additional Information

Facebook

Facebook, being one of the most popular social networking sites in the world, presents numerous opportunities for gathering evidence. You can recover messages that are sent and received, status updates and wall posts, and pages and pictures that the user views. On mobile devices, you can also recover user profiles and contacts.

Facebook can provide background information about a user, as well as evidence of who they are communicating with or associated with. Status and location updates can provide details about where a user has been and what they've been doing.

Forensic notes

The Facebook Pictures artifact represents cached pictures found on the system that originated from Facebook. When caching pictures, Facebook names the pictures using a particular format which allows forensic tools to know that they come from Facebook. These pictures can be user profile pictures, friends' pictures, or any other picture that gets cached while browsing Facebook.

Artifacts

Related resources

How important are Facebook artifacts?

Recovering Facebook artifacts

Android Facebook Pictures

Description	Android Facebook Pictures contains Facebook pictures that are recovered from the device.
Recovery method	Parsing

Attribute	Description
URL	The URL of the Facebook picture.
Filename	The file's absolute path on the device.
Image	The picture that was recovered.

Additional Information

Facebook Contacts

Description	Facebook Contacts contains contact information stored by the Facebook application.
Recovery method	Parsing and carving

Attribute	Description
Profile ID	The Facebook profile ID of the contact.
First Name	The Facebook contact's first name.

Attribute	Description
Last Name	The Facebook contact's last name.
Display Name	The Facebook contact's display name.
Small Picture URL	The URL to the the small picture.
Big Picture URL	The URL to the big picture.
Huge Picture URL	The URL to the huge picture.
Phone Numbers	The contact's phone numbers.

Additional Information

Facebook User/Friends

Description	Facebook User/Friends contains the profile information of the Facebook users and friends recovered from the device.
Recovery method	Parsing and carving

Attribute	Description
Friend/User	Indicates whether the information is for the user or a friend.
User ID	The user ID of the user/friend.
First Name	The first name of the user/friend.
Last Name	The last name of the user/friend.

Attribute	Description
Display Name	The display name of the user/friend.
User Image URL	The URL to the user's/friend's profile picture.
Image	The profile picture.
Phone Number	The user's/friend's phone number.
Other	Additional information about user/friend.
Email(s)	The user's/friend's email address(es).
Birthday (MM/DD/YYYY)	The user's/friend's birthday.

Additional Information

Twitter Tweets

Description	Twitter Tweets contains carved and noncarved tweets from the Twitter application.
Recovery method	Parsing and carving

Attribute	Description
Author ID	The numeric ID of the account that posted the tweet.
Status ID	The unique ID of the tweet.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the tweet was created.

Attribute	Description
Tweet	The text content of the tweet.
Tweet Source	The interface that was used to post the tweet.
Favorited	Indicates whether the tweet has been favorited.
Latitude	The latitude of the location where the tweet was posted.
Longitude	The longitude of the location where the tweet was posted.
Retweet Count	The number of times thatr the tweet has been retweeted.

Additional Information

Twitter Users

Description	Twitter Users contains information about users that were cached on the local user's device.
Recovery method	Parsing and carving

Attribute	Description
User ID	The user's Twitter user ID.
User Name	The user's Twitter username.

Attribute	Description
Full Name	The user's full name.
Profile Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the user's Twitter profile was created.
Description	The short profile description that the user writes for themself.
Web URL	The user's website URL.
Following	'Yes' if the local user is following this account, 'No' otherwise. If this attribute is empty, it's undetermined whether the local user is following this account.
Locale	The location the user is from.
Protected	Whether or not the user's account was protected.
Followers	The number of followers that the user has.
Friends	The number of friends that the user has.
Statuses	The number of different statuses that the user has had.
Image URL	The URL to the user's profile picture.
Friend Metadata Updated Date/Time - UTC (yyyy-mm-dd)	The date and time that the user's meta information was last updated.
Header URL	The URL to the user's profile banner picture.

Additional Information

Web Related

Google Analytics First Visit Cookies

Description	Google Analytics First Visit Cookies contains information about Google Analytics first-visit cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Creation DateTime	The date and time when the site was first visited.
Most Recent Visit Date/Time	The date and time of the most recent session.
2nd Most Recent Visit Date/Time	The date and time of the previous session.
Hits	The number of visits.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics First Visit Cookies Carved

Description	Google Analytics First Visit Cookies Carved contains information about Google Analytics first-visit cookies that are recovered using carving.

Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Creation DateTime	The date and time when the cookie was created.
Most Recent Visit Date/Time	The date and time of the most recent session.
2nd Most Recent Visit Date/Time	The date and time of the previous session.
Hits	The number of visits.

Additional Information

Google Analytics Referral Cookies

Description	Google Analytics Referral Cookies contains information about Google Analytics referral cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Cookie Source	The source URL used to reach the site.
Host	The domain of the URL.
Update Date/Time	The last time that the cookie was updated.

Attribute	Description
Campaign	The method of referral.
Access Method	Indicates whether the site was accessed organically or was referred.
Keyword	The keywords that were used to arrive at the site.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics Referral Cookies Carved

Description	Google Analytics Referral Cookies Carved contains information about Google Analytics referral cookies that are recovered using carving.
Recovery method	Carving

Attribute	Description
Cookie Source	The source URL used to reach the site.
Host	The domain of the URL.
Update Date/Time	The last time that the cookie was updated.
Campaign	The method of referral.
Access Method	Indicates whether the site was accessed organically or was referred.
Keyword	The keywords used to arrive at the site.

Additional Information

Google Analytics Session Cookies

Description	Google Analytics Session Cookies contains information about Google Analytics session cookies that are discovered in other artifacts.
Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start time of the current sesion.
Outbound Link Events Left	
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics Session Cookies Carved

Description	Google Analytics Session Cookies Carved contains information about Google Analytics session cookies that are recovered using carving.

Recovery method	Carving

Attribute	Description
Host	The domain of the URL.
Page Views	The number of visits to this page from the user.
Start Current Session Date/Time	The start date and time of the current sesion.
Outbound Link Events Left	

Additional Information

Google Analytics URLs

Description	Google Analytics URLs contains URLs that are discovered in other artifacts that are related to Google Analytics.
Recovery method	Carving

Attribute	Description
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	The domain of the URL. This value is carved from the source starting after

Attribute	Description
	'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.
Artifact	The name of the artifact that the URL was discovered in.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Google Analytics URLs Carved

Description	Google Analytics URLs Carved contains information about Google Analytics URLs that are recovered using carving.
Recovery method	Carving

Attribute	Description
URL	The URL of the website. If the URL cannot be recovered, the source of the URL containing all the metadata is displayed instead.
Page Title	The name of the website. This value is carved from the source starting after 'utmdt=' and ending at '&'.
Host Name	The domain of the URL. This value is carved from the source starting after

Attribute	Description
	'utmhn=' and ending at '&'.
Page Requested	The URL path to the requested page. This value is carved from the source starting after 'utmp=' and ending at '&'.
Referrer URL	The original source that referred the user to the new URL. This value is carved from the source starting after 'utmr=' and ending at '&'.

Additional Information

Kindle Silk Web History

Description	Kindle Silk Web History contains the browsing history from the Silk web browser recovered from a Kindle device.
Recovery method	Parsing and carving

Attribute	Description
Last Visited Date/Time - UTC (yyyy-mm-dd)	The date and time when the URL was last visited.
URL	The URL that was recorded in the web history for Silk.
Title	The title that the webpage displayed.
Visit Count	The number of visits to the webpage using the Silk browser.
Is Bookmarked	Indicates whether or not the URL has been bookmarked

Attribute	Description
	in the browser.
Is Favorited	Indicates whether or not the URL has been favorited in the browser.

Additional Information

Malware/Phishing URLs

Description	Malware/Phishing URLs contains records that are believed to be either malware or phishing related URLs.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the website.
URL	The URL of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact that the URL belongs to.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information

Pornography URLs

Description	Pornography URLs contains records that are believed to be pornography related URLs.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the website.
URL	The URL of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time associated with the artifact.
Artifact	The name of the artifact that the URL belongs to.
Artifact ID	The row ID of the URL in the original artifact table.

Additional Information
You can find a list of the domains that are supported by this refined result at Pornography URLs.

YARA Rules

YARA Rule Matches

Description	The YARA artifact contains information about files and processes that matched with conditions specified in a YARA rule.
Recovery method	Parsing

Attribute	Description
File Name	The name and extension of the file whose content matched with the condition(s) from the YARA rule. The value is blank if the match came from a process (executable/application that was loaded into memory at the time of the memory dump) during memory analysis using the Comae plugin option.
File size (bytes)	The size of the file in bytes. The value is blank if the match came from a Process.
Process Name	The name of the process that matched with the condition(s) from the YARA rule. The value is blank if the match came from a file.
Process ID	The ID of the process (PID). The value is blank if the match came from a File.
Matched rule set(s)	List of the paths and respective YARA rule sets that had a match.
Matched rule	The YARA rule name that a match was found for.
Matching conditions	List of conditions for the YARA rule that had a match.

Additional Information

Refined Results

Media

Potential Facebook Pictures

Description	Potential Facebook Pictures contains any cached pictures that are recovered that potentially originate from Facebook.
Notes	

Attribute	Description
File Name	The name and extension of the file that the picture came from.
Image	The actual picture content.
Size (Bytes)	The size of the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Potential Profile ID or Picture ID	The potential Facebook profile ID or picture ID.
Tags	The tags associated with the picture content.
Skin Tone Percentage	The percentage of the picture that is likely to be skin tone.
Created Date/Time - UTC	The date and time when the picture was created.

Attribute	Description
(yyyy-mm-dd)	
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the picture was last accessed.
MD5 Hash	The MD5 hash of the picture content.
SHA1 Hash	The SHA1 hash of the picture content.
PhotoDNA Hash	The PhotoDNA hash of the picture content.
Category	The category that the picture is assigned if known hashes were loaded for categorization.
Artifact	The artifact that the picture is from.
Artifact ID	The ID of the artifact where the picture comes from.

Refined Results

Classifieds URLs

Description	Classifieds URLs contains all of the URLs that are associated with classifieds websites.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the classifieds website.

Attribute	Description
URL	The URL of the classifieds website.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact that the classifieds URL is from.
Artifact ID	The ID of the artifact where the classifieds URL comes from.

Additional Information
You can find a list of the domains that are supported by this refined result at Classifieds sites domains.

Cloud Passwords and Tokens

Description	Cloud Passwords and Tokens contains cloud passwords and tokens that are found on the system. These accounts and their corresponding tokens can be used to acquire more evidence from the cloud.
Recovery method	Not applicable

Attribute	Description
User Name	The username for the cloud account.
Password/Token	The password/token for the cloud account.
Platform	The application/platform for which the account is used (e.g. Facebook, Twitter, Google, etc).

Attribute	Description
Service	The name of the service that has stored data.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time that the token was created.
Modified Date/Time - UTC (yyyy-mm-dd)	The date and time that the token item was last modified or accessed.
Artifact	The artifact that the cloud account is from.
Artifact ID	The ID of the artifact where the cloud account comes from.

Additional Information

Cloud Service URLs

Description	Cloud Service URLs contains all of the URLs that are associated with cloud service websites.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the cloud service website.
URL	The URL of the cloud service website.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.

Attribute	Description
Artifact	The artifact the cloud service URL is from.
Artifact ID	The ID of the artifact where the cloud service URL comes from.

Additional Information
You can find a list of the domains that are supported by this refined result at Cloud service domains.

Dating Sites URLs

Description	Dating Sites URLs contains all of the URLs that are associated with dating websites.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the dating website.
URL	The URL of the dating website.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact that the dating site's URL is from.
Artifact ID	The ID of the artifact where the dating site's URL comes from.

Additional Information

You can find a list of the domains that are supported by this refined result at Dating site domains.

Email Attachments

Description	Email Attachments contains any information about email attachments that have been discovered within other recovered artifacts.
Recovery method	Not applicable

Attribute	Description
File Name	The name of the attachment.
Artifact	The name of the artifact where this refined result was recovered from.
Artifact ID	The ID of the individual artifact hit where this refined result was recovered from.
Subject	The subject of the email.
File Extension	The extension of the attachment.
File Size (Bytes)	The file size of the attachment in bytes.
Created Date/Time	The date and time that the attachment was originally created.
Accessed Date/Time	The date and time that the attachment was last accessed.

Attribute	Description
Modified Date/Time	The date and time that the attachment was last modified.
MD5 Hash	An MD5 hash of the attachment.
SHA1 Hash	A SHA-1 hash of the attachment.
Skin Tone Percentage	The percentage that appears to be visible skin (if the attachment is a picture or video).
To Address(es)	The recipient(s) of the email.
From Address	The sender of the email.
Email Timestamp Date/Time	The date of the email. This field can mean different things to different email hits, so we have not defined what this column actually means.
CC	The recipients that receive the email by CC.
BCC	The recipients that receive the email by BCC.

Additional Information

Facebook URLs

Description	Facebook URLs contains all of the URLs that are associated with Facebook websites.
Recovery method	Not applicable

Attribute	Description
URL	The URL of the Facebook website.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Potential Activity	The activity that may have been performed at the URL.
Artifact	The artifact that the Facebook URL is from.
Artifact ID	The ID of the artifact where the Facebook URL comes from.

Additional Information

Google Searches

Description	Google Searches contains all of the URLs that are associated with the Google search engine.
Recovery method	Not applicable

Attribute	Description
Search Term	The string that was searched.
URL	The URL of the Google search.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Original Search Query	The query at the start of the search session.

Attribute	Description
Search Session Start Date/Time - (UTC) (yyyy-mm-dd)	The date and time when the search session started. This fragment originates from the 'ei' value in the search URL.
Previous Page Load Date/Time - (UTC) (yyyy-mm-dd)	The date and time when the page prior to the returned search result was loaded. This fragment originates from the 'sxsrf' value in the search URL.
Page Load Date/Time - (UTC) (yyyy-mm-dd)	The date and time when the returned search page was loaded. This fragment originates from the 'ved' value in the search URL.
Web Page Title	The title of the webpage.
Previous Queries	Other queries that were searched during the search session.
Artifact	The artifact that the URL is from.
Artifact ID	The ID of the artifact where the URL comes from.

Additional Information

Google Search URLs can contain important insight for your investigation. To learn more about Google Search URLs, sign in to the Support Portal to read the article Analyzing timestamps in Google Search URLs.

Google Translate

Description	Google Translate contains all of the translations done using google translate.
Recovery method	Not applicable

Attribute	Description
Language Translated From	The original language of the translation string.
Language Translated To	The language that the translation string was translated to.
Translation String	The string that was translated.
Date/Time - (UTC) (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact that the URL is from.
Artifact ID	The ID of the artifact where the URL comes from.

Additional Information

Human Trafficking Site URLs

Description	Human Trafficking Site URLs identifies any URLs that link to escort services that are associated with human trafficking operations. Many classified advertisement sites also provide escort services, but the primary purpose of the sites in this list are providing escort services that are tied to human trafficking operations.
Recovery method	Not applicable

Attribute	Description
URL	The URL of human trafficking/escort site.

Attribute	Description
Site Name	The name of the site.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Date/Time - Local Time (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact that the URL comes from.
Artifact ID	The ID of the artifact where the human trafficking/escort URL comes from.

Additional Information

You can find a list of the domains that are supported by this refined result at Human Trafficking sites.

Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Identifiers

Description	Identifiers contains all of the IDs of the people that are found on the system.
Recovery method	Not applicable

Attribute	Description
Identifier	The ID of the person.

Attribute	Description
Column Name	The column where the ID is discovered.
Artifact	The artifact that the ID comes from.
Artifact ID	The ID of the artifact where the identifier comes from.

Additional Information

Identifiers - Device

Description	Identifiers - Device contains all of the IDs of the unique devices that are found on the system.
Recovery method	Not applicable

Attribute	Description
Identifier	The ID of the device.
Column Name	The column where the ID is discovered.
Artifact	The artifact that the ID comes from.
Artifact ID	The ID of the artifact where the identifier comes from.

Additional Information

Identifiers - People

Description	Identifiers - People contains all of the IDs of the people that are found on the system.
Recovery method	Not applicable

Attribute	Description
Identifier	The ID of the person.
Column Name	The column where the ID is discovered.
Artifact	The artifact that the ID comes from.
Artifact ID	The ID of the artifact where the identifier comes from.

Additional Information

Locally Accessed Files and Folders

Description	Locally Access Files and Folders is a refined result that contains information about local and network resources that have been accessed by the user.
Recovery method	Not applicable

Attribute	Description
Path	The path to the file or folder being accessed, which might be located on a drive or on the network.
Path Type	The type of path to the file or folder. 'Drive' indicates that the accessed resource was located on a locally mounted drive, a mapped network drive, or an attached USB drive. 'Network' indicates that the accessed resource was located on the network. 'Virtual' indicates that the resource may have been accessed using a shortcut like 'Windows Explorer' from the task bar, 'Win+E', 'F1', or a scripted event during a third party program execution.
Accessed Date/Time - UTC (yyyy-mm-dd)	The last recorded date that the resource was accessed.
Accessed Date/Time - Local time (yyyy-mm-dd)	The last recorded date that the resource was accessed.
User	The local user on the system.
Access Count	The number of times that the resource was accessed.
Artifact	The type of artifact where this refined result was recovered from.
Artifact ID	The ID of the individual artifact hit where this refined result was recovered from.

Additional Information

This refined result is primarily sourced from Windows Internet Explorer WebCache. Windows Explorer and Internet Explorer are tightly coupled together, which allows us to find Windows Explorer history in the Internet Explorer Web Cache.

Parsed Search Queries

Description	Parsed Search Queries contains all of the URLs that are associated with search engines, except for Google.
Recovery method	Not applicable

Attribute	Description
Search Term	The string that was searched.
URL	The URL of the search.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Search Engine	The search engine that was used to perform the search.
Original Search Query	The query at the start of the search session.
Web Page Title	The title of the webpage.
Artifact	The artifact that the URL is from.
Artifact ID	The ID of the artifact where the URL comes from.

Additional Information

You can find a list of the domains that are supported by this refined result at Parsed Search Queries domains.

Passwords and Tokens

Description	Passwords and Tokens is a refined result that collects passwords and tokens that are associated with user accounts. This refined results only applies to accounts that are recovered from mobile and computer sources. For accounts that are recovered from cloud sources, see Cloud Passwords and Tokens.
Recovery method	Not applicable

Attribute	Description
User Name	The username associated with the account.
Password/Token	The password/token for the account.
Service	The application/website for which the account is used.
Artifact	The artifact where the account is recovered from.
Artifact ID	The ID of the artifact where the account is recovered from.

Additional Information

Potential Facebook Pictures

Description	Potential Facebook Pictures contains any cached pictures that are recovered that potentially originate from Facebook.
Recovery method	Not applicable

Attribute	Description
File Name	The name and extension of the file that the picture came from.
Image	The actual picture content.
Size (Bytes)	The size of the picture.
Original Width	The original width of the picture, before any applied resizing.
Original Height	The original height of the picture, before any applied resizing.
Potential Profile ID or Picture ID	The potential Facebook profile ID or picture ID.
Tags	The tags associated with the picture content.
Skin Tone Percentage	The percentage of the picture that is likely to be skin tone.
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the picture was created.
Last Accessed Date/Time - UTC (yyyy-mm-dd)	The date and time when the picture was last accessed.

Attribute	Description
MD5 Hash	The MD5 hash of the picture content.
SHA1 Hash	The SHA1 hash of the picture content.
PhotoDNA Hash	The PhotoDNA hash of the picture content.
Category	The category that the picture is assigned if known hashes were loaded for categorization.
Artifact	The artifact that the picture is from.
Artifact ID	The ID of the artifact where the picture comes from.

Additional Information

Potentially Unwanted Apps

Description	Potentially Unwanted Apps contains records of applications that are believed to be potentially unwanted, such as spyware applications.
Recovery method	Not applicable

Attribute	Description
Application Name	The name of the application.
Package Name	The name of the package.
Artifact	The name of the artifact that the potentially unwanted application belongs

Attribute	Description
	to.
Artifact ID	The row ID of the potentially unwanted application in the original artifact table.

Additional Information
You can find a list of the domains that are supported by this refined result at Potentially unwanted applications.

Shipping Site URLs

Description	Shipping Site URLs contains all of the URLs that are associated with shipping websites.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the shipping website.
URL	The URL of the shipping website.
Tracking Number	The tracking number that is associated with the URL.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact that the shipping website URL is from.
Artifact ID	The ID of the artifact where the shipping website URL comes from.

Additional Information

You can find a list of the domains that are supported by this refined result at Shipping site domains.

Social Media URLs

Description	Social Media URLs contains all of the URLs that are associated with social media websites.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the social media website.
URL	The URL of the social media website.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact that the social media URL is from.
Artifact ID	The ID of the artifact where the social media URL comes from.

Additional Information

You can find a list of the domains that are supported by this refined result at Social media domains.

Tax Site URLs

Description	Tax Site URLs contains all of the URLs that are from a list of websites approved by IRS tax forms.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the tax website.
URL	The URL of the tax website.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact that the URL comes from.
Artifact ID	The ID of the artifact where the tax website URL comes from.

Additional Information

You can find a list of the domains that are supported by this refined result at Tax site domains.

Tor URLs

Description	Tor URLs identifies any .onion sites that were accessed via Tor or Tor proxy.
Recovery method	Not applicable

Attribute	Description
URL	The URL of the Tor/Onion website.
Site Name	The name of the website.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Date/Time - Local Time (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact that the URL comes from.
Artifact ID	The ID of the artifact where the Tor URL comes from.

Additional Information
Because this artifact has a local timestamp, sorting and filtering might not behave as expected. To learn more, see Understanding sorting and filtering for artifacts with local timestamps.

Torrent URLs

Description	Torrent URLs contains all of the URLs that are associated with torrent websites.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the torrent website.
URL	The URL of the torrent website.

Attribute	Description
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact that the torrent URL is from.
Artifact ID	The ID of the artifact where the torrent URL comes from.

Additional Information
You can find a list of the domains that are supported by this refined result at Torrent site domains.

User Accounts

Description	User Accounts contains all of the local user's application accounts that are found on the system.
Recovery method	Not applicable

Attribute	Description
Service Name	The name of the application from which the data is coming.
User ID	The ID associated with the account.
User Name	The user name associated with the account.
Email Address(es)	The email address(es) associated with the account.
Phone Number	The phone number associated with the account.

Attribute	Description
Created Date/Time - UTC (yyyy-mm-dd)	The date and time when the account was created.
Profile Image URL	The URL to the account's profile image.
Profile Image	The account's profile image.

Additional Information

Web Chat URLs

Description	Web Chat URLs contains all of the URLs that are associated with web chat websites.
Recovery method	Not applicable

Attribute	Description
Site Name	The name of the web chat website.
URL	The URL of the web chat website.
Date/Time - UTC (yyyy-mm-dd)	The date and time that's associated with the artifact where the URL is from.
Artifact	The artifact that the web chat URL is from.
Artifact ID	The ID of the artifact where the web chat URL comes from.

Additional Information

You can find a list of the domains that are supported by this refined result at Web chat domains.

Learn more about artifacts

Parsing and carving

Parsing is a method of interpreting structured information. Magnet AXIOM can parse videos, pictures, and other documents when it encounters a file with a known extension and format. And, for applications that store their data in the known structure (like a SQLite database), Magnet AXIOM can parse the information from the database into meaningful artifacts.

Carving involves searching raw data to identify headers or other patterns. For example, when a scan identifies the following stream of bytes xFF xD8 xFF[xC0 xC4 xDB xE0- xE3 xE8 xEA xEE xFE], this signifies the beginning of a .jpg picture and is what allows Magnet AXIOM to recover artifacts even when they're recovered from unallocated space. However, carving does not necessarily indicate that the data came from unallocated space or that it was inaccessible to the user – carved artifacts can come from anywhere.

Parsing almost always recovers more data about an item than with carving. Carved results often don't include metadata about a file, such as datestamps and file locations that parsing otherwise recovers.

Supported media and file types

Magnet AXIOM can recover many different file and media types. This section highlights the artifacts that contain file and media content, identifies the file types that each artifact supports, and indicates whether Magnet AXIOM can parse or carve each type.

Videos

Magnet AXIOM can supports a number of different video container formats, using both parsing and carving, and displays results in the Videos artifact. For information about what it means for a file to be parsed or carved, see Parsing and carving.

Type	Extension	Parsing support	Carving support
Audio Video Interleave	.avi	Yes	Yes
DivX	.divx	Yes	No
Matroska	.mkv	Yes	No
MPEG-1, MPEG-2	.mpg, .mpg1, .mpg2, .mpeg, .mpeg1, .mpeg2, .m2v, .m2p, .mod, .vob	Yes	Yes
MPEG-4	.mp4, .mp4v, .f4v, .lrv, m4v	Yes	Yes
QuickTime	.3gp	Yes	Yes
	.3ga	Yes	No
	.3g2	Yes	No
	.m4a, .m4p	Yes	No
	.mov	Yes	Yes
	.qt	No	Yes

Type	Extension	Parsing support	Carving support
WebM	.webm	Yes	No
Windows Media Video	.wmv, .wm, .asf, .dvr-ms	Yes	Yes

Pictures

Any pictures that Magnet AXIOM recovers are reported in the Pictures artifact. This artifact uses both parsing and carving techniques to recover a range of different picture formats. Magnet AXIOM can also recover many different types of RAW picture formats which are typically used with cameras.

Type	Extension	Parsing support	Carving support
BMP	.bmp	Yes	Yes
	.dib	Yes	Yes
JPEG	.jpg	Yes	Yes
	.jpe	Yes	Yes
	.jpeg	Yes	Yes
GIF	.gif	Yes	Yes
HEIC	.heic	Yes	No
HEIF	.heif	Yes	No
ICO	.ico	Yes	No
iThmb	.ithmb	Yes	No

Type	Extension	Parsing support	Carving support
PNG	.png	Yes	Yes
TIFF	.tiff	Yes	Yes

Raw pictures

Extension	Parsing support	Carving support
.3fr	Yes	No
.arw	Yes	No
.cr2	Yes	No
.crw	Yes	No
.dcr	Yes	No
.dng	Yes	No
.erf	Yes	No
.k25	Yes	No
.kdc	Yes	No
.mef	Yes	No
.raw	Yes	No
.rw2	Yes	No
.sr2	Yes	No
.srf	Yes	No

Extension	Parsing support	Carving support
.x3f	Yes	No
.tif	Yes	Yes
.tiff	Yes	Yes

Audio

The Audio artifact contains the MP3 and WAV files that are recovered during a scan. On mobile devices, the AMR Files artifact contains voicemail messages.

Type	Extension	Parsing support	Carving support
AMR	.amr	No	Yes
MP3	.mp3	Yes	Yes
WAV	.wav	Yes	No

Documents

Documents are recovered in the following artifacts: OpenOffice Calc Documents , CSV Documents , Microsoft Excel Documents , Hangul Word Processor , OpenOffice Impress Documents , PDF Documents , Microsoft PowerPoint Documents , RTF Documents , Text Documents , Microsoft Word Documents , OpenOffice Writer Documents .

Type	Extension	Parsing support	Carving support
CSV	.csv	Yes	No
Hangul Word	.hml .hwpx	Yes	Yes

Type	Extension	Parsing support	Carving support
	.hwp		
	.hwt		
Microsoft Excel	.xlm	Yes	Yes
	.xls		
	.xlsx		
	.xlt		
	.xltx		
	.xlsm		
Microsoft Power-Point	.pot	Yes	Yes
	.potm		
	.potx		
	.ppam		
	.pps		
	.ppsm		
	.ppsx		
	.ppt		
	.pptm		
	.pptx		
	.sldm		
	.sldx		

Type	Extension	Parsing support	Carving support
Microsoft Word	.doc	Yes	Yes
	.docm		
	.docx		
	.dot		
	.dotx		
	.dotm		
OpenOffice Calc	.odf	Yes	Yes
	.ods		
	.sxc		
	.stc		
OpenOffice Impress	.odp	Yes	Yes
	.otp		
	.sxi		
	.sti		
OpenOffice Writer	.odm	Yes	Yes
	.odt		
	.ott		
	.swx		
	.stw		

Type	Extension	Parsing support	Carving support
PDF	.pdf	Yes	Yes
RTF	.rtf	Yes	Yes
Text	.txt	Yes	No

Recovered artifacts by carving only

By default, AXIOM Process will parse and carve for all the artifacts you have selected. Selecting to parse only selected artifacts will not include artifacts that are found exclusively by carving. The below table lists artifacts that are recovered by carving only for the installed version of AXIOM Process.

Note: Carved artifacts can come from anywhere on a user's system, not only from unallocated space or inaccessible locations.

Android

Carved only artifacts:

- Amazon Alexa Web Resource
- AMR Files
- Coinomi Transactions
- Google Analytics First Visit Cookies Carved
- Google Analytics Referral Cookies Carved
- Google Analytics Session Cookies Carved
- Google Analytics URLs Carved
- Google Maps

Carved only artifacts:

- Google Maps Directions
- Google Meet Meeting History
- IP Addresses - Audio/Video Calls
- Potential Browser Activity
- Snapchat Photo Transfers - Android
- Torrent File Fragments
- WebKit Browser Web History (Carved)

Chromebook

Carved only artifacts:

- Google Analytics First Visit Cookies Carved
- Google Analytics Referral Cookies Carved
- Google Analytics Session Cookies Carved
- Google Analytics URLs Carved
- Google Maps
- IP Addresses - Audio/Video Calls

Cloud

Carved only artifacts:

- Adium Chat
- AIM

Carved only artifacts:

- Amazon Alexa Web Resource
- AMR Files
- Ares Downloads
- Ares Incomplete Downloads
- Ares Search Keywords
- Ares Shared Files
- Ashley Madison
- Backpage Ads
- Bebo
- Bitcoin Debug Logs
- Carbonite Log File
- Chatroulette
- Chatstep Messages
- Coinomi Transactions
- Craigslist Ads
- Dropbox (Web-based)
- Facebook Chat
- Facebook Email
- Facebook Email Snippets
- Facebook Pages
- Facebook Status Updates/Wall Posts/Comments
- Firefox Private Browsing History
- Flash Cookies
- Flickr

Carved only artifacts:

- Frostwire.props Files
- Gigatribe Chat
- Gmail Fragments
- Gmail Webmail
- GMX Webmail
- Google Analytics First Visit Cookies Carved
- Google Analytics Referral Cookies Carved
- Google Analytics Session Cookies Carved
- Google Analytics URLs Carved
- Google Docs
- Google Drive
- Google Maps
- Google Maps Directions
- Google Meet Meeting History
- Google+ Chat
- GoogleTalk
- Hotmail Webmail
- Hushmail Fragments
- Hushmail Inbox
- IE InPrivate/Recovery URLs
- Instagram Images
- Instagram Posts
- Internet Explorer Cookie Records
- Internet Explorer Daily History

Carved only artifacts:

- Internet Explorer Downloads
- Internet Explorer Leak Records
- Internet Explorer Main History
- Internet Explorer PrivacIE Records
- Internet Explorer Redirect Records
- Internet Explorer Weekly History
- IP Addresses - Audio/Video Calls
- Limewire 5.x Searches
- Limewire.props Files
- Limewire/Frostwire 4.x Searches
- LinkedIn Emails
- Lync / OC Calls
- Lync / OC File Transfers
- Lync / OC Fragments
- Lync / OC Messages
- Mail.ru
- Mailinator Inbox Access
- Mailinator Snippets
- mIRC
- MSN Plus!
- MSN Protocol Fragments
- MySpace Chat - Messages
- MySpace Chat - User Info
- MySpace Inbox Messages

Carved only artifacts:

- Omegle
- Opera Search Field History
- Opera Typed History
- Outlook Web App Email Fragments
- Outlook Web App Email Inbox
- Outlook Webmail Fragments
- Outlook Webmail Inbox
- Outlook Webmail Inbox Fragments
- Paltalk Chat
- Plenty of Fish
- Potential Browser Activity
- QQ
- Second Life
- SharePoint Discussions
- SharePoint Recycle Bin
- SharePoint Shared Documents
- Sina Weibo Carved Searches
- Sina Weibo Microblogs
- Snapchat Photo Transfers - Android
- Torrent File Fragments
- Trillian
- Twitter
- Usenet Binary Files
- VK Wall Posts

Carved only artifacts:

- VK Web Messages
- Web Video Fragments
- WebKit Browser Session/Tabs (Carved)
- WebKit Browser Web History (Carved)
- WhatsApp Messages - Windows
- Windows Live Messenger / MSN
- Windows Phone Contacts Carved Fragments
- World of Warcraft
- XBox 360 Internet Explorer Cache Records
- XBox 360 Internet Explorer Daily History
- XBox 360 Internet Explorer Favorites/Recent/Featured Items
- XBox 360 Internet Explorer Main History
- XBox 360 Internet Explorer Weekly History
- Yahoo! Diagnostic Chats
- Yahoo! Diagnostic Logs
- Yahoo! Group Chat
- Yahoo! Messenger Chat
- Yahoo! Non-Encrypted Chat
- Yahoo! Webmail
- Yahoo! Webmail Chat

Computer

Carved only artifacts:

- Adium Chat
- AIM
- Ares Downloads
- Ares Incomplete Downloads
- Ares Search Keywords
- Ares Shared Files
- Ashley Madison
- Backpage Ads
- Bebo
- Bitcoin Debug Logs
- Carbonite Log File
- Chatroulette
- Chatstep Messages
- Craigslist Ads
- Dropbox (Web-based)
- Facebook Chat
- Facebook Email
- Facebook Email Snippets
- Facebook Pages
- Facebook Status Updates/Wall Posts/Comments
- Firefox Private Browsing History
- Flash Cookies
- Flickr

Carved only artifacts:

- Frostwire.props Files
- Gigatribe Chat
- Gmail Fragments
- Gmail Webmail
- GMX Webmail
- Google Analytics First Visit Cookies Carved
- Google Analytics Referral Cookies Carved
- Google Analytics Session Cookies Carved
- Google Analytics URLs Carved
- Google Docs
- Google Drive
- Google Maps
- Google+ Chat
- GoogleTalk
- Hotmail Webmail
- Hushmail Fragments
- Hushmail Inbox
- IE InPrivate/Recovery URLs
- Instagram Images
- Instagram Posts
- Internet Explorer Cookie Records
- Internet Explorer Daily History
- Internet Explorer Downloads
- Internet Explorer Leak Records

Carved only artifacts:

- Internet Explorer Main History
- Internet Explorer PrivacIE Records
- Internet Explorer Redirect Records
- Internet Explorer Weekly History
- IP Addresses - Audio/Video Calls
- Limewire 5.x Searches
- Limewire.props Files
- Limewire/Frostwire 4.x Searches
- LinkedIn Emails
- Lync / OC Calls
- Lync / OC File Transfers
- Lync / OC Fragments
- Lync / OC Messages
- Mail.ru
- Mailinator Inbox Access
- Mailinator Snippets
- mIRC
- MSN Plus!
- MSN Protocol Fragments
- MySpace Chat - Messages
- MySpace Chat - User Info
- MySpace Inbox Messages
- Omegle
- Opera Search Field History

Carved only artifacts:

- Opera Typed History
- Outlook Web App Email Fragments
- Outlook Web App Email Inbox
- Outlook Webmail Fragments
- Outlook Webmail Inbox
- Outlook Webmail Inbox Fragments
- Paltalk Chat
- Plenty of Fish
- Potential Browser Activity
- QQ
- Second Life
- SharePoint Discussions
- SharePoint Recycle Bin
- SharePoint Shared Documents
- Sina Weibo Carved Searches
- Sina Weibo Microblogs
- Torrent File Fragments
- Trillian
- Twitter
- Usenet Binary Files
- VK Wall Posts
- VK Web Messages
- Web Video Fragments
- WebKit Browser Session/Tabs (Carved)

Carved only artifacts:

- WebKit Browser Web History (Carved)
- WhatsApp Messages - Windows
- Windows Live Messenger / MSN
- World of Warcraft
- XBox 360 Internet Explorer Cache Records
- XBox 360 Internet Explorer Daily History
- XBox 360 Internet Explorer Favorites/Recent/Featured Items
- XBox 360 Internet Explorer Main History
- XBox 360 Internet Explorer Weekly History
- Yahoo! Diagnostic Chats
- Yahoo! Diagnostic Logs
- Yahoo! Group Chat
- Yahoo! Messenger Chat
- Yahoo! Non-Encrypted Chat
- Yahoo! Webmail
- Yahoo! Webmail Chat

iOS

Carved only artifacts:

- Amazon Alexa Web Resource
- AMR Files
- Coinomi Transactions
- Google Analytics First Visit Cookies Carved

Carved only artifacts:

- Google Analytics Referral Cookies Carved
- Google Analytics Session Cookies Carved
- Google Analytics URLs Carved
- Google Maps
- IP Addresses - Audio/Video Calls
- Potential Browser Activity
- Torrent File Fragments
- WebKit Browser Web History (Carved)

Kindle

Carved only artifacts:

- Google Analytics First Visit Cookies Carved
- Google Analytics Referral Cookies Carved
- Google Analytics Session Cookies Carved
- Google Analytics URLs Carved
- Google Maps
- IP Addresses - Audio/Video Calls

Linux

Carved only artifacts:

- Google Analytics First Visit Cookies Carved
- Google Analytics Referral Cookies Carved
- Google Analytics Session Cookies Carved

Carved only artifacts:

- Google Analytics URLs Carved
- Google Maps
- IP Addresses - Audio/Video Calls

Mac

Carved only artifacts:

- Firefox Private Browsing History
- Google Analytics First Visit Cookies Carved
- Google Analytics Referral Cookies Carved
- Google Analytics Session Cookies Carved
- Google Analytics URLs Carved
- Google Maps
- IP Addresses - Audio/Video Calls
- Web Video Fragments
- WebKit Browser Session/Tabs (Carved)
- WebKit Browser Web History (Carved)

Windows Phone

Carved only artifacts:

- Bebo
- Facebook Chat
- Facebook Email
- Facebook Email Snippets

Carved only artifacts:

- Facebook Pages
- Facebook Status Updates/Wall Posts/Comments
- Firefox Private Browsing History
- Flash Cookies
- Gmail Fragments
- Gmail Webmail
- Google Analytics First Visit Cookies Carved
- Google Analytics Referral Cookies Carved
- Google Analytics Session Cookies Carved
- Google Analytics URLs Carved
- Google Maps
- Google+ Chat
- Hotmail Webmail
- Hushmail Fragments
- Hushmail Inbox
- IE InPrivate/Recovery URLs
- Instagram Images
- Instagram Posts
- Internet Explorer Cookie Records
- Internet Explorer Daily History
- Internet Explorer Downloads
- Internet Explorer Leak Records
- Internet Explorer Main History
- Internet Explorer PrivacIE Records

Carved only artifacts:

- Internet Explorer Redirect Records
- Internet Explorer Weekly History
- IP Addresses - Audio/Video Calls
- LinkedIn Emails
- Lync / OC Calls
- Lync / OC File Transfers
- Lync / OC Fragments
- Lync / OC Messages
- Mailinator Inbox Access
- Mailinator Snippets
- MySpace Chat - Messages
- MySpace Chat - User Info
- MySpace Inbox Messages
- Opera Search Field History
- Opera Typed History
- Outlook Web App Email Fragments
- Outlook Web App Email Inbox
- Outlook Webmail Fragments
- Outlook Webmail Inbox
- Outlook Webmail Inbox Fragments
- Potential Browser Activity
- Sina Weibo Carved Searches
- Sina Weibo Microblogs
- Twitter

Carved only artifacts:

- Web Video Fragments
- WebKit Browser Session/Tabs (Carved)
- WebKit Browser Web History (Carved)
- Windows Phone Contacts Carved Fragments
- Yahoo! Webmail

Magnet Forensics

156 Columbia Street West, Unit #2, N2L 3L3

Waterloo, ON, N2K 0A8

1 (519) 342-0195