Skype Forensics: Analyzing Call and Chat Data From Computers and Mobile

Even before being acquired by Microsoft in 2011, Skype had already established a strong presence in the VoIP and instant messaging sectors. By 2012, Skype's market share for total international calls had risen to 34 percent and the number of users continues to grow. Skype offers a range of features for paid and unpaid users including voice, video calling, instant messaging, and file transfers much like the now discontinued MSN Messenger. Overall, Skype offers the traditional services of a mobile device or landline with the additional features of a modern IM or mobile chat application.

From an investigative standpoint, this proliferation of new technology almost always increases the likelihood that it will be used to commit a crime, or for other nefarious purposes. By their very nature, chat and social networking applications are often used as a platform for harassment or bullying incidents due to the perception that an individual's actions are anonymous while on the Internet, but that is not always the case. Armed with the right tools and techniques, Skype forensic analysis can yield valuable digital evidence for investigators. For example, call and chat conversation data can reveal a suspect's actions, intent, accomplices and victims. File transfers can reveal evidence of illicit images or IP theft.

In the following sections, we'll offer insight into where and how to recover evidence from a user's account, calls, messages, group chat, contacts, file transfers, voicemails, and SMS messages.

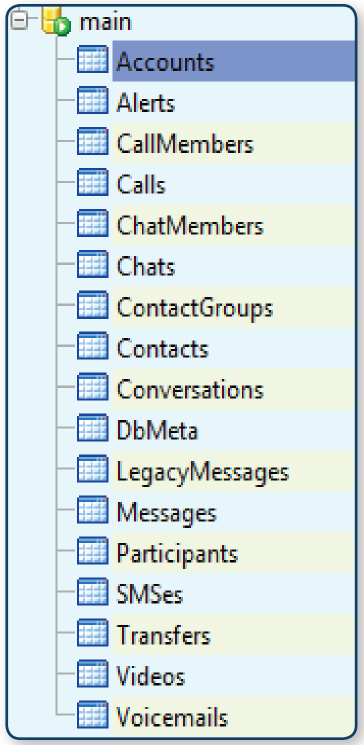
We'll then offer a more in-depth demonstration and some tips on analyzing forensic artifacts from Skype (PC or mobile) using Internet Evidence Finder (IEF).

Sources of Digital Evidence From Skype Installations

Main.db

On a Windows PC, most of these artifacts can be found in the main.db file located at
ROOT\Users\%userprofile%\AppData\Roaming\Skype\%SkypeName%\main.db
or
ROOT\Documents and Settings\%userprofile%\Application Data\Skype\%SkypeName%
for Windows XP installations.

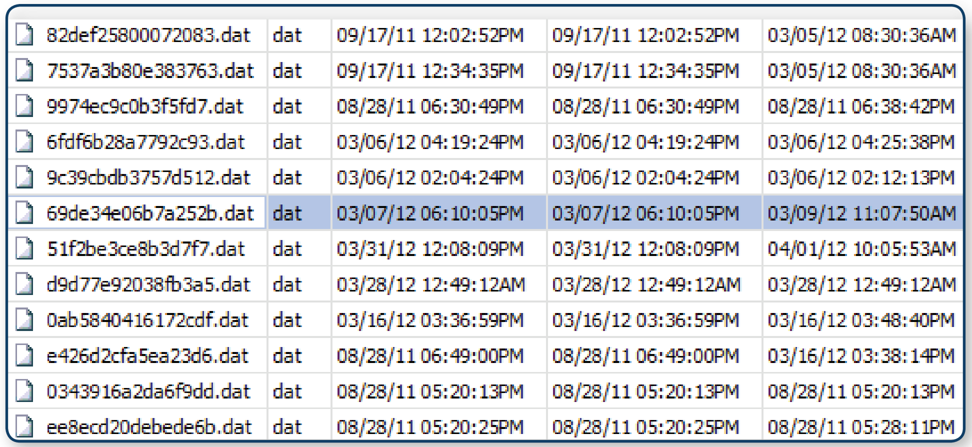
This database contains information on a user's account, calls, messages, group chat, contacts, file transfers, voicemails, and SMS messages. This is a regular SQLite database that can be viewed with any SQLite viewing tool. The timestamp data stored in the main.db database is based on UNIX epoch time and must be converted to a readable format for the investigator.



main
- Accounts
- Alerts
- CallMembers
- Calls
- ChatMembers
- Chats
- ContactGroups
- Contacts
- Conversations
- DbMeta
- LegacyMessages
- Messages
- Participants
- SMSes
- Transfers
- Videos
- Voicemails

Chatsync Folder

Located in the same folder as main.db, another evidence source is the chatsync folder. This folder contains several .DAT files relevant to the conversations had by the user. The file names are sixteen character strings and their purpose is to help with synchronization between multiple devices. Otherwise when a call is answered on one device, it will continue to ring on any other device where the same account resides.



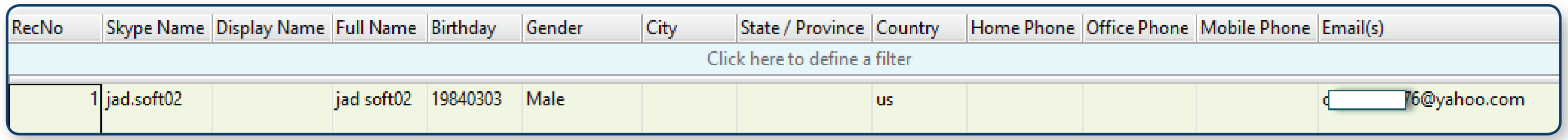
82def25800072083.dat	dat	09/17/11 12:02:52PM	09/17/11 12:02:52PM	03/05/12 08:30:36AM
7537a3b80e383763.dat	dat	09/17/11 12:34:35PM	09/17/11 12:34:35PM	03/05/12 08:30:36AM
9974ec9c0b3f5fd7.dat	dat	08/28/11 06:30:49PM	08/28/11 06:30:49PM	08/28/11 06:38:42PM
6fdf6b28a7792c93.dat	dat	03/06/12 04:19:24PM	03/06/12 04:19:24PM	03/06/12 04:25:38PM
9c39cbdb3757d512.dat	dat	03/06/12 02:04:24PM	03/06/12 02:04:24PM	03/06/12 02:12:13PM
69de34e06b7a252b.dat	dat	03/07/12 06:10:05PM	03/07/12 06:10:05PM	03/09/12 11:07:50AM
51f2be3ce8b3d7f7.dat	dat	03/31/12 12:08:09PM	03/31/12 12:08:09PM	04/01/12 10:05:53AM
d9d77e92038fb3a5.dat	dat	03/28/12 12:49:12AM	03/28/12 12:49:12AM	03/28/12 12:49:12AM
0ab5840416172cdf.dat	dat	03/16/12 03:36:59PM	03/16/12 03:36:59PM	03/16/12 03:48:40PM
e426d2cfa5ea23d6.dat	dat	08/28/11 06:49:00PM	08/28/11 06:49:00PM	03/16/12 03:38:14PM
0343916a2da6f9dd.dat	dat	08/28/11 05:20:13PM	08/28/11 05:20:13PM	08/28/11 05:20:13PM
ee8ecd20debede6b.dat	dat	08/28/11 05:20:25PM	08/28/11 05:20:25PM	08/28/11 05:28:11PM

Each .DAT file contains conversation details about the chat participants, who initiated the chat, the chat messages, date/timestamps, status of each message, and whether it was sent by the local user. A wealth of information on a user's Skype history is available from examining the main.db and chatsync files. While some of the information contained within both sources might be duplicated, there is almost always unique evidence available from each of the artifacts.

Artifacts Found Within the Main.db and Chatsync Folders

Accounts

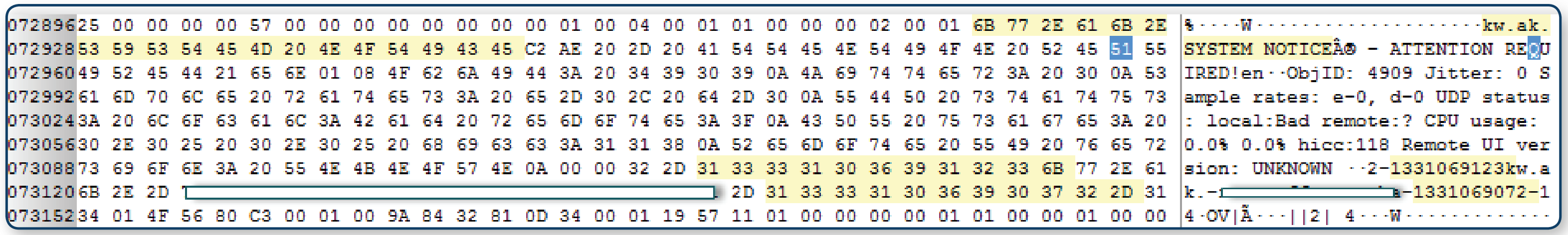
Within main.db there is a table labelled "Accounts" where details on any Skype user account is stored on the local machine. Accessing this database allows investigators to identify the user's Skype name, full name, birthday, gender, languages, location data, telephone details (if available), email address, when the profile was created and last modified, and any additional information that they might have included when creating the account.



RecNo	Skype Name	Display Name	Full Name	Birthday	Gender	City	State / Province	Country	Home Phone	Office Phone	Mobile Phone	Email(s)
1	jad.soft02		jad soft02	19840303	Male			us				[redacted]6@yahoo.com

Calls

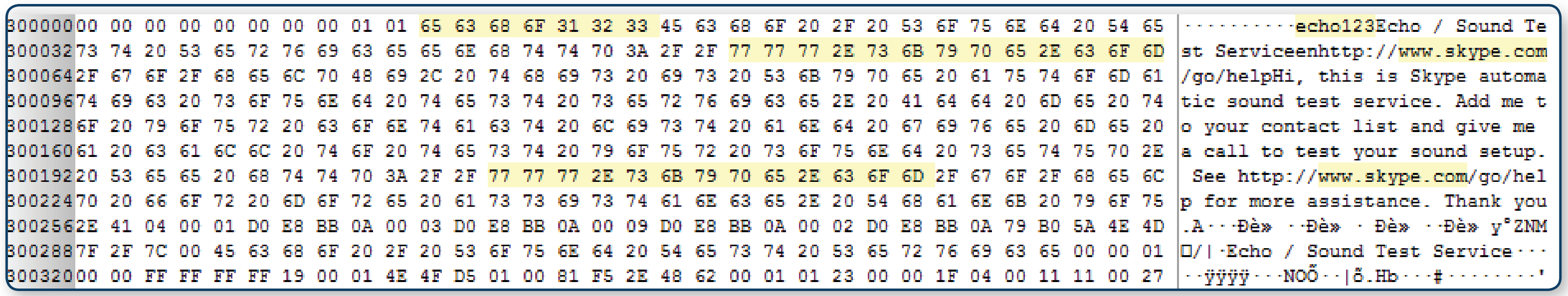
Also within the main.db is a table detailing any call records that might have taken place using Skype. Each call record indicates the date/time it started, the type of call (incoming vs outgoing), local user details, remote user details and duration of the call.



```
07289625 00 00 00 00 57 00 00 00 00 00 00 00 00 01 00 04 00 01 01 00 00 00 02 00 01 6B 77 2E 61 6B 2E %····W····················kw.ak.
07292853 59 53 54 45 4D 20 4E 4F 54 49 43 45 C2 AE 20 2D 20 41 54 54 45 4E 54 49 4F 4E 20 52 45 51 55 SYSTEM NOTICEÂ® - ATTENTION REQU
07296049 52 45 44 21 65 6E 01 08 4F 62 6A 49 44 3A 20 34 39 30 39 0A 4A 69 74 74 65 72 3A 20 30 0A 53 IRED!en··ObjID: 4909 Jitter: 0 S
07299261 6D 70 6C 65 20 72 61 74 65 73 3A 20 65 2D 30 2C 20 64 2D 30 0A 55 44 50 20 73 74 61 74 75 73 ample rates: e-0, d-0 UDP status
0730243A 20 6C 6F 63 61 6C 3A 42 61 64 20 72 65 6D 6F 74 65 3A 3F 0A 43 50 55 20 75 73 61 67 65 3A 20 : local:Bad remote:? CPU usage:
07305630 2E 30 25 20 30 2E 30 25 20 68 69 63 63 3A 31 31 38 0A 52 65 6D 6F 74 65 20 55 49 20 76 65 72 0.0% 0.0% hicc:118 Remote UI ver
07308873 69 6F 6E 3A 20 55 4E 4B 4E 4F 57 4E 0A 00 00 32 2D 31 33 33 31 30 36 39 31 32 33 6B 77 2E 61 sion: UNKNOWN ··2-1331069123kw.a
0731206B 2E 2D [redacted] 2D 31 33 33 31 30 36 39 30 37 32 2D 31 k.-[redacted]-1331069072-1
07315234 01 4F 56 80 C3 00 01 00 9A 84 32 81 0D 34 00 01 19 57 11 01 00 00 00 00 01 01 00 00 01 00 00 4·OV|Å···||2| 4···W·············
```

Contacts

Main.db stores details on any contacts the Skype user might have as well as any groups they might be a part of. Many of the details found in this table are the same as the details in the accounts table about the local user, but there are some additional details demonstrating whether the local user has the contact blocked. It also includes timestamps surrounding the last time they were online.



```
30000000 00 00 00 00 00 00 00 01 01 65 63 68 6F 31 32 33 45 63 68 6F 20 2F 20 53 6F 75 6E 64 20 54 65 ··········echo123Echo / Sound Te
30003273 74 20 53 65 72 76 69 63 65 65 6E 68 74 74 70 3A 2F 2F 77 77 77 2E 73 6B 79 70 65 2E 63 6F 6D st Serviceenhttp://www.skype.com
3000642F 67 6F 2F 68 65 6C 70 48 69 2C 20 74 68 69 73 20 69 73 20 53 6B 79 70 65 20 61 75 74 6F 6D 61 /go/helpHi, this is Skype automa
30009674 69 63 20 73 6F 75 6E 64 20 74 65 73 74 20 73 65 72 76 69 63 65 2E 20 41 64 64 20 6D 65 20 74 tic sound test service. Add me t
3001286F 20 79 6F 75 72 20 63 6F 6E 74 61 63 74 20 6C 69 73 74 20 61 6E 64 20 67 69 76 65 20 6D 65 20 o your contact list and give me
30016061 20 63 61 6C 6C 20 74 6F 20 74 65 73 74 20 79 6F 75 72 20 73 6F 75 6E 64 20 73 65 74 75 70 2E a call to test your sound setup.
30019220 53 65 65 20 68 74 74 70 3A 2F 2F 77 77 77 2E 73 6B 79 70 65 2E 63 6F 6D 2F 67 6F 2F 68 65 6C  See http://www.skype.com/go/hel
30022470 20 66 6F 72 20 6D 6F 72 65 20 61 73 73 69 73 74 61 6E 63 65 2E 20 54 68 61 6E 6B 20 79 6F 75 p for more assistance. Thank you
3002562E 41 04 00 01 D0 E8 BB 0A 00 03 D0 E8 BB 0A 00 09 D0 E8 BB 0A 00 02 D0 E8 BB 0A 79 B0 5A 4E 4D .A···Ðè» ··Ðè» · Ðè» ··Ðè» y°ZNM
3002887F 2F 7C 00 45 63 68 6F 20 2F 20 53 6F 75 6E 64 20 54 65 73 74 20 53 65 72 76 69 63 65 00 00 01 □/|·Echo / Sound Test Service···
30032000 00 FF FF FF FF 19 00 01 4E 4F D5 01 00 81 F5 2E 48 62 00 01 01 23 00 00 1F 04 00 11 11 00 27 ··ÿÿÿÿ···NOÕ··|õ.Hb···#·······'
```

File Transfers

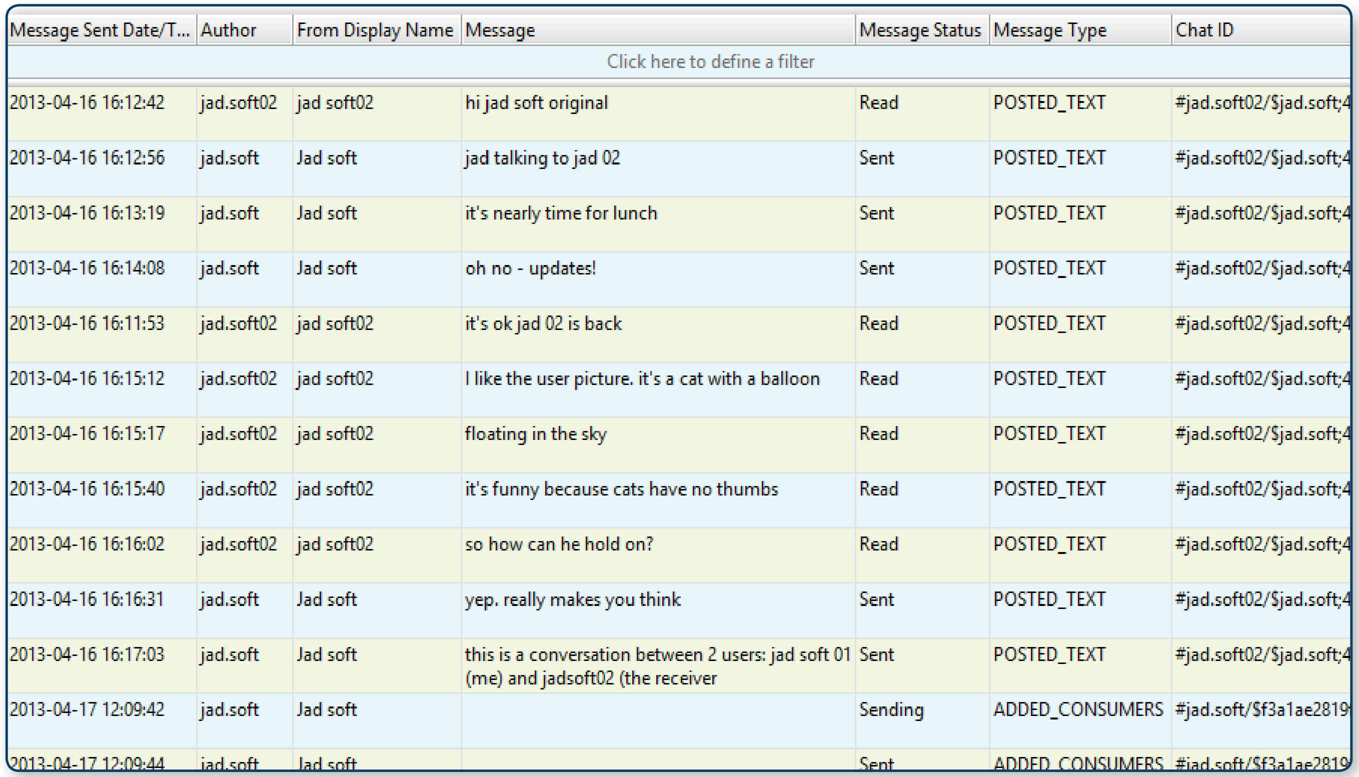
Main.db stores details on any contacts the Skype user might have as well as any groups they might be a part of. Many of the details found in this table are the same as the details in the accounts table about the local user, but there are some additional details demonstrating whether the local user has the contact blocked. It also includes timestamps surrounding the last time they were online.

Of the details the transfers table in main.db contains information about any files that might have been transferred between two Skype users. Details regarding the date/time the file was transferred, file name, size, sender/receiver and delivery status are all included in the table. Once transferred, these files are stored in
ROOT\Users\%userprofile%\AppData\Roaming\Skype\My Skype Received Files
by default.

This is an excellent location to look for evidence if you suspect any users of stealing intellectual property from your organization, as it is not a regularly monitored exfiltration point. While IT departments evaluate and monitor well-known methods a malicious employee might employ to steal data from the company (email and USB for example), Skype is not a familiar tool for transferring documents and files in or out of sensitive areas. Security professionals must be aware of these features in order to protect against any potential loss of data as a result of allowing these tools in the corporate network.

Chat Messages

Skype stores its chat messages in two locations: the main.db and chatsync folders previously mentioned. Microsoft added the chatsync files in order to correct some syncing issues between users using multiple computers or devices. It is essential that an investigator understand that although there is some overlap, both these locations store unique data and should be examined individually.

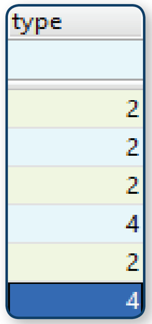


Message Sent Date/T...	Author	From Display Name	Message	Message Status	Message Type	Chat ID
2013-04-16 16:12:42	jad.soft02	jad soft02	hi jad soft original	Read	POSTED_TEXT	#jad.soft02/$jad.soft;4
2013-04-16 16:12:56	jad.soft	Jad soft	jad talking to jad 02	Sent	POSTED_TEXT	#jad.soft02/$jad.soft;4
2013-04-16 16:13:19	jad.soft	Jad soft	it's nearly time for lunch	Sent	POSTED_TEXT	#jad.soft02/$jad.soft;4
2013-04-16 16:14:08	jad.soft	Jad soft	oh no - updates!	Sent	POSTED_TEXT	#jad.soft02/$jad.soft;4
2013-04-16 16:11:53	jad.soft02	jad soft02	it's ok jad 02 is back	Read	POSTED_TEXT	#jad.soft02/$jad.soft;4
2013-04-16 16:15:12	jad.soft02	jad soft02	I like the user picture. it's a cat with a balloon	Read	POSTED_TEXT	#jad.soft02/$jad.soft;4
2013-04-16 16:15:17	jad.soft02	jad soft02	floating in the sky	Read	POSTED_TEXT	#jad.soft02/$jad.soft;4
2013-04-16 16:15:40	jad.soft02	jad soft02	it's funny because cats have no thumbs	Read	POSTED_TEXT	#jad.soft02/$jad.soft;4
2013-04-16 16:16:02	jad.soft02	jad soft02	so how can he hold on?	Read	POSTED_TEXT	#jad.soft02/$jad.soft;4
2013-04-16 16:16:31	jad.soft	Jad soft	yep. really makes you think	Sent	POSTED_TEXT	#jad.soft02/$jad.soft;4
2013-04-16 16:17:03	jad.soft	Jad soft	this is a conversation between 2 users: jad soft 01 (me) and jadsoft02 (the receiver	Sent	POSTED_TEXT	#jad.soft02/$jad.soft;4
2013-04-17 12:09:42	jad.soft	Jad soft		Sending	ADDED_CONSUMERS	#jad.soft/$f3a1ae2819
2013-04-17 12:09:44	jad.soft	Jad soft		Sent	ADDED_CONSUMERS	#jad.soft/$f3a1ae2819

For example, main.db stores chat details on when a message was sent, author, content of the message, status, type, chat ID, and recipient(s). Similarly, the .DAT files in the chatsync folder contain much of the same information but also stores who initiated the conversation and the message status.

Group Chat

Skype also stores details around any group chat conversations between multiple users. This data is stored within the same main.db table as chat but are uniquely identified by the type field.

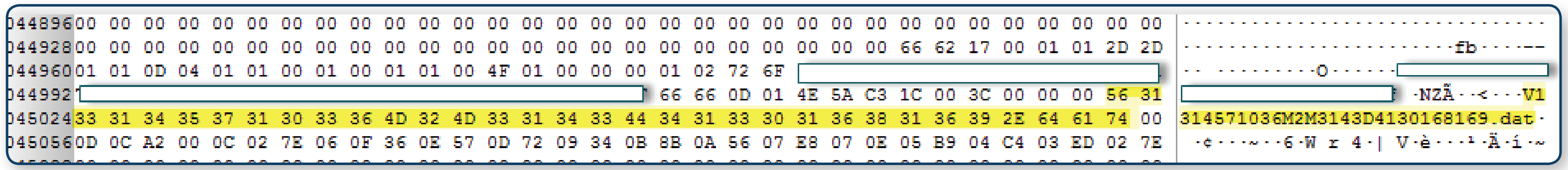


type
2
2
2
4
2
4

The group chat conversations are categorized as type 4 and do not reflect the number of participants. Regular conversations are stored as type 2. The information stored for group chat is the same as a regular chat but typically has more than two Skype users participating at the same time.

Voicemails

Finally, the main.db database contains a table detailing any voicemails that the Skype user might have received. Metadata around the user, subject, date/time, duration, status, type and the location of the audio file are all stored within this table and can be easily read by any SQLite database reader.



```
044896 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ································
044928 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 66 62 17 00 01 01 2D 2D  ························fb····--
044960 01 01 0D 04 01 01 00 01 00 01 01 00 4F 01 00 00 00 01 02 72 6F [redacted]                       ·· ·········O······[redacted]
044992 [redacted]                                  66 66 0D 01 4E 5A C3 1C 00 3C 00 00 00 56 31  [redacted]·NZÃ··<···V1
045024 33 31 34 35 37 31 30 33 36 4D 32 4D 33 31 34 33 44 34 31 33 30 31 36 38 31 36 39 2E 64 61 74 00  314571036M2M3143D4130168169.dat·
045056 0D 0C A2 00 0C 02 7E 06 0F 36 0E 57 0D 72 09 34 0B 8B 0A 56 07 E8 07 0E 05 B9 04 C4 03 ED 02 7E   ·¢···~··6·W r 4·| V·è···¹·Ä·í·~
```

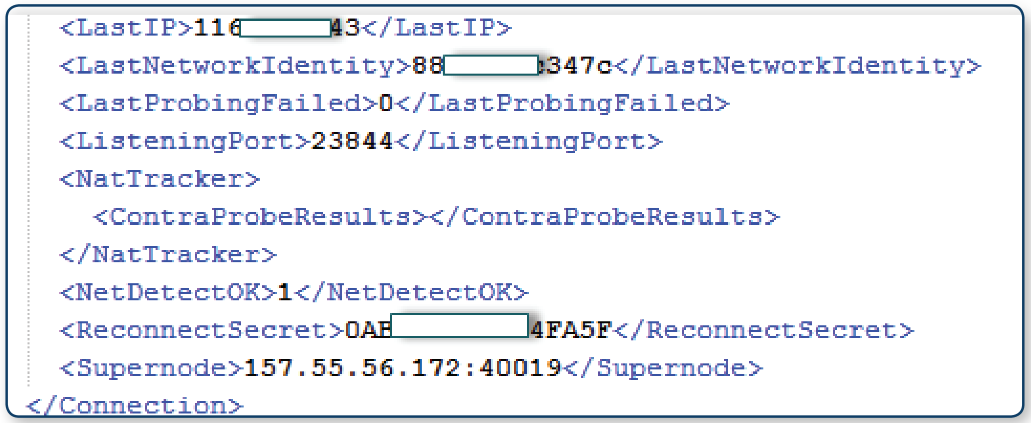
The actual voicemail audio files are stored at a different location:
ROOT\Users\%userprofile%\AppData\Roaming\Skype\%SkypeName%\voicemail

One challenge for investigators dealing with Skype voicemails is that Microsoft stores these audio files in a proprietary format, so they cannot be replayed outside of the Skype application. To get around this, you can create a Skype account as an investigator, record a voicemail, and then replace the voicemail file you just recorded with the voicemail from your case. Skype will then allow you to play the suspect's voicemail through the investigator's account. This method is time-consuming but effective and can often reveal valuable evidence.

IP Addresses

Another valuable artifact found in the chatsync folders are the IP addresses associated with any Skype activity on the system. Skype stores both the local NAT'ed IP addresses for a user as well as the outward facing public IP addresses. Paring these addresses with the associated timestamps will allow an investigator to identify which users sent specific messages and help correlate any external data that might have been obtained from an ISP or other external provider.

The majority of the IP address information can be found in the chatsync .DAT files but this information can also be found in the shared.xml file located in the Skype folder.

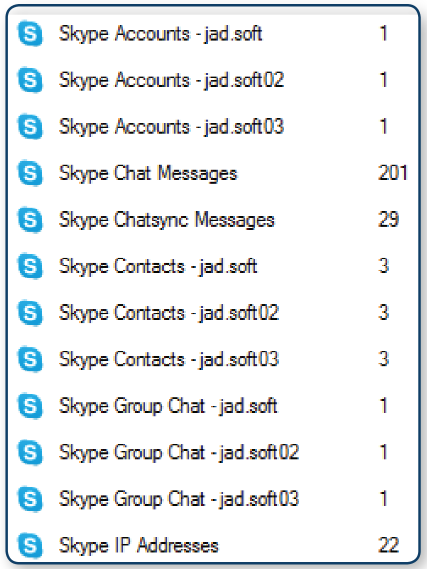


```
    <LastIP>11[redacted]43</LastIP>
    <LastNetworkIdentity>88[redacted]347c</LastNetworkIdentity>
    <LastProbingFailed>0</LastProbingFailed>
    <ListeningPort>23844</ListeningPort>
    <NatTracker>
      <ContraProbeResults></ContraProbeResults>
    </NatTracker>
    <NetDetectOK>1</NetDetectOK>
    <ReconnectSecret>0A[redacted]4FA5F</ReconnectSecret>
    <Supernode>157.55.56.172:40019</Supernode>
  </Connection>
```

The shared.xml file contains a tag called “ContraProbeResults” that will store IP addresses for the host which Skype is installed. The tag “LastIP” also stores the user’s previous external IP address in decimal form, which can easily be converted by most calculators. While there is a lot of useful information for an investigator in the shared.xml file, the challenge is that some of it may be encoded and difficult to parse without additional details from Microsoft on how it is stored.

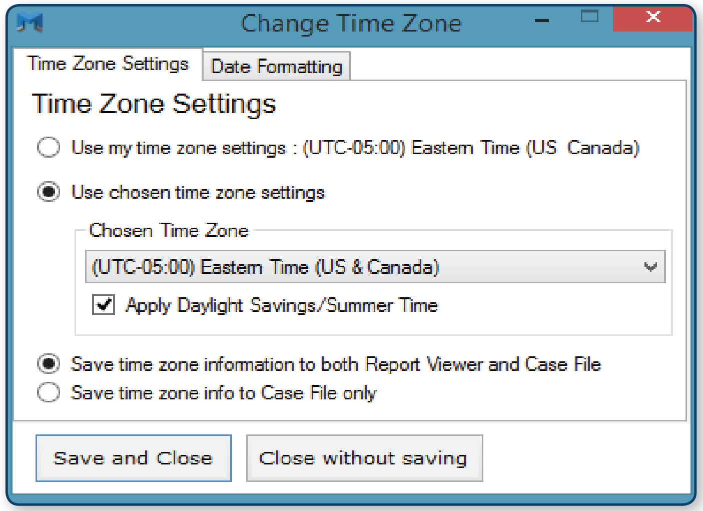
Analyzing Skype Artifacts Using IEF

Internet Evidence Finder (IEF) is able to parse and carve many of the artifacts found in these locations, allowing examiners to focus on the investigation rather than manually searching and piecing together each artifact. The IEF Report Viewer will sort each artifact type into their respective groups and organize the data into relevant columns that can be easily searched or sorted by the investigator to find what they are looking for.



Skype Accounts - jad.soft	1
Skype Accounts - jad.soft02	1
Skype Accounts - jad.soft03	1
Skype Chat Messages	201
Skype Chatsync Messages	29
Skype Contacts - jad.soft	3
Skype Contacts - jad.soft02	3
Skype Contacts - jad.soft03	3
Skype Group Chat - jad.soft	1
Skype Group Chat - jad.soft02	1
Skype Group Chat - jad.soft03	1
Skype IP Addresses	22

IEF will also take all of the timestamps from main.db in UNIX time and automatically convert the data for the investigator into either UTC or any regional time zone indicated by the investigator.



Change Time Zone

Time Zone Settings | Date Formatting

Time Zone Settings

○ Use my time zone settings : (UTC-05:00) Eastern Time (US Canada)

● Use chosen time zone settings

Chosen Time Zone

(UTC-05:00) Eastern Time (US & Canada)

☑ Apply Daylight Savings/Summer Time

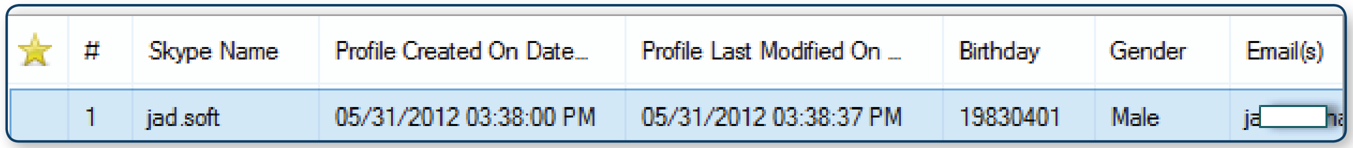
● Save time zone information to both Report Viewer and Case File

○ Save time zone info to Case File only

This allows investigators to standardize any time zone data to reflect the physical location where the device was used or in cases where it was a laptop or mobile device which could have spanned multiple time zones during the course of an incident.

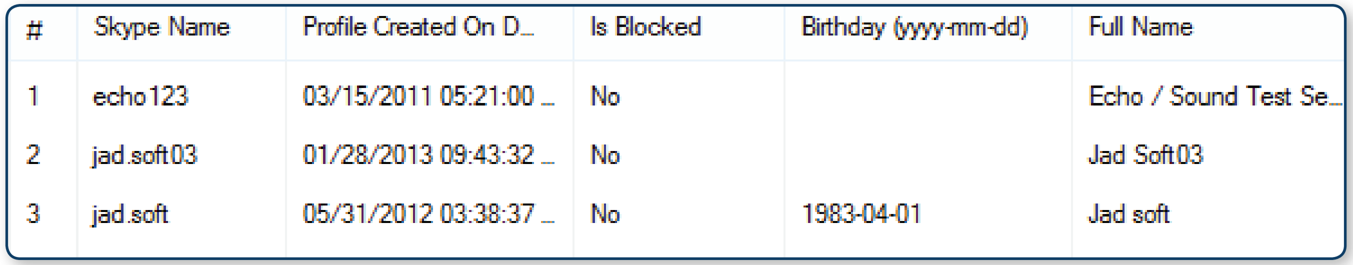
IEF Results

IEF automatically pulls all of the account details for each Skype user from the main.db and organizes them into the most relevant categories for investigators allowing for easy analysis.



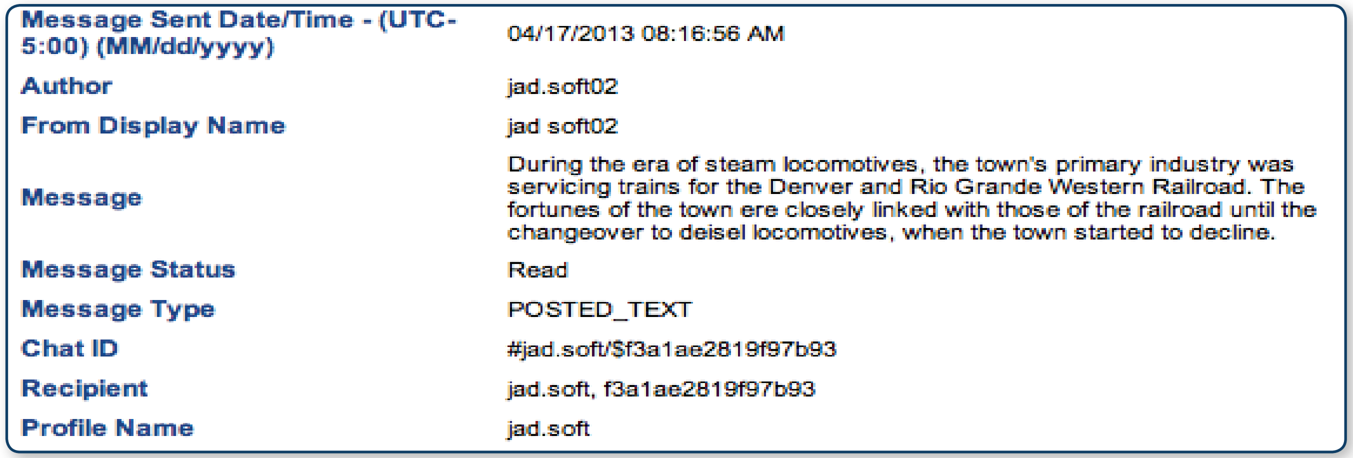
☆	#	Skype Name	Profile Created On Date...	Profile Last Modified On ...	Birthday	Gender	Email(s)
	1	jad.soft	05/31/2012 03:38:00 PM	05/31/2012 03:38:37 PM	19830401	Male	[redacted]

The example above details the Skype user's name, creation and last modified timestamps, email address and all the other values previously mentioned. Below, contacts are displayed similarly to the user accounts and will help examiners tie suspects, accomplices, or victims to the crime or complaint being investigated.



#	Skype Name	Profile Created On D...	Is Blocked	Birthday (yyyy-mm-dd)	Full Name
1	echo123	03/15/2011 05:21:00 ...	No		Echo / Sound Test Se...
2	jad.soft03	01/28/2013 09:43:32 ...	No		Jad Soft03
3	jad.soft	05/31/2012 03:38:37 ...	No	1983-04-01	Jad soft

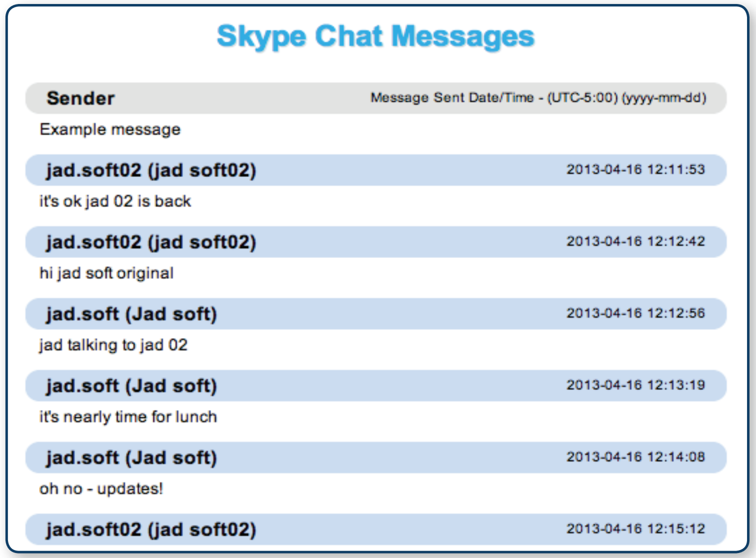
IEF also collects all of the chat information from the main.db and chatsync folders and presents the results to investigators. All of the previously mentioned chat and chatsync artifacts are available to the investigator and can be sorted by sender, receiver, time, or any other column in the database.



Message Sent Date/Time - (UTC-5:00) (MM/dd/yyyy)	04/17/2013 08:16:56 AM
Author	jad.soft02
From Display Name	jad soft02
Message	During the era of steam locomotives, the town's primary industry was servicing trains for the Denver and Rio Grande Western Railroad. The fortunes of the town ere closely linked with those of the railroad until the changeover to deisel locomotives, when the town started to decline.
Message Status	Read
Message Type	POSTED_TEXT
Chat ID	#jad.soft/$f3a1ae2819f97b93
Recipient	jad.soft, f3a1ae2819f97b93
Profile Name	jad.soft

Chat Threading

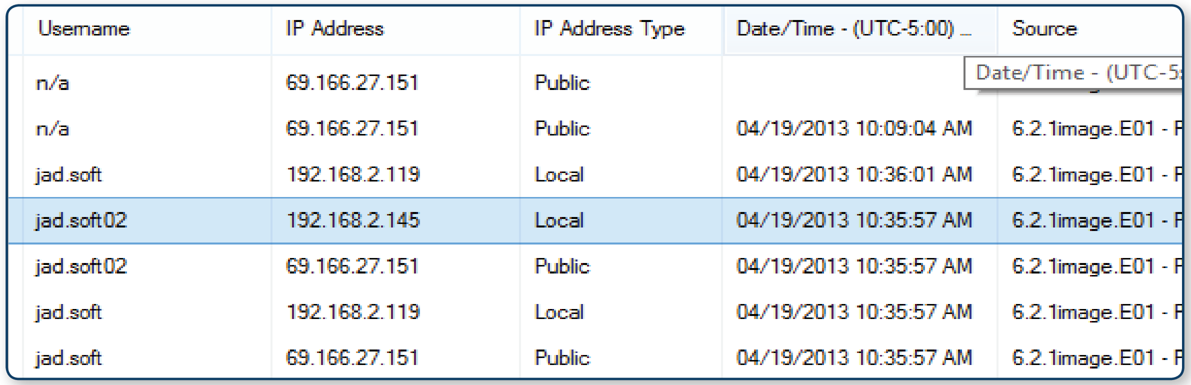
Another valuable feature of IEF that can assist investigators dealing with Skype artifacts is IEF's ability to take the individual chat messages and thread them into an easier-to-read format. This allows investigators to view entire conversations quickly and accurately without having to manually piece together the conversation with the given timestamps.



Skype Chat Messages

Sender	Message Sent Date/Time - (UTC-5:00) (yyyy-mm-dd)
Example message	
jad.soft02 (jad soft02)	2013-04-16 12:11:53
it's ok jad 02 is back	
jad.soft02 (jad soft02)	2013-04-16 12:12:42
hi jad soft original	
jad.soft (Jad soft)	2013-04-16 12:12:56
jad talking to jad 02	
jad.soft (Jad soft)	2013-04-16 12:13:19
it's nearly time for lunch	
jad.soft (Jad soft)	2013-04-16 12:14:08
oh no - updates!	
jad.soft02 (jad soft02)	2013-04-16 12:15:12

A new feature of version 6.3, IEF is also able to parse the IP address details from shared.xml and chatsync folders, giving both the internal private IP address for the host as well as any external IP address associated with the computer that might have been either statically or dynamically assigned, helping investigators correlate any network data that might be part of the investigation as well.

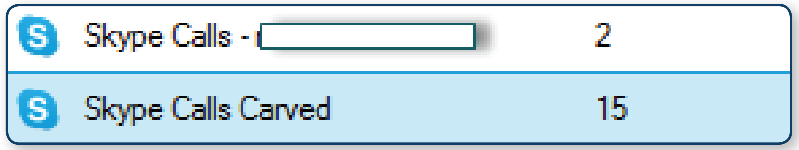


Usemame	IP Address	IP Address Type	Date/Time - (UTC-5:00) ...	Source
n/a	69.166.27.151	Public		
n/a	69.166.27.151	Public	04/19/2013 10:09:04 AM	6.2.1image.E01 - F
jad.soft	192.168.2.119	Local	04/19/2013 10:36:01 AM	6.2.1image.E01 - F
jad.soft02	192.168.2.145	Local	04/19/2013 10:35:57 AM	6.2.1image.E01 - F
jad.soft02	69.166.27.151	Public	04/19/2013 10:35:57 AM	6.2.1image.E01 - F
jad.soft	192.168.2.119	Local	04/19/2013 10:35:57 AM	6.2.1image.E01 - F
jad.soft	69.166.27.151	Public	04/19/2013 10:35:57 AM	6.2.1image.E01 - F

Carving Deleted Database Records

Not only is IEF able to parse any call data out of main.db, it will also carve out any deleted records from memory dumps, unallocated space, slack, or any other unstructured area of the drive. IEF does not require the entire SQLite database to be present, just the individual records are enough to identify the artifact.

In our example below, main.db reported only two call records available from the given Skype account, but after running IEF on the same profile, it is evident that there were 15 additional call records carved out of unallocated space.



Skype Calls - [redacted]	2
Skype Calls Carved	15

Similar to the call records, IEF can also carve chat message details from unallocated space or memory, identifying a wealth of additional information that a manual search or other tools might have missed.

Skype on Mobile

IEF is also able to analyze Skype installations on both iOS and Android devices. The relevant files are located at
/data/data/com.skype.raider/files/%SkypeName%
for Android, and
/Library/Application Support/Skype/%SkypeName%/
for iOS devices.

The installation is very similar to a PC and your investigation would follow the same process as indicated above with the main.db and chatsync folders. Carving evidence out of unallocated space can also be done by IEF to uncover any deleted records that might still reside on the device.

With rising popularity of this VoIP service, there is a high likelihood that a forensic examiner will need to analyze Skype evidence over the course of an investigation. Evidence of collusion or conspiracy between two parties, data or IP theft using Skype's file transfer capabilities, or cases of harassment or bullying are just a few examples of how Skype can be used in the commission of a crime or part of a larger investigation. Using Internet Evidence Finder can streamline your overall investigative process, giving you more time to focus your efforts on interpreting data instead of manually piecing it together.

As always, please let me know if you have any questions, suggestions or requests. I can be reached by email at jamie.mcquaid@magnetforensics.com. For more advice and information on relevant topics, visit the Magnet Forensics blog.

Jamie McQuaid
Forensics Consultant, Magnet Forensics

For more information call us at 519-342-0195
or email sales@magnetforensics.com

MAGNET
FORENSICS®