THE RISE OF MOBILE CHAT APPS:
RECOVERING EVIDENCE FROM KIK MESSENGER,
WHATSAPP & BBM
TABLE OF CONTENTS

INTRO: THE RISE OF THIRD-PARTY APPS AS A CRITICAL SOURCE OF EVIDENCE ........................................ 1

RECOVERING KIK MESSENGER FORENSIC ARTIFACTS ................................................................. 3
  Kik Contacts .............................................................................................................................. 4
  Kik Messages .......................................................................................................................... 4
  Kik Attachments ..................................................................................................................... 5

RECOVERING WHATSAPP FORENSIC ARTIFACTS ................................................................. 7
  Android ...................................................................................................................................... 7
  iOS ........................................................................................................................................... 9

RECOVERING BBM FORENSIC ARTIFACTS ........................................................................... 10

MAKING THIRD-PARTY APP DISCOVERY AND ANALYSIS EASIER WITH INTERNET EVIDENCE FINDER (IEF) ...................... 13
THE RISE OF THIRD-PARTY APPS
AS A CRITICAL SOURCE OF EVIDENCE

Over the last few years, we have seen a massive shift in the mobile communications market. Smartphones have taken over the world, and mobile users spend the majority of their on-device time emailing, browsing the web, using social media, and chatting with others using various applications.

This shift has created a new problem for digital forensics investigators, who must now recover and analyze data contained within thousands of widely-used third-party mobile applications. The sheer number of mobile apps is overwhelming, and it seems like new ones emerge and explode in popularity all the time. Furthermore, each application on each device stores data in a different way. If an investigator isn’t up-to-date on the apps people are using, or doesn’t know where to look for data, critical evidence is likely being missed.

Mobile chat apps are amongst the most popular types of third-party applications used on mobile devices today. They are used by billions of people worldwide, and are quickly surpassing traditional SMS in terms of message volume and usage.
The infographic above shows that it’s imperative that forensic professionals are prepared with the knowledge and tools necessary to efficiently recover data from third-party mobile chat applications, as they’re often the richest sources of evidence today. This whitepaper will detail how to recover evidence from popular third-party mobile chat apps, including Kik Messenger, WhatsApp and BBM. We’ll also offer tips for staying up-to-date with updated and emerging apps in a rapidly evolving landscape.

**WHAT YOU’LL LEARN FROM THIS WHITEPAPER**
RECOVERING KIK MESSENGER
FORENSIC ARTIFACTS

With over 150 million users worldwide, Kik Messenger has exploded in popularity because of its cross-platform functionality and zero-dollar price tag. Kik allows users to send messages and files to contacts using iOS, Android, and Windows Phone devices.

WHY ARE KIK MESSENGER ARTIFACTS IMPORTANT TO YOUR MOBILE FORENSICS INVESTIGATIONS?

In today’s world where mobile phones are the technology of choice used by millions to communicate, chat applications like Kik Messenger are often used in the commission of crimes like online harassment, or to plan or facilitate crimes like drug trafficking, robbery, or murder. More and more digital forensics examiners are seeing the need to investigate Kik Messenger as a vital source of evidence, and the ability to recover data from this app is becoming critical to their investigations.

For both iOS and Android, most Kik artifacts relevant to forensic investigations are stored within SQLite databases—similar to other mobile chat applications.

For iOS, Kik artifacts can be found at:
/root/var/mobile/Applications/com.kik.chat/Documents/kik.sqlite

For Android, Kik artifacts can be found at:
/data/data/kik.android/databases/kikdatabase.db

These databases store details on the Kik user’s contacts, messages, and attachments sent and received through the Kik Messenger application; however, they are structured very differently.
THE KEY ARTIFACTS THAT NEED TO BE FOUND WHEN INVESTIGATING KIK MESSENGER

1. KIK CONTACTS

Kik stores user contacts within the SQLite database, in a table called KIKcontactsTable (Android) or ZKIKUSER (iOS). This list contains valuable information for all the user’s contacts and can vary depending on if they are using the Android or iOS application.

The database for both Android and iOS contains a user name and display name for each contact. The user name is a unique identifier for every Kik user. The display name, on the other hand, is the name shown in the user’s chat window, which can be modified by the user at any time. The user name can also be verified with the JID column—a unique identifier appearing in an email address format, ending in an underscore, a 3 character string, and a “@talk.kik.com” domain. For example, if my user name was jmcmquaid, my JID would be “jmcmquaid_rbs@talk.kik.com” where “rbs” could be a different string value used internally by Kik. In our testing, we have found multiple string values in the JID and while many of them are common across users, we cannot determine their meaning. They are likely used to categorize users internally within the Kik servers.

Kik Contacts Table

The Kik contacts tables can also contain profile picture links and timestamps, as well as group and block lists (depending on which application is used).

2. KIK MESSAGES

Given that Kik is a messaging application, it’s likely that the most valuable evidence will be found in the messages themselves. Messages are stored in the messagesTable (Android) or the ZKIKMESSAGE table (iOS).
All messages appear together in the messages table, which can be challenging to sift through if multiple conversations occurred at the same time. To analyze these conversations on Android, investigators need to refer to partner_jid, which will identify who the conversation was with, and was_me, which will indicate which party sent or received the message. Additionally, the read_state column will show whether or not the user has read a given message (a value of 500 means read while 400 means unread). In reference to iOS, the ZUSER column refers to the conversation partner, while the ZTYPE column identifies the sender and receiver.

Kik Messages Table

While both applications have similar features, the artifacts recovered from each operating system will differ slightly as a result of their respective SQLite database structures.

3. KIK ATTACHMENTS

Kik Messenger also supports the transfer of photos and attachments. Photos—sent from either the camera or gallery—are stored on the mobile device as a JPG with no file extension. These files are named with a GUID and are referenced in the attachment table for the SQLite database.

It is also worth noting that an attachment can include a message; however, the messages and attachments are sent separately in the Kik database. The attachments are represented in the message table as a (null) message but will link to a GUID in the attachments table.
Attachments Displayed in the Kik Messages Table

<table>
<thead>
<tr>
<th>ZMESSAGE</th>
<th>ZLASTACCESTIMESTAMP</th>
<th>ZTIMESTAMP</th>
<th>ZCONTENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 (null)</td>
<td>39521-04-03 16:2400.490</td>
<td>1e25761f-8cc7-4-ds1-8b8c-c7bb799d8cc6</td>
<td></td>
</tr>
<tr>
<td>15 (null)</td>
<td>39521-07-16 19:29:31.135</td>
<td>002798b4-2:b15-4030-8a3c-b2:c0ea8249</td>
<td></td>
</tr>
<tr>
<td>16 (null)</td>
<td>39521-09-14 23:05:59.050</td>
<td>19:77e4-e5c5-439d-85f7-0a384888c6d</td>
<td></td>
</tr>
<tr>
<td>18 (null)</td>
<td>39521-11-07 20:46:32.937</td>
<td>50842a27-57fa-4281-8df9-9854199e25d</td>
<td></td>
</tr>
<tr>
<td>20 (null)</td>
<td>39522-04-08 18:17:24.831</td>
<td>20018afe-8985-48ed-9eb7-eb0e040b5</td>
<td></td>
</tr>
<tr>
<td>23 (null)</td>
<td>39522-06-07 07:53:45.775</td>
<td>93e0d099-94fd-3-d1d-9a91-e1fe1b7a56d</td>
<td></td>
</tr>
<tr>
<td>25 (null)</td>
<td>39522-07-10 21:00:59.155</td>
<td>6438e11-0574-4e30-9dd1-0881e35f50</td>
<td></td>
</tr>
<tr>
<td>27 (null)</td>
<td>39522-10-08 08:11:44.733</td>
<td>2656e2d-3-c16-4-c22-9400-c662c211451c</td>
<td></td>
</tr>
<tr>
<td>28 (null)</td>
<td>39522-12-05 05:18:25.633</td>
<td>2aebe80f-63f4-4556-a13c-bcf7ff82ca</td>
<td></td>
</tr>
<tr>
<td>30 (null)</td>
<td>39523-02-27 15:28:57.242</td>
<td>bcf3ac2-5-002-4a23-aac8-968d82215573</td>
<td></td>
</tr>
<tr>
<td>33 (null)</td>
<td>39523-04-08 16:00:14.977</td>
<td>9a0bed1-465d-45ee-99e6-927114f2b</td>
<td></td>
</tr>
<tr>
<td>34 (null)</td>
<td>39523-06-22 19:50:39.320</td>
<td>9088d2a6-035-4d1b-0b15-54e7739411</td>
<td></td>
</tr>
<tr>
<td>35 (null)</td>
<td>39523-08-20 09:37:59.969</td>
<td>681eb4d8-9a85-4109-81ec-ef51476561</td>
<td></td>
</tr>
<tr>
<td>37 (null)</td>
<td>39523-09-14 08:57:04.694</td>
<td>b230c85e-5c59-49d4-9a7e-0c29e28d957f</td>
<td></td>
</tr>
</tbody>
</table>
RECOVERING WHATSAPP FORENSIC ARTIFACTS

Another popular mobile chat application is WhatsApp. Like Kik Messenger, WhatsApp is cross-platform instant messenger service that has over 600 million users. It was purchased by Facebook in February 2014 and continues to grow in popularity.

WHY ARE WHATSAPP ARTIFACTS IMPORTANT TO YOUR MOBILE FORENSICS INVESTIGATIONS?

Much like other mobile chat applications, WhatsApp contacts, messages, and attachments can be valuable to examiners looking to recover evidence for a variety of different investigation types. Whether you’re analyzing the mobile device of a suspect or a victim, these chat artifacts can contain valuable information to help solve a case.

THE KEY ARTIFACTS THAT NEED TO BE FOUND WHEN INVESTIGATING WHATSAPP

ANDROID

For Android devices, there are two SQLite databases of value for investigators recovering WhatsApp artifacts: msgstore.db and wa.db. The msgstore.db contains details on any chat conversations between a user and their contacts. Wa.db stores information on all the WhatsApp user’s contacts. Both of these databases can be found under the databases folder at the following locations:

/data/data/com.whatsapp/databases/msgstore.db

/data/data/com.whatsapp/databases/wa.db

The msgstore.db is a relatively simple SQLite database with two tables: chat_list and messages. The messages table contains a listing of all the messages that a user sends or receives from his/her contacts. Unlike Kik or BBM, where a user is required to have a unique username or PIN, WhatsApp uses the user’s phone number as a unique identifier for both the user and their contacts. This table will include the contact’s phone number, message contents, message status, timestamps, and any details around attachments included in the message. Attachments being sent through WhatsApp have their own
Table entry and the message contents will contain a null entry with a thumbnail and link to the photo/image being shared. This attachment is stored directly in the msgstore.db file. Additionally, the table may contain latitude and longitude coordinates for messages being sent, allowing the investigator to map out the geolocation details of a user.

**WhatsApp Messages Table**

The chat_list table contains a listing of all the phone numbers that a user communicated with; however, this is not a complete listing of the user's contacts. For that we must look at the wa.db.

The wa.db contains a complete listing of a WhatsApp user's contacts including phone number, display name, timestamp, and any other information given upon registering with WhatsApp.

In order to gain access the msgstore.db and wa.db, an investigator must root or get a physical acquisition of the Android device. Otherwise, WhatsApp also stores a copy of the msgstore.db on the SD card, which is used for backups at the following location:

/sdcard/WhatsApp/Databases/msgstore.db.crypt

One caveat with this file is that it is encrypted and must be decrypted prior to analysis. WhatsApp uses several different types of encryption on this database depending on the version of WhatsApp being used.

Recovering WhatsApp contacts, messages, and attachments on Android is relatively straightforward once you have access to the appropriate databases. The process is similar in iOS, but with some minor differences.
iOS

Unlike Android, which uses multiple SQLite databases, iOS stores all relevant WhatsApp data in one database called ChatStorage.sqlite, stored in the following location:

`net.whatsapp.WhatsApp/Documents/ChatStorage.sqlite`

The ZWAMEMESSAGE and ZWAMEDIAITEM tables are excellent locations for collecting items of evidentiary value including messages, sender, recipient, timestamps, geolocation data, and the path/location of any media being shared between two contacts. Many of the same artifacts mentioned for Android are found in these locations; however, the table names and structure may be different.

In addition to the ChatStorage.sqlite database, there is also a Contacts.sqlite database in the same location. While there are some extra details about a user’s WhatsApp contacts, this database does not include the JID for each contact that uniquely identifies the user to the WhatsApp servers.
RECOVERING BLACKBERRY MESSENGER FORENSIC ARTIFACTS

BlackBerry Messenger (BBM) was the original mobile messaging application, geared towards business users and productive consumers. Originally available only on BlackBerry devices, BBM has since gone cross-platform and is now accessible to Android and iOS users.

WHY ARE BBM ARTIFACTS IMPORTANT TO YOUR MOBILE FORENSICS INVESTIGATIONS?

While consumer interest in BlackBerry devices has been on the decline, the recent OS extension of BBM has increased the application’s user-base substantially. It’s become widely popular in North America, but even more noteworthy is the adoption of BBM in countries such as Indonesia and South Africa, where it is the number one mobile chat application.

THE KEY ARTIFACTS THAT NEED TO BE FOUND WHEN INVESTIGATING BBM

Imaging and gaining root access to BlackBerry devices can be challenging, making it difficult to retrieve key artifacts from its operating system. The analysis of BBM artifacts from Android and iOS, on the other hand, is relatively straightforward.

BBM artifacts are stored in a SQLite database called master.db, which can be found in the following locations:

For Android, BBM artifacts can be found at:
/data/data/com.bbm/files/bbmcore/master.db

For iOS, BBM artifacts can be found at:
/private/var/mobile/Applications/%GUID%/Library/bbmcore/master.db

The master.db database contains several tables that provide a wealth of information on a user’s BBM contacts, invitations, messages, file transfers, profiles, and GPS data (if enabled on the device). This data is unencrypted on the device and can be viewed with any SQLite viewer.

There are quite a few tables of interest that store the data mentioned above. The TextMessages table contains the messages along with
timestamps and other relevant data. The Contacts, Profile and Users tables store contact and user details including profile pictures and registration details. The FileTransfers and FileTransferData store data on any files that were transferred between BBM users. There are some additional tables found in the master.db database that might be of forensic value to an investigator.

The screenshot below is an example of the detailed information available in the TextMessages table for a BBM conversation between two parties. Included in this information is message content, timestamps for sent and received messages, status, state (whether the message has been delivered, read, etc.), PINs, participants, and attachments (if applicable).

**BBM TextMessages Table**

<table>
<thead>
<tr>
<th>RowNo</th>
<th>TextMessageId</th>
<th>Ordered</th>
<th>ParticipantId</th>
<th>ConversationId</th>
<th>ParticipantField</th>
<th>Unbound</th>
<th>Type</th>
<th>Status</th>
<th>Timestamp</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>138253197</td>
<td>Hey! I have some information that might be of value to you...</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>138253126</td>
<td>What kind of information and how much will it cost me?</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>138252325</td>
<td>Good stuff, usual rate</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>138252555</td>
<td>A list of contacts and some internal docs</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>138252975</td>
<td>Sounds good - how do you want to get them to me?</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>138253404</td>
<td>Not email, it's monitored</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>7</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>138253466</td>
<td>I'll put them in a Dropbox account we can use</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>8</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>138253461</td>
<td>OK, let me know when and where</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>138253900</td>
<td><a href="https://www.dropbox.com/sh/bbeo2x2c7x7h0cwi?dl=0">https://www.dropbox.com/sh/bbeo2x2c7x7h0cwi?dl=0</a></td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>10</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>138254099</td>
<td>Thank you!</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>11</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>138254097</td>
<td>I sent payment the usual way</td>
</tr>
</tbody>
</table>

BBM for iOS and Android has also recently been updated to include BBM Channels. Previously only available on BlackBerry devices, BBM Channels allows users to subscribe to various “channels” of interest such as a famous person, brand, or organization. Users can interact with that channel by posting and responding to comments and questions.
BBM TableChannels

There are various tables located within the master.db file which will identify channels that a user has subscribed to. Specifically, investigators should examine TableChannels, ChannelPosts, and ChannelComments for artifacts that may be relevant to their case.
MAKE THIRD-PARTY APP DISCOVERY AND ANALYSIS EASIER WITH INTERNET EVIDENCE FINDER (IEF)

Internet Evidence Finder (IEF) makes recovering mobile evidence easy. Our software automates the artifact discovery process on iOS and Android devices, eliminating the need for manual carving and parsing work. Once IEF is finished searching for evidence, all recovered artifacts are compiled in a case file, where they can be viewed and analyzed by a digital forensic investigator in IEF Report Viewer.

IEF will recover artifacts from hundreds of apps, including the mobile chat apps explored in this guide: Kik Messenger, WhatsApp, and BBM. Typically, an IEF search will find message contents, sender/receiver details, time stamps, and file transfers (depending on the app’s features).

AN EXAMPLE OF WHAT IEF FINDS USING KIK MESSENGER

To demonstrate how IEF can improve your investigation of mobile chat apps, here is an example using Kik Messenger. IEF is able to recover Kik contacts, messages, and attachments from iOS and Android devices. It will parse the SQLite database to identify details such as sender, receiver, message, attachment, timestamps, as well as several other values found in the database. IEF will even carve data from unallocated space in the event that some of the data has been deleted, potentially providing investigators with additional messages and artifacts that aren’t found in the SQLite database tables.
This screenshot shows how a Kik Artifact recovered by IEF would appear in the IEF Report Viewer, where:

1. Shows whether the message was sent or received by the user
2. Unique identifier for the other Kik user in conversation
3. Shows the message status
4. Contents of the message (this message was an attachment so there is no body)
5. Timestamp details
6. Attachment thumbnail

**WHAT’S MORE, WE STAY UP-TO-DATE WITH EVOLVING APPLICATIONS (SO YOU CAN CONTINUE TO RECOVER EVIDENCE)**

Our team dedicates significant engineering resources to keep IEF current, and ensure our customers continue to find the evidence they need from new and updated third-party applications. With the rapidly changing mobile landscape, we stay up-to-date with apps (so you don’t have to), as they are often the richest sources of digital evidence.

Learn how IEF can help you find more evidence on mobile devices by [joining a live online product demonstration](#), or [give IEF a try for free for 30 days](#).