Implementation of Forensic Analysis Procedures for WhatsApp and Viber Android Applications

Auqib Hamid Lone
Department of Computer Science and Engineering,
Jamia Hamdrad
New Delhi, India

Firdoos Ahmad Badroo
Department of Computer Science and Engineering,
Jamia Hamdrad
New Delhi, India

Khairaj Ram Chudhary
Department of Computer Science and Engineering,
Jamia Hamdrad
New Delhi, India

Aqeel Khalique
Department of Computer Science and Engineering,
Jamia Hamdrad
New Delhi, India

ABSTRACT

Communication in today's world is mostly dependent on mobile phones allowing users to exchange messages, ideas, videos and audios. Numerous instant messengers are available for mobile devices which are better alternative over SMS technology. However, increased use of instant messengers also gave rise to its negative impact including unwanted activities pertaining to cyber crimes. WhatsApp and Viber are mostly used instant messengers on Android mobile devices. In this paper, we perform forensic analysis procedures to obtain artifacts of WhatsApp and Viber applications. During analysis, we focus on artifacts such as messages, contacts, chat history, attachments etc. from the memory of mobile device. We present our research findings after implementation of forensic procedures using freely available tools and software. The artifacts obtained during analysis are relevant to use as evidences in court of law against any criminal incident.

General Terms

Android Forensic, Instant Messenger Forensics.

Keywords

Android Forensics, Instant Messenger Forensics, Viber Forensics, WhatsApp Forensics.

1. INTRODUCTION

Communication is a process of connecting people to exchange facts, ideas, impressions or feelings. Communication system requires sender, receiver and a medium. In today's world, several medium are present to conduct effective communication. Technology has given birth to a new communication medium known as wireless communication. Mobile phones use wireless communication media to transmit and receive audio, video or text messages across the world using wireless connection of service providers. One of the required aspects of communication is non-repudiation, where sender cannot deny sending or transmitting intended message to receiver. Excessive use of communication over mobile phones leads to non-repudiation in certain instances where a risk is involved with sender. Most often in litigation and prosecution cases of financial and criminal activities, accused personnel may deny or may not be available for investigation. In such instances, technology helps us to investigate into the matter or testify the true facts to bring digital evidence acceptable in court of law. Digital or cyber forensic is the process of collecting, preserving, analyzing and presenting the digital evidence which is legally acceptable. In digital forensic, analysis is done on data available pertaining to the specific case. Therefore, if there is a heap of data, more chances are to extract fruitful evidences or information out of the heap.In this paper, we implement forensic analysis procedures on two widely used instant messengers namely WhatsApp and Viber. We have organized the paper in the following order: In Section 2 introduces Technology review for Digital Forensics. In Section 3, we study database schema of WhatsApp and Viber applications on Android. In Section 4, we implement the methodologies for analyzing artifacts of WhatsApp and Viber. In Section 5, we present results based on our research findings. In Section 6, we conclude our work and present future scope in digital forensic over mobile phones.

2. TECHNOLOGY REVIEW FOR DIGITAL FORENSICS

2.1 Android Application Data Storage

Android is the world's most popular mobile platform having a large user base. Android provides several options to save persistent application data [1]. Location of data storage depends on accessibility between applications and user and size of applications. Table 1 shows Android Application Data Storage options with mapped with several parameters such as file type, data type, location, access level and their forensic use [2].

2.2 WhatsApp Messenger

WhatsApp is a cross-platform instant messaging application available for Symbian, Asha, Windows Mobile, Android, iOS and Blackberry operating systems [3]. WhatsApp was developed in 2009 by Brian Acton and Jan Koum and was acquired by Facebook in 2014 . WhatsApp has more than 900 million registered users and handling 64 billion messages per day. WhatsApp uses WiFi or mobile internet plan for communicating with other users. WhatsApp is available for free during the first year and later a nominal subscription fee is charged annually. WhatsApp can auto sync to the phone address book allowing unlimited message to the contacts using WhatsApp application. Messages also include attachments to share multimedia like audios, videos, locations, images etc. WhatsApp has started calling feature to the contacts using WhatsApp application. WhatsApp Web is launched to give user device flexibility for running WhatsApp from desktop PC using internet browser. Thus, WhatsApp is an important application for obtaining vital data or information in an hour of need to cyber forensic analyst [4].

Table 1. Android Application Data Storage

Android Application Data Storage Options					
	Shared Preference	**Internal Storage**	**External Storage**	**SQLite**	**Network**
File Type	Key-Value pairs of primitive data stored in light-weight XML format	Files of different formats. Developer based, no restriction	Files of different formats. No restriction	SQLite format (.db). Compact single cross-platform file	Config and network based files mainly. No restriction
Data Type	Boolean, float, int, long, strings	Complicated data structures allowed	Complicated data structures allowed	SQLite supported data types	Complicated data structures allowed
Location	*/data/data/com.android.phone/shared_prefs*	*/data/data* subdirectory	*/mnt/sdcard* or emulated SD card on */mnt/emmc*	internal storage */data/data/<packageName>/databases*	Depends on network settings, info from log files in *data/data/files*
Access Level	Owner can access	Developer controlled unless owner has root access	Owner can access MS FAT32 file system, no security mechanism	Encrypted unless owner has root access	Network level
Forensic Use	Rich source of forensic data	Rich source of forensic data if root access	Rich source of forensic data	Rich source of forensic data	Forensic data from Java.net and android.net

2.3 Viber

Viber is a cross-platform instant messaging application available for Symbian, Asha, Windows Mobile, Android, iOS and Blackberry operating systems. Viber application is developed by four Israeli and Belarusian partners; Talmon Marco, Igor Magazinnik, Sani Maroli and Ofer Smocha in 2010 [5]. Viber is used for making phone calls and send text messages to contacts using Viber application. WhatsApp uses WiFi or mobile internet plan for communicating with other users. Viber is available for free for its registered users. Viber has nearly 600 million registered users. Now, Viber Desktop is launched enabling user to install Viber application on desktop PC and use it for communicating other users with Viber on any device [6]. Viber is also considered an important application from usage perspective and hence, we have included it in our research for conducting cyber forensic analysis.

2.4 Features & Characteristics Comparison of WhatsApp and Viber

In this subsection, we present features and characteristics of WhatsApp and Viber application. Table 2 shows feature comparison of WhatsApp and Viber. Table 3 shows characteristic comparison of WhatsApp and Viber.Figure 1 and Figure 2 show annual population growth of registered users on WhatsApp and Viber applications respectively [7] [8].

Table 2. Feature Comparison of WhatsApp and Viber

	WhatsApp	**Viber**
Text Chat	✓	✓
Send & Receive Videos	✓	✓
Send & Receive Audio	✓	✓
Group Chat	✓	✓
Sharing V-Cards & Contact Information	✓	✓
Free Voice Calling	✓	✓

Free Texting	✓	✓
Free Video Calling	×	✓
Location Data	✓	✓
Desktop Compatibility	✓	✓

Table 3. Characteristic Comparison of WhatsApp and Viber

Characteristics	WhatsApp		Viber	
Supported OS	iOS	✓	iOS	✓
	Android	✓	Android	✓
	Windows Phone	✓	Windows Phone	✓
	BlackBerry	✓	BlackBerry	✓
	Symbian	✓	Symbian	✓
Price	First year free usage, later subscription USD 0.99 per year		Free	
Emoticons	Standard Emoji keyboard		Custom emoticons and stickers	
Group Chat	100 Participants		100 Participants	
Backup Restore	Available		Only text backup available	
Reported Users	≈900 million users		≈600 million users	

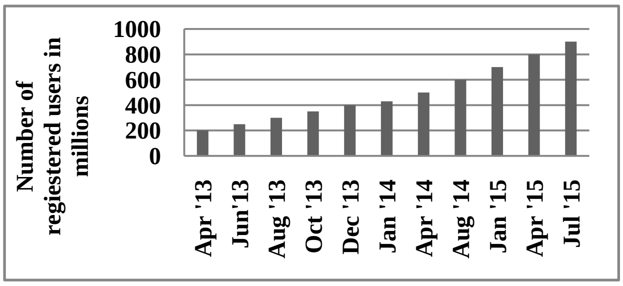


Figure 1: Global population growth of registered users on WhatsApp

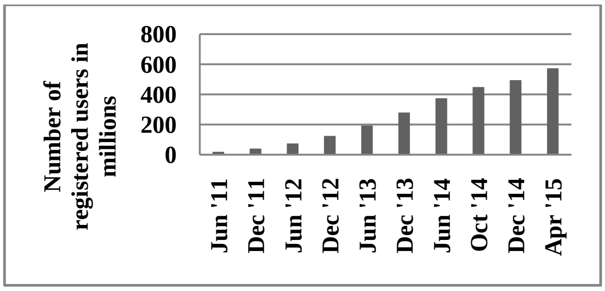


Figure 2: Global population growth of registered users on Viber

3. DATABASE SCHEMA OF WHATSAPP AND VIBER ON ANDROID

3.1 Forensic Analysis of Database Schema of WhatsApp on Android

WhatsApp artifacts such as contacts, messages and attachments can be valuable to examiners looking for recovering evidences during investigation. The key artifacts that need to be found during investigating WhatsApp on Android are SQLite databases *msgstore.db* and *wa.db*. The *msgstore.db* contains details of any chat conversation between user and their contacts. The *wa.db* stores information of user's contact list. Figure 3 shows WhatsApp Database schema containing *msgstore.db* and *wa.db*. Both databases can be found under the database folder at the following defined locations:

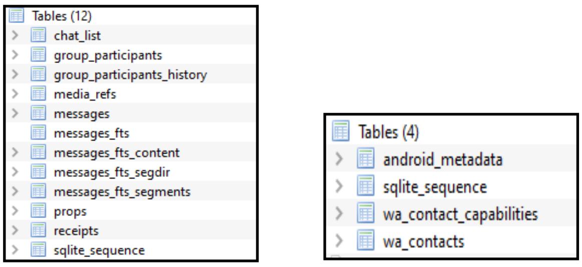
msgstore.db→ /data/data/com.whatsapp/database/msgstore.db

wa.db → /data/data/com.whatsapp/database/wa.db.

The *msgstore.db* is a SQLite database containing two tables namely *chat_list* and *messages*. The *msgstore.db* database contains contacts numbers, message contacts, message status, timestamps, geolocation details of senders and attachments. The attachments have their own table entry linked with message content including thumbnail and link of the attachment. In *messages* table, messages sent or received from contacts are stored. The *wa.db* database contains a complete listing of WhatsApp user contacts including phone numbers, display name, time stamp [9]. WhatsApp stores a copy of *msgstore.db* and *wa.db* on memory (flash/SD card) of mobile device at the following location:

/sdcard/whatsapp/databases/msgstore.db.cypt

However, *msgstore.db* and *wa.db* databases are encrypted and therefore must be decrypted for analysis by rooting the mobile device after acquisition [9].


Tables (12)
chat_list
group_participants
group_participants_history
media_refs
messages
messages_fts
messages_fts_content
messages_fts_segdir
messages_fts_segments
props
receipts
sqlite_sequence

Tables (4)
android_metadata
sqlite_sequence
wa_contact_capabilities
wa_contacts

a) msgstore.db Schema **b) wa.db Schema**

Figure 3: Snapshot of WhatsApp Database Schema in SQLite Browser

3.2 Forensic Analysis of Database Schema of Viber on Android

Viber artifacts relevant to forensic investigations are stored within SQLite databases. To access important Viber artifacts, analyst must root or get a physical acquisition of the Android device. Viber artifacts on Android are stored found at the following locations:

/data/data/com.viber.voip/databases/viber_data

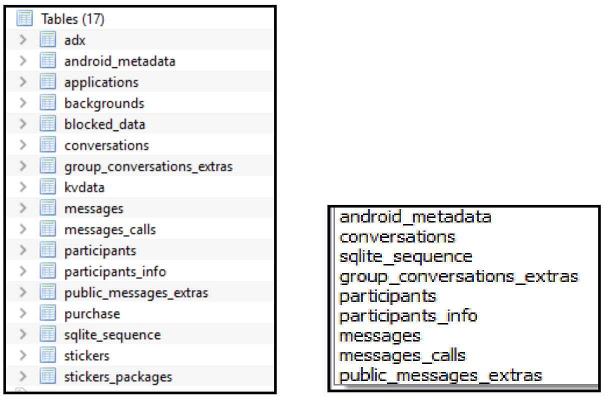
/data/data/com.viber.voip/databases/viber_messages

These databases store details on the Viber user’s contacts, messages and attachments sent and received through Viber application.

- Viber Contacts - User contacts in Viber are stored within the *viber_data* SQLite database.
- Viber Messages - Given that Viber is an IM with call capability, it’s likely that the most valuable evidence will be found in the conversation.
- Viber Attachments - Viber also supports the transfer of photos. Photos – sent from either the camera or gallery are stored on the mobile device. Attachment also includes a “description” entered by the sender of the attachment.

Figure 4 shows a snapshot of database tables of Viber application available through SQLite Browser and Cerbero.

Further, Table 4 presents collective list of WhatsApp and Viber application with available databases along with tables present in corresponding databases [10].



Tables (17)
adx
android_metadata
applications
backgrounds
blocked_data
conversations
group_conversations_extras
kvdata
messages
messages_calls
participants
participants_info
public_messages_extras
purchase
sqlite_sequence
stickers
stickers_packages

android_metadata
conversations
sqlite_sequence
group_conversations_extras
participants
participants_info
messages
messages_calls
public_messages_extras

(a) Snapshot from SQLite Browser (b) Snapshot from Cerbero

Figure 4: Database Tables in Viber Application

Table 4. Application Database and Table name

Application	File Name	Table Name
WhatsApp	*msgstore.db*	messages chat_list
	wa.db	wa_contacts sqlite_sequence
Viber	*viber_call_log.db*	Viber_call_log
	viber_data	android_metadata phonebook raw contact phonebook contact phonebook data Viber numbers Calls
	viber_messages	android_metadata messages’ sqlite_sequence threads participants

4. IMPLEMENTATION OF FORENSIC PROCEDURES

In this paper, we implement forensic procedures to determine available evidences which might be helpful in determining results during forensic analysis. We have targeted the scope of our research to WhatsApp and Viber only for sole reason of their prevalent use. For analysis, we have taken a sample device Micromax Canvas A74 smartphone running Android 4.2.2 JellyBean operating system as acquired device. List of required software and tools for forensic procedures are tabulated in Table 5 below:

Table 5. List of Application Required for Forensic Procedures

Application	Available at	Paid/Free
Titanium Backup Android Application	Google Play Store	Free
FramaRoot	www.framaroot.net	Free
RootChecker	Google Play Store	Free
WhatsApp Viewer	http://andreas-mausch.github.io/whatsapp-viewer/	Free
Cerbero Profiler 2.4	http://cerbero.io /profiler/	Free (Trial Version)
SQLite Browser	sqlitebrowser.org/	Free

We will present stepwise methods which were implemented during our research to determine artifacts. In subsection 4.1, initial prerequisite tasks are performed on mobile device such rooting the mobile device and backing up of required application. In subsection 4.2, we focus on WhatsApp and Viber applications.

4.1 Initial Pre-requisite Tasks on Mobile Device

Step 1: Mobile device is rooted using Android rooting application FramaRoot.

Table 6 shows detailed methods of rooting the mobile device using FramaRoot application.

Further, we can verify that mobile device is successfully rooted or not by installing RootChecker Application and running it. However, this verification is optional method.

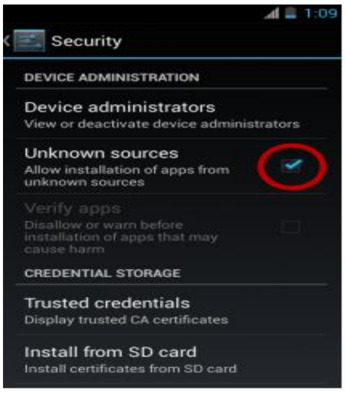
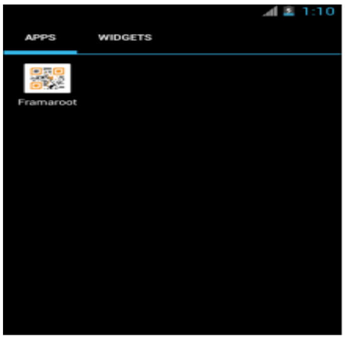
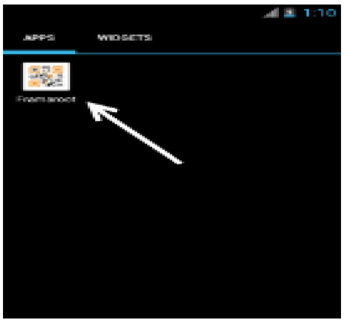
Step 2: Backup of messages using Titanium Backup Application

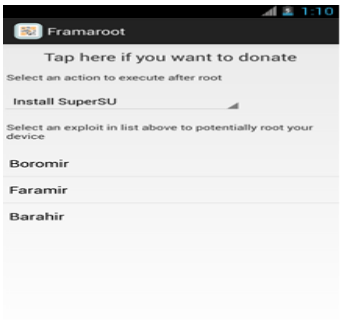
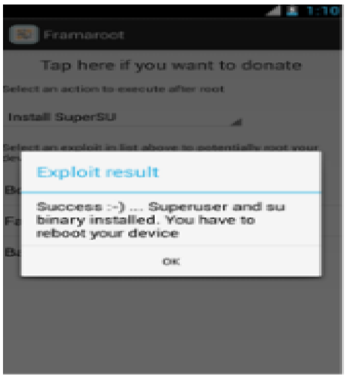
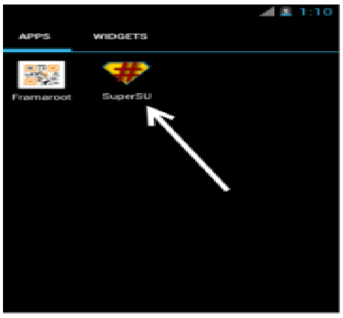
After rooting mobile device, backup of message are done using Titanium Backup Application. Manual setting of Titanium Backup is done to corresponding application either WhatsApp or Viber.

Step 3: Identify and locate zip folder within Titanium Backup folder on SD card location of mobile device. Copy the identified zipped folder from Titanium Backup folder to desktop PC after connecting mobile device to desktop PC. (For WhatsApp, zipped folder starts with name com.whatsapp and for Viber, zipped folder starts with com.viber.voip)

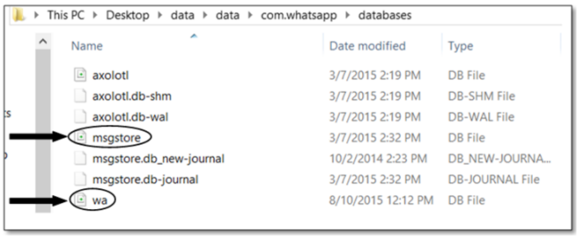
Step 4: Backup Extracted from Titanium Backup Application on Desktop PC.

Table 6. Rooting Mobile Device using FramaRoot Application

S. No.	Methods	Snapshots
1.	Enable installation of third party apps on mobile device. To enable, open Settings > Security > Device Administration > Unknown Sources (check to enable).	 1:09 Security DEVICE ADMINISTRATION Device administrators View or deactivate device administrators Unknown sources ☑ Allow installation of apps from unknown sources Verify apps □ Disallow or warn before installation of apps that may cause harm CREDENTIAL STORAGE Trusted credentials Display trusted CA certificates Install from SD card Install certificates from SD card
2.	Download and install FramaRoot Application on mobile device. After installation, FramaRoot icon is displayed in the App Menu.	
3.	Run FramaRoot, by tapping on the FramaRoot App icon.	

4.	When FramaRoot Application is launched, image shown beside is visible on the screen of mobile device.	 1:10 Framaroot Tap here if you want to donate Select an action to execute after root Install SuperSU Select an exploit in list above to potentially root your device Boromir Faramir Barahir
5.	In earlier snapshot, two options (Boromir and Faramir) are available. Select any option to start rooting process (for example, we select Boromir). A success message will be displayed and prompt to restart the mobile device.	 1:10 Framaroot Tap here if you want to donate Select an action to execute after root Install SuperSU Exploit result Success :-) ... Superuser and su binary installed. You have to reboot your device OK
6.	After restarting, the mobile device is rooted and an additional application SuperSU is available in App Menu confirming successful rooting of the mobile device.	 1:10 APPS WIDGETS Framaroot SuperSU

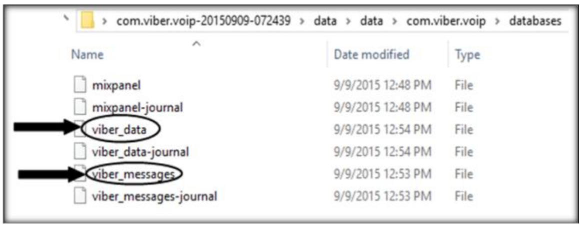
After copying the zipped folder, we unzipped the required folder. Figure 5 shows required directory structure of copied folder from com.whatsapp (WhatsApp backup is done using Titanium Backup Application) and Figure 6 shows required directory structure of copied folder from com.viber.voip. In Figure 5, *msgstore.db* and *wa.db* files as encircled in figure are required for forensic analysis (applicable for WhatsApp) whereas in Figure 6, *viber_data* and *viber_messages* files as encircles in figure are required for forensic analysis (applicable for Viber).



This PC › Desktop › data › data › com.whatsapp › databases

Name	Date modified	Type
axolotl	3/7/2015 2:19 PM	DB File
axolotl.db-shm	3/7/2015 2:19 PM	DB-SHM File
axolotl.db-wal	3/7/2015 2:19 PM	DB-WAL File
msgstore	3/7/2015 2:32 PM	DB File
msgstore.db_new-journal	10/2/2014 2:23 PM	DB_NEW-JOURNA...
msgstore.db-journal	3/7/2015 2:32 PM	DB-JOURNAL File
wa	8/10/2015 12:12 PM	DB File

Figure 5: Snapshot of Unzipped *com.whatsapp* Folder Directory



com.viber.voip-20150909-072439 › data › data › com.viber.voip › databases

Name	Date modified	Type
mixpanel	9/9/2015 12:48 PM	File
mixpanel-journal	9/9/2015 12:48 PM	File
viber_data	9/9/2015 12:54 PM	File
viber_data-journal	9/9/2015 12:54 PM	File
viber_messages	9/9/2015 12:53 PM	File
viber_messages-journal	9/9/2015 12:53 PM	File

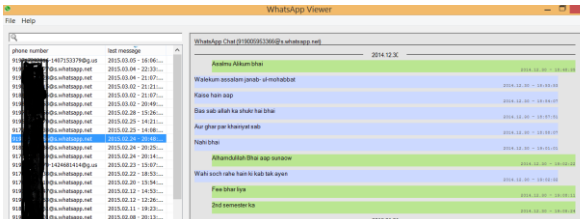
Figure 6: Snapshot of Unzipped *com.viber.voip* Folder Directory

4.2 Forensic Analysis of WhatsApp and Viber

In this subsection, we focus on WhatsApp application for forensic analysis to determine artifacts from the mobile device. After taking backup of WhatsApp application data, tools like WhatsXtract, SQLite browser, WhatsApp Viewer etc. are required to determine artifacts. These tools present artifacts to the analyst in readable and presentable format. WhatsApp Viewer is a small tool to display chats from WhatsApp files such as *msgstore.db.crypt5*, *msgstore.db.crypt7* and *msgstore.db.crypt8*. Among all available tools, WhatsApp Viewer is most convenient and simple to use because of the following features listed below [11].

- View WhatsApp chats on PC
- Phone backup
- Conveniently read old conversations without pressing "load older messages"
- Search all messages
- No need to install Python, SQLite or additional libraries
- Small application, no dependencies, no need to install

4.2.1 For analysis of WhatsApp artifacts, we have used WhatsApp Viewer. Figure 7 shows snapshot of WhatsApp messages in WhatsApp viewer. Analyst can browse through available contacts and read messages exchanged between user of mobile device and contacts.



[redacted]

phone number	last message
-1407153379@g.us	2015.03.05 - 16:06:...
@s.whatsapp.net	2015.03.04 - 22:33:...
@s.whatsapp.net	2015.03.04 - 21:07:...
@s.whatsapp.net	2015.03.02 - 21:21:...
@s.whatsapp.net	2015.03.02 - 21:07:...
@s.whatsapp.net	2015.03.02 - 20:49:...
@s.whatsapp.net	2015.02.28 - 15:26:...
@s.whatsapp.net	2015.02.25 - 14:21:...
@s.whatsapp.net	2015.02.25 - 14:08:...
@s.whatsapp.net	2015.02.24 - 20:48:...
@s.whatsapp.net	2015.02.24 - 20:25:...
@s.whatsapp.net	2015.02.24 - 20:14:...
-1424681414@g.us	2015.02.23 - 15:07:...
@s.whatsapp.net	2015.02.22 - 18:53:...
@s.whatsapp.net	2015.02.20 - 15:54:...
@s.whatsapp.net	2015.02.12 - 14:53:...
@s.whatsapp.net	2015.02.12 - 12:26:...
@s.whatsapp.net	2015.02.11 - 19:23:...
@s.whatsapp.net	2015.02.08 - 20:13:...

WhatsApp Chat (919005953366@s.whatsapp.net)

2014.12.30

Asalmu Alikum bhai 2014.12.30 - 18:48:55

Walekum assalam janab- ul-mohabbat 2014.12.30 - 18:53:53

Kaise hain aap 2014.12.30 - 18:54:07

Bas sab allah ka shukr hai bhai 2014.12.30 - 18:57:51

Aur ghar par khairiyat sab 2014.12.30 - 18:58:07

Nahi bhai 2014.12.30 - 19:01:01

Alhamdulilah Bhai aap sunaow 2014.12.30 - 19:02:22

Wahi soch rahe hain ki kab tak ayen 2014.12.30 - 19:02:42

Fee bhar liya 2014.12.30 - 19:08:11

2nd semester ka 2014.12.30 - 19:08:24

Figure 7: Snapshot of WhatsApp Viewer

4.2.2 For analysis of Viber artifacts, we have used Cerbero and SQLite Browser. The unzipped folder com.viber.voip obtained from Titanium Backup Application contains *viber_messages* and *viber_data*. Figure 8 and Figure 9 shows snapshot of Viber artifacts in *viber_messages* and *viber_data* respectively available in Cerbero.

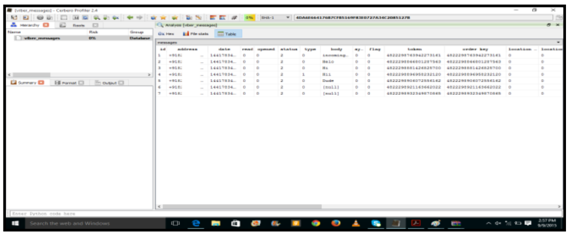


Figure 8: Snapshot of Cerbero displaying Viber artifacts obtained from *viber_messages*

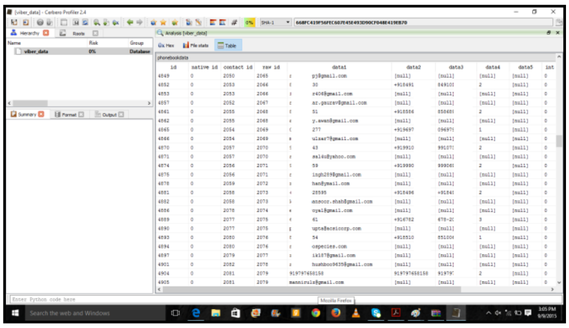


Figure 9: Snapshot of Cerbero displaying Viber artifacts obtained from *viber_data*

We have also studied Viber artifacts from files *viber_message* and *viber_data* using SQLite Browser. Figure 10 and Figure 11 shows snapshot of Viber artifacts in *viber_messages* and *viber_data* respectively available in SQLite Browser. Although, we observe differences in displayed artifacts in Cerbero and SQLite Browser. For instance, database schema of Viber is not available in Cerbero, however, displayed in SQLite Browser. Location of sender is not available in SQLite Browser, however, it is available in Cerbero.

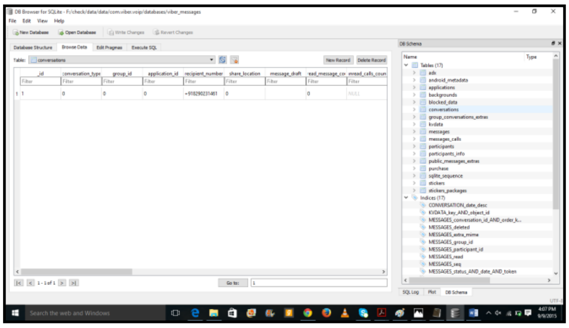


Figure 10: Snapshot of SQLite Browser displaying Viber artifacts obtained from *viber_messages*

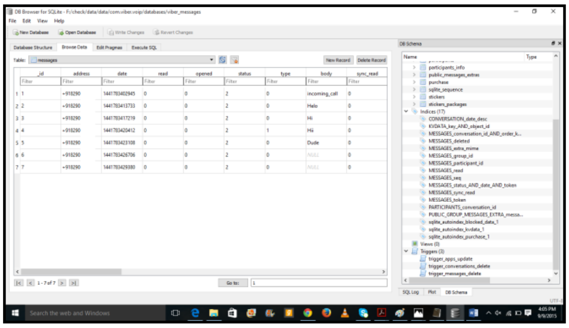


Figure 11: Snapshot of SQLite Browser displaying Viber artifacts obtained from *viber_data*

5. RESULTS OF RESEARCH FINDINGS AND FORENSIC ANALYSIS

In this section, we present our research findings based on our analysis for WhatsApp and Viber. Table 7 presents the research findings of forensic analysis for WhatsApp. In this table, different artifacts such as phone numbers, messages, media files etc. have been obtained. However, these artifacts are encrypted and thus unreadable to analyst. When we perform our analysis after rooting the mobile device, these artifacts are obtained in readable and presentable form. Legends used in Table 6 are shown below with their intended meaning.

Table 7. Research Findings of Forensic Analysis for WhatsApp

	Unrooted Mobile Device	Rooted Mobile Device
msgstore.db	✓□	✓
wa.db	✗	✓
Phone Numbers	✓□	✓
Messages	✓□	✓
Media Files	✓□	✓

Contact Cards	✓□	✓
Location	✓□	✓
SQL queries	✓□	✓
Profile Pictures	✓	✓
Logs	✗	✓□
Directory Structure	✗	✓□
Deleted Messages	✗	✓□
WhatsApp Call	✗	✓□

Legends used in Table 7

✓□ *.....Found Encrypted*

✗ *………. Not Found*

✓*………. Found*

Table 8 presents the research findings of forensic analysis for Viber. Both files *viber_data* and *viber_messages* are analyzed and results are presented. Table 8 shows different artifacts such as Viber numbers, messages, number of calls etc. have been obtained.

Table 8. Research Findings of Forensic Analysis for Viber

Artifacts Found in *viber_data*	**Artifacts Found in *viber_messages***
Viber Numbers	Messages to Viber users
Total number of calls made	Phone numbers of the recipient of messages
Phone numbers at which calls were made	Phone numbers of the sender of messages
Duration of each calls	Time and date of sent and received messages
Time and date of calls	Message statistics for each contact

The scope of this research is focused on obtaining artifacts from Android instant messengers (specifically Viber and WhatsApp). These artifacts such as text messages, audio calls to any suspicious contact, image/video or location coordinates etc. are used in investigation for providing digital evidence that is acceptable in court of law against any criminal activity. These research findings help in forensic investigation as proofs for prosecuting a criminal who has committed any crime.

6. CONCLUSION

In this paper, we have presented forensic analysis of WhatsApp and Viber Android applications. We performed implementation of forensic procedures for WhatsApp and Viber applications. We performed comparative study of database design and features available in WhatsApp and Viber applications. The aim was to determine key artifacts present in memory of mobile devices using available tools and software. We have tabulated our research findings obtained from WhatsApp and Viber applications. The research findings include artifacts that help forensic investigators and investigation agencies during any criminal incident and can be used as evidence in court of law. In future, recovery of artifacts of instant messenger applications residing on RAM of mobile device can be a part of our research scope.

7. ACKNOWLEDGMENTS

We thank our friends for motivation and support in presenting this paper.

8. REFERENCES

[1] [Online]https://en.wikipedia.org/wiki/Android_(operating_system)

[2] Thakur. S. N. 2013 Forensic Analysis of WhatsApp on Android Smartphones. University Of New Orleans

[3] [Online] http://www.whatsapp.com

[4] [Online] http://blog.whatsapp.com/

[5] [Online] https://en.wikipedia.org/wiki/Viber

[6] [Online] http://www.viber.com/en/

[7] [Online] http://www.statista.com/statistics/316414/viber-messenger-registered-users/

[8] [Online] http://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/

[9] [Online] http://iloapp.cybersecurityspecialist.com/blog/blog?Home&category=5

[10] Mahajan A., Dahiya M. and Sanghvi H. 2003. Forensic Analysis of Instant Messenger Applications on Android Devices. International Journal of Computer Applications (April 2013), 0975 – 8887.

[11] [Online]http://andreas-mausch.github.io/whatsapp-viewer/