Scholars Journal of Engineering and Technology
OPEN ACCESS
Abbreviated Key Title: Sch J Eng Tech
ISSN 2347-9523 (Print) | ISSN 2321-435X (Online)
Journal homepage: https://saspublishers.com/journal/sjet/home

Digital Forensic Investigation of WhatsApp on Android

Ming-Sang Chang*

Department of Information Management, Central Police University, Taoyuan, Taiwan

***Corresponding author:** Ming-Sang Chang
| **Received:** 15.03.2019 | **Accepted:** 27.03.2019 | **Published:** 30.03.2019
DOI: 10.36347/sjet.2019.v07i03.002

Abstract | **Original Research Article**

The trend in social networking is changing people's life style. Therefore, the modes of cybercrime have also changed in accordance with the users' activities. In order to identify crimes, it is necessary to use appropriate forensic techniques to retrieve these traces and evidence. This study considers the social network, WhatsApp Messenger, as the research subject. We analyze the artifacts left on the WhatsApp Messenger application and show evidences of gathering on the Android platform. This study explores the differences between the traces that are left on Non-Rooted and Rooted Android platform. It proves to be helpful to forensic analysts and practitioners because it assists them in mapping and finding digital evidences of WhatsApp Messenger on Android smart phone.
Keywords: Social Networking, Mobile Forensics, Crime Investigation, WhatsApp Messenger.

INTRODUCTIOIN

Nowadays, social networking sites are increasingly popular. The popularity of social networking sites has given rise to the number of social networking users for business, recreation or any other likely purposes. Over the past few years, social networking sites have been significant mediums for people to enhance their interpersonal relationships. The prevalence of social networking websites has changed the living habits of many people. They share their emotion or daily life with their friends via texting, photographing or videoing. There is no doubt that people have incorporated social networking sites into their lives and made using social networking sites a frequent daily activities.

WhatsApp Messenger is a freeware and cross-platform messaging service owned by Facebook. The application allows the sending of text messages and exchange photos, videos, stickers, audio, documents, and user location. The service also supports voice and video calling. The application can be run on a mobile device, and it is also accessible from desktop computers. The service requires users to provide a cellular mobile number. By February 2018, WhatsApp had 1.5 billion monthly active users. That made it the most popular messaging application at the time [1].

Social networking websites provide a virtual exchange space on the Internet for people with common interests, hobbies, and activities to easily share, discuss, and exchange their views without any limitation of space and time. Therefore, social networking websites continue to accumulate a large number of users. According to the Metcalfe's law, the value of a telecommunications network is proportional to the square of the number of connected users of the system [2]. As a result, social networking has become a great force in today's society. However, this has also brought about endless criminal activities on social networks, such as cyberbullying, social engineering, and identity theft, among the other issues.

There are four main characteristics about cybercrime. They are anonymity, diffuseness, cross-regional feature, and vulnerability of Evidence. Users are often unaware of the true identity of their counterpart in a social network because they are dealing with a fake account. Therefore, in the case of a social network cybercrime, it is difficult to extract the suspect's information and make arrests immediately [3]. Any news published on the social network will be forwarded or shared immediately, which generates the diffusion effect [4]. Therefore, if a social network crime is not responded to immediately, it may cause the victim to suffer some serious damage. Due to the nature of Internet, the location of the cybercrime is not necessarily the place where the criminal suspects are located. A bottleneck is formed during the crime investigation due to the difficulty in locating the suspects [5]. The evidences obtained on social networks are in the form of digital data. In addition to the highly volatile nature of the digital evidences in the processing program from collection to storage, it is easy to change,

delete, lose, or contaminate the digital evidences due to the anti-forensics operation of the suspects or negligence of the investigators [6]. Due to these characteristics, the detecting cybercrime on social networks is different in comparison to other cybercrime [7]. Therefore, to assist the investigators in improving their efficiency of solving crimes, researches focusing on these upcoming technologies are needed [8].

This study considers the social network, WhatsApp Messenger, as the study subject. User activities are performed through Android smart phones. Forensic analysis is conducted to understand what type of user behavior leaves digital evidence on Android. We explore the differences between the traces that are left on Non-Rooted and Rooted Android platform. The results will be served as a reference for the future researchers in social network cybercrime investigation or digital forensics.

The rest of this paper is organized as follows. In the next section, we present the related works. In Section 3, we present our methodology. In section 4, we present the results and findings of digital forensics on WhatsApp Messenger. In section 5, we discuss the findings. Finally, we summarize conclusions.

RELATED WORKS

The evidences were stored on three principle areas by using instant messenger (IM). They are hard drive, memory, and network. Some IM services have the ability to log information on the user's hard drive. To use an IM, an account must be established to create a screen name provided with user information. Some instant messenger providers might assist the investigation with information of the account owner.

Evidence can be found in various internet file caches used by Internet Explorer for volatile IM and each cache holds different pieces of data. Apart from the normal files, files left by instant messenger on a hard drive can be in temp file format and will generally be deleted could be very difficult to retrieve once the machine is power down. An operating system generally stores information of all the installed and uninstalled applications in the system. The uninstalled application also leaves evidence. If a user has deleted an instant messenger application, there is a chance that a record can be found in the registry to prove that the instant messenger has once installed onto the system. Information is also stored within the memory. Since every application requires memory to execute, it is logical to think that there evidence could be left behind in the system's memory. The analysis on live memory allows us to extend the possibility in providing additional contextual information for any cases.

Presently, various researches focusing on the forensic analysis of social networking are being conducted. Artifacts of instant messaging have been of interest in many different digital forensic studies. Many work focused on artifacts left behind by many instant messaging applications. Sgaras analyzed Skype and several other VoIP applications for iOS and Android platforms [9]. It was concluded that the Android apps store far less artifacts than of the iOS apps. Iqbal studied the artifacts left by the ChatON IM application [10]. The analysis was conducted on an iPhone running iOS6 and a Samsung Galaxy Note running Android 4.1. Walnycky added that artifacts of the Facebook Messenger could vary depending on user settings, OS version, and manufacturer [11]. Azfar adapt a widely used adversary model from the cryptographic literature to formally capture a forensic investigator's capabilities during the collection and analysis of evidentiary materials from mobile devices [12]. William Glisson explored the effectiveness of different forensic tools and techniques for extracting evidences on mobile devices [13]. Christoforos Ntantogian made a privacy assessment of Android mobile devices and their apps for forensic analysis and found some security concerns in certain Android apps [14]. Nikos Virvilis presented studies based on the security of web browsers and reported the shortcomings and vulnerabilities of browsers operated on desktop and mobile devices. It was found that some browsers using secure browsing protocols had actually limited their own protection level [15]. Nor Zarina Abidin published a forensic analysis study of Instagram on iPhone and reported the integrity and address of some material evidences of user behaviors extracted [16]. Jia-Rong Sun proposed the viewpoints of cybercrime investigation and forensic procedures for the research of investigation and forensic procedures [17]. Yusoff report the results of investigation and analysis of three social media services (Facebook, Twitter, and Google +) as well as three instant messaging services (Telegram, OpenWapp, and Line) for forensic investigators to examine residual remnants of forensics value in Firefox OS [18]. Song-Yang Wu describes several forensic examinations of Android WeChat and provides corresponding technical methods [19].

This paper investigated the user activities of WhatsApp Messenger through Android smart phones. We conducted forensics on Non-Rooted and Rooted Android platform, and explored and compared the type of user behavior that leaves digital evidence on the device. The results will be served as a reference for the future researchers in the social network cybercrime investigation or digital forensics.

METHODOLOGY

In our research, we use the smart phone with an installation of WhatsApp Messenger. The study was focused on identifying data remnants of the activities of WhatsApp on an Android platform. This is undertaken to determine the remnants an examiner should search for when Instant Messenger is suspected. Our research

includes the circumstances of Non-Rooted and Rooted Android platform.

Rooting is a process of allowing users to gain privileged control which is known as root over the various Android systems. The devices include mobile phones, tablets or any other electronic device that is running Android mobile operating system could obtain highest authority when they rooted the phone. Rooting is often carried out with the aim of overcoming limitations that mobile operators and developers put on some devices. Therefore, in order to obtain more information on the mobile phone, the investigators should execute a series of rooting processes before examining a mobile phone.

Research Goal

This paper studies the user behaviors, including logging into WhatsApp Messenger, uploading files, exchanging information, GIS location sharing, and other application functions under the Non-Rooted and Rooted Android environment. The study also explored and compared the type of user behavior that leaves digital evidence on the device. We explore the differences between the artifacts that are left on Non-Rooted and Rooted Android platform. We checked the changes and discrepancies in the residual digital data and relevant material evidence on the Android smart phone.

Experimental Environment and Tools

- In this paper, all the experiments were conducted on the real system. This study is built on Sony Xperia Z1 C6902 with Android 4.3. Under the Android operating environment, the WhatsApp Messenger social networking application was installed to run the WhatsApp features directly.
- XRY is a commercial digital forensics and mobile device forensics product by the Swedish company Micro Systemation. It used to analyze and recover information from mobile devices. XRY is designed to recover the contents of a device in a forensic manner so that the contents of the data can be relied upon by the user. The XRY system allows for both logical examinations and also physical examinations.
- Autopsy is free computer software that makes it simpler to deploy many of the open source programs. The graphical user interface displays the results from the forensic search of the underlying volume making it easier for investigators to flag pertinent sections of data.
- WinHex is a hex editor useful in data recovery and digital forensics. WinHex is a free powerful application that you can use as an advanced hex editor, a tool for data analysis, editing, and recovery, a data wiping tool, and a forensics tool used for evidence gathering.
- SQLite is a software library that provides a relational database management system. SQLite database is integrated with the application that accesses the database. The applications interact with the SQLite database read and write directly from the database files stored on disk. SQLite is an open source. SQL database stores data to a text file on a device. Android comes in with built in SQLite database implementation. The physical smart phone uses SQLite to read and analyze the database files on mobile devices.
- Android debug bridge (ADB) is a versatile command-line tool that lets users communicate with connected Android devices or emulators. Android debug bridge command also facilitates a variety of devices actions, for example, installing or debugging applications.
- All the specifications of the tools we used are listed in the Table 1.

Table-1: List of hardware and software used for analysis

Devices / Tools	Description	Specification / Versions
Sony Xperia Z1 C6902	Android Smart Phone	Android 4.3, Memory 2GB/16GB
XRY	Mobile Forensics Tool	Version v7.4.1
Autopsy	Digital Forensics Tool	Version v4.4.1
WinHex	Digital Forensics Tool	Version v18.9
SQLite Expert Personal	Database Management Tool	Version v3.5.96.2516
WhatsApp Messenger	Social Networking App	Version v2.17.395
Minimal ADB and Fastboot	ADB Tool	Version v10.0.16299.371

Experiment Elaboration

We separated the experiments into two categories: Non-Rooted and Rooted Android platform. We do the same experiments in the Non-Rooted and Rooted Android platform and compare the relevant evidences.

We divided the experiments into following three scenarios according to the different forensics tools, XRY, Autopsy, WinHex, to ensure the integrity of digital evidence and avoid the interference between digital evidences. Based on the experimental environment designed, we run WhatsApp features, including logging in, sending messages, exchanging photos, videos, audio, and files, making a call, etc. Finally, the relevant evidence on each device was extracted and analyzed using forensic tools.

They are three experiment scenarios such as scenario 1: XRY, scenario 2: Autopsy, and scenario 3: WinHex. In the three experiment scenarios, we do the same experiment steps but replace the forensics tool.

XRY is a commercial tool specifically for mobile phone forensics. Besides XRY tool, we need backup the image file of smart phone to analyze for Autopsy and WinHex. We create an image file for physical memory on the smart phone and use forensic tools to extract and analyze important digital evidences from the image file.

We can extract data and create image file from physical memory. We connect the mobile phone with the computer by using the phone cable. First, we enter "adb devices" command to connect the two devices. If the two devices are connected, the message will show the list of devices attached. Next, we enter "adb shell" command to execute remote control and now the mark sign will become "$". Then, we need to obtain the administrator-level permissions. Thus, we enter "su' command and the mark sign will become "#". Now, we can enter "busybox df -h" command to inspect the system partition, path, volume, space usage, available space and so on. However, most of the application data installed and stored on the phone would locate at the data partition. Therefore, we are interested in this data partition. The path of data partition is "/dev/block/by-name/data". Now, we use "dd" command to create an image file for this partition. "dd" command can perform physical imaging by adopting bit-by-bit method. We enter "busybox dd if=/dev/block/by-name/data of=/storage/MicroSD/test conv=noerror bs=4096" command to create an image file. The string behind "if" is a partition that we would create an image file. The string behind "of" is image output path. In the experiment, we name the output image file "test.img" and store it on the external SD card. The "conv=noerror" represents that there is no interruption when there is an error occurs. The "bs" represents the block size that we would write and read per time.

After we complete the image file creation, we need to put this image file into the computer in order to facilitate analyzing it. Therefore, we enter "adb pull /storage/MicroSD/tset.img C:\ImageFile". We put this image file into the "ImageFile" folder on the drive C. After that, we make use of Autopsy and WinHex to analyze this image file.

The experiment steps are summarized as follows

- We install WhatsApp Messenger on the smart phone, and the forensic tool on the personal computer.
- We logged into WhatsApp Messenger for running various features for any material evidence left by the users.
- After the activities completed, WhatsApp Messenger is logged out.
- Use the forensic tool to find out all kinds of artifacts about WhatsApp Messenger on smart phone.
- Perform a comprehensive evidences analysis.

RESULTS AND FINDINGS

In this section, we will use three scenarios to describe the result and findings. Each scenario has two modes that are rooted mode and Non-Rooted mode. The details of result and findings are as follows.

Scenario 1: XRY

In the scenario 1, we follow the experiment steps as Experiment Elaboration section and use the XRY tool to find the evidences of the activities on the WhatsApp.

Non-Rooted Mode

The mobile version of WhatsApp needs to use the mobile phone number to login and set up the account and other user information. In addition, WhatsApp does not have a password setting. We use the forensic tool XRY to extract various artifacts from WhatsApp, including its own nickname, account profile picture, registered phone number, friend nickname, etc. Because XRY can downgrade the version of WhatsApp to bypass the protection mechanism, we can extract more artifacts from the downgrading version.

Using the XRY tool to find the evidences on the WhatsApp, we can find the user account information. The artifacts of user account can be found as Figure 1. The phone number is +886978878121. The account name is mousepig494949. WhatsApp number is 886978878121@s.whatsapp.net. The profile picture is me.jpg. The location of profile picture is /data/data/com.whatsapp/files/Avatars/.

The artifacts of friend account can be found as Figure 2. The phone number is +886985028322. The account name is Whatsapptest. WhatsApp number is 886985028322@s.whatsapp.net. The nickname is Test_1. The profile picture is 886985028322@s.whatsapp.net.jpg. The location of profile picture is /data/data/com.whatsapp/files/.

The artifacts of sending text, image, audio, video, GIS location, and GIF animation can be found. For an example, we show the artifacts of GIS location as Figure 3. The location name, longitude, latitude, location sharing time, and basic information of both parties can be found.

The artifacts of making a call can be found. We can find the calling record that includes the call time, and who making the call. For an example, the artifacts of making a call are as Figure 4. The first line of Figure 4 shows that "Test_1" made a voice call to "mousepig494949" at "2017/11/15 12:41:28", and "mousepig494949" did not answer the call.

Fig-1: The artifacts of user account

Fig-2: The artifacts of friend list

Fig-3: The artifacts of GIS location

WhatsApp	Missed	2017/11/15 下午 12:41:28 UTC (Network)		Device	Test_1 +886985028322	mousepig494949 886978878121
WhatsApp	Dialed	2017/11/15 下午 12:42:16 UTC (Network)	Video	Device	mousepig494949 886978878121	Test_1 +886985028322
WhatsApp	Dialed	2017/11/15 下午 12:47:29 UTC (Network)		Device	mousepig494949 886978878121	Test_1 +886985028322

Fig-4: The artifacts of making a call

About the database, there are two main databases for the recovered WhatsApp artifacts. They are msgstore.db and wa.db database. The messages are stored in the msgstore.db database, and the account information is stored in the wa.db database. The wa.db are located on /data/data/com.whatsapp/databases/. There are two important tables in the wa.db database. They are wa_contacts table, and sqlite_sequence table. The wa_contacts table is shown in Figure 5. There are many columns in Figure 5. WhatsApp ID is in the JID column. The input status is in the STATUS column. The UNIX time of the input status is in the STATUS_TIMESTAMP column. The registered phone number is in the NUMBER column. The nickname is in the DISPLAY_NAME column. The sqlite_sequence table contains the number of friends.

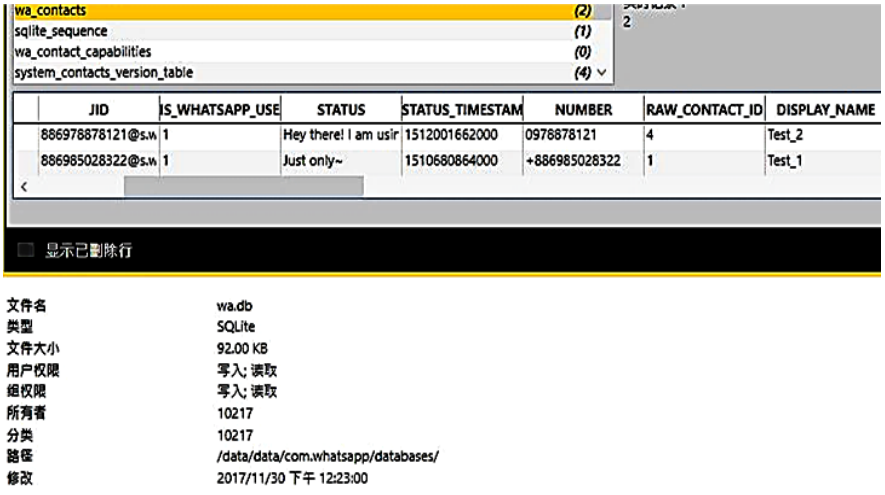

Fig-5: The artifacts of wa_contacts table

There are three important tables in the msgstore. db database. They are sqlite_master table, chat_list table, and messages table. The sqlite_master table shows the meaning of all tables in the msgstore. db database. The chat list table contains the number of all friends and the total number of messages sent. The

messages table contains the content of exchanging messages. The messages table is shown in Figure 6. There are many columns in Figure 6. WhatsApp number is in the KEY_REMOTE_JID column. The message delivery direction is in the KEY_FROM_ME column. The message number is in the KEY_ID column. Types of message are in the STATUS column. The content of message is in the DATA column. The time of delivery message is in the TIMESTAMP column.

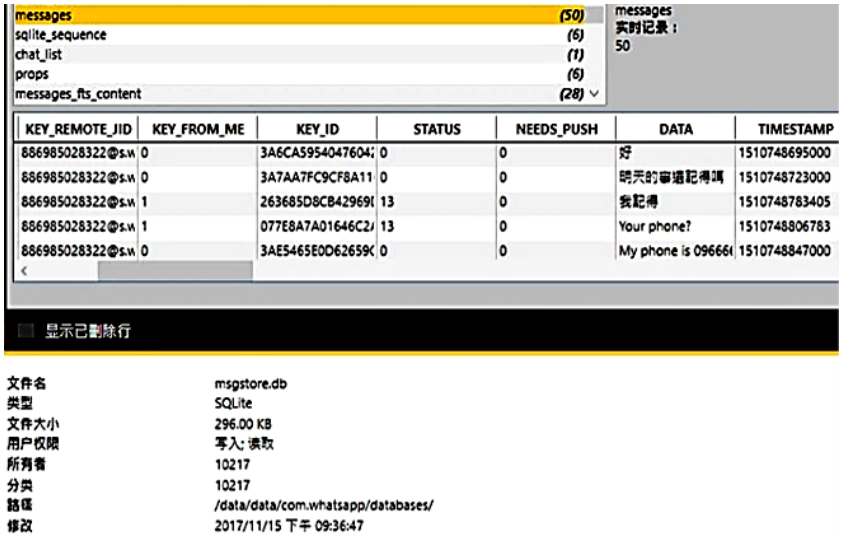

Fig-6: The artifacts of messages table

Table-2: The storage path of various traces in WhatsApp

Artifacts	Storage Path
Profile Picture	/data/data/com.whatsapp/files/
Friend Profile Picture	/data/data/com.whatsapp/files/Avatars/
Image	/data/data/com.whatsapp /Media/WhatsApp Images/
Video	/data/data/com.whatsapp /Media/WhatsApp Video/
GIFAnimation	/data/data/com.whatsapp /Media/WhatsApp Animated Gifs/
Audio	/data/data/com.whatsapp /Media/WhatsApp Voice Notes/201746

The storage path of different artifacts is shown as Table 2.

Rooted Mode

Root is the highest privilege of the mobile phone, which is equivalent to the administrator privilege in the computer window system. After obtaining the root privilege, all the files of the mobile phone can be read and modified.

Using the forensic tool XRY, we can find the artifacts of the WhatsApp account. It includes nickname, friend nickname, profile picture, phone number, network number, etc. The sending text message, picture, video, GIF animation, audio file, GIS location, and calling records are also can be found. It includes message content, sending time, name of the database, information about the sender and the recipient, etc. The Rooted mobile phone experiment has the same results as the Non-rooted mobile phone experiment. The reason is that the forensic tool XRY is in the state of Non-rooted mobile phone, using the way to downgrade WhatsApp version to get a lot of traces as rooted mobile phone.

The comparison of findings on Rooted Mode and Non-Rooted Mod

The comparisons of findings between Rooted Mode and Non-Rooted Mode using XRY are as Table 3.

Scenario 2: Autopsy

In the scenario 2, we follow the experiment steps as Experiment Elaboration section and use the Autopsy tool to find the artifacts of the activities on the WhatsApp.

Non-Rooted Mode

The Autopsy is a free information security forensics tool that provides a graphical interface for digital forensic investigation. It can analyze Windows and UNIX disks and file systems such as NTFS, FAT, UFS1/2 and Ext2/3. In the case of Non-rooted mobile phone, we use the Autopsy tool to open the smart phone backup image file and analyze it. We can find many artifacts, including: images, videos, audio files, GIF animations, and account profile image, but can't find any account, text messages, stickers, friend contact information, GIS location sharing, and friend account pictures.

Table-3: The findings of Rooted Mode and Non-Rooted Mode using XRY

Evidences	Rooted Mode	Non-Rooted Mode
Account	Found	Found
Registered Phone Number	Found	Found
Profile Picture	Found	Found
Nickname	Found	Found
Friend Account	Found	Found
Friend Nickname	Found	Found
Friend Phone Number	Found	Found
Friend Profile Picture	Found	Found
Text	Found	Found
Image	Found	Found
Video	Found	Found
GIF Animation	Found	Found
Stickers	Found	Found
Audio	Found	Found
GIS Location	Found	Found
Calling	Found	Found

Rooted Mode

We use the Autopsy tool to open the backup image file of smart phone. Our registered phone number, account profile picture, friend account, friend nickname, friend registration phone number, friend accounts profile picture, text, image, video, GIF animation, audio file, GIS location sharing, friend contact information and calling log can be found. But the account can't be found. We also find the wa. db database and msgstore. db database. We also find the wa. db database and msgstore. db database. But the sqlite_sequence table and sqlite_master table cannot be found in the wa.db and msgstore. db databases respectively. The Autopsy shows the artifacts of WhatsApp is as Figure 7.

Fig-7: The artifacts of WhatsApp using Autopsy

Table-4: The findings of Rooted Mode and Non-Rooted Mode using Autopsy

Evidences	Rooted Mode	Non-Rooted Mode
Account	None	None
Registered Phone Number	Found	None
Profile Picture	Found	Found
Nickname	Found	None
Friend Account	Found	None
Friend Nickname	Found	None
Friend Phone Number	Found	None
Friend Profile Picture	Found	None
Text	Found	None
Image	Found	Found
Video	Found	Found
GIF Animation	Found	Found
Stickers	None	None
Audio	Found	Found
GIS Location	Found	None
Calling	Found	None

The comparison of findings on Rooted Mode and Non-Rooted Mod

The comparisons of findings between Rooted Mode and Non-Rooted Mode using Autopsy are as Table 4.

Scenario 3: WinHex

In the scenario 3, we follow the experiment steps as Experiment Elaboration section and use the WinHex tool to find the artifacts of the activities on the WhatsApp.

Non-Rooted Mode

WinHex is a disk editor and a hex editor useful in data recovery and digital forensics. WinHex is a free powerful application that you can use as an advanced hex editor, a tool for data analysis, editing, and recovery, and a forensics tool used for evidence gathering. In the case of Non-rooted mobile phone, we use the WinHex tool to open the smart phone backup image file and analyze it. As a result, no artifacts about WhatsApp can be found.

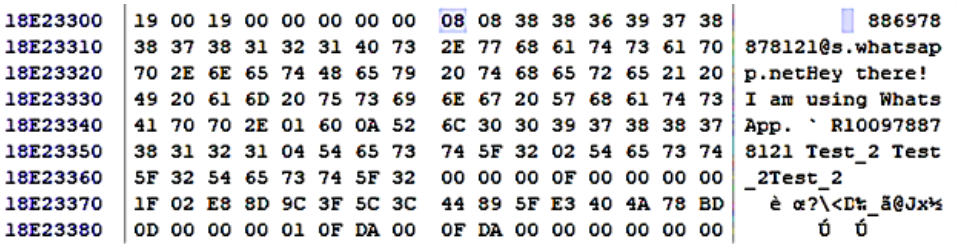

Fig-8: The artifacts of user account using WinHex

Rooted Mode

We use the WinHex tool to open the backup image file of smart phone. Our account, our registered phone number, friend nickname, friend registered phone number, text, image, video, GIF animation, calling log, and GIS location sharing can be found. But the account profile picture, friend profile picture, sticker, and audio file can't be found. For an example, we find the account information as Figure 8. WhatsApp number is 886978878121@s.whatsapp.net. The nickname is Test_2.

The comparison of findings on Rooted Mode and Non-Rooted Mod

The comparisons of findings between Rooted Mode and Non-Rooted Mode using WinHex are as Table 5.

Table-5: The findings of Rooted Mode and Non-Rooted Mode using WinHex

Evidences	Rooted Mode	Non-Rooted Mode
Account	Found	None
Registered Phone Number	Found	None
Profile Picture	None	None
Nickname	Found	None
Friend Account	Found	None
Friend Nickname	Found	None
Friend Phone Number	Found	None
Friend Profile Picture	None	None
Text	Found	None
Image	Found	None
Video	Found	None
GIF Animation	Found	None
Stickers	None	None
Audio	None	None
GIS Location	Found	None
Calling	Found	None

DISCUSSIONS

Using XRY tool, there are two main storage locations of WhatsApp that are /data/ data/ com. whatsapp/ Media/, and /data/data/com. whatsapp/ files/. Under the paths, the multimedia artifacts and account information can be found. In addition, the storage path after the smart phone has been Rooted is the same as that of Non-rooted, but the pathname is changed to/ userdata/ data/ com. whatsapp/ Media/ and / user data/ data/com. whatsapp/ files/. Both the Non-rooted smart phone and the rooted smart phone have the same artifacts. The reason is that the forensic tool XRY uses the way to downgrade the version of WhatsApp to bypass the protection mechanism in the case of the Non-rooted mode.

In the case of the Non-rooted smart phone, WinHex could not find any artifacts of WhatsApp. Autopsy can find fewer artifacts than XRY. On the contrary, use the forensic tool XRY to bypass the security protection mechanism by downgrading the WhatsApp version. We can obtain many artifacts of the WhatsApp. Therefore, it is proved that the use of the forensic tool XRY to perform the forensic analysis in the Non-rooted smart phone is better.

In the Rooted smart phone, using the forensic tool Autopsy can find many traces, but the account name cannot be found. Using the forensic tool WinHex also can find many artifacts, but the profile picture cannot be found. It is proved that the use of the forensic tool XRY to perform the forensic analysis in the Rooted smart phone and Non-Rooted smart phone is better than Autopsy and WinHex. However, considering the funding or other restrictions, we can try to use the free forensic tool, Autopsy or WinHex, to assist in the forensic analysis work.

We know the investigation step of instant messaging from the research of the experiments. First, we find the basic information of the user, and then search for the behavior of the user through the keyword strings such as account name, WhatsApp number, and phone number. Using the user information artifacts to estimate possible crimes. It also can use other accounts that may be additionally discovered during the search period. It may help to expand the search scope to see if there are accomplices or other victims.

We also can analyze the relationship between the criminal modus operandi and the timing chain. The investigator can infer the motives and tactics of possible crimes through the timing chain, and discover the criminal accomplices, transaction content, plans, time and place. When investigators find all kinds of traces of crimes, they can prevent crimes in advance.

Finally, we summary the findings of three forensic tools based on Non-rooted mode and Rooted mode as Table 6.

Table-6: The findings of three forensic tools

WhatsApp Artifacts	Forensic Tools					
	Autopsy		WinHex		XRY	
	Non-rooted	Rooted	Non-rooted	Rooted	Non-rooted	Rooted
Account	None	None	None	Found	Found	Found
Registered Phone Number	None	Found	None	Found	Found	Found
Profile Picture	Found	Found	None	None	Found	Found
Nickname	None	Found	None	Found	Found	Found
Friend Account	None	Found	None	Found	Found	Found
Friend Nickname	None	Found	None	Found	Found	Found
Friend Phone Number	None	Found	None	Found	Found	Found
Friend Profile Picture	None	Found	None	None	Found	Found
Text	None	Found	None	Found	Found	Found
Image	Found	Found	None	Found	Found	Found
Video	Found	Found	None	Found	Found	Found
GIF Animation	Found	Found	None	Found	Found	Found
Stickers	None	None	None	None	Found	Found
Audio	Found	Found	None	None	Found	Found
GIS Location	None	Found	None	Found	Found	Found
Calling	None	Found	None	Found	Found	Found

CONCLUSIONS

Although the instant messaging software has the advantages of convenience and immediacy, it is always inevitable that it will be abused by cyber criminals. Crimes are often exploited from software, website and web application exploits, using cloud services to spread malware, and further exploiting social media posts and links to trick users into fraud traps.

In this paper, we investigated the apps of WhatsApp Messenger to conduct a forensic analysis of the user behaviors in Android environments. The study found that different activities can lead to the discrepancies in recording the user behaviors on the same social network.

While investigating cybercrime on WhatsApp Messenger, we recommend that the first goal should be finding the account name, WhatsApp number, and phone number of the criminal suspect. Using the account name and WhatsApp number, the operational behaviors of the criminal suspect on the social network can be searched, such as, uploading pictures, sending text, calling logs, and timestamps. Then, based on the contents of the operation, the possible criminal activity or victimization practice can be deduced or estimated. At the same time, using the additional account information that is possibly discovered during the

evidence gathering phase, the scope of the investigation can be expanded to find the possible accomplices or other victims. The full evidence scenario obtained in a step-by-step and layer-by-layer outward expansion will be the key to solving the case.

REFERENCES

1. Rani Molla. "WhatsApp is now Facebook's second-biggest property, followed by Messenger and Instagram", Retrieved January 16, 2019. https://www.recode.net/2018/2/1/16959804/whatsapp-facebook-biggest-messenger-instagram-users
2. Metcalfe B. Metcalfe's law after 40 years of ethernet. Computer. 2013 Dec;46(12):26-31.
3. Denzil Correa, Leandro Silva, Mainack Mondal, Fabricio Benevenuto, Krishna P. Gummadi. The many shades of anonymity: characterizing anonymous social media content. In Proceedings of the 9th International AAAI Conference on Weblogs and Social Media (ICWSM'15). 2015.
4. Paulo Shakarian, Abhinav Bhatnagar, Ashkan Aleali, Elham Shaabani, Ruocheng Guo. Diffusion in Social Networks, Springer. 2015.
5. Elena Martellozzo, Emma A. Jane. Cybercrime and its victims, Routledge. 2017.
6. Doris Karina Oropeza Mendoza. The vulnerability of cyberspace - The Cyber Crime. Journal of Forensic Sciences & Criminal Investigation. 2017; 2(1).
7. Golbeck J. Introduction to social media investigation: a hands-on approach. Syngress; 2015 Mar 14.
8. Quick D, Choo KK. Pervasive social networking forensics: intelligence and evidence from mobile device extracts. Journal of Network and Computer Applications. 2017 May 15;86:24-33.
9. Sgaras C, Kechadi MT, Le-Khac NA. Forensics acquisition and analysis of instant messaging and VoIP applications. InComputational forensics. 2012; 11: 188-199. Springer, Cham.
10. Iqbal A, Marrington A, Baggili I. Forensic artifacts of the Chat ON Instant Messaging application. In2013 8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE). 2013; 21:1-6.
11. Walnycky D, Baggili I, Marrington A, Moore J, Breitinger F. Network and device forensic analysis of android social-messaging applications. Digital Investigation. 2015 Aug 1;14:S77-84.
12. Azfar A, Choo KK, Liu L. An android social app forensics adversary model. In2016 49th Hawaii International Conference on System Sciences (HICSS). 2016; 5: 5597-5606.
13. Glisson WB, Storer T, Buchanan-Wollaston J. An empirical comparison of data recovered from mobile forensic toolkits. Digital Investigation. 2013 Jun 1;10(1):44-55.
14. Ntantogian C, Apostolopoulos D, Marinakis G, Xenakis C. Evaluating the privacy of Android mobile applications under forensic analysis. Computers & Security. 2014 May 1;42:66-76.
15. Virvilis N, Mylonas A, Tsalis N, Gritzalis D. Security Busters: Web browser security vs. rogue sites. Computers & Security. 2015 Jul 1;52:90-105.
16. Walnycky D, Baggili I, Marrington A, Moore J, Breitinger F. Network and device forensic analysis of android social-messaging applications. Digital Investigation. 2015 Aug 1;14:S77-84.
17. Sun JR, Shih ML, Hwang MS. A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure. IJ Network Security. 2015 Sep 1;17(5):497-509.
18. Yusoff MN, Dehghantanha A, Mahmod R. Forensic investigation of social media and instant messaging services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp, and Line as case studies. InContemporary Digital Forensic Investigations of Cloud and Mobile Applications. 2017;1: 41-62. Syngress.
19. Wu S, Zhang Y, Wang X, Xiong X, Du L. Forensic analysis of WeChat on Android smartphones. Digital investigation. 2017 Jun 1;21:3-10.