Evidence Gathering of Facebook Messenger on Android

Ming Sang Chang and Chih Ping Yen
(Corresponding author: Chih Ping Yen)

Department of Information Management, Central Police University
Taoyuan 33304, Taiwan
(Email: peter@mail.cpu.edu.tw)

(Received Aug. 28, 2019; Revised and Accepted Feb. 5, 2020; First Online Feb. 26, 2020)

Abstract

The trend in social networking is changing people's lifestyle. Since both the smart phone and computers are connected to the same tools, the newly developed applications must serve both ends to please the users. 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, Facebook Messenger, as the research subject. We analyze the artifacts left on the Facebook Messenger application and show evidence of gathering, such as sending texts, pictures, and videos and making calls on the Android platform. This study explores the differences between the traces that are left on Non-Rooted and Rooted Android platform. Finally, the forensic analysis found, due to the differences in privacy control, can lead to discrepancies in recording the user behaviors on the same social network. It proves to be helpful to forensic analysts and practitioners because it assists them in mapping and finding digital evidences of Facebook Messenger on Android smart phone.

Keywords: Cybercrime; Digital Forensics; Facebook Messenger; Social Network

1 Introduction

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 integrated social networking sites into their lives and turned the use of social networking sites into daily activities.

Facebook Messenger is a messaging application. Originally developed as Facebook Chat in 2008, the company revamped its messaging service in 2010. It released standalone iOS and Android apps in August 2011. Over the years, Facebook has released new apps on a variety of different operating systems, launched a dedicated website interface, and separated the messaging functionality from the main Facebook app. Users can send messages and exchange photos, videos, stickers, audio, and files, as well as react to other users' messages and interact with bots. The service also supports voice and video calling. After being separated from the main Facebook app, Facebook Messenger had 600 million users in April 2015. This grew to 900 million in June 2016, 1 billion in July 2016, and more 1.3 billion monthly active users in October 2019 [22].

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. 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. Due to the following characteristics, the detecting cybercrime on social networks is different in comparison to other cybercrime [10]. Therefore, to assist the investigators in improving their efficiency of solving crimes, researches focusing on these upcoming technologies are needed [16].

1) Anonymity: 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 [1].

2) Diffuseness: Any news published on the social network will be forwarded or shared immediately, which generates the diffusion effect [21]. Therefore, if a social network crime is not responded to immediately, it may cause the victim to suffer some serious damage.

3) Cross-Regional feature: 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 [13].

4) Vulnerability of evidence: 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 [14].

This study considers the social network, Facebook 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 our related works. In Section 3, we present our methodology. In Section 4, we present the results and findings of digital forensics on Facebook Messenger. In Section 5, we discuss the findings. Finally, we summarize our conclusions.

2 Related Works

The evidences were stored on three principle areas by using instant messenger program (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. Early work focused on artifacts left behind by many instant messaging applications, such as MSN Messenger [7], Yahoo Messenger [8], and AOL Instant Messenger [17]. In 2013 Mahajan performed forensic analysis of Whatsapp and Viber on five android phones using UFED and manual analysis [12]. Katie Corcoran forensic 7 Messaging applications and first analyzed the evidence of Facebook Messenger [5]. Levendoski concluded that artifacts of the Yahoo Messenger client produced a different directory structure on Windows Vista and 7 [11]. Wong and Al Mutawa demonstrated that artifacts of the Facebook web-application could be recovered from memory dumps and web browsing cache [15, 25].

Said investigated Facebook and other IM applications, it was determined that only BlackBerry Bold 9700 and iPhone 3G/3GS provided evidence of Facebook unencrypted [19]. Sgaras analyzed Skype and several other VoIP applications for iOS and Android platforms [20]. It was concluded that the Android apps store far less artifacts than of the iOS apps. Chu focused on live data acquisition from personal computer and was able to identify distinct strings that will assist forensic practitioners with reconstruction of the previous Facebook sessions [4]. The analysis was conducted on an iPhone running iOS6 and a Samsung Galaxy Note running Android 4.1. Walnycky analyzed 20 popular instant messaging applications for Android, of which Facebook Messenger can get evidences such as text chat, voice call, audio, video, image, location, and stickers [24]. 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 [2].

William Glisson explored the effectiveness of different forensic tools and techniques for extracting evidences on mobile devices [9]. In 2015, 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 [23]. Dezfouli examine four social networking: Facebook, Twitter, LinkedIn and Google+, on Android and iOS platforms, to detect remnants of users' activities that are of forensic interest [6]. In 2017, 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 [27]. Song-Yang Wu describes several forensic examinations of Android WeChat and provides corresponding technical methods [26]. Imam Riadi performed a comparison of tool performance to find digital and chat and pictures from Instagram Messenger [18]. Although Zhang et al. analyzed the local artifacts of the 4 Instant Messaging applications, the types of these local artifacts are incomplete [28]. Jusop Choi analyzed the personal data files in three instant messaging applications (KakaoTalk, NateOn, and QQ) which are the most popularly used in China and South Korea [3].

This paper investigated the user activities of Facebook 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.

3 Methodology

In our research, we use the smart phone with an installation of Facebook Messenger. The study was focused on identifying data remnants of the activities of Messenger 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.

3.1 Research Goal

This paper studies the user behaviors, including logging into Facebook Messenger, uploading images, exchanging information, GIS location sharing, and special 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 evidence on the Android smart phone.

3.2 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 Facebook Messenger social networking application was installed to run the Messenger features directly. In addition, if Facebook Messenger have ever been installed, the "/com.facebook.orca" folder will appear in the directory structure.

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. In order to obtain more information on the mobile phone, the investigators should execute a series of rooting processes before examining a mobile phone.

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 a 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 that 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.

3.3 Development of Experiments

Based on the experimental environment designed, we run the Messenger features, including logging in, sending messages, exchanging photos, videos, audio, and files, making a call, etc. After that, the relevant evidence on each device was extracted and analyzed using forensic tools.

3.3.1 Extract Data

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

Table 1: List of hardware and software used

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
Messenger	Social Networking App	Version v141.0.0.31.76
Minimal ADB and Fastboot	ADB Tool	Version v10.0.16299.371

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 an 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" shows 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.

3.3.2 Design of Analysis

In order to ensure the integrity of digital evidence and avoid interference between digital evidence, we divide the experiment into the following three cases according to different forensic tools XRY, Autopsy and WinHex. The three experimental scenarios include Scenario 1: XRY, Scenario 2: Autopsy, and Scenario 3: WinHex. And each experimental scenario, the same experimental steps are performed.

In addition, each of the above experimental scenarios is further divided into two models: non-root and root Android platforms.We then performed the same experiments on non-root and root Android platforms and compared the relevant evidence.

3.3.3 Experiment Elaboration

The experiment steps are summarized as follows.

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

4 Results and Findings

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

4.1 Scenario 1: XRY

In the scenario 1, we follow the experiment steps as Section 3.3 and use the XRY tool to find the evidences of the activities on the Messenger.

4.1.1 Non-Rooted Mode

Using the XRY tool to find the evidences on the Messenger, we can't find the user account and password. The artifacts of user account can be found as Figure 1. The user's information is as Figure 1 that are phone number +886985028322, nickname Huang Gordon, profile picture URL, and Facebook number 100021304820523.

The friend list can be found as Figure 2. It includes the name and the profile picture URL of friends.

The artifacts of sending text, image, audio, video, GIS location, and GIF animation can be found. For an example, we could show the artifacts of sending video as Figure

Figure 1: The artifacts of user account

Related Application	Display Name	Name	Category	Related URL
Facebook	Nan Chia	Nan Chia	Friend	https://scontent.ftpe7-1.f...
Facebook	Shane Chen	Shane Chen	Friend	https://scontent.ftpe7-1.f...
Facebook	La Chen	La Chen	Friend	https://scontent.ftpe7-1.f...
Facebook Messenger		Nan Chia		

Figure 2: The artifacts of friend list

3. The video delivery time, the video URL of storage location, who sending the video can be found.

Figure 3: The artifacts of sending video

The artifacts of making a call can be found. We can find the calling record that includes the calling time, who making the call, and threads_db2 database. For an example, the artifacts of making a call is as Figure 4.

About the database, there are three main databases for the recovered Messenger artifacts. The threads_db2 database contains the sending messages. The call_log_db_10021304820523 database contains the setting of user account. 10021304820523 is the network login number. The contacts_db2 database contains the user information. The contacts_db2 database is on /data/data/com.facebook.katana/databases/. The threads_db2 database and the call_log_db_10021304820523 database are on /data/data/com.facebook.orca/databases. There are three significance tables in the threads_db2 database. It includes the message table, the thread users table, and the message_reactions table. The message table stores the sending messages. An example of message table is as Figure 5. The evidences of text, sender, and timestamp can be found on the table. We can find the user name, nickname, and network number in the thread users table. The stickers can be found on message_reactions table.

From the call_log_db_10021304820523 database, we can find the user network number. The contacts_db2 database contains the contacts table. It includes friend list. The nickname and the URL of profile picture are on the table. The path, /data/data/com.facebook.orca/, is the main storage location of Messenger. All the storage path of different artifacts is shown as Table 2.

Figure 4: The artifacts of making a call

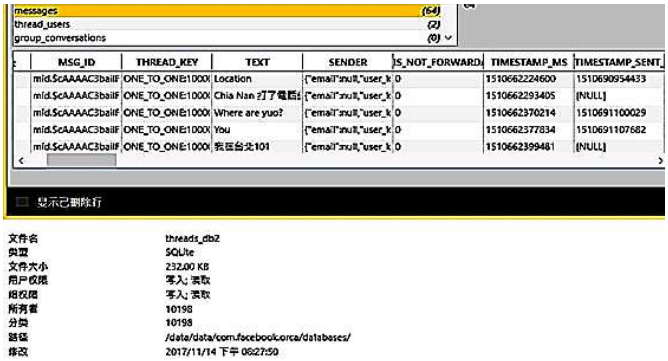

Figure 5: The artifacts of message table

Table 2: The storage path of various traces

Artifacts	Storage Path
Profile Picture	/data/data/com.facebook.orca/files/image/v2.ols100.1/52/
Friend Picture	/data/data/com.facebook.orca/files/image/v2.ols100.1/88/
Image	/data/data/com.facebook.orca/cache/image/v2.ols100.1/84/
Video	/data/data/com.facebook.orca/files/ExoPlayerCacheDir/videocache/
GIFAnimation	/data/data/com.facebook.orca/cache/image/v2.ols100.1/32/
Sticker	/data/data/com.facebook.orca/cache/image/v2.ols100.1/99/
Audio	/data/data/com.facebook.orca/cache/audio/v2.ols100.1/88/

4.1.2 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 Messenger account. It includes nickname, friend nickname, profile picture, user name, phone number, network number and related data URL. But the account and password cannot be found. The sending text message, picture, video, GIF animation, sticker, 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. According to the experiment, the sending message is stored in the threads_db2 database, the account data is stored in the contacts_db2 database, and the network login number of the Messenger is known by the call_log_db_10021304820523database. The Rooted mobile phone experiment has the same results as the Non-rooted mobile phone experiment, and can find artifacts on various tables in the different database.

4.1.3 The Comparison of Findings on Rooted Mode and Non-Rooted Mode

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

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

Evidences	Rooted	Non-Rooted
Account	None	None
Password	None	None
Profile Name	Found	Found
Nickname	Found	Found
Friend Nickname	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

4.2 Scenario 2: Autopsy

In the scenario 2, we follow the experiment steps as Section 3.3 and use the Autopsy tool to find the artifacts of the activities on the Messenger.

4.2.1 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. As a result, no artifacts about Messenger can be found.

4.2.2 Rooted Mode

We use the Autopsy tool to open the backup image file of smart phone. Our nickname, friend nickname, text, image, video, GIF animation, sticker, audio file, GIS location, and calling record can be found. But the account number, password, and user name can't be found. We also find the databases such as threads_db2, call_log_db_10021304820523 and contacts_db2. There is no data on the message_reactions table in the threads_db2 database. The Autopsy displays the artifacts of Messenger is as Figure 6.

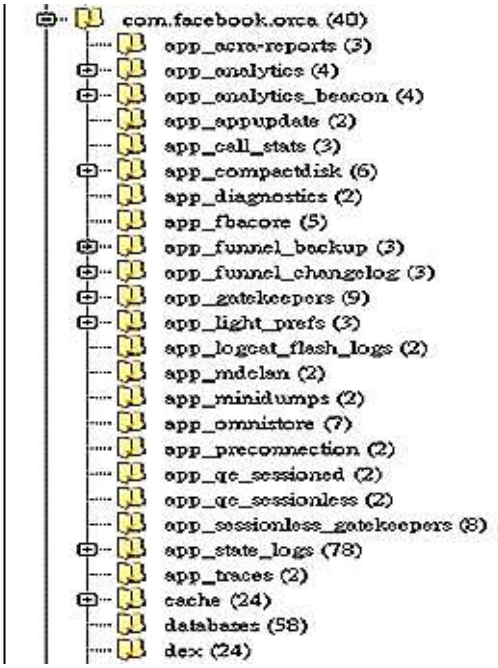

Figure 6: The artifacts of Messenger using Autopsy

User nickname and the network number can be found on the thread_users table in the threads_db2 database. We also find the sending text, sticker, GIS location, calling record on the messages table in the same database. The artifacts of video are located on data/com.facebook.orca/files/ExoPlayerCacheDir/videocache/. We find the artifacts of audio on data/com.facebook.orca/cache/audio/. The Image and GIF animation are on data/com.facebook.orca/cache/image/. For an example, the artifact of GIS location is shown in Figure 7.

Figure 7: The artifacts of GIS location using Autopsy

4.2.3 The Comparison of Findings on Rooted Mode and Non-Rooted Mode

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

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

Evidences	Rooted	Non-Rooted
Account	None	None
Password	None	None
Profile Name	None	None
Nickname	Found	None
Friend Nickname	Found	None
Text	Found	None
Image	Found	None
Video	Found	None
GIF Animation	Found	None
Stickers	Found	None
Audio	Found	None
GIS Location	Found	None
Calling	Found	None

4.3 Scenario 3: WinHex

In the scenario 3, we follow the experiment steps as Section 3.3 and use the WinHex tool to find the artifacts of the activities on the Messenger.

4.3.1 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 Messenger can be found.

4.3.2 Rooted Mode

We use the WinHex tool to open the backup image file of smart phone. Our nickname, friend nickname, text, can be found. But the image, video, GIF animation, sticker, audio file, GIS location, calling record, account number, password, and user name can't be found. For an example, we find the user login email and nickname using the "username" keyword as Figure 8.

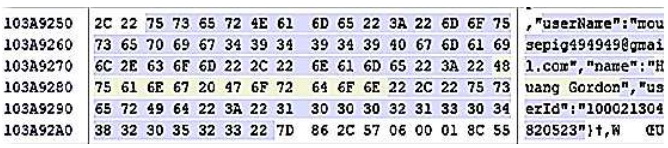

Figure 8: The artifacts of the user under using WinHex

4.3.3 The Comparison of Findings on Rooted Mode and Non-Rooted Mode

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

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

Evidences	Rooted	Non-Rooted
Account	None	None
Password	None	None
Profile Name	None	None
Nickname	Found	None
Friend Nickname	Found	None
Text	Found	None
Image	None	None
Video	None	None
GIF Animation	None	None
Stickers	None	None
Audio	None	None
GIS Location	None	None
Calling	None	None

5 Discussions

Using XRY tool, the path, /data/data/com.facebook.orca/, is the main storage location of Messenger. Under this path, there are two folders, files, and cache, have more multimedia artifacts. They include the profile picture, image, GIF animation, sticker, and audio files. The video artifacts are located in the ExoPlayerCacheDir folder. 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.facebook.orca/. 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 Messenger to get a lot of artifacts.

According to the experiments, in the case of the Non-rooted smart phone, the forensic tools, Autopsy, and WinHex, could not find any artifacts of Messenger. On the contrary, use the forensic tool XRY to bypass the security protection mechanism by downgrading the Messenger version. We can obtain many artifacts of the Messenger. But the account number and password cannot be found. 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 number, password and user name cannot be found. Using the forensic tool WinHex can find our nickname, friend nickname, and text. According to the results of the experiments, it is

Table 6: The findings of three forensic tools

Forensic Tools / Messenger Artifacts	XRY		Autopsy		WinHex	
	Non-Rooted	Rooted	Non-Rooted	Rooted	Non-Rooted	Rooted
Account	None	None	None	None	None	None
Password	None	None	None	None	None	None
User name	Found	Found	None	None	None	None
My nickname	Found	Found	None	Found	None	Found
Friend nickname	Found	Found	None	Found	None	Found
Text	Found	Found	None	Found	None	Found
Image	Found	Found	None	Found	None	None
Video	Found	Found	None	Found	None	None
GIF animation	Found	Found	None	Found	None	None
Sticker	Found	Found	None	Found	None	None
Audio	Found	Found	None	Found	None	None
GIS location	Found	Found	None	Found	None	None
Calling log	Found	Found	None	Found	None	None

Table 7: The results of forensic analysis of relevant researchers for Facebook messenger

Researcher	**Artifacts**
Katie Corcoran [5]	User name, my nickname, friend nickname, text, GIS location, timestamp
Hao Zhang [28]	User name, my nickname, friend nickname, text, image, audio, GIS location, timestamp
Ming-Sang Chang & Chih-Ping Yen (this work)	User name, my nickname, friend nickname, text, image, video, GIF animation, sticker, audio, GIS location, calling log, timestamp

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. 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 number, nickname ,and network number. Using the user 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 summarize the findings of three forensic tools based on Non-rooted mode and Rooted mode as Table 6. It also presents the results of forensic analysis of relevant researchers for Facebook Messenger, as shown in Table 7.

6 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 Facebook 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 Facebook Messenger, we recommend that the first goal should be finding the account number, nickname, and network number of the criminal suspect. Using the account number and nickname, the operational behaviors of the criminal suspect on the social network can be searched, such as, uploading pictures, sending text, calling log, 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 numbers that are 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] N. Al-Suwaidi, H. Nobanee, and F. Jabeen, "Estimating causes of cyber crime: Evidence from panel data fgls estimator," *International Journal of Cyber Criminology*, vol. 12, pp. 392–407, 2018.

[2] A. Azfar, K. Choo, and L. Liu, "An android social app forensics adversary model," in *Proceedings of the International Conference on System Sciences*, pp. 5597–5606, 2016.

[3] J. Choi, J. Yu, S. Hyun, and H. Kim, "Digital forensic analysis of encrypted database files in instant messaging applications on windows operating systems: Case study with kakaotalk, nateon and QQ messenger," *Digital Investigation*, vol. 28, pp. 50–59, Apr. 2019.

[4] H. C. Chu, D. J. Deng, and J. H. Park, "Live data mining concerning social networking forensics based on a facebook session through aggregation of social data," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 7, pp. 1368–1376, 2011.

[5] K. Corcoran, A. Read, J. Brunty, and T. Fenger, "Messaging application analysis for android and iOS platforms," *Research and Seminar in Forensic Science Graduate Program*, 2013. (`http://www.marshall.edu/forensics/research-and-seminar/class-of-2013`)

[6] F. N. Dezfouli, A. Dehghantanha, B. Eterovic-Soric, and K. R. Choo, "Investigating social networking applications on smartphones detecting facebook, twitter, linkedin and google+ artefacts on Android and iOS platforms," *Australian Journal of Forensic Sciences*, vol. 48, pp. 469–488, 2016.

[7] M. Dickson, "An examination into msn messenger 7.5 contact identification," *Digital Investigation*, vol. 3, no. 2, pp. 79–83, 2006.

[8] M. Dickson, "An examination into yahoo messenger 7.0 contact identification," *Digital Investigation*, vol. 3, no. 3, pp. 159–165, 2006.

[9] W. B. Glisson, T. Storer, and J. Buchanan-Wollaston, "An empirical comparison of data recovered from mobile forensic toolkits," *Digital Investigation*, vol. 10, no. 1, pp. 44–55, 2013.

[10] J. Golbeck, *Introduction to Social Media Investigation*, pp. 273-278, 2015. ISBN: 9780128016565.

[11] M. Levendoski, T. Datar, and M. Rogers, "Yahoo! messenger forensics on windows vista and windows 7," *Digital Forensics and Cyber Crime*, vol. 88, pp. 172–179, 2012.

[12] A. Mahajan, M. S. Dahiya, and H. P. Sanghvi, "Forensic analysis of instant messenger applications on android devices," *International Journal of Computer Applications*, vol. 68, no. 8, pp. 38–44, 2013.

[13] E. Martellozzo and E. A. Jane, *Cybercrime and Its Victims*, 2017. ISBN10: 1138639443.

[14] D. K. Mendoza, "The vulnerability of cyberspace – the cyber crime," *Journal of Forensic Sciences & Criminal Investigation*, vol. 2, no. 1, 2017.

[15] N. Mutawa, I. Awadhi, I. Baggili, and A. Marrington, "Forensic artifacts of facebook's instant messaging service," in *Proceedings of the International Conference for Internet Technology and Secured Transactions (ICITST'11)*, pp. 771–776, 2011.

[16] D. Quick and K. K. Choo, "Pervasive social networking forensics: Intelligence and evidence from mobile device extracts," *Journal of Network and Computer Applications*, vol. 86, pp. 24–33, 2017.

[17] J. Reust, "Case study: Aol instant messenger trace evidence," *Digital Investigation*, vol. 3, no. 4, pp. 238–243, 2006.

[18] I. Riadi, A. Yudhana, and M. C. F. Putra, "Forensic tool comparison on instagram digital evidence based on android with the nist method," *Scientific Journal of Informatics*, vol. 5, no. 2, pp. 235–247, Nov. 2018.

[19] H. Said, A. Yousif, and H. Humaid, "Iphone forensics techniques and crime investigation," in *Proceedings of the International Conference and Work-shop on Current Trends in Information Technology*, pp. 120–125, 2011.

[20] C. Sgaras, M. T. Kechadi, and N. A. Le-Khac, "Forensics acquisition and analysis of instant messaging and voip applications," *Computational Forensics*, pp. 188–199, 2015.

[21] P. Shakarian, A. Bhatnagar, A. Aleali, E. Shaabani, and R. Guo, "Diffusion in social networks," *Computer Science*, 2015. ISBN: 978-3-319-23105-1.

[22] Statista, *Most Popular Global Mobile Messenger Apps as of October 2019, Based on Number of Monthly Active Users [Online]*, 2020. (`https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps`) [last accessed 10.01.2020].

[23] N. Virvilis, A. Mylonas, N. Tsalis, and D. Gritzalis, "Security busters: Web browser security vs.rogue sites," *Computer & Security*, vol. 52, pp. 90–105, 2015.

[24] D. Walnycky, I. Baggili, and A. Marrington, *et al.*, "Network and device forensic analysis of android social-messaging applications," *Digital Investigation*, vol. 14, pp. 77–84, 2015.

[25] K. Wong, A. Lai, J. Yeung, and W. Lee, *et al.*, "Facebook forensics," valkyrie-x security research group, 2011. (`https://www.fbiic.gov/public/2011/jul/facebook_forensics-finalized.pdf`)

[26] S. Y. Wu, Y. Zhang, and X. P. Wang *et al.*, "Forensic analysis of wechat on android smartphones," *Digital Investigation*, vol. 21, pp. 3–10, 2017.

[27] M .N. Yusoff, A. Dehghantanha, and R. Mahmod, "Chapter 4 – forensic investigation of social media and instant messaging services in firefox os: Facebook, twitter, google+, telegram, openwapp, and line as case studies," *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, pp. 41–62, 2017.

[28] H. Zhang, L. Chen, and Q. Liu, "Digital forensic analysis of instant messaging applications on android smartphones," *International Conference on Computing, Networking and Communications (ICNC'18)*, pp. 647–651, 2018.

Biography

Ming Sang Chang received the Ph.D. degree from National Chiao Tung University, Taiwan, in 1999. In 2001 he joined the faculty of the Department of Information Management, Central Police University, where he is now a Professor. His research interest includes Computer Networking, Network Security, Digital Investigation, and Social Networks.

Chih Ping Yen is an Associate Professor, Department of Information Management, Central Police University. Received his Ph.D. degree from Department of Computer Science and Information Engineering, National Central University, Taiwan, in 2014. His research interest includes Digital Investigation, Artificial Intelligence & Pattern Recognition, Image Processing, and Management Information Systems.