Analysis of WeChat on IPhone

Feng Gao
Key Laboratory of Information Network Security,
Ministry of Public Security,
People's Republic of China (The Third Research Institute of Ministry of Public Security)
Shanghai, China
gaofeng@stars.org.cn

Ying Zhang
Key Laboratory of Information Network Security,
Ministry of Public Security,
People's Republic of China (The Third Research Institute of Ministry of Public Security)
Shanghai, China
zhangying@stars.org.cn

***Abstract*—With the popularization of smart phone, more and more applications emerge especially in the aspect of social network services. Take China for example, WeChat has become the most universal communication applications in recently several years. In the meantime, forensic technicians start to pay attention to the data contained in them. Furthermore, the latent evidence could be concealed in those devices and they are generally supposed to be recovered and extracted via utilizing the proper tools. This paper demonstrates a method on analyzing latent evidences in iPhone regarding the application WeChat.**

Keywords-smartphone, application, social network service, iPhone, iOS

I. INTRODUCTION

A brand new approach of online communication, known as social network services, emerges and develops rapidly in recent decades. People use them to interact and socialize, sharing information, comments, photographs and videos, as well as communicate with colleagues.[1] In a word, those services could be treated as in important source of information.

Meanwhile with the popularization of smart phones, more and more software manufactures have pay their attention to the applications concerning social network services in smart phones. A survey conducted by Ruder Finn (a PR agency) showed that 91% of smart phone users use them to socialize compared to only 79% of traditional desktop users. And 43% of above users are used to communicating friends on social network websites.[2] It is known to all that Twitter and Facebook are two popular ones in American and Europe while WeChat is the most widely used application in China.

The above applications described above bring about not only convenience but also different issues to smart phone users. Concretely speaking, despite being primarily used to communicate and socialize with friends, the diverse and anonymous nature of social networking websites makes their users vulnerable to cybercrimes. Phishers, fraudsters, child predators and other cyber criminals can register for these services with fake identities, hiding their malicious intentions behind innocent appearing profiles.[1] That means, those users are exposed in the danger of privacy leak due to utilization of social network services.

As we all known, a lot of valuable information is stored in smart phones, including text, voice message, photographs and videos. It is important, therefore, for the investigator to understand how the application stores the user's data. This paper will provide the investigators a method conducting forensic analysis on the most popular application regarding social network services in China, which is called WeChat.

For the scope of this paper, the focus will be on the concrete procedures regarding capturing digital evidences of WeChat on iPhone. The rest of the paper is organized as follows. The purpose and principle of evidence acquisition is described in section 2. Section 3 explains proper approaches to implement evidence acquisition. Test environment and requirements will be described in section 4. Examination and analysis will be illustrated in section 5. Conclusion is in section 6.

II. PURPOSE AND PRINCIPLE

A. Purpose

The main purpose of this paper is to figure out whether operations performed by the applications regarding social network services are stored in the internal memory of these devices and whether above data can be recovered.

B. Principle

*1) Conditions:*The experiments were conducted using forensically approaches and under forensically acceptable conditions to fulfill a crucial rule in digital forensics, which is to preserve the integrity of the original data and to prevent it from any contamination that would interfere with its acceptance in court.

*2) Standards:*The test and examination procedure was derived from the Computer Forensics Tool Testing program guidelines established by the National Institute of Standards and Technology (NIST) to ensure the quality of the testing methods and the reliability and validity of the results.[5]

III. ACQUISITION

There are two kinds of data-copying methods for acquisition of data from mobile devices, known as physical acquisition and logical acquisition.

A. *Physical acquisition*

Physical extraction involves a bit-by-bit copy of an entire physical store (e.g. flash memory). This process has the advantage of allowing deleted files and data remnants to be examined.[3] In some cases, it may be necessary to use the chip-off technique in order to obtain a memory image. This technique can be used when the device is damaged or in some cases is used to bypass the password protection. The chip-off is a technique where the flash memory is physically removed from the device and examined externally.

B. *Logical acquisition*

Logical acquisition implies a bit-by-bit copy of logical storage objects (e.g. directories and files) that reside on a logical store. But it is possible in selected cases. By contrast, there are several tools that can help the investigator.[4] Many commercial tools perform the acquisition and then create a report with the extracted data, but this process takes time. Examples include:

- Cellebrite UFED
- Oxygen Forensic Suite
- InMOBILedit! Forensic
- AccessData's MPE

IV. TEST ENVIRONMENT AND REQUIREMENTS

Prior to conducting the experiments, a forensic workstation was set up and configured. Once the forensic workstation was ready, it was isolated from the lab's network. The hardware and software used to conduct the experiment is listed in table 1.

TABLE I. MEANING OF THE SUBFOLDERS

No.	Name	Version
1	iPhone 5	version 6.1.4, Firmware:10B350
2	Apple iTunes	version 11.0.2.26
3	MOBILedit! Forensic	version 6.9.0.2876
4	SQLite Expert Professional	version 3.4.65.2295

V. IMPLEMENTATION

A. *Acquisition*

1) Tools:iTunes is a synchronization and management application which is available on the Apple official website. It is used to create backup or obtain a logical image from the Apple device and save it on the computer. However iTunes is not designed for forensic acquisition although it is an option.

2) Procedures:The logical acquisition of data on iPhone 5 is performed via using iTunes as well. Backup files may also exist on the suspect's computer if he had performed a synchronization operation or a software update or restored their device to its factory settings previously.

It is critical for forensic technicians to ensure the integrity of acquired evidence. Therefore, the acquisition is required to be conducted in a forensic environment. Before attaching the device to the forensic workstation, it is important to disable automatic synchronization option in iTunes. Then the first step is to gain access to back up the device using iTunes as showed in Figure 1.

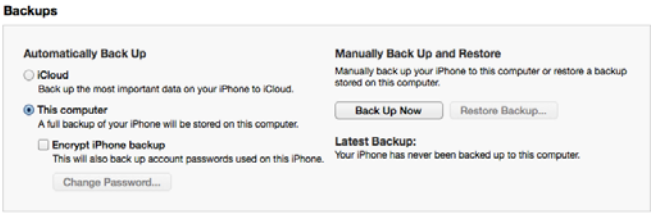


Figure 1. Back up.the device using iTunes

iTunes created a backup of iPhone, and by default, it placed the files in the following directory: C:\Users\[user]\AppData\Roaming\Apple Computer\

MobileSync\Backup\[unique identifier]. Once the process was completed, the device is supposed to be disconnected from the forensic workstation.

B. *Collection*

Then the forensic technicians are required to read the backup data, list the applications installed on the target device, and extract the WeChat Data via using MOBILedit! Forensic as described in figure 2.

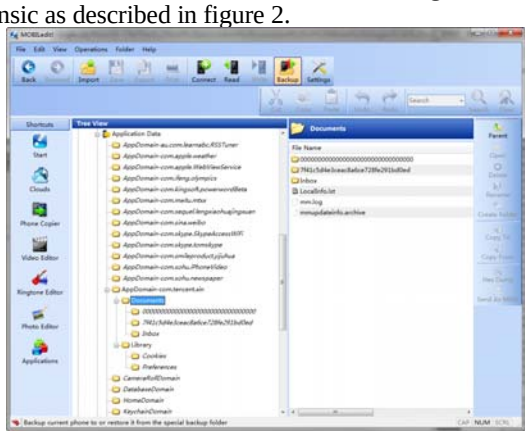


Figure 2. Read the iPhone's backup and extrat WeChat data

VI. ANALYSIS

According to the search and analysis, the data folder of WeChat locates in the directory "AppDomain/ com.tenxin.xin/Documents", which is named "7f41c5d4e3ceac8a6ce728fe291bd0ed" as listed in figure 3.

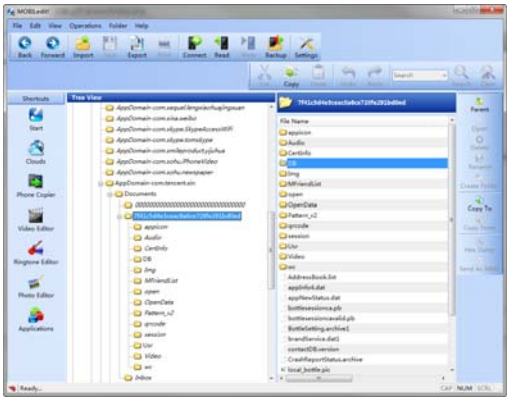


Figure 3. Wechat data Foler

There are different types of data locating in different subfolders under the data folder. Table 1 explains the concrete meaning of the subfolders.

TABLE II. MEANING OF THE SUBFOLDERS

No.	Name	Stored file types	Meaning
1	Audio	***.aud**	Store the voice message
2	DB	**MM.sqlite**	Store the text message
2	Img	***.pic, *.pic_thum**	Store the picture message
3	Usr	***pic_usr, *.pic_hd**	Store the user's profile photographs
4	Video	***.mp4, *.thum**	Store the video message

A. *Analysis of MM.sqlite files*

1) friends_data tables: The table with the name Friend shows the user information of each friend as shown in figure 4.

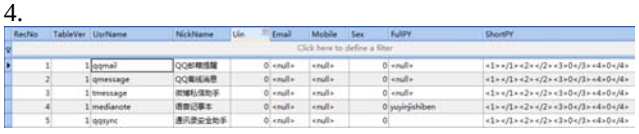


Figure 4. Friends_data table

2) connections tables: The file named MM.sqlite can be read using the tool SQLite Expert Professional (version 3.4.65.2295). The table with MD5 hashed name beginning with "chat_XXX" shows the content of connections associated with the accounts which are listed in friends_data table as demonstrated in Figure 5.

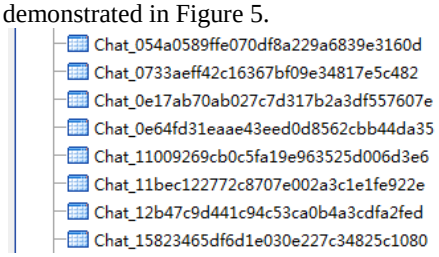


Figure 5. Connections tables

B. *Analysis of audio files*

The subfolders named with MD5 hash under the folder "Audio" stores the voice message, which is explained in figure 6. Besides that, the name of audio file is the same with that of shown in the table filed MesSverID as shown in figure 7.

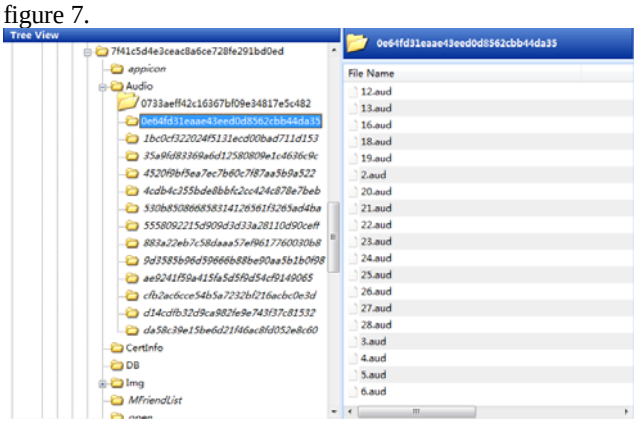


Figure 6. Voice message file

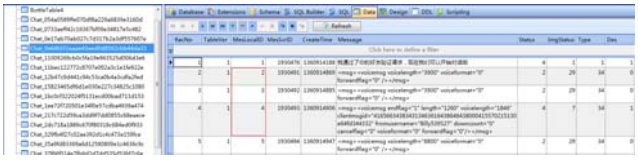


Figure 7. Connections associate with the voice message file

C. *Analysis of picture and video files*

The analysis method for picture and video files is similar to that of audio messages. But if the picture or video is not downloaded from the server, investigators can only find the thumbnails in the folder named "Img" or "Video". Concrete analysis is shown in figure 8, figure9, figure 10 and figure 11.

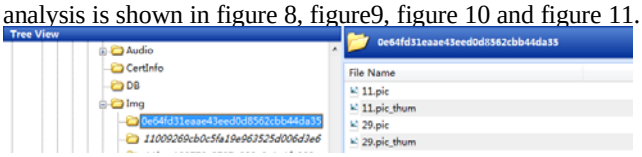


Figure 8. Picture message file

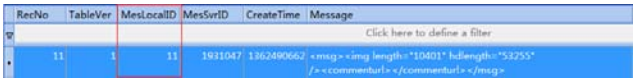


Figure 9. Connections associate with the picture message file

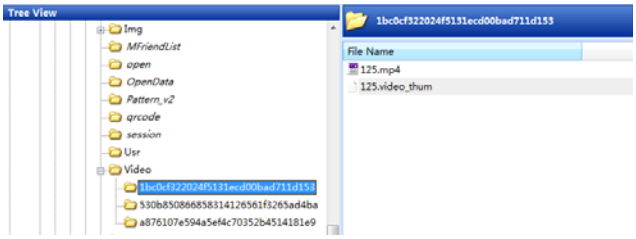
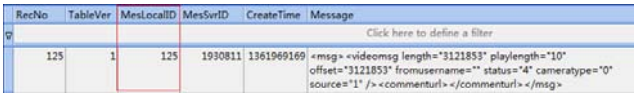


Figure 10. Video message file



RecNo	TableVer	MesLocalID	MesSvrID	CreateTime	Message
					Click here to define a filter
125	1	125	1930811	1361969169	<msg> <videomsg length="3121853" playlength="10" offset="3121853" fromusername="" status="4" cameratype="0" source="1" /> <commenturl> </commenturl> </msg>

Figure 11. Connections associate with the video message file

VII. CONCLUSION

Few studies committed the recovery and analysis of activities performed by applications regarding social network services on smart phones in the past decades. Therefore the data of WeChat that we analyze from the device will provide us evidence that may be of considerable value in an investigation. The information we obtain will help us understand the subject better under scrutiny by identifying, inter alia, their contacts and affiliations, habits and interests, ideas and beliefs.

This paper explores the examination and analysis of the wechat data on iPhone. We hope it can inspire the creation of digital forensics tools to extract and reconstruct the wechat data from iPhone in the future.

ACKNOWLEDGMENT

This work was financially supported by the basic science project of Ministry of public security, project number: 2012GABJC035 and National Development and Reform commission, project number: [2012]1424.

REFERENCES

[1] Andrew Hoog, “Android Forensics: Investigation, Analysis, and Mobile Security for Google Android”

[2] Noora Al Mutawa, Ibrahim Baggili, Andrew Marrington, “Forensic analysis of social networking applications on mobile devices”

[3] Mobile Device Forensics: “http://en.wikipedia.org/wiki/Mobile_device_forensics”

[4] Massimo Barone, “Step by step analysis of Facebook and Twitter data on Android devices”

[5] National Institute of Standards and Technology, 2001.