Iphone data common extraction method comparison research

Zihao Zhang

People's Public Security University of China, Beijing, Daxing 100076, China

ppsuczzh@163.com

Abstract

Iphone is a very high-using smartphone, which brings a lot of convenience to people's life and work, but now criminals are increasingly using Iphone for fraud, rumors, murder and other criminal activities. The forensic work on Iphone data has not received the attention it deserves. This paper compares the common extraction methods of three kinds of iPhone data, and determines the scope, advantages and disadvantages of each method, so that the public security organs can choose better data extraction method for different situations.

Keywords

Iphone ; data extraction method; comparison study.

1. Preface

With the rapid development of electronic devices and Internet technologies, people are increasingly relying on mobile phones in their daily lives. The functions of mobile phones are becoming more and more powerful. They have evolved from simple voice call tools to modern electronic devices with multiple functions such as line navigation, instant messaging, video calling, and mobile payment. During my internship at the grassroots police station, I found that the criminal activities of criminals are closely related to mobile phones, especially Iphone, which have a high usage rate. However, the police handling the case does not have a certain understanding of the data extraction of Iphone. This article focuses on the comparative study of common Iphone data extraction methods in the cases.

2. Iphone overview of Iphone operating system

Apple's IOS smart system is based on Apple's Mac OS X. IOS is used in Iphone and Ipad. Just like the operating system used by Apple computers, this system is divided into four parts, including the core operating system layer, core service layer, media layer, and touchable layer. Since it is a closed operating system, the performance of the system is very stable and has high security, but the degree of freedom of this system is relatively low. And because Apple's IOS system adopts closed-source measures, which makes it difficult for researchers to research evidence of iPhone data. In the investigation and evidence collection of the mobile phone, the investigator can input the *3001#12345# to display mobile phone RSSI signal strength information, UMTS and GSM base station, neighboring base station and base station identification information [1] through the dialing interface of the mobile phone.

3. Experimental preparation

3.1 Experimental design

There are three methods for extracting the common data of two iPhones (Jailbreaking and Not Jailbreaking), which respectively are using Itunes for data backup, using the PP assistant's directory structure to view the Iphone directory file and then manually extract it and using data extraction function of the PP assistant to extract data. After using these three methods, I will compare the three different extraction methods for the common data extraction range and the advantages and disadvantages of each method in mobile phones.

3.2 Experimental conditions, materials and software

1 Experimental conditions: laboratory at room temperature with signal shielding measures;

2 equipment: unconnected computers, data lines;

3 software: Itunes, Itools, PP assistant.

3.3 Extracted content

In this experiment, the most common and most useful types of information in the case are extracted, including the following categories: one is the address book of the mobile phone; the second is the mobile phone call record; the third is the short messages sent and received by the mobile phone; The fourth is the picture photo in the mobile phone; the fifth is the keyboard cache; the sixth is the log information in the mobile phone; the seventh is the memo; the eighth is the browser information [2].

Not jail broken Iphone6Plus: 123 photos, 120 address books, 32 call records, 5 text messages, 6 bookmarks, 5 memos.

Jail broken iphone6Plus: 321 photos, 123 contacts, 12 call logs, 23 SMS messages, 12 bookmarks, 4 memos.

Note: For Apple devices, jailbreak is a crack operation that aim to damage the Apple operating system (IOS system) that restricts the user's storage read and write permissions. The jail broken IPhone has read and write access to the underlying system, allowing IPhone to use the cracked App Store software (equivalent to piracy) for free.

4. Experiment procedure

4.1 Signal shielding before extraction

Firstly, the forensic personnel should keep the mobile phone on and perform signal shielding. The common method is to put the mobile phone into the signal shielding box. The shielding box is generally small in size and easy to carry. The top of the box is made of transparent shielding material, which allow the inspector to look through the contents of the mobile phone directly. Meanwhile, the forensic personnel should draw a data line from the outside of the box to connect with other synchronous devices, synchronize the data to the computer under the condition of ensuring signal shielding, and ensure that the Iphone is connected to the computer after the signal is shielded [3].

4.2 Data Extraction

1. Extract jail broken IPhone mobile phone data by Itunes data backup method

According to Apple's official database, ITunes can automatically back up the following contents of the IPhone: address book, contacts, browser settings, memos, photos and pictures saved in the phone camera film, calendar events, call history, text messages, applications program data information, network configuration information and some other configuration information [4].

After connecting the jail broken Iphone6 Plus to your computer, open Itool and click iTunes Backup to add new backup information. ITunes will save the corresponding backup file in the following location C:\Users\%username%\AppDate\Roaming\Apple Computer\ MobileSync [5].

The backup files mainly include the following kinds: Info.Plist: the file provides some detailed information about the device, which is similar with the manifest.Plist, including UDID, device name, IOS version, ICCID, etc. It also includes the device serial number, a complete list of device installation applications, a list of synchronized applications, synchronization time, and iTunes software version used for backup. . Status.Plist: the file displays some backup information such as the time of the IPhone backup, the status of the backup, and the backup device ID. Manifest.Plist: the file saves the Apps information installed on the phone. The main function is to ensure the integrity of the data between the backup files. The Manifest.mbdb: the file contains information such as the file name and path of the backup. Backup data files: these files are composed of 40-digit numbers or letter combinations. Generally, they do not have an extension. These files are the contents of the data portion of the backup, including JPEG photos, Safari's web cache information, and various applications. file. SQLite database file: This type of file saves the contact information of the IPhone mobile phone [6].

For the files in the Iphone backup information, you need to use special software (such as IPhone Backup Extractor) to export before you want to view it.

2.Extract unsecured iPhone data by Itunes data backup method

When using iTunes to extract the data of the not jail broken IPhone, it is found that the extracted content is the same as the above-mentioned types of files.

3.Extract jailbreak iPhone data by manual extraction method

When manually extracting the data in the iPhone, the directory structure is necessary if you want to view the file directory quickly. Whether the Iphone is jail broken or not, the specific content you can observed will be affected. For the Iphone that is not jailbroken, only the Media directories can be extracted， and these directories mainly store some photos, log information, etc. If you need to access the root directory of the iPhone, you need to jailbreak the iPhone. The following is the data extraction of the jailbroken Iphone, using the PP assistant file to view the Iphone directory.

(1)The extraction of text messages

In the Iphone, all SMS messages and MMS messages are saved in the SQLite database file named sms.db. This file is saved in User/Library/SMS. For SQLite database files, you can use the SQLite Database Browser to view the specific content.

(2)The extraction of call records

The call records of the Iphone are also stored in the SQLite database. The file name is call_history.db. The Iphone can store the latest 100 call history records by default, including incoming call records, dial-out records and missed call records. By analyzing the specified data files, the forensics personnel can completely obtain the call record number, time and duration information of the iPhone.

You can use the call_history.db under private/var/wireless/Library/CallHistory to extract the file. It can be seen that the file’s format is the same with the sms.db file that stores the SMS information. You can use SQLite to view the file. [7].

(3)The extraction of contacts

In the IPhone, the relevant information of the contacts is stored in two databases, respectively AddressBook.sqlitedb that stores contacts information and AddressBookImages.sqlitedb that stores contacts pictures information. The forensics personnel can extract contact files under private/var/mobile/Library/AddressBook.

(4)The extraction of photos

The photos in the Iphone are stored in the DCIM folder in the file directory. After opening the Iphone file directory with the file management software, you can directly copy the DCIM folder in the first layer interface to extract the photos from the iPhone.

(5)The extraction of keyboard cache

The keyboard cache of the IPhone is located under the “Library/Keyboard”, and the data information is stored in the “dynamic-text.dat” file. It also should use file management software to find the corresponding storage location and extract the information [8].

(6)The extraction of log information

The Iphone log information is located under "Library/Logs" and stored in the file ADDataStore.plist or ADDataStore.db. The analysis of the file can get the application name of the mobile phone, the number of times used, and the total time used.

(7)The extraction of browser information

Safari is the default browser in Iphone. Under "Library/Safari", browser information can be extracted.

(8)The extraction of memo

The memo information in the mobile phone is stored in the Notes.db file and recorded in the SQLite3 database format.Under User/Library/Notes, memo information can be extracted.

4.Extract data from not jail broken IPhone by manual extraction method

When you use the file management software to view the not jail broken Iphone directory，You will find that you can't view the Iphone's root directory, instead, only contacts, browser information, calendars, memos, and photos can be extracted.

5.Extract jailbroken IPhone data by software extraction method (taking PP assistant as an example)

First open the pp assistant, and then click on the "Information" menu bar to see the following contents: Click on the backup, you can extract the address book, log, bookmarks, memos, so the file will be saved in the form of a compressed package on the PC.

6.Extract not jail broken IPhone data by Software extraction method (taking PP assistant as an example)

When data is extracted from the Iphone that is not jail broken, the information of the address book, log, bookmark, and memo can be extracted. However, when the short messages and the call records are extracted, it will display that the device cannot be extracted by the pp assistant because the device is not jail broken.

5. Experimental results and discussion

When using Itunes data backup for two Iphones, the jailbreak status of the phone does not affect the backup and retrieval of data. Extracting information includes address book, contacts, browser settings, memos, photos and pictures saved in mobile phone camera, calendar events, call history, text messages, application data, network configuration information, and other configuration information.

When using the manual extraction method to extract several common data, we can see the extraction scope of this method:

Table 1 Range of data extracted by manual extraction

	Message	Photo	Contact	Call record	Log	Browser information		Memo	Keyboard cache
Jail broken iphone	√	√	√	√	√	√	√	√	
Not jail broken iphone	×	√	√	×	×	√	√	×	

When using the PP assistant data extraction function to extract data, it can be seen that the extraction scope of this method:

Table 2 Range of data extracted by software data extraction

	Message	Photo	Contact	Call record	Log	Browser information	Memo	Keyboard cache
Jail broken iphone	√	×	√	√	√	√	√	×
Not jail broken iphone	×	×	√	×	√	√	√	×

From the above experimental results, it can be concluded that the Itunes data backup method has the widest range of Iphone data, and can extract text messages, camera film photos, contact information, historical call records, log information, browser information, memos, keyboard cache information, and even application configuration information and other configuration information for the phone. The extraction range of the manual extraction method is smaller than the backup extraction method, but larger than the data extraction function using the mobile phone management software. The data extraction function of the mobile phone management software has the smallest extraction range. In terms of the impact of the jailbreak status of the iPhone on mobile data extraction, the jail broken status has no effect on the Itunes data backup method to extract mobile phone data. It has a greater impact on the other two extraction methods. In terms of extraction efficiency, using the mobile phone software data extraction function takes the shortest time to extract , and the manual extraction method takes the longest time. In terms of the degree of disclosure of the extracted mobile phone data information, the mobile phone data obtained by the Itunes backup method needs to be exported by a more specialized technical means, but the files extracted by the other two methods need only be opened by using a special SQLite visualization tool. Then you can view it.

6. Conclusion

It should be emphasized that the primary task in extracting Iphone mobile data is how to deal with the Iphone involved in the case. It should be considered whether the closed Iphone can be opened and whether the mobile phone can be packaged. At this time, protecting evidence is the first problem that Iphone data extraction needs to consider, and it is also the precondition for all follow-up work to be carried out smoothly.It has three meanings, including avoiding pollution detection materials, blocking communication channels by scientific means, and improving the safety of case handlers [9]. In this paper, a comparison of several common Iphone data extraction methods is carried out, and the applicable scope, advantages and disadvantages of various methods are analyzed. The purpose of Iphone forensics is to find out the facts of the case, provide clues for investigation, and provide evidence for solving crimes, prosecutions and trials. In criminal cases, the results of the mobile phone check can provide users with information such as mobile phone user identity information, mobile phone communication information, mobile phone location information, phone book and calendar. This information can help the investigation work in many aspects, and to a certain extent, it can also determine the investigation direction of the investigation department. This shows that the role of mobile data electronic evidence in today's era is very important. Criminal technology develop Iphone forensics and network supervision, national security, technical investigation and other departments develop physical evidence extraction in the types of equipment have the same characteristics, but their respective business focus is different, because the number of criminal cases is large, so the criminal technology field for Iphone data extraction should have the broadest development space [10].

References

[1] Tang Wei, Wang Zhishuai. A Method of WeChat Forensics Analysis Based on IOS Platform[J]. Software Industry and Engineering, 2014(01): 3-4.

[2] Xu Yu. Research on Several Issues of Mobile Phone Forensics [D]. Beijing: China University of Political Science and Law, 2008.

[3] Li Junhui, Li Jinyue, Deng Qiang. Discussion on the Protection and Extraction of Mobile Phone Data in Electronic Material Certificate[J]. Computer Knowledge and Technology, 2015(20): 3.

[4] Tang Wei，Wang Zhishuai. A Method of WeChat Forensics Analysis Based on IOS Platform[J]. Software Industry and Engineering, 2014(01): 49.

[5] Du Jiang. IPhone third-party software forensics research [J]. Computer CD software and applications, 2013 (13): 53.

[6] Li Bolan. Software Security Analysis of IOS Platform [D]. Shanghai: Shanghai Jiao Tong University, 2011.

[7] He Yingrui. Electronic Data Forensics Analysis for IPhone [J]. Information Network Security, 2013, (10): 88.

[8] Gao Feng. Application Research of IPhone Forensics [J]. Electronic Forensics, 2011 (3): 41.

[9] Zhou Junchen. On the Extraction and Inspection of Mobile Material Evidence in Criminal Cases[J]. Legal System Expo, 2015,8(3): 3-4.

[10] Xie Jianjiang. On the important role of electronic evidence in criminal cases [J]. Information Network Security, 2011 (08): 3.