Digital Forensics Security Analysis on iOS Devices

Min-Hao Wu, Ting-Cheng Chang* and Yi Li-Min

College of Information Engineering, Guangzhou Panyu Polytechnic, Guangdong, 511483, China
E-mail: 18250922163@qq.com
**Corresponding Author*

Received 25 March 2021; Accepted 25 April 2021;
Publication 02 June 2021

Abstract

With the rapid development of the Internet era, cell phones play an essential and indispensable role in nowadays life. Smartphones have profoundly influenced our social relationships and our daily lives. Generally speaking, the most common tools we hear about in our daily lives are QQ, WeChat, and other Internet communication services that allow users to send text messages, pictures, and documents, providing a more convenient and faster medium for people to communicate and chat. The popularity and convenience of mobile technology have changed people's habits of communication. People no longer need to rely on computers to communicate, and computers cannot communicate anytime and anywhere. In the kernel of Linux and Windows, as long as the Message Hooker will install, it can monitor the messages of other programs, including WeChat and QQ, in this research. We can provide relevant law enforcement officers with effective evidence collection so that criminals will not be able to hide. The suspects often delete their WeChat or QQ records after committing the crime. It impossible for our law enforcement agencies to obtain evidence directly from the cell phone and the crime facts. Our research hopes to use some technology to help law enforcement units effectively obtain strong evidence in the iPhone not to hide the crime facts.

Journal of Web Engineering, Vol. 20_3, 775–794.
doi: 10.13052/jwe1540-9589.20310

Keywords: Mobile forensics, iOS forensics, Instant messaging, Social networking, WeChat, QQ, Jailbreak.

1 Introduction

The technology and the rapid did development of information on the Internet. The information in smartphones has also become one of the most critical components of communicating with people anytime, anywhere. Due to the development of communication devices and networks, some criminals can use cell phones through specific cyber fraud platforms to become a tool that allows criminals to facilitate communication. The suspect smartphone to detect the investigation, making it possible to find some strong evidence about the detection of criminal cases, helps us in life or other relevant cases encountered in the investigation and detection. Smartphones are always on and continuously updated data, which may make some strong evidence lost. However, the iOS operating system on which the iOS series devices did equip has higher security and stability than other operating systems such as Android and Windows. The Apple system for iOS has a closed feature, unlike other systems, not open source. It does not allow any operation or modification of its system iOS software, causing the iOS series features. The operation did restrict to the range allowed by Apple. Hence, Apple users want to operate as they wish on the system because security and system stability are protected. There is bound to be some sacrifice. In the end, the extraction of criminal evidence is even more difficult.

In 2020, the smartphone operating system is still iOS and Android as the mainstream. People of all ages love the iOS system due to the unique closed system that makes the phone relatively smooth and some appearance factors, and it has a pivotal and vital position in the smartphone industry. Besides, iOS is a closed-source operating system. The factory settings prohibit changes to the operating system so that the forensic analysis will face more challenges and bottlenecks than other systems. Therefore, to effectively solve the forensic limitations and bottlenecks of iOS smartphones, we attempted to uncover jailbreak the iOS-equipped series of cell phones and analyzed and compared the digital forensic results before and after the uncover jailbreak to conduct related research. As there may already know, iOS is faster than Android in terms of operating system updates. That is because the iOS operating system and the software used are developed exclusively by Apple. It is a mobile device such as iPhone, iPad, iPod, and other users. With the Apple App Store

platform, it is possible to display and place the many software available and run online in the iOS App Store. It also needs Apple strict confirmation and identification and can only be downloaded on the store shelf after passing, a robust security guarantee.

On the contrary, there are too many cell phone brands equipped with an Android system. The types of devices are very diversified, so the operating system updated by each cell phone brand is prone to some incompatibility reasons, and the latest system cannot immediately repair the bugs. In contrast, Google releases the Android operating system. Google releases the Android operating system, and the system update speed by Google is much slower than the iOS system update speed.

The reason for an OS update should be the same, most of the original functions are modified and strengthened, and the system security is strengthened and protected. Bugs and vulnerabilities are repaired, which enriches our user experience and makes our privacy content on the device more secure and safe and gives us more peace of mind after the update of the operating system security protection method. It is not only through the system of some settings and access to some enhancements, for the operation of the device to adjust the behavior of changes and restrictions on permissions, encryption of some critical data document security. Therefore, in the intruder view, the original breaking into the system may have been blocked, and it is necessary to find another way to break through.

Compared to the Google Android system, Apple operating system will have tighter security and more privileges. Faster fixes for vulnerabilities and the release of updated versions will make it impossible to quickly discover the security of digital forensic extraction methods in iOS. Several available forensic tools specifically for digital markers and iOS extraction can accelerate with newer versions and subject to certain restrictions.

The digital identification of smartphone devices still relies mainly on digital identification software tools for forensics to iOS series devices. Apple has updated its iOS version at an alarming rate. Moreover, in order to enhance the security of the iOS operating system. Gradually, most of the identification tools are facing challenges and supporting the extraction of digital traces. iPhone is the updated iOS version of the forensics tool. The newer the iOS version of the forensic tool, the less documentation is available. Even the more unsupported versions are available. With uncover, the operator and the forensic tool can increase the access to the iOS device, break the system permissions and the closed extraction pipeline, and increase the quality and

quantity of the data obtained, making it possible to significantly increase the likelihood of obtaining data and effectively improve the results of digital trace extraction.

iOS is the Apple mobile operating system available on the iPhone, iPad and iPod touch. Any third-party applications developed for iOS devices must go through the Apple application review process and be approved to appear in the official iTunes App Store. When an app is downloaded from the Store and installed on an iOS device, it did give a limited set of permissions enforced by the iOS app sandbox. Although Apple keeps the details of the review process and sandbox as a black box, these iOS security mechanisms are generally considered effective in defending against malware.

In this work, the medium allows third-party applications to launch attacks on un-jailbroken iOS devices. They include attacks via dynamically loaded frameworks and attacks via private C functions. With these attack vectors, attackers can access the public and private APIs of the iOS framework. Following this common attack mechanism, we can construct multiple proof-of-concept attacks. These include cracking device PINs, blocking phone calls, taking snapshots without user knowledge, sending SMS and emails, and posting tweets on Twitter. The application in which we embedded the attack code has passed the Apple review process and works appropriately on non-jailbroken devices. Our proof-of-concept attack shows weaknesses in the Apple review process and iOS sandbox that third-party applications can exploit.

This paper did structure in the following. Section 2 gives some backgrounds—Section 3 describe the mobile forensic procedures in iOS. Section 4 reports the artefacts found on iOS and discusses the results—finally, our conclusion given in Section 5.

2 Backgrounds

2.1 iOS Digital Forensics

The iOS operating system is highly protected and closed and is available on a wide range of devices, such as the iPhone, iPad, iPod, and other devices. Only applications authorized by Apple and available on the App Store platform can be installed and executed. Other applications cannot be installed and run on iOS devices [1], which may cause problems with support for digital identification and related software tools. Besides, iOS series devices have only internal memory and no external memory card configuration, so the

only way to retrieve data stored on the device is through internal memory, making data extraction more difficult. The internal memory of the iOS device divided into two sections. One is the system partition, which stores the operating system and default programs that Apple uses to protect the iOS operating system from changes. Apple protects the iOS operating system from changes by setting this partition to read-only mode, prohibiting users from viewing and changing any partition settings systems. Another partition is the user data partition, which stores the user usage information on the iOS device, including application accounts, user profiles, photos and videos, text messages sent, and contacts saved. This user data partition is the subject area for digital signage extraction. For digital forensic operations, digital data extraction divided into three main types: manual extraction, logical extraction, and physical extraction [2]. The characteristics and details of the digital forensic operation for digital data extraction divided into three main categories: manual extraction, logical extraction and physical extraction [3]:

(1) Manual Extraction
Manual extraction generally requires direct manipulation of the device evidence and browsing of the device file system and internal memory information. The data stored in the device to present on the screen through actual operations [3]. The information presented on the screen to use to determine the data stored inside the device. The digital evidence obtained is usually a screenshot of the device. Therefore, deleted data must not present on the device screen, i.e., deleted data cannot obtain by manual extraction.

(2) Logical extraction
The scope of logical extraction is the scope of the logical structure of the operating system. The path data linked to the directories and indexes in the scope will extract by the bit-by-bit stream. Therefore, if a file or data to delete, its index directory will be deleted as well. Therefore, the deleted files or data cannot retrieve by logical extraction. The jailbreak is not run for iOS devices—the iTunes logical backup method investigates the instant messaging software records on the iPhone [4]. However, the logical structure of the operating system of smart mobile devices is clear. This feature facilitates forensic software to organize the logical structure and data extraction. Therefore, forensic software is usually more supportive of logic extraction [5].

(3) Entity extraction

The method of entity extraction is to make bit-by-bit copies of the entire physical memory. Therefore, the advantage of entity extraction is that all digital evidence in physical memory can be retained [6]. In physical memory includes data that has been deleted and can view by forensic software tools to restore the original data inside the device. However, physical extraction is more difficult to perform. The prerequisite is that the necessary forensic software must first install on the system partition, and the full image of the user data partition can run through the forensic tool. However, the forensic tool is not an Apple-licensed application tool. Therefore, it must install and run after the Jailbreak program [7] has been used to gain supreme control of the iOS device.

To overcome the restrictions of not allowing third-party applications to be installed on iOS devices and locking out telecommunication service providers. The jailbreaks have developed to overcome these two restrictions. Such attacks reveal the vulnerability of iOS device security [8]. Jailbreak allows users to gain full administrative privileges on iOS devices, enabling them to install third-party software, change system files, and remove factory restrictions [7]. However, the implementation of jailbreak is legal under the Digital Millennium Copyright Act (DMCA) and does not violate the law [9].

The jailbreak enables iOS devices to bypass many of Apple restrictions. The ability to download non-Apple-approved and signed apps from platforms other than the AppStore. The ability to control the device with full privileges and gain complete installation and access capabilities. SSHServer and other essential Unix tools can be installed [10]. Many service access and directory view permissions can open after the device.com.apple.afc2 service will install when the jailbreak. The service allows computers trusted by iOS devices to access and download the entire internal system files. The service will run without any prompts on the iOS device screen [11]—the changes to the user data stored on iOS devices due to jailbreak. The pre-Jailbreak application and its user data are still intact and have not been changed or lost [12].

The installation of SSH Server allows users to access their iOS devices remotely without the constraints of a physical connection over distance, but it also raises security concerns [11]. It does not change the user data, and even assuming that some current or future Jailbreak method will modify the user data partition, there is still much valuable information to be gained as long as it is clear what changes jailbreak has made to the device. The primary forensic approach to recovering a complete image file from a device did ultimately based on the Jailbreak principle [10].

2.2 Jailbreaking

The iOS devices (iPhone, iPad and iPod touch) have just entered the user's hands, and the entire iOS device is in a closed source state. As ordinary users, we do not have the right to obtain the highest privileges from Apple, so we cannot install software not certified by Apple. The only way to download software is through iTunes or the Apple Store. Of course, most of the commonly used software is free, and now some software can be pirated directly without jailbreak. Only through the Apple certification, in these processes, make of the Apple devices we users installed software signed by the developer and has not been tampered. Apple ensures the safety of user information and prevents leakage and breaches. The software obtained by legal download transmitted to the phone for use [13]. The security is guaranteed, so this way, many users are firmly under Apple jurisdiction. That thing is good for us may not be in their interest. WiPlug is an excellent multi-screen interactive product that works with the iPhone and iPad to achieve more powerful functions. It is like casting the whole screen of that phone or tablet to display on the TV. There is no need to have a laptop connected to the projector when that have a meeting, connect the projector to the WiPlug and then connect everyone phone to the WiPlug via Wi-Fi and that can present the PPT directly on that phone and then display it on the projector. This feature is impossible without jailbreaking, and only jailbroken phones and tablets can operate so freely.

Jailbreaking is the process of gaining access to the highest privileges on iOS that are not available on regular Apple phones. It allows the user to operate the device in any area of the operating system. After jailbreaking, the plug-ins and software needed to operate the device can only be installed and used. After jailbreaking, the Uncover software will access all the IOS of the device directories and operations (iPhone, iPad or iPod touch) and install plug-ins to change the system functions and use the software not certified by the Apple Store after the jailbreak completed. To put it more simply, jailbreaking is the use of specific vulnerabilities in the iOS system, through some instructions to obtain the highest cracked root access to iOS, making changes to some programs, so that the iOS of the device functionality is enhanced, breaking through the closed source of restrictions, and thus breaking through the IOS security system.

Uncover is a jailbreak tool. It has more advantages over other jailbreak tools, with more detailed error messages, no malicious program code, and automatic detection of jailbreak status. Uncover enables the iOS devices to bypass many Apple restrictions and download applications that Apple

does not approve from platforms other than the App Store, which can have full authority control. Get the complete installation and access capabilities to install SSH Server and other essential Unix tools. Many service access and directory viewing permissions can open after the device uncovered. The com.apple.afc2 service will install when the uncover program executed. This service allows computers trusted by the iOS device to access and download the entire internal system file. When the service is running, no prompts appear on the iOS device screen and uncover changes to the iOS device memory usage data. The application program and the user data stored in it before uncover will be kept intact. There has been no change or loss.

2.3 Cydia Software

Cydia software is a kind of similar crack able software that runs on Apple devices (such as iPhone, iPad, and iTouch), just like Apple own APPstore store, which can download things. It is the same as our original system software after jailbroken, and it is not easy to be deleted and installed on our mobile phone. Most of this software are patches and the like, mainly used to make up for system deficiencies. It did jointly develop by Jay Freeman, the father of Cydia, and some universities. The primary mission of Cydia is to provide high-end decorative appliances with graphical and shaped interfaces for jailbroken iOS users to install programs that are not certified in the App-Store. It is an aggregator of many software, with several sources trusted by the community to avoid excessive dependence on a particular server [13]. We can find the stable software version we need in this software. Make it easier for users to add sources and then download software. Let the system resources that initially closed iOS be as open as possible. Allow some users to manage their favorite software, and updates can also share in the community. Cydia will download the package directly and install it in the same /Applications directory as the built-in iOS program. At the same time, this will not affect the original purchase and download of software in the App Store.

In September 2009, after providing Cydia software, Cydia also provided a new feature. That is, the device can restore to the un-jailbroken state after the jailbreak. This method is called SSH. There also got the legality of Apple to restore the firmware. A process used to restore iOS firmware. The system version of the iOS device did restore to the earlier version.

Cydia software requires a specific jailbreak. Before July 2010, jailbreaking the iPhone was always impossible. Therefore, we have been unable to escape from prison. However, as the United States announced the Digital

Millennium Copyright Act illegal regulations, our jailbroken iPhone slowly became legal. Therefore, Apple has also adopted relevant policies for this measure. After the device jailbroken, the warranty cannot carry out. Therefore, for some IOS users, the successful launch of Cydia symbolizes the beginning of a perfect escape. After the perfect jailbreak, the IOS system will not guarantee that device. Many software installations through the Cydia application will obtain device system permissions, which may bring some danger to that device. Apple policy on this is that jailbreaking will invalidate the device warranty.

The usage of Cydia software is as follows

(1) After the jailbreak is successful, the icon named Cydia is in the main interface of the iOS device. Click the icon to start Cydia. There can enter the main interface of the Cydia software.
(2) Next, there have to set up for Cydia "software source". Only after adding "software sources" can there download various application plug-ins and system patches from these sources. Click "Software Sources" below by default. There will be five sources displayed in Cydia. However, these are foreign sources. The domestic connection speed is very problematic and often cannot be accessed. Therefore, we need to add domestic well-known software sources. Click the "Edit" button in the upper right corner, and then click "Add" in the upper left corner. Now we have completed the initial settings of Cydia. In the future, various plug-ins and patches can be downloaded directly from domestic sources. If there want to use Cydia, there must have network support. Although it is a foreign-created software, we can still use our country network, and there is no need to overturn the wall. When using Cydia software, the following problems are often encountered:
Cannot find any software in Cydia software, and the jailbreak source and some software categories are empty, then we should find the refresh button at the top of the page. Wait for the update operation to come out. If there cannot find the software there need, there need:

    (1) Check whether the typing is correct when searching.
    (2) Some software names may contain spaces. Please pay attention to whether there are spaces when we search.
    (3) Whether the user identity is selected correctly or not, some software packages will not display in the software user identity, and the user identity can change in the Cydia settings.

3 Mobile Forensic Procedure

3.1 iPhone 8 Plus Jailbreak

This time, the jailbroken device uses Apple 8plus as the research object, equipped with iOS 11.3 version, and uncovering the program software for jailbreaking. First, go to the Internet to download the uncover jailbreak software, as shown in Figure 1.

After opening the uncover software, there have to turn off that of the phone wireless, and the phone needs to turn on the airplane mode. Then click

Figure 1 Open the uncover software.

jailbreak. If the software Cydia does not appear after clicking, there have to try again, usually within three times. After completion, the Cydia software will appear on the desktop, proving that the jailbreak is successful.

3.2 Use Cydia

Open Cydia software if the page shows no network connection. 1. Download the APP called "Lewang" through Aisi Assistant. The Lawang Plus downloaded in the AppStore does not work. 2. Open the global interception. There need to install the configuration file in the middle. If successful, there will be a VPN logo on the status bar. Because the Cydia mechanism automatically refreshes other sources, there will find that other sources are no longer blank.

When everything is ready, there will add a jailbreak source to Cydia. The jailbreak source is equivalent to the address of the software download of our mobile phone, similar to the application download center. Open the Cydia software, click the jailbreak source, click edit, and then click add. In this research, we mainly add the following two jailbreak source URLs, http://apt.cydiami.com/ [15] and http://apt.cydia.love [16], to add these two jailbreak sources, respectively. After adding, click back to Cydia, and then click the software source. There can see the jailbreak source and the added.

4 Analysis and Discussion

4.1 iOS Backup Management

The identification process and jailbreak of the device may change the memory status of the device. There can lead to destructive errors in the trace extraction process or dangerous experiments. The device memory data can restore to a certain extent. In the Jailbreak program, there is also a chance of unexpected errors. It caused the execution progress of jailbreak to stagnate, and the device crashed. However, after the jailbreak, there want to restore the device to the Jailbreak state. It is necessary to use the previous backup file, the last line of defense, for device data preservation. After jailbreaking the device and installing the Cydia software, the memory status of the iOS device will change. Therefore, we need to back up the device to avoid disruptive operations after the device permissions can change during the forensic extraction process. The data in the device can restore to a certain extent. After the installation of Cydia, the same damage may also cause, causing some situations where Cydia stops during execution and the iOS device freezes and becomes a white apple. However, after uncovering, there want to restore

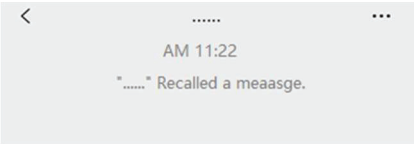

Figure 2 WeChat withdrew the wrong message.

the device to a state without jailbreak. The data and some necessary settings are not lost; that is, the previous data needs backup. The backup is the last line of defense for the preservation of the data equipment. Download Aisi Assistant, install and open it, click Backup/Restore Data, click Full Backup, and then click Back Up Now. That ensures that the data will not be lost.

4.2 Forensic Analysis Based on Anti-withdrawal of WeChat Chats Records After iOS Jailbreak

iOS jailbreak anti-withdraw operation. As there are hundreds of millions of users, WeChat frequently uses WeChat as an essential tool for daily communication. In the process of communication, some of us permanently withdrew some wrong messages. However, he withdrew in time. However, there is a need to see the content of the message he sent, as shown in Figure 2.

Use the software in Cydia for forensics, as shown in Figure 3.

(1) Open Cydia software.
(2) Click on the software source.
(3) Enter the source site of bees.
(4) Click on WeChat.
(5) Find a WeChat Assistant and click install.

After the installation is complete, there must restart of SpringBoard. After clicking, the phone will restart. If there do not click to restart SpringBoard, the setting is invalid and does not affect. After setting, when there open WeChat, click When setting. There will find an extra line in the list of settings. Click "WeChat Confidant" to open the message to prevent withdrawal. WeChat detects the anti-withdrawal effect of iOS. After the opening does complete, whenever someone sends a message to withdraw, we can see the withdrawal content from time to time and carry out evidence collection, as shown in Figure 4.

Based on iOS jailbreak, the WeChat chat history contact is deleted and then recovered for forensic analysis. IOS WeChat contact does delete, and

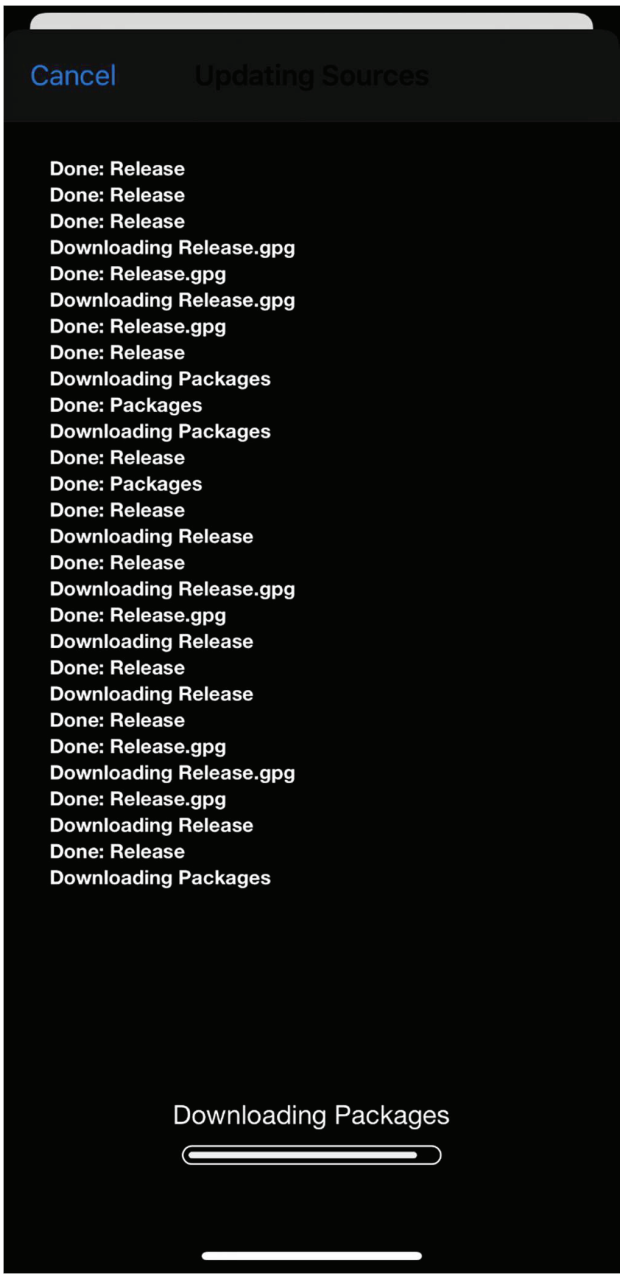

Figure 3 Use the software in Cydia for forensics.

Figure 4 WeChat detects the anti-recalling effect of iOS.

Figure 5 The WeChat chat history contact is deleted and then recovered for forensic analysis.

then the contact is restored. In daily life, we can quickly delete others accidentally, which leads to the inability to find friends. At this time, we will first download software called Apple Recovery Master on Baidu. The user will not immediately clear the data from the storage device when deleting the data. The data will exist on the storage device, and the storage is here. The storage area does mark for deletion. If this storage area does not fill with new data, Apple Recovery Master will wake up the marked storage area, find the previously deleted information and perform recovery. Use it to retrieve WeChat contacts. After downloading Apple Recovery Master, install it and open it, click Next, and find the WeChat address book in the text data, as shown in Figure 5.

IOS WeChat recovery contact effect. When the scan does complete, there will find all the contacts there deleted before. After comparing with all the contacts in the WeChat, the person there deleted, as shown in Figure 6.

4.3 Anti-withdraw Forensic Analysis of QQ After iOS Jailbreak

Test the effect of QQ withdrawal after iOS jailbreak. With the rapid development of the Internet era of big data, we need software in all aspects of our lives. QQ is a communication tool, like a phone, to contact relatives and friends in this deep place at any time. In daily life, sometimes in group chats, some people make some nasty comments and then immediately withdraw them, others see them, but he still refuses to admit them. Some criminal

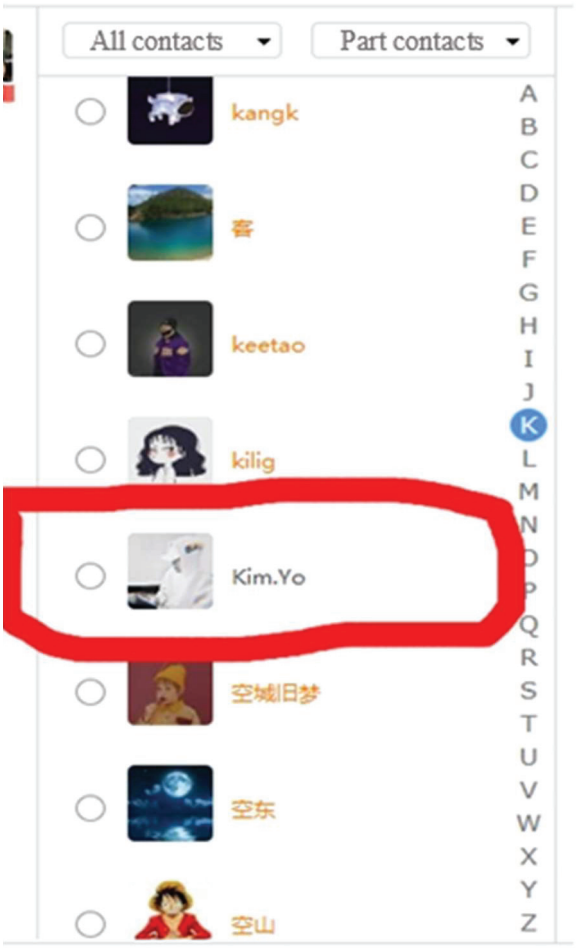

Figure 6 WeChat recovery contact effect.

suspects also hold the attitude of not admitting. This time I studied how QQ can prevent other man information and provide evidence to those in need. The result of QQ withdrawal without any measures.

Next, there must first activate the iOS jailbreak environment. There must ensure that the jailbreak status of the device has turned on. When the Cydia software cannot open, the jailbreak state does not turn on. There need to re-jailbreak. (1) Open Cydia. (2) Click on the software source and find our previous Two installed software sources. (3) Find RecallPatch in the "QQ withdraw" software source. (4) Click Install. Then execute the code or click

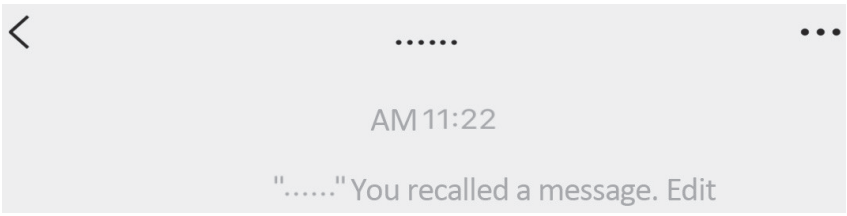

Figure 7 The iOS jailbreak environment in the QQ is recalling.

Restart SpringBoard after the installation does successful, and the phone will restart immediately. The code will execute the software, as shown in Figure 7.

5 Conclusion

The QQ, WeChat, and some network communication services allow users to send text messages, pictures, and documents, providing people with a more convenient and fast medium for communicating and chatting. Instant messaging services are not only more and more common in the use of normal activities between friends. Related illegal criminal activities may also use it as a tool of contact. This research proposes to use the iPhone to synchronize backups to find out that the instant messaging software used by the phone may store call records and chat records and send documents and pictures. Investigate and research social communication software such as QQ and WeChat commonly used in the iPhone. Prevent criminal evidence from being deleted by interested persons. As a result, it is impossible to present favorable evidence to prove their criminal behavior. Through the Jailbreak process, iOS devices can indeed further improve the data extraction results of iOS devices. This digital evidence is all types of usage records in the device, such as phone book, SMS, calendar, memo and storage information of various apps. And the private information of many device users, such as account and password. This chapter integrates and discusses the effectiveness of the Jailbreak method proposed in this study for data extraction. Compare the differences in quality and quantity of extraction results. The following will be for iOS -Discussion and analysis of research findings of Jailbreaking Forensics. Before jailbreak, enter the file system through the interface. The files that users can view are limited to user files. However, after running jailbreak, we have permission to view system files. Compared with before Jailbreak, there are many more options. View and change items, and compare the items that can view before and after jailbreak.

Acknowledgements

This paper belongs to the project of the "Intelligent and Convenient Physical Test System for the Elderly", No. 210113263; in Guangzhon Panyu Polytechnic Innovation and Entrepreneurship Education Center and "Panyu Polytechnic Innovation Team", No. 2020CXTD003.

References

[1] L. Alex, S. Bill and J. Daryl, "Third Party Application Forensics on Apple Mobile Devices", Proceedings of the 44th Hawaii International Conference on System Sciences, IEEE, 2011.

[2] L. Gomez-Miralles and J.Arnedo-Moreno, "Universal, Fast Method for iPad Forensic Imaging Via USB Adapter", Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2011.

[3] S. Azadegan, W. Yu, H. Liu, M. Sistani and S. Acharya, "Novel Anti-forensics Approaches for Smart Phones", Proceedings of the 45th Hawaii International Conference on System Sciences, IEEE, 2012.

[4] M. I. Husain and R. Sridhar, "iForensics: Forensic Analysis of Instant Messaging on Smart Phones," Digital Forensics and Cyber Crime, vol. 31 of the series Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 9–18, 2010.

[5] M. Bader and I. Baggili, "iPhone 3GS Forensics: Logical Analysis Using Apple iTunes Backup Utility", Small Scale Digital Device Forensics Journal, vol. 4, no. 1, September 2010.

[6] C. Yates, L. Ray, and J. Yang, "An Investigation into iPod Touch Generation 2", Information Security Curriculum Development Conference, 2011.

[7] N. Kala and R. Thilagaraj, "A Framework for Digital Forensics in I-Devices: Jailed and Jail Broken Devices", Journal of Advances in Library and Information Science, vol. 2, pp. 82–93, April–June 2013.

[8] S. Salerno, A. Sanzgiri, and S.Upadhyaya, "Exploration of Attacks on Current Generation Smartphones", Procedia Computer Science, vol. 5, pp. 546–553, 2011.

[9] V.R. Pandya and M. Stamp, "iPhone Security Analysis", Journal of Information Security, vol. 1, no. 2, pp. 74–87, 2010.

[10] K. Barmpatsalou, D. Damopoulos, G. Kambourakis, and V. Katos, "A Critical Review of 7 Years of Mobile Device Forensics", Digital Investigation, vol. 10, pp. 323–349, 2013.
[11] J. Zdziarski, "Identifying Back Doors, Attack Points, and Surveillance Mechanisms in iOS Devices", Digital Investigation, vol. 11, pp. 3–19, 2014.
[12] Y.T. Chang, K.C. Teng, Y.C. Tso, and S.J. Wang, "Jailbroken iPhone Forensics for the Investigations and Controversy to Digital Evidence", accepted in Journal of Computers, 2015.
[13] L. Gomez-Miralles and J.Arnedo-Moreno, "Versatile iPad Forensic Acquisition Using the Apple Camera Connection Kit", Computers and Mathematics with Applications, vol. 63, pp. 544–553, 2012.
[14] L. Gomez-Miralles and J. Arnedo-Moreno, "AirPrint Forensics: Recovering the Contents and Metadata of Printed Documents from iOS Devices", Mobile Information Systems, Article ID 916262, 10 pages, 2015.
[15] cydiami, https://apt.cydiami.com/, 2021/02. [Online]. Available: https://apt.cydiami.com/
[16] cydia, https://apt.cydia.love/, 2021/02. [Online]. Available: https://apt.cydia.love/, 2020

Biographies

Min-Hao Wu received his Ph.D. degree in Computer Science and Information Engineering from National Central University, Taiwan, in 2016. He is an associate professor in the College of Information Engineering, Guangzhou Panyu Polytechnic, Guangdong Province, China. His research interests include System Security, Mobile Device Security, Web Security, Information Hiding, and Networks.

Ting-Cheng Chang received the M.S. and Ph.D. degrees in Process Control and Mechanical Engineering in 1992 and 1996, respectively, from the University of Houston and University of Texas at Arlington, Texas, USA. He is a professor at the College of Information Engineering, Guangzhou Panyu Polytechnic, Guangdong Province, China. His research interests lie in the Internet of Things, Data Mining, Big Data, and Optimal Theory.

Yi Li-Min graduated with a Bachelor of Arts degree in 2014. Then she continued to study for a master's degree in 2018. In 2020, she graduated from Shaanxi Normal University with a master's degree. She now is a lecture and works in Guangzhou Panyu Polytechnic, Guangdong Province, China. She has been engaged in educational work in colleges since graduating from college and has specific student management experience and academic research ability. Her research interests are Artificial Intelligence-assisted Educational Management, Data Analysis, and Educational Network Security.