Jailbroken iPhone Forensics for the Investigations and Controversy to Digital Evidence

Ya-Ting Chang[1] Ke-Chun Teng[1] Yu-Cheng Tso[1] Shiuh-Jeng Wang[1,*]

[1] Department of Information Management, Central Police University

Taoyuan 33304, TAIWAN

{bowrose, e0616316, im771138}@gmail.com

[*] sjwang@mail.cpu.edu.tw

[*] whom correspondence

Received 15 April 2015; Revised 5 January 2015; Accepted 4 April 2015

Abstract. The smartphone has gradually become an indispensable assistant in our daily life. Apple's iPhone is one of the most popular smartphones. However, once the iPhone has become a criminal tool for assisting the offender, the electromagnetic record in the iPhone will become the key digital evidence to reconstruct the scene of the crime. There is a high probability that offenders perform the Jailbreak procedure in order to gain more powerful functions on iPhones. When the Jailbreak work has processed, this will make the implementation of digital forensic extraction smoother. Otherwise, there is controversy surrounding iPhone evidence-handling if the forensic investigators perform the Jailbreak procedure for the non-Jailbroken iPhone just to make the implementation of digital forensic extraction easier. Therefore, this paper observes the diversification of iPhone evidence via the comparison between before and after performing Jailbreak procedure by using XRY forensic commercial tool kit and Apple iTunes logical extraction. We not only clarify the controversy of whether the key-evidence on the iPhone after its Jailbroken will be varied or not, but also provide a summary report about iPhone evidence and digital forensics as a court reference.

Keywords: iPhone, iOS, Jailbreak, Apple iTunes, digital forensics, digital investigation

1 Introduction

The smartphone, combining the features of mobile phone, camera, satellite navigation, computer and multimedia entertainment platform, has become the most popular and best-selling technology product in the world because of convenience, portability and various functionality. According to the market research company Gartner, global smartphone sales increased 47.3% in the fourth quarter of 2011. Total smartphone sales for the full year increased 58% and accounted for 31% of all mobile devices sold. Obviously smartphones play an important role in our daily lives. In addition, according to new research from the NPD Group, Apple passed LG and Samsung to become the top-selling U.S. handset brand in the fourth quarter of 2011. Combined, the three available models of the iPhone (iPhone 4S, iPhone 4 and iPhone 3GS) accounted for 43% of the U.S. smartphone market. Obviously the iPhone is still favored by the user even if the price is higher than the others.

The design of the iPhone does not contain the external memory card. There is also some constraints of iPhone's iOS operating system. Lots of users perform a process named "Jailbreak" in order to gain more powerful functions and permissions. Users who gain the highest permission of iPhone can perform more functions and change the system settings, such as themes, rings and user interfaces, and can install any kinds of mobile applications, even update or change different version of iOS. For the users accustomed to Jailbroken iPhone, they are more familiar with the Jailbroken iPhone.

Users are easier to expose in technological environment. Inevitably, offenders also evolve into high-tech criminal activities. There is a lot of information stored in the iPhone's internal memory, such as contacts, memos, SMS, call history, pictures, emails, GPS information, web history, and etc. Once the iPhone becomes a criminal tool to the offender, the iPhone itself and relative information will become very important critical digital evidence.

Therefore, there are two states of iPhone evidence when the forensic investigators encountered a case of a crime that the iPhone is used as a criminal tool to assist the offender. One is Jailbroken, the other is non-Jailbroken. However, according to many studies, the implementation of digital forensic extraction for non-Jailbroken iPhones is difficult, but will be easier in the opposite state. Certainly, offenders never expected that the Jailbreak procedure would not only allow them to gain more powerful functions of iPhone, but also lead to

the easier extraction of criminal digital evidence. Otherwise, in the non-Jailbroken state, there are controversial comments for the iPhone evidence-handling if the forensic investigators perform the Jailbreak procedure for the non-Jailbroken iPhones just to smooth over the implementation of digital forensic extraction.

In traditional digital forensics, if the forensic investigators want to extract digital evidence from the storage device, they first need to make at least two image copies of the storage device. Then, the forensic investigators can perform the extraction from the image file. But for the digital forensics on iPhone, we cannot guarantee that the Jailbreak procedure won't change the evidence in the iPhone's internal memory. Only seldom studies discuss about this issue. If the offender claims that the Jailbreak procedure performed by the forensic investigators has changed the internal memory of iPhone and the forensic investigators cannot provide relevant reports to defend against it, this evidence will be excluded. Therefore, in this paper we examine the impact of the Jailbreak procedure on key-evidence of iPhone by manual extraction, physical extraction and logical extraction. We clarify the controversy of whether the key-evidence on the iPhone will be changed or not after Jailbreaking by using XRY forensic commercial tool kit [12] and Apple iTunes logical extraction. We also provide a summary report as the court reference about iPhone evidence and digital forensics.

This paper is organized as follows. Section 2 introduces the background of the Jailbreak procedure and how it works, and the related works and methods of iPhone digital forensics. Jailbreak procedure through experimental design and operations is given in this Section 3. Section 4 analyzes the impact of the Jailbreak procedure on digital forensic reports. We give the conclusions in Section 5.

2 Background

2.1 Jailbreak

Apple products using an iOS operating system have implemented their own protection mechanisms in order to avoid users intentionally or unintentionally modifying the settings of the operating system and causing failures. Therefore, users cannot directly access the system files and settings. The so-called Jailbreak procedure is a technique to crack the iOS operating system of Apple products. Users can use this technique to obtain the highest authority, access the iOS system file, and unlock the restrictions on GSM providers and network usages. The Jailbreak procedure is applicable in iOS of Apple products, such as iPhone, iPod touch, iPad, and Apple TV 2. Apple products performed still with the iOS operating system and can be normally perform other functions after Jailbroken.

The process of Jailbreaking inquires entering Device Firmware Update (short for DFU) mode. The DFU mode is one of the Apple product state to wait for the update in order to upgrade the system firmware. The iPhone needs to perform the boot-after-shutdown procedure for entering DFU mode. Actually, the boot-after-shutdown procedure has been confirmed that would cause variation on mobile phone [4]. After switching to DFU mode, users can perform the Jailbreak procedure by common Jailbreak tools, such as redsn0w, PwnageTool, Sn0wbreeze, Jailbreakme, GreenPois0n, and so on. Although those tools may cause variation on the system storage space of iPhone, there are seldom studies to verify the actual variation.

After the user executes Jailbreak, program management tools such as Cydia, which is an unofficial mobile application management tool, can be installed on Apple products. Cydia provides users with extra mobile applications, background theme or the source of system modification program. Its internal program sources are all recommended by communities, so the sources are stable and reliable. Users can install the mobile applications, which are not from App Store, as well as change the theme appearance, install or modify system settings through Cydia, and even change for other operating systems.

For this, the Copyright Office belongs to the U.S. National Library focus on 1998 Digital Millennium Copyright Act to conduct a review for the procedure of Jailbreak on July 26, 2010. And announced that "When the user crack the phone in order to let the smartphone operating system be compatible with independent authoring applications without phone or its operating system manufacturers approved. This purely modification only for compatibility is a fairly use" [10]. Therefore, the majority of users Jailbreak the iPhone in order to obtain the highest authority of control of the iPhone, install more applications and change the background theme. In fact, Jailbreak For iPhone user, has been a very popular and concerned method.

2.2 iPhone and Digital Forensics

While focusing on digital forensics for iPhone, we will face the problems of the special features of Apple's products in the first step. We can only install and run the applications which are authorized by Apple and bought

or downloaded from App Store on Apple Company launched products, such as: iPad, iPod Touch, iPhone, etc. because of the restriction of the closed environment of the iOS operating system and the protection mechanism [1]. The applications which are not officially authorized by Apple are unable to be installed and run on Apple products. In fact, it will face some problems of compatibility if forensics officers want to execute mobile digital forensics software tools on the iPhone. Secondly, iPhone, Apple's design and R&D, has been equipped with enough storage space internally and it means that no external memory card can be extended. Furthermore, only charging through the original special cable or using a computer with USB connection are allowed. Thus, access for the iPhone internal memory will include a certain degree of difficulty.

Implementation of digital forensic extraction of iPhone can be started from three aspects: annual extraction, entity extraction and logic extraction [2]. Various extraction methods used in digital forensics software tools and technology are different and have their advantages and disadvantages according to the environment and selection of suitable extraction. The three aspects and the implementation of digital forensic extraction of iPhone will be discussed in the following sections.

Manual Acquisition. One of the characteristics of digital evidence is that it is not easy to be understood through human perception of the content of the evidence. Digital evidence must be presented through the interpreted media tools or interfaces. For manual extraction, it use itself as the interpretation of the interface. And present the information that the forensic staff is able to understand by using iPhone internal digital evidence. Manual extraction usually requires forensic officers directly operating the phone evidence. Through the browser interface and directory function provided from iOS, we can browse the phone's file system and information of internal memory, showing the internal digital information on screen through the actual operation [2].

The evidence from manual extraction is usually shown on the screen. We also identify the data of iPhone by the information on the screen. Therefore, in the presentation of the report is usually composed of many pictures captured from the screen. After obtaining of the information presented by the pictures, forensic officers can convert it into document files. The disadvantage of manual extraction is that forensic officers may operate incorrectly and cause errors while adding, modifying, and deleting files.

Physical Acquisition. Entity extraction method is to copy the entire physical memory bit-by-bit. We use forensic tools to make out the complete image files of physical memory and interpret it. In general operating systems, deleting the file or data is to delete the linking index only. We cannot find a deleted file by the browser provided from operating system. In fact, if there is no other new data coverage on the memory, the deleted data will still exist in the physical memory. Therefore, the advantage of entity extraction is that it can retain all digital evidence of physical memory which contains removed digital information and restore the original internal phone.

However, for the iPhone, there are difficulties in entity extraction. The internal memory of the iPhone is divided into two blocks, one is the system partition and stores the applications. In order to protect the iPhone's iOS operation system and avoid users changing the system default settings due to improper operation or other factors, Apple sets this partition to read-only mode. The other partition stores user information and contains highly sensitive personal user profile, data, and settings. This partition is concerned by the digital evidence forensic officers and entity extraction is needed. But when forensic officers try to execute entity extraction, forensic tools must be installed in the system partition and generate the complete image data for further analysis of digital forensics. The forensics tools are not authorized by Apple so we have to Jailbreak the iPhone to get the highest authority in order to install and execute the tools. In 2008, Zdziarski [8] used this method to execute entity extraction on iPhone.

Since Zdziarski, many scholars began to conduct in-depth digital forensics research of various products, and have put forward the entity extraction research report. In 2011, Luis and Joan put forward the method of rapid entity extraction for the Apple iPad [6]. The method is to Jailbreak the iPhone and install Cydia, then download the required programming toolkit through Cydia. Next, install SSH and DD in the system partition, and give the command to make out the image data through Wi-Fi connection. Finally, we can successfully make out the image data and rapidly remove it through the Apple official USB kit. This method is faster than Zdziarski's method, which delivers image data by Wi-Fi connection. [8] But Jailbreak procedure is still cannot turn away. At the same time, Yates, Ray and Yang also put forward the method of entity extraction for second-generation Apple iPod touch in 2011 [7]. Although the uses of the subject of digital forensics are different, it still needs to perform this step of Jailbreak. It can be found that, without pre-treatment procedures of Jailbreak, difficulties will be encountered in the digital forensics entity extraction work for Apple's products.

Logical Acquisition. Logical extraction method is in accordance with the logic structure of the file system storage, execute the extraction of digital evidence through the operating system compiled directory and path. The covered extracted range is the logical architecture of the operating system, the path information linking directory and index in range will be extracted bit-by-bit. Therefore, if the file or data has been deleted, logical extraction cannot extract it because its index has also been deleted. Due to the definitude of logical architecture

of operating systems, we can easily execute logical extraction and establish the logical organization by the forensics tools. Therefore, the advantage of logical extraction is high support for forensics tools.

To execute a logical extraction for the iPhone, we can use two ways. The first way is to use a commercial cell phone forensic software tools to execute simple logical extraction and output a detailed forensic report through the user interface, provided from the forensic tool, by linking the iPhone and computer. Those methods, which use forensic tools, have been inspected and ranked for installation, extraction, report, and accuracy by Hoog and Gaffaney by using 8 different tools to extract non-Jailbroken iPhone 3GS in 27 environments [5]. Also, because of the relationship of market competition, the functions provided by forensic software tools of the various types of mobile phones are constantly updated to meet the needs of forensic personnel, and expect to obtain a court authorization. Another way is to use the backup files of Apple's official application, iTunes, and obtain the internal information through parsing it. In 2010, Bader and Baggili, that is, to use this method that execute the logical extraction of backup file in the platform of iPhone 3GS and iOS [3]. Apple iTunes can be regarded as the driver and management platform between the products of Apple and personal computer. It's developed by Apple and free to download and install. It has the function of full audio and video player, synchronization, backup, burn, share, and browse the App Store. For iPhone synchronization and backup support, it includes music, videos, photos, applications, contacts, to act calendars and e-mail accounts, and bookmarks, etc. And the backup file of the different operating system will store in different paths [11], compiled in Table 1.

Table 1. The path of iTunes backup file

Operating system	File path
Mac	~/User/Library/Application Support/MobileSync/Backup/
Windows XP	\Documents and Settings\（User name）\Application Data\Apple Computer \MobileSync\Backup\
Windows Vista, Windows 7	\User\（User name）\App Data\ Roaming\AppleComputer\MobileSync \Backup\

"Backup" folder memory placed a combination of hexadecimal numbers and characters (0-9 and a, f), length of 40 characters of the name of the folder. The HASH code is a special encoding given by iTunes through SHA-1. In this folder are also stored the file names of identification, which are also given a special 40-character by SHA-1. These files are backup files of Apple iTunes copied from internal memory of iPhone [9], as shown in Fig. 1.

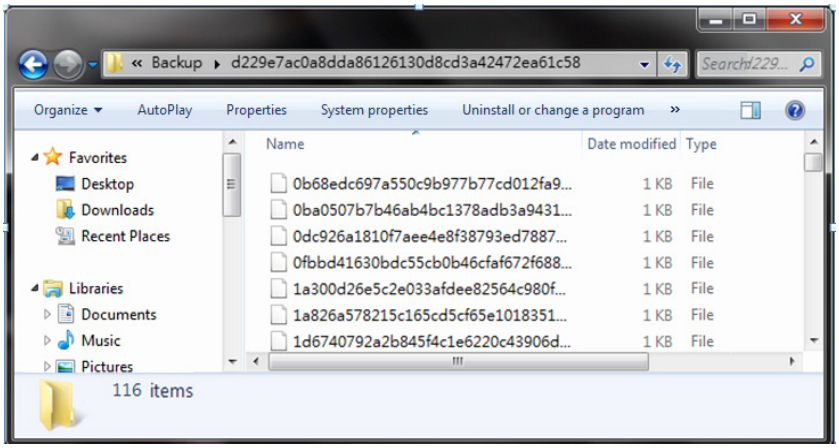

Fig. 1. The backup files generated by iTunes

These backup files are in two different file formats for data storage formats: plist and SQLite. Two different file formats can be browsed by the software tool. And the backup mechanism of iTunes is comparison backup. iTunes compares the data of the backup file with the data of the iPhone. If the same is skipped; coverage if the contents of the backup file has been modified; create a new backup file if new data is created; finds that the data has been deleted, the backup files are also just delete. Therefore, the extraction of digital evidence through this method is called logical extraction.

3 Jailbreak Forensic Experiments

Because the method of iPhone digital forensics is restricted by its protection mechanisms of the iOS operating system. Therefore, when execute the digital forensics, we will face the problem of whether the Jailbreak should executed or not. Besides, there are two kinds of the iPhone evidence, which offenders used found in the process of searching or arresting. One is “non-Jailbroken”, and the other is “Jailbroken”. Therefore, we will focus on these two states of the implementation of digital forensic extraction of iPhone, non-Jailbroken and Jailbroken, and compare the evidence and the output report from these two states. Also, we discuss the need that whether the iPhone evidence should perform the Jailbreak to provide a reference in the practice of forensic personnel and look forward to do the basis of discretion for the court trial.

We will conduct in-depth study through two kinds of iPhone digital forensics. First of all, we will try to use Mobile Forensic Software XRY as the measuring tool. XRY designed by Micro Systemation Company is a forensic tool specifically for mobile devices. It can support more than 4,000 different kinds of traditional mobile phones, smart phones, GPS devices, SIM cards and tablet PCs to conduct in-depth digital forensic extraction and analysis. XRY , a complete forensic toolkit , is not only for the software part also contains the complete connect the phone line group, the XRY communication unit, the SIM card reader, SIM card, copy the sample card and write-protected memory card reader. The report of XRY is encryptable, and its file extension is “.xry”. In the level of support of smartphone, XRY supports Android, Black Berry, iPhone, Symbian and the Windows Mobile. The latest version of XRY can also focus on various types of digital forensics for mobile applications. Because XRY has a more complete scale of hardware and software support, and more Practice authorities and schools the choice of cell phone forensic software tools. Therefore, if we can explore the level of support of digital forensics for non-Jailbroken and Jailbroken iPhone by using this set of software tools. We will have more reference value to forensic personnel. Besides, we will use Apple's official application, Apple iTunes, to perform a file backup of the iPhone. And observe the status of the backup files of non-Jailbroken and Jailbroken iPhone through the extraction and analysis of the backup file. We also try to analyze the degree of influence and the change of Jailbreak procedure for this logic extraction, and provide the reference for forensic personnel using this method to execute the implementation of digital forensic extraction of the iPhone.

3.1 Environment

In the setting of this experiment, we will use the most popular iPhone 4 as an experimental subject matter. iOS version of the experiment is the latest version 5.1.0 and modem firmware version 04.11.08. In order to get the most simple and most interference-free experimental data, we will reset the iPhone 4 to factory settings, and use the default SIM card to retain all the settings to show the most primitive state. In the part of computer, we use the PC has Windows 7 operating system and version 6.1.1 XRY installed. Besides, we also complete the establishment of version 10.6 Apple iTunes. When executing the implementation of digital forensic extraction of XRY, we will use the special adapter provided by XRY linking the iPhone, the PC and the dongle key to complete the pre-setting of the implementation of digital forensic extraction.

3.2 Operational Processes

We will follow the pre-planning operation flow chart to execute the implementation of digital forensic extraction of non-Jailbroken and Jailbroken iPhone. The detail is shown in Fig. 2.

In accordance with the flowchart of operation, we will have these following steps: Predefinition, Acquisition before Jailbreak, Jailbreak-in-Progress and Acquisition after Jailbreak.

Advance preparation. In order to store the corresponding data within the iPhone, so that we can actually extract the data we stored in the extraction process, we will pre-set a group of internal data within the iPhone including: contact information, call logs, SMS, calendar events, memos, E-mail accounts, bookmarks, web browsing history, the virtual keyboard input record, geographic information records, pictures and music, and more information. Among them, the part of the record of the call, SMS, calendar events and memos, we deliberately enter as two pieces of information, and delete one of them, to test the degree of extraction of deleted information. In addition, in order to make the default data with the network connection records, we use the SIM card 3G network and Wi-Fi network in the laboratory as a network connection.

Acquisition before Jailbreak. After setting default data, we will focus on the implementation of digital forensic extraction of non-Jailbroken and Jailbroken iPhone. The first is XRY tool for physical and logical extraction. We link the iPhone and the PC by the provided XRY adapter, and use XRY software to execute the

implementation of digital forensic extraction. In the physical extraction part, we find that XRY cannot execute physical extraction in this current state of the iPhone. In the logical extraction part, we should only need to follow the instructions of the XRY operating interface, and then we can complete the implementation of digital forensic extraction. We store the result of extraction file named "Non-JB.xry"

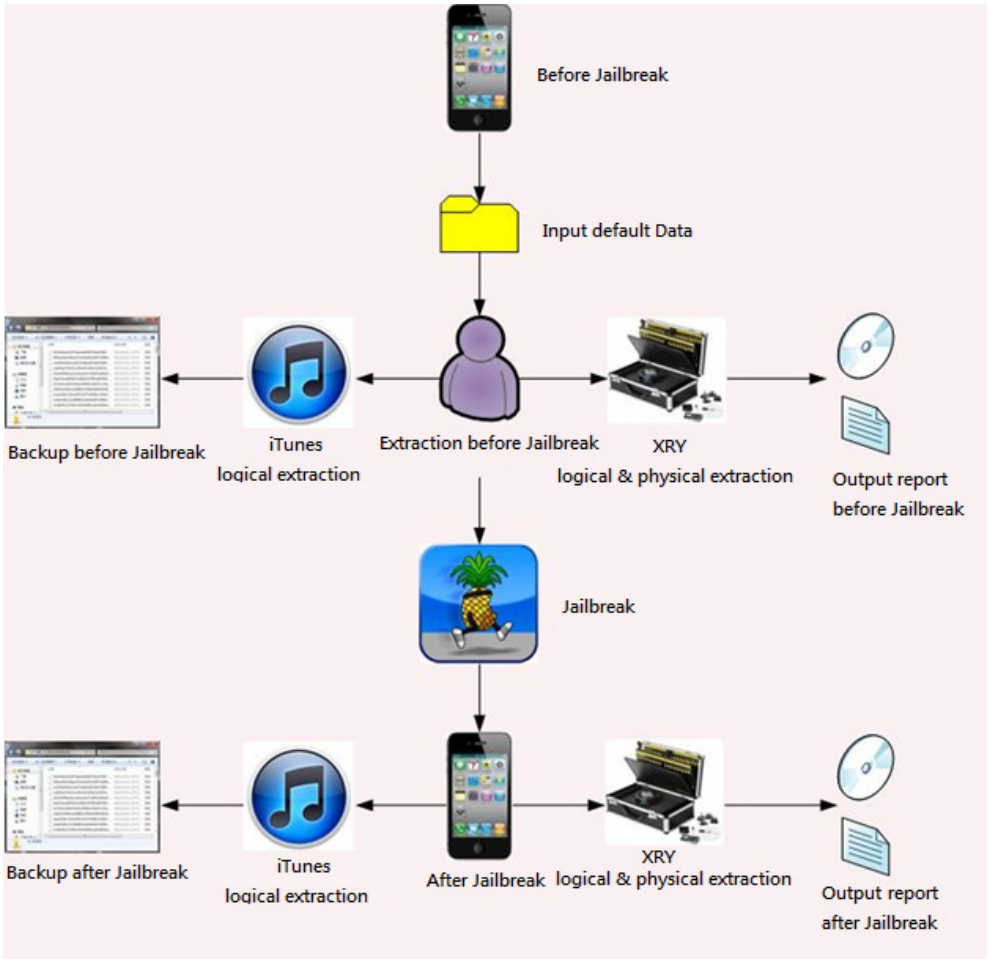

Fig. 2. Operation flowchart

Second, we use Apple's iTunes backup mechanism to enforce the logical extraction. The default setting of Apple iTunes is that when the iPhone links to the computer, the PC will automatically open Apple iTunes, and automatically performs the synchronization and backup. Therefore, all we need is to link the iPhone and the PC, and then we can complete the backup. In addition, we open the "Backup" file in the backup file path, copy the file inside and store the file we copied in the pre-new file named "Non-JB".

Jailbreak-in-Progress. After the extraction of non-Jailbroken is completed, we are going to execute the iPhone Jailbreak procedure. Before the program is executed, we deliberately do not restore the iPhone to factory settings. This act is to simulate the state that the forensic personnel acquiring the iPhone evidence at the scene then executing Jailbreak procedure. Therefore, there are still retaining the default information we set within the iPhone. Due to the same time we executing this experiment , coincides with the iOS version updated to version 5.1.0, so the latest tools redsn0w Jailbreak software version 0.9.10b6c version, in the meantime can only be semi-perfect Jailbreak to iOS 5.1.0 version. This means that every time the iPhone reboot, the iPhone will need to link the computer and re-run the Jailbreak, but this state for this experiment does not have any impact. Therefore, we will accord the instructions of the redsn0w tool to complete Jailbreak procedure.

Acquisition after Jailbreak. After Jailbreak, we start to execute digital extraction of the iPhone. Likewise, we first execute entity extraction and logical extraction by using XRY. The iPhone linked to a computer through XRY provided dedicated adapter for the extraction work. In entity extraction part, we found that the iPhone, after Jailbreak, is still unable to entity extraction. And the logical part of the extraction, the same only in

accordance with the instructions of the XRY operation interface, namely complete logic extraction. Extraction results file name “JB.xry”.

Secondly, we also execute logical extraction of Apple iTunes backup mechanism. In order to ensure the accuracy of the backup, we advance the implementation of the delete existing backup action. We first open the Apple iTunes manually and switch to the device page in the Preferences section. Before Jailbreak is executed once the backup program is executed, so we will see the screen shown in Fig. 3, the backup data is already exist. We tap delete the backup after highlight the backup, and after Apple iTunes close to complete the deletion. Then we will be like the previous extraction iPhone, linked to the PC, the Apple iTunes automatically perform synchronization and backup. Then open the “backup” folder, copy the folder inside and save in the pre-new folder, named “JB”.

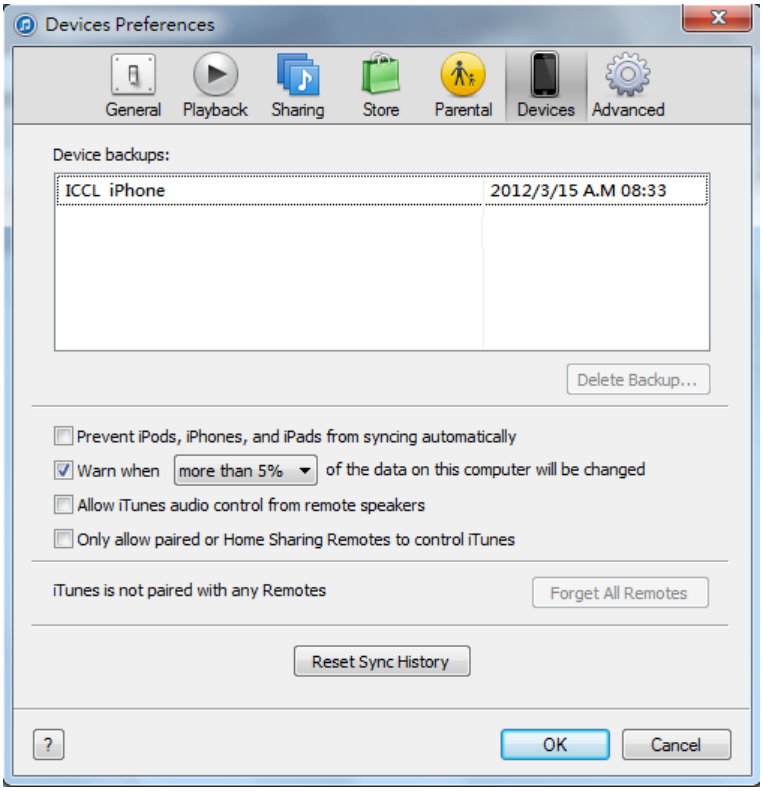

Fig. 3. The already exists backup file

4 Analyses and Discussions

The experimental results will be divided into three parts. The first and the second are the physical acquisition and logical acquisition results by using the XRY forensic commercial tool kit. The third one is the logical acquisition result by Apple iTunes backup mechanism. The following is our analysis and discussion.

4.1. XRY Reports

Physical Acquisition. In the part of the physical acquisition by using XRY forensic commercial tool kit, we find that the iPhone states of non-Jailbroken and Jailbroken are all unable to be performed the physical acquisition by using XRY version 6.1.1 which we used at the time of the experiment. However, recently Micro Systemation released an updated software of XRY version 6.2 while this paper is written stage. This newer version is advertised can perform the physical acquisition and physical decoding for iOS version 4.3 and 5.1. But if we want to perform the new functions above-mentioned, we need to verify the serial number and update the dongle key to Micro Systemation. The process will need to take some time to wait for. Therefore, the physical acquisition result of the latest XRY version is not discussed in this paper. But according to Fig. 4, we can see that the latest XRY version supports the status of the iPhone physical acquisition.

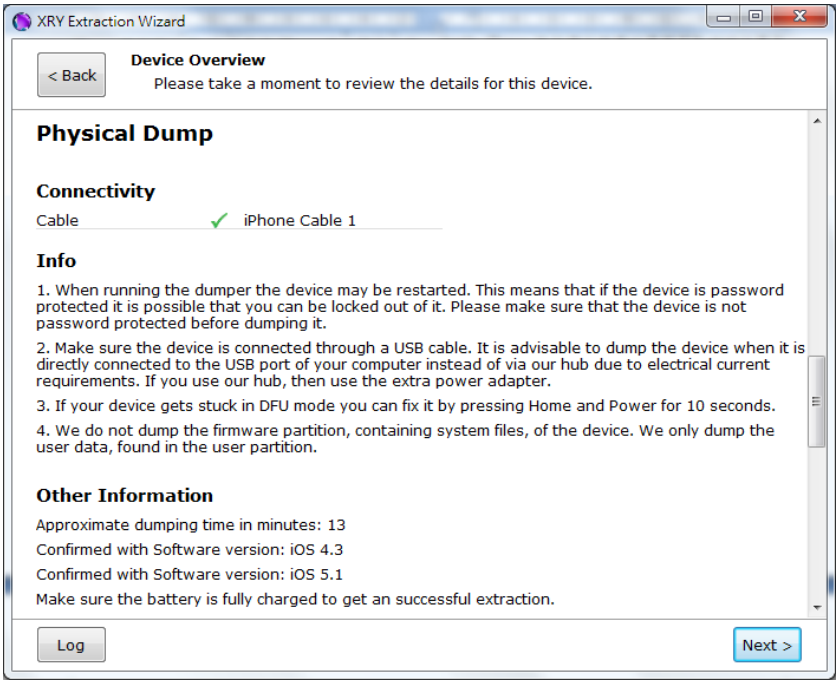

Fig. 4. The XRY version 6.2 supports the status of the iPhone physical acquisition

Logical Acquisition. In the part of the logical acquisition result by using XRY's forensic commercial tool kit, we have generalized the iPhone logical acquisition states of non-Jailbroken and Jailbroken by observing and recording the two acquisition files, as shown in Table 2. Among them, the category of the home directory and subdirectories is the default classification method of acquisition results in accordance with XRY. The following "JB" in Table 2 is the abbreviation of "Jailbreak".

Table 2. The XRY logical acquisition result juxtaposes in the states of non-Jailbroken and Jailbroken

Items		Non-JB	JB
File Name		Non-JB.xry	JB.xry
File Size		15.4MB	1.55GB
Execution Time		20 sec	23 min
Home directory	Sub-directories	Non-JB	JB
Device	General Information	1	1
	Network Information	None	3
	App Usage	None	12
	Keyboard Cache	2	2
	Accounts	1	1
Contacts	N/A	1	1
Calls	N/A	2	2
Calendar	Calendar Events	1	1
	Notes	2	2
Messages	SMS	2	2
	Emails	None	50
Locations	History	1	609
Web	History	2	2
	Bookmarks	1	1
Files	Pictures	5	3776
	Audio	None	112
	Documents	78	14536
	Archives	None	60
	Unrecognized	51	11207

Compared with “Non-JB.xry”, there are extra items in “JB.xry”, such as Network Information, App Usage, Emails, Audio, and Archives. The dissimilar items between “Non-JB.xry” and “JB.xry” in addition to the basic states of File Name, File Size, and Execution Time, including Locations / History, Pictures, Documents, and Unrecognized.

The extra items in “JB.xry” are described as follows. In Network Information, there are listed the information of the two types internet card interface build-in iPhone, which are 3G and Wi-Fi. The detail is shown in Fig. 5.

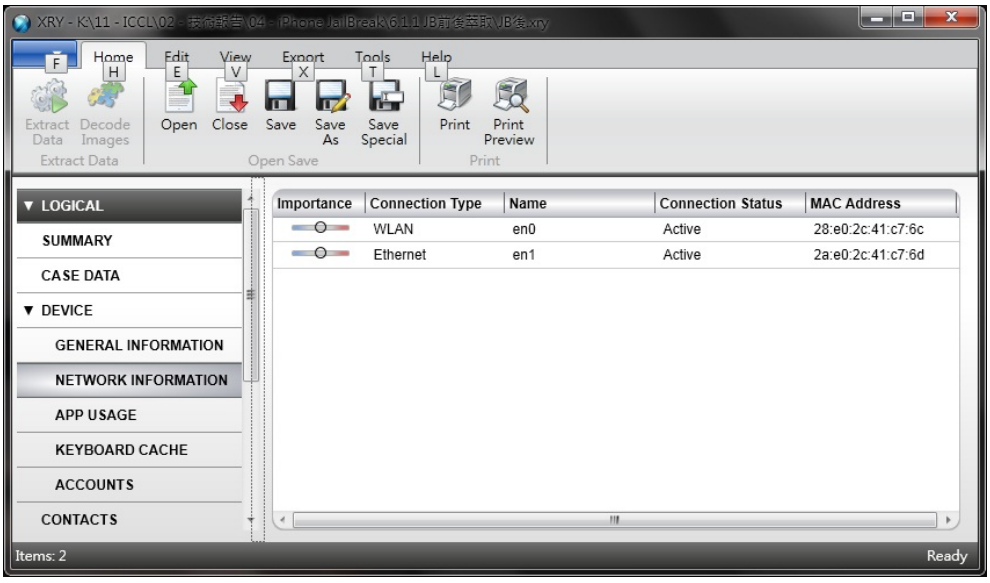

Fig. 5. The extra item: Network Information, extract from the state of Jailbroken iPhone

In App Usage, there are listed the usage count, the last use time, and duration of each the application build in iPhone and installed by users. The detail is shown in Fig. 6.

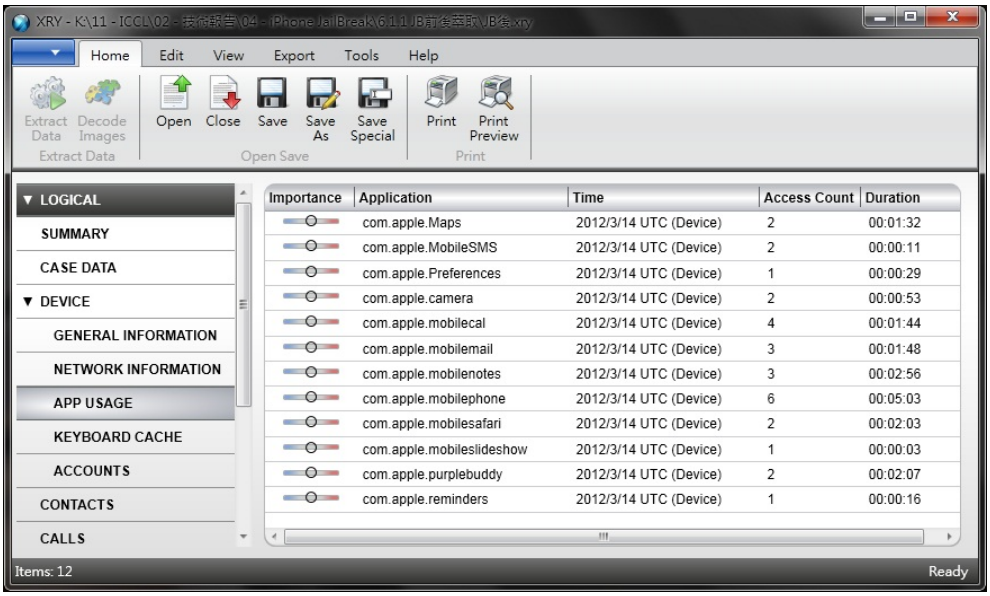

Fig. 6. The extra item: App Usage, extract from the state of Jailbroken iPhone

In Emails, there are listed full emails information downloaded in the iPhone from the email server which has been synchronized to the iPhone. The default servers provided to synchronized to the iPhone are including iCloud, Microsoft Exchange, Gmail, Yahoo, Aol, Microsoft Hotmail, Mobile me, and Other option. Users can choose to use and set. The mechanism of the iPhone synchronization is default set to download the first 50 full content emails at most to iPhone from the synchronized email server. The email information contains sender, recipient, CC address, BCC address, subject, body, send and receive time, and attachments. Because the listed

information is very complete and detailed, it can be one of the key pieces of digital evidence when the forensic investigator performs the extraction. Fig. 7 shows the details of Emails.

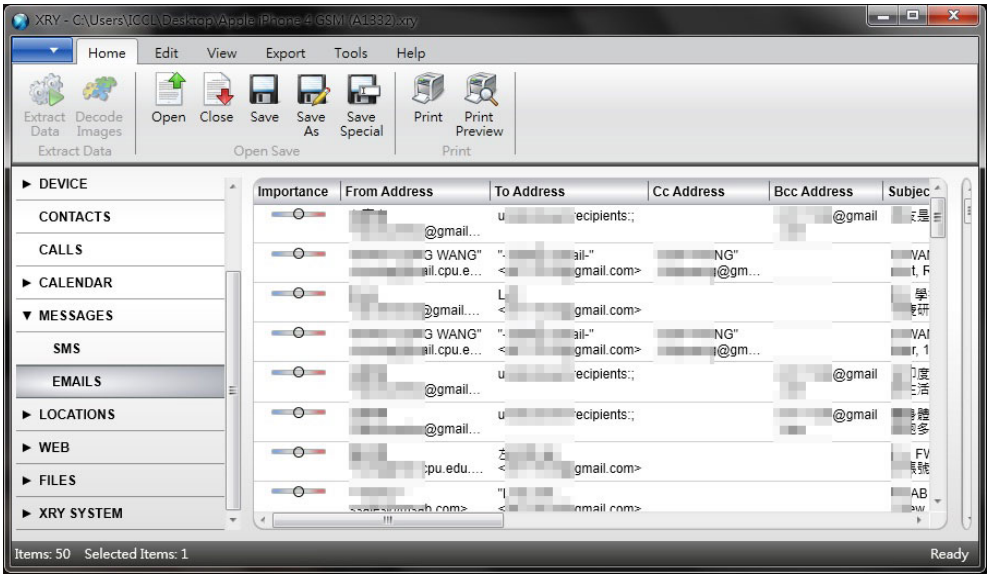

Fig. 7. The extra item: Emails, extract from the state of Jailbroken iPhone

In Audio, there is not only listed the music which we pre-synchronized to iPhone via Apple iTunes, but also the other system default 111 music and rings. The 111 music and rings are scattered in the path of / System / Library /..., / System / Library / Audio /..., and / private / var / stash / Library / Ringtones /.... The detail is shown in Fig. 8.

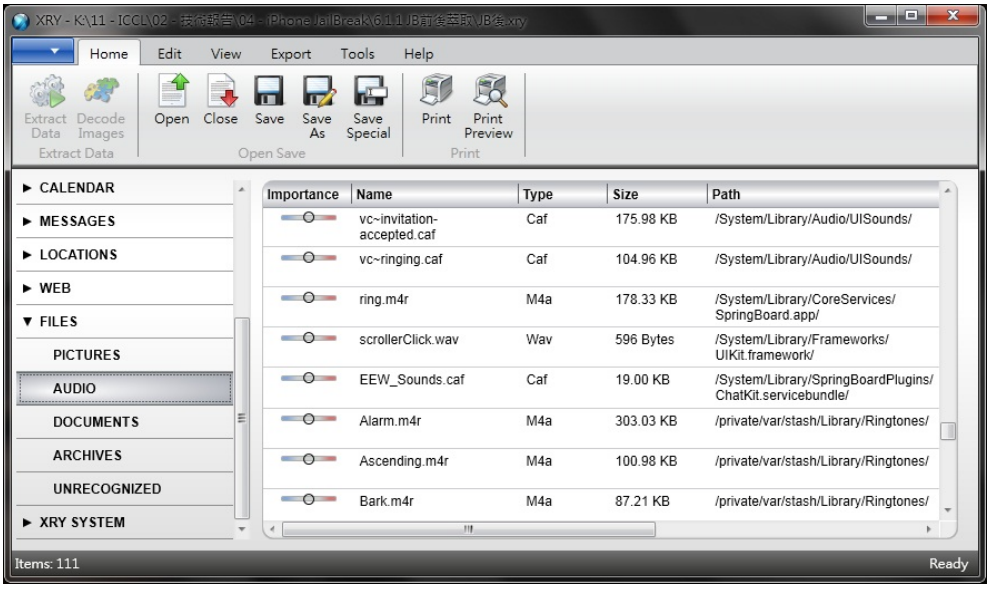

Fig. 8. The extra item: Audio, extract from the state of Jailbroken iPhone

In Archives, there are listed the system creation and modification files information, including creation and modification date, file type, file name, storage path, and file size. The detail is shown in Fig. 9.

The dissimilar items between “Non-JB.xry” and “JB.xry” are described as follows. We can easily observe the difference of the basic states between non-Jailbroken and Jailbroken via the execution time of two extractions and the size of two generated files. In the Jailbroken state, the execution time of extraction and the size of the generated file compared to the non-Jailbroken state are improved significantly. Reason for the variation we can easily know from the extraction content of Jailbroken as the following.

In the state of Locations / History, there is only one record shown in the “Non-JB.xry”. This record is Google Map location information that we key in when predefinition. However, in the “JB.xry”, there are not only GSM

and Wi-Fi location records which are automatically generated by iPhone, but also the above-mentioned Google Map location information. The Locations / History details of "JB.xry" are shown in Fig. 10.

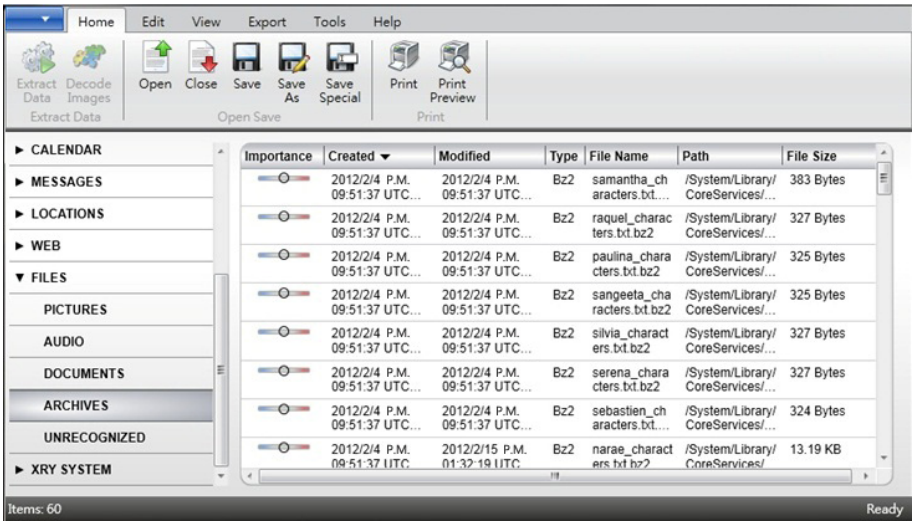

Fig. 9. The extra item: Archives, extract from the state of Jailbroken iPhone

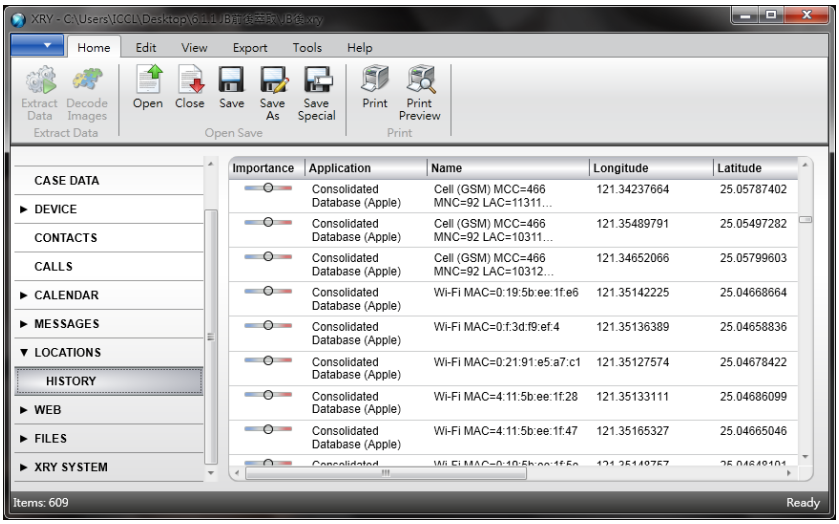

Fig. 10. The GSM and Wi-Fi location records can be found in "JB.xry"

In Pictures, iPhone is default to automatically generated thumbnail of the background image in user interface and the other non-default image of the system. The photograph taken through the built-in lens and the cover image of the music which pre-synchronized to iPhone have automatically generated thumbnails by iPhone itself when predefinition. Therefore, we can find 5 images in the Pictures item of the "Non-JB.xry", such as the thumbnail of the background image, the photograph and its thumbnail taken through the built-in lens, and the cover image and its thumbnail of the music which pre-synchronized to iPhone, as shown in Fig. 11.

Therefore, there are not only the 5 images the above-mentioned, but also extra 3,771 system images and thumbnails in the Pictures item of the "JB.xry". If the forensic investigators want to extract the digital evidence about the image file from the Pictures of the "JB.xry", they must exclude the 3,771 system images at first to obtain the valuable digital image evidence. Thence, compared with the state of non-Jailbroken, searching of the digital image evidence will be more difficult in the state of Jailbroken. The Pictures item of the "JB.xry" is shown in Fig. 12.

In Document and Unrecognized, these two items of the "Non-JB.xry" just list the files under the storage path / private / var /….

In Documents and Unrecognized part, the data in 「Non-JB.xry」 is only extracted through the path /private/var/…, but the data in 「JB.xry」 is including the data through the path /System/Library/…, /private/var/… and other system path. Therefore, if forensic officers search the part of Documents and Unrec-

ognized after JB, they will also face the problem like Picture, need to filter a large amount of system information. Fig. 13 is the state of Documents after JB.

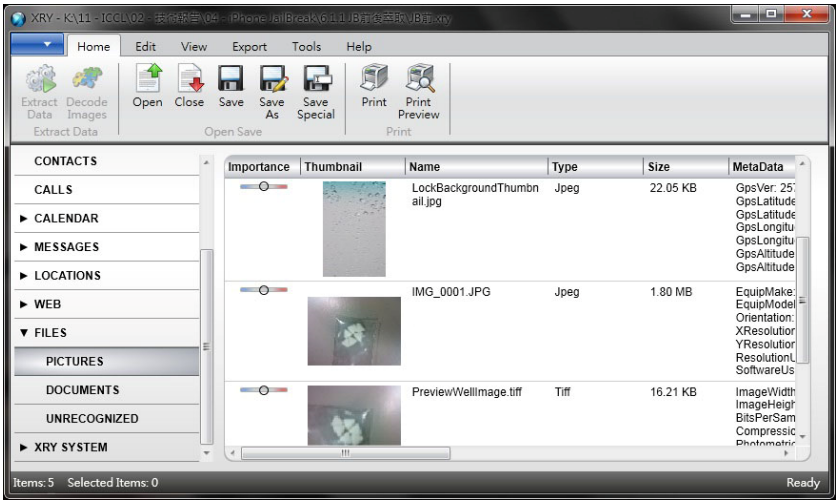

Fig. 11. The 5 images found in the Pictures item of the "Non-JB.xry"

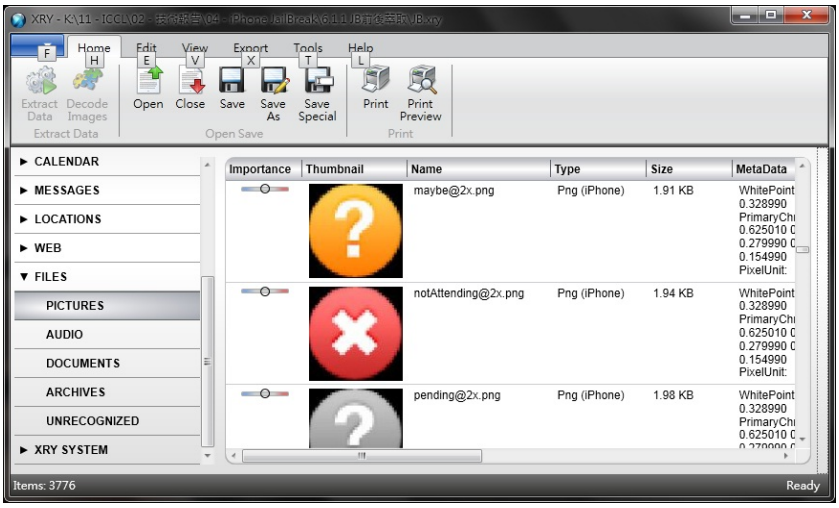

Fig. 12. The 3,771 system images can be found in the Pictures item of the "JB.xry"

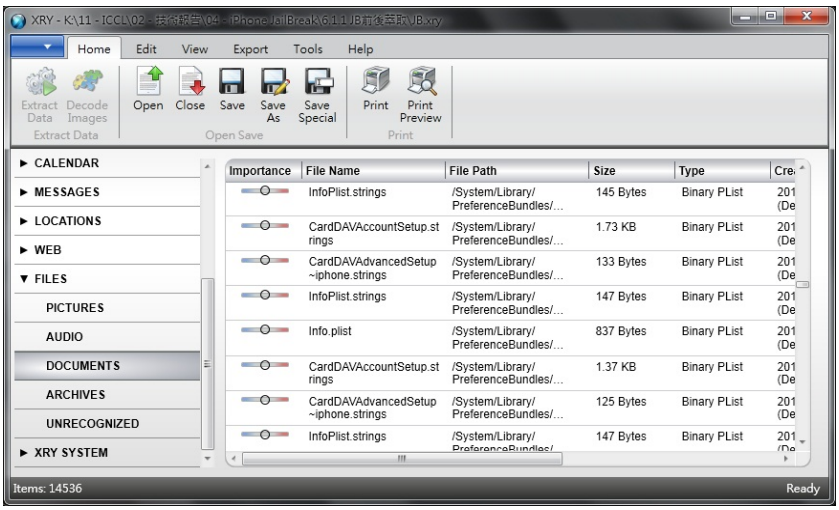

Fig. 13. The Documents item records in the state After Jailbreak

After observing the new and transacted item, we view the part of call logs, text messages, calendar events, and memorandum for the information we deliberately add 2 and delete one. We found that in the part of call logs, text messages, and memorandum, the extraction of "Non-JB.xry" and "JB.xry" can both show the data deleted. But in the part of calendar events can not show it. The information of call logs extracted before Jailbreak, as shown in Fig. 14.

In the other part of the same result of item extracted through "Non-JB.xry" and "JB.xry", we also compare it one by one. After comparison, we can confirm that the data extracted from the same item have consistency.

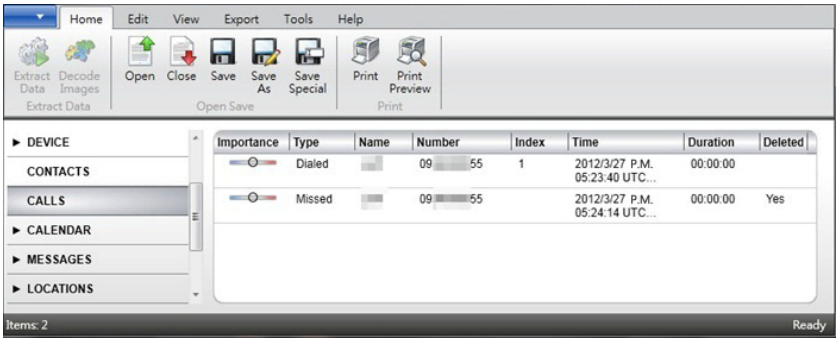

Fig. 14. Call records extracted before Jailbreak

4.2. Apple iTunes Backup

We have special discovery when using Apple iTunes backup to execute logical extraction before/after Jailbreak for iPhone. We compare the backup file Jailbreak and non-Jailbroken. We found that the number of data of backup file extracted from these two states are both 114.

For confirming the differences of the data of backup file before/after Jailbreak, we compare every data for name and the size. The result found that, the data name and size of each 114 data of two files "Before Jailbreak" and "After Jailbreak" are the same. As the result, we can believe that the mobile phone digital forensic extraction way using Apple iTunes backup files for logical extraction, will not be effected by executing Jailbreak. The backup files extracted before/after Jailbreak, as shown in Fig. 15 and Fig. 16.

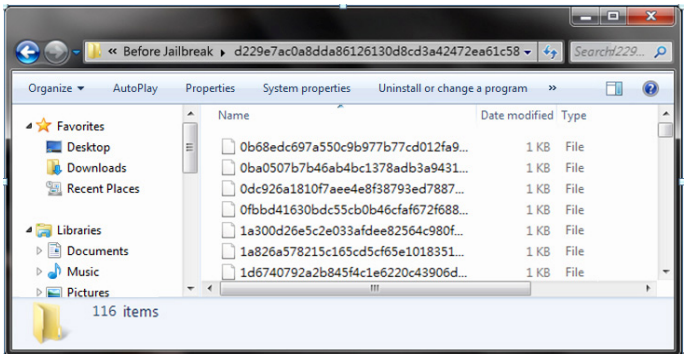

Fig. 15. Backup file extracted before Jailbreak

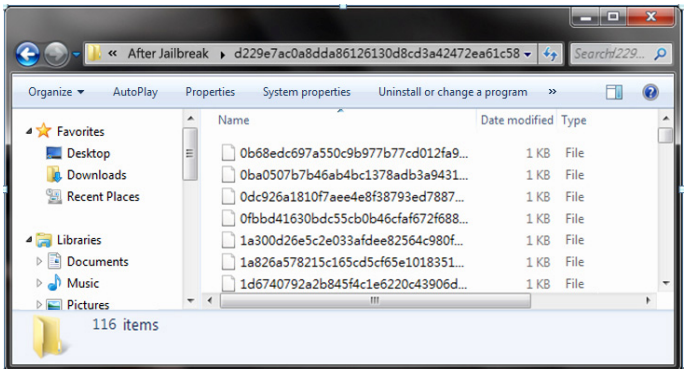

Fig. 16. Backup file extracted after Jailbreak

4.3. Discussions

In this examination, we both use the forensic tool XRY and Apple iTunes to execute the extraction of digital forensics. The comparison is shown in Table 3.

Table 3. The comparison before and after Jailbreak by two extraction methods

Jailbreak status / Extraction method	Before Jailbreak	After Jailbreak
XRY	Fewer media and files are extracted.	More data are extracted such as system images, documents, item records, call logs and e-mail records.
iTunes backup files	All the media, records and files leave unchanged.	All the media, records and files leave unchanged.

For the level of support of XRY for iPhone, in version 6.1.1, we cannot execute entity extraction whether Jailbreak or not. In the part of logical extraction, we can discuss for three oriented for presenting the critical digital forensic evidence for Jailbreak and non-Jailbroken. First, for the same item, whether Jailbreak or not, we found that it can completely show the information of call logs, message, calendar and memos that have been deleted. Besides, comparing the evidences of these items, we can also found Jailbreak procedure will not affect these items for showing the information of digital forensic evidence. Therefore, Jailbreak procedure will not change these items.

Secondly, for the items that only can be extracted after Jailbreak, the part of Network Information, Emails and Audio has critical digital forensic evidence value. Through the data of Network Information, we can realize the internet card number of iPhones used by criminals, and further investigate the connection records of this card. It's worth mentioning, in the part of Emails, because iPhone will automatically download and synchronize the top 50 e-mails from the e-mail sever which is synchronized. It is different from directly connecting through a Web link to the mail server to read the letter. Therefore, there are 50 complete e-mail records in the iPhone. And after Jailbreak, it could be shown by XRY extraction. It's very critical digital evidence. Now if criminals only use e-mail for pipeline to communicate and contact, when forensic officers execute digital forensic extraction for non-Jailbroken iPhone of criminals, they will find nothing strange. However, if forensic officers try to Jailbreak the iPhone and extract it again, they could possibly extract the evidence of e-mails and further help the project. But, though the item Audio is as valuable as the other critical digital evidence, user's music and other sounds, which are synchronized by Apple iTunes, will also store in the same Audio file as other system music. So, forensic officers will pre-empting the system music when searching.

Last, for the changing items before/after Jailbreak, all digital evidence, which can be extracted before Jailbreak, can also be extracted after Jailbreak, and still have consistency. In the part of changing items, Locations/ History and Pictures also have the value for being critical digital forensic evidence. In particular, Locations / History can only show one default information of location before Jailbreak, but after Jailbreak, the information can show more GSM and Wi-Fi records. And we can easily realize the movement trajectory of criminals through these records. We can also do the two-way comparisons with other evidence. Otherwise, for the evidence of Pictures, forensic officers can possibly extract the pictures directly/indirectly connected to the crime for evidence.

In fact, we can discover that, if iPhone already executed Jailbreak, the 5 contents under the main Files: Pictures, Audio, Documents, Archives and Unrecognized will all create large data including from user and system. This is a thorny problem for forensic officers when extracting. Not only for the long time it takes, but also for the difficulties when processing this large data.

According to the above analysis, whether Jailbreak will have effect on the critical digital evidences can be clarified after this examination. After our examination, we can consider that Jailbreak procedure will not change the evidences of iPhone mobile digital forensics. And it can help forensic officers extract more critical digital evidence.

5 Conclusions

Because of the uniqueness of the iPhone, iPhones have become more and more popular. But it also means that there are more criminals that use iPhone as a tool for committing a crime. However, due to the protection mechanism of iPhone, forensic officers will face Jailbreak and non-Jailbroken two states of iPhone for evidence. It's

easier to execute digital extraction for a Jailbreak iPhone. But it will be a difficult problem for non-Jailbroken iPhone. Directly Jailbreaking the iPhone is one of the methods that can be used, but it may also bring many problems for the transaction dispute. Through our examination, we execute logical extraction by XRY tool and Apple iTunes backup file. We successfully aggregate the effect of Jailbreak procedure. And clarify the controversy part of digital evidence. As the examination result, under our research environment, Jailbreak is an acceptable pre-processing procedure for iPhone digital forensics. This procedure will not change the internal digital evidences of iPhone. Instead, it can provide forensic officers more valuable digital evidence. This paper focuses on the extraction through the official backup service. The version update of official backup service would preserve the main process and similar form of backup files. Thus the valuable point of view we offered leaves unchanged even on newer version of iOS or forensic tools. We expect that this paper can be provided for consultation of legality and the reporting of digital forensics.

Acknowledgement

This research was partially supported by the National Science Council of the Republic of China under the Grant NSC 100-2221-E-015-001-MY2-, NSC 102-2221-E-015-001-, and MOST 103-2221-E-015-002-.

References

[1] A. Levinson, B. Stackpole, D. Johnson, "Third Party Application Forensics on Apple Mobile Devices," in *Proceedings of 44th Hawaii International Conference on System Sciences (HICSS)*, IEEE Press, pp. 1-9, 2011.

[2] S. Azadegan, W. Yu, H. Liu, M. Sistani, S. Acharya, "Novel Anti-forensics Approaches for Smart Phones," in *Proceedings of 45th Hawaii International Conference on System Sciences (HICSS)*, pp. 5424-5431, 2012.

[3] M. Bader, I. Baggili, "iPhone 3GS Forensics: Logical Analysis Using Apple iTunes Backup Utility," *Small Scale Digital Device Forensics Journal*, Vol. 4, No. 1, pp. 1-15, 2010.

[4] A. Di Stefano, A. Grillo, A. Lentini, G. Me, D. Tulimiero, "Mobile Forensics Data Integrity Assessment by Event Monitoring," *Digital Investigation*, Vol. 4, No. 1, 2010.

[5] A. Hoog and K. Gaffaney, iPhone Forensics White Paper, 2009.

[6] G. M. Luis and A. M. Joan, "Universal, Fast Method for iPad Forensic Imaging via USB Adapter," in *Proceedings of Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, IEEE Press, pp. 200-207, 2011.

[7] C. Yates, L. Ray, J. Yang, "An Investigation into iPod Touch Generation 2," in *Proceedings of the 2011 Information Security Curriculum Development Conference*, pp. 94-98, 2011.

[8] J. Zdziarski, *iPhone Forensics*, 1st ed., O'Reilly Media, Chap. 4, 2008, pp.43-64.

[9] A. Crosby, *iPhone forensics, sans iPhone*, 2010 (available online at http://www.slideshare.net/hrgeeks/iphone-forensics-without-the-iphone).

[10] D. Kravets, "Jailbreaking iPhone Legal, U.S. Government Says," ABC News, 2010 (available online at http://abcnews.go.com/Technology/us-government-Jailbreaking-iphone-legal/story?id=11254253).

[11] iOS: Back up and Restore Your iOS Device with iCloud or iTunes (available online at http://support.apple.com/kb/HT1766?viewlocale=zh_TW).

[12] Micro Systemation XRY (available online at http://www.msab.com/).