Design and Implementation of Digital Forensic Software for iPhone

Chung-Nan Chen
Graduate Institute of Information and Computer Education
National Kaohsiung Normal University
Kaohsiung, Taiwan
r0941703960@yahoo.com.tw

Raylin Tso
Department of Computer Science
National Chengchi University
Taipei, Taiwan
raylin@cs.nccu.edu.tw

Chung-Huang Yang
Graduate Institute of Information and Computer Education
National Kaohsiung Normal University
Kaohsiung, Taiwan
chyang@nknucc.nknu.edu.tw

***Abstract*—IPhone, which is equipped with the iOS operating system has become one of the most popular smart phones since its release in June, 2007; with its popularity and extensive use, it has certainly become the microcomputer that is necessary in our daily lives. However, the increasing trend of safety and criminal issues has made the development of iPhone forensics become a must. Because of the gradual development and the increasing attention it receives, it's required to develop forensic software. The aim of the research is to develop and implement Mac operating system forensic software towards iOS system which uses Objective-C and Shell Script.**

We conduct logical acquisition through the forensic program combined with open source device--libimobiledevice <short for libiphone > to conduct logical collection on the device. to extract phone calls, text messages, photos, contact list, web browsing information, SIM card information, memos, etc; use the characteristic of SQLite to recover old and deleted data to assist the investigators to conduct the acquisition and analysis of digital evidence.

Keywords—iPhone; iOS; libimobiledevice; Mobile forensics; Digital evidence

I. INTRODUCTION

With the continuing releases and development of mobile devices, smart phones have become the necessary devices in human's lives, Due to people's dependence and fondness, the functions of smart phones have to evolve towards more convenience and being smarter. Aside from the traditional audio communication and texting, it equips the functions of internet, GPS, digital cameras, multi-media as well and it also provides higher volume of storage space and diverse apps. Therefore cell phones have become enormous personal database. As a result, the development of forensic program system of smart phones has become the necessary trend of the development of digital forensic technology.

Since its release, iPhone has dominated the market of cell phones. According to the latest research of Gartner organization, the sales amount of the fourth quarter of 2011 has surpassed Samsung and LG and taken the third place in the cell phone market share [7]. It has still remained in the first three places till the third quarter in 2012; the amount of download of applications of Apple Store has grown from 3 billion to 10 billion from January 2010 till now [1]. This shows that iPhone plays a crucial role in smart phones. The study uses Objective-C as the developing device and uses the National Institute of Standards and Technology to design and implement smart phones forensic program system of iOS platform [9], to help forensic investigators to retrieve crucial information from cell phones via simple installation and operating procedures, and to offer digital evidence related collection investigation and analysis report.

II. IOS FORENSICS

The research emphasizes on data collection in smart phones on iOS platform, conducting the development and design of mobile forensics and computer forensics program system and doing literature review based on the related terms needed in the research.

A. iOS operating system

iOS is an operating system developed towards smart device by Apple Inc, just like Mac OS X operating system, which s based on Darwin-a kind of Unix-core open source operating system. iOS system consists of four layers: the Cocoa Touch layer, the Media layer, the Core Services layer and the Core OS layer and the system takes nearly one GB memory stick volume [10].

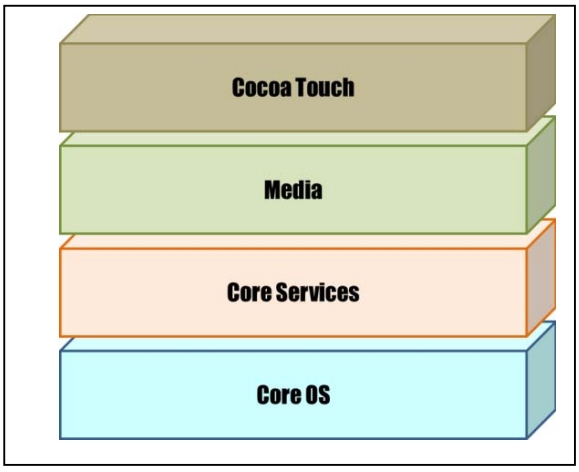

Fig. 1. Layers of iOS.

978-0-7695-5075-6/13 $26.00 © 2013 IEEE
DOI 10.1109/ASIAJCIS.2013.21

B. Mobile phone forensics

The data in mobile phones are basically electronic record. As long as mobile phones are processed by acceptable means-that is digital forensics. Digital forensics investigates digital evidence, the data extracted from mobile phones, which includes phone calls, text messages, phone logs, media files, browsing record, GPS and e-mail.

According to NIST, mobile phone forensic procedures can be divided into four phases: Preservation, Acquisition, Examination and Analysis and Reporting [9].

Preservation: to ensure to identify or search for possible existing digital evidence storage devices. Because of the quality of being invisible, digital evidence is prone to be damaged during processing or compromised while extracting. To avoid effecting the ability of digital evidence to testify, we have to keep digital evidence in its original form with extreme care.

Acquisition: to extract digital data from digital devices via reading database files or through image.

Examination and Analysis: Examination: to reveal the collected data, including the concealed and deleted files. Analysis: to quantify or combine the collected digital evidence with the highly related evidence.

Represent: the analysis of digital evidence in a clear and plain manner, just like report.

C. Digital evidence

Digital evidence is also known as electronic evidence or electronic information, which is stored or transmitted in digital form and is admissible in court [2].

Digital evidence is a kind of concrete material but can't be perceived by our senses. It must be read, analyzed or revealed by the use of electronic equipment to make the data form be readable visually. Unlike the usual physical evidence, digital evidence is abstract and is stored in binary condition in electronic devices. It has the following characteristics: being hard to extract and preserve, hard to be proven its integrity and sources, hard to establish the connection, impossible to be directly perceived and understood its content, easily be compromised, copied and erased.

While conducting digital investigation, we have to keep the original evidence from being changed or damaged and prove that the collected data can be traced back to the impounded evidence. We can cause the evidence to be changed or damaged while analyzing it.

D. iPhone digital evidence processing

When iPhones or other iOS devices are being impounded or confiscated as evidence, we should take some precautious measures to prevent the data from being overridden.

The sequences of these measures will be dependent on the status of the devices at that moment.

If the device is turned off, we need to keep it that way. Turning the device back on might risk the data being overridden. If the device is turned on, we have to keep an eye on whether it's password protected and the version of the operating firmware in the cell phone.

Be sure to recharge the device. If the device is turned off, we need to notice that recharging might turn the cell phones on. Under this circumstance, we can reset the device to restore mode or DFU mode to conduct the processing [3].

E. Strings dump

Strings dump is the last resort to extracting data from the native disk image. Strings can be extracted from the device and stored as files. The output of Strings dump is enormous but it can conduct loose search towards specific data. To extract strings from the native disk image, we must operate in accordance with Mac or Windows operating system.

Mac OSX system: strings tool is one of the standard Unix tools in Mac OSX, so we only need to give command from the terminal.

Windows system: download Strings V2.5 from Microsoft website (http://technet.microsoft.com/en-us/sysinternals/bb897439.aspx) to download the tools of Strings. By doing so, we can command from the command prompt [6].

F. The range of iOS database

We can use the corresponding tools to check its catalogue and content in the database to acquire the forensic targeted data [4]. Table 1 consists of iOS database catalogue, types and the devices used to examine the data.

TABLE I. IOS DATABASE CATALOGUE, TYPES AND THE DEVICES USED TO EXAMINE THE DATA

Directory	File(s)	Artifact	Tool to Be Used
AddressBook	AddressBook.sqlitedb	Contact information	Froq, SQLite Database Browser
Caches	Consolidated.db	Cell tower geodata, screenshot images	Froq, SQLite Database Browser
Calendar	Calendar.sqlitedb	Event data	Froq, SQLite Database Browser
Call History	call_history.db	Call history data	Froq, SQLite Database
Configuration Profiles	PasswordHistory.plist	Passcode history	Property List Editor
Cookies	Cookies.plist	Internet cookies	Property List Editor
Logs	ADDataStore.sqlitedb	Application usage	Froq, SQLite Database Browser
Keyboard	Dynamic-text.dat	Keyboard logger	TextEdit, Lantern
LockBackground.jpg	Image	Wallpaper background	Preview

Maps	Bookmarks.plist Directions.plist History.plist	Map bookmarks, map route directions, map route history	Property List Editor
Notes	Notes.db	Notes	Froq, SQLite Database Browser
Preferences	Numerous property lists	System/app data	Property List Editor
Safari	Bookmarks.plist	Safari bookmarks, Internet history, suspended web pages	Property List Editor
SMS	sms.db	SMS and MMS messages	Froq, SQLite Database Browser
Voicemail	.amr	Voicemails	QuickTime
Webclip	.png info.plist	Web icons	Preview, Property List Editor

G. Libimobiledevice

Libimobiledevice is a kind of open source software library for iOS devices like iPhone, iPod Touch, iPad and Apple TV and is mainly developed and used in Linux operating system and support Mac OSX and Windows operating system; it doesn't have to rely on the current iOS special database without the need to jailbreak to extract the system files in the device and index the data in iOS devices [11].

III. SYSTEM ARCHITECTURE

The research designs and implements on Mac to adopt logical acquisition of extracting information, like mobile phone hardware, SIM card content, phone record, text messages, phone log, photos, web browser, memos towards iOS platform smart phone forensic program system via USB connection to libimobiledevice open source.

The forensic operation of the study is the procedure to investigate iOS platform smart phones. As shown in Fig.2, first we need to install libimobiledevice and its packages to the computer and connect the mobile phone to the computer. We need to confirm whether the screen password autolock is deactivated and run setups in cell phones. Then we activate investigation application programs to extract data. After that output, the investigation results on investigation programs. The acquired investigation results table can be used to undertake post-investigation data analysis.

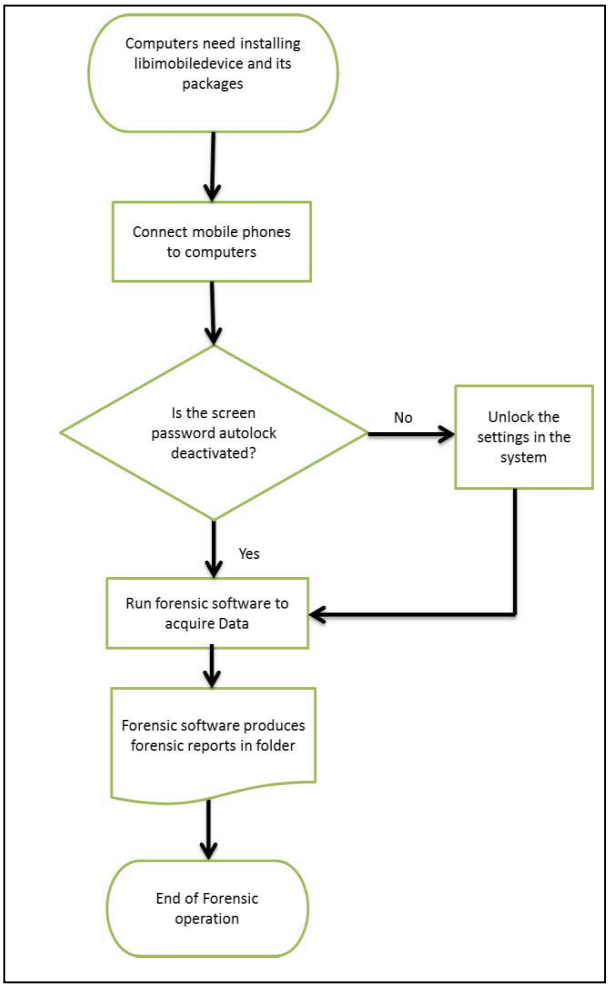

Fig. 2. Flow chart of forensic operation.

IV. SYSTEM IMPLEMENTATION

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

A. development tools and environment

As to the part of development, the research uses Objective C as the developing language along with X code applications to integrate the development environment and Mac OSXSDD to conduct the design and implementation of investigation program. We list the environment and tools in system development in Table 2.

TABLE II. TOOLS AND ENVIROMENT FOR DEVELOPMENT

Item	Tools
Operating System	Mac OS X
Development Tools	Xcode 4.6 OS X Library OS X SDK
Programming Language	Objective-C Shell script SQLite
Smart phone for test	iPhone 4S

B. System Procedures

The research exploits the concise design concept to run program design and development, uses Objective-C to combine with the libimobiledevice and its related package to implement a forensic software, adopts libimobiledevice to conduct logics acquisition toward iOS cell phone devices via Standard USB teleport and uses simple operating models to assist forensic operations to acquire data from iOS platform cell phone devices.

First, the device needs to be connected to the computer via USB. When forensic applications are in progress, as shown in Fig.3, we run “Acquire Data” to finish processing the devices. Then we can use “Examine the Acquired Data” to examine the information inside the device. After undertaking the function of recovering the erased data, and use "examine the recovered data, "we can see the deleted data.

Fig. 3. Main screen of Forensic Software.

Fig.4 is the image shown after we choose to run “Acquire Data”. The investigators can categorize the file names based on the different devices and cases. It's more convenient for them to sort out the processed data.

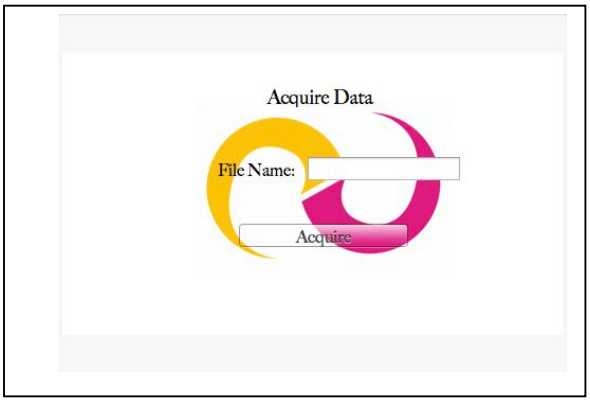

Fig. 4. The screen of Acquire Data.

Fig.5 to edit file names and click the button to conduct gathering. The forensic software will extract data from the device and the image of " Data acquiring" will appear.

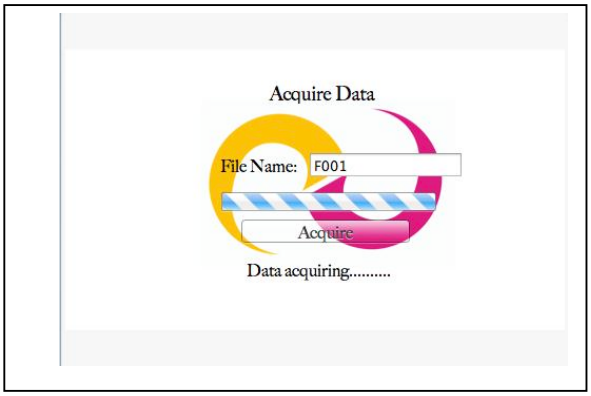

Fig. 5. The state of Data acquiring

After the forensic software finishes data gathering, an input file folder will appear, which, includes all the data collected from mobile phones. Investigators can directly open them to examine the collected data according to the file categories.

Fig.6 and Fig.7 individually represent the image after using the corresponding file programs.

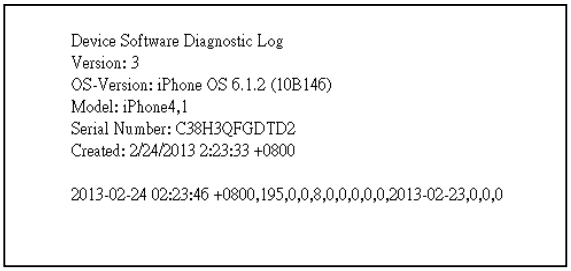

Fig. 6. The information of the device.

Fig. 7. SMS of the device.

Fig.8 is the image shown after clicking the button of recovering the erased data. The function only works after we conduct data gathering.

Fig. 8. The screen of Recover Data.

Fig.9 is shown as to click the recovery button. The program undertakes Strings dump towards the collected SQLite files [5]. We recover the data in database form. This is the image shown when it is in the middle of data recovering.

Fig. 9. The state of Data recovering.

Fig.10 is the recovered files. After being stored and exported in text only form, investigators can directly examine the recovered data record. Its helps the investigators run data analysis towards the devices.

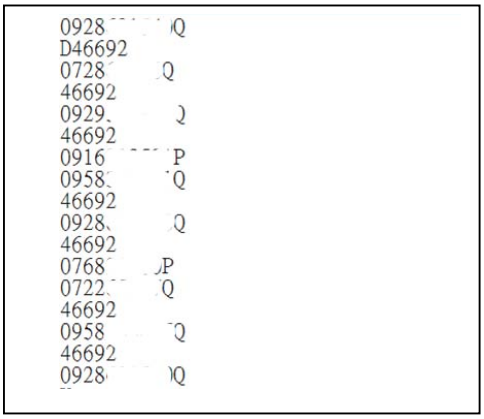

Fig. 10. The recovered data of call history.

V. CONCLUSION

iPhone is a steady, fast and widely used smart phone device. It possesses a versatile and vastly expandable applications and trustworthy application market, Apple Store. It even has many unauthorized but still best-selling application market. It owns even more versatile investigation content than traditional cell phones. The research adopts logical acquisition, implement forensic application software on Mac towards iOS smart devices via Mac operating system standard application developing platform without the need to run jailbreaking procedures and install other applications when iPhone is fully developed [8]. It provides investigators quick access to forensic information through the official USB teleport.

The research will head toward vast data extraction and multi-media images recovery and overcome the difficulty operating when cell phone screens are locked. Besides, the search will also offer the comparison and contrast between iTunes and libimobiledevice in the middle of accessing data in order to provide more complete contrast and contribution.

ACKNOWLEDGEMENT

This work was supported in part by the National Science Council of Taiwan (NSC 101-2221-E-017-013).

References

[1] N. Seriot, “iPhone Privacy”, Black Hat DC 2010, USA, 2010.

[2] W. Jansen and R. Ayers, “Guidelines on Cell Phone Forensics”, National Institute of Standards and Technology, May 2007.

[3] A. Hoog and K. Strzempka, iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad, and iOS Devices, Elsevier Science Ltd, 2011, pp. 195–202.

[4] S. Morrissey, iOS Forensic Analysis for iPhone, iPad, and iPod touch, Springer-Verlag New York Inc, 2010, pp.140-142.

[5] J. Zdziarski, Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It, Oreilly & Associates Inc, 2012, pp.87-117.

[6] J. Zdziarski, iPhone Forensics, Oreilly & Associates Inc, 2008, pp.61-62.

[7] Gartner Says Worldwide Smartphone Sales Soared in Fourth Quarter of 2011 With 47 Percent Growth, http://www.gartner.com/it/page.jsp?id=1924314.

[8] K. David, "Jailbreaking iPhone Legal", U.S. Government Says, July 27, 2010. http://abcnews.go.com/Technology/us-government-jailbreaking-iphone-legal/story?id=11254253.

[9] NIST, Smart Phone Tool Specification, Version 1.1, http://www.cftt.nist.gov/documents/Smart_Phone_Tool_Specification.pdf.

[10] iOS Developer Library, http://developer.apple.com/library/ios/#documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/IPhoneOSOverview/IPhoneOSOverview.html#//apple_ref/doc/uid/TP40007898-CH4-SW1, Apple Inc. 2010.

[11] Libimobiledevice, http://www.libimobiledevice.org/.