Design and Implementation of Forensic System in Android Smart Phone

Xinfang Lee[1], Chunghuang Yang[1], Shihjen Chen[2], Jainshing Wu[2]

[1]Graduate Institute of Information and computer Education
National Kaohsiung Normal University, Taiwan
podu76@gmail.com， chyang@nknucc.nknu.edu.tw
[2]Networks and Multimedia Institute Institute for Information Industry
{sjchen, jsw}@nmi.iii.org.tw

Abstract. Since technology is booming on its high astonishingly, digital devices are getting popular in our daily life and record people's life insensibly. The most proliferation product in our life is the Mobile phones, and especially the smart phone, it's gaining a lot popularity and importance in terms of convenient and large storage database. Due to its large storage, smart phones become a great provider of digital evidences in crimes. Smart phones provide users with the combined of several capabilities which will lead to the user information and be used as evidence in criminal cases. The finding shows the information security issue of smart phone is getting more important in today's society. The purpose of the study is based on National Institute of Standards and Technology (NIST) the digital forensics and regulations, and to examine the forensics of Android smart phones with the integration of open source digital forensics tools.

Keywords: Digital evidence, Mobile forensics, Smart phone, Android, Mobile forensic tool.

1 Introduction

Despite the lagging economy, smart phones remain a hot market. According to Gartner, the international research-cum-consultancy, the fourth quarter smart phone market research report in 2010, the sales volume of smart Phones was 53.8 million in year 2009, and compared with year 2008 had growth 41.1% [1]. The similar situation was also mentioned in the market research from NPD Group, a leading market research company; smart phone Android operating system market place in the first quarter (Q1) of 2010 has changed to second position and increased 28 percent based on unit sales [2].

With the trend, smart phones become a very popular and indispensable tool in daily life and work, because smart phone have a special feature, single-user feature. Recently, due to the vigorous development of wireless networks, when people decide to take the actions through smart phones, it has also arises the mobile security issue. Therefore, smart phones become an important item in digital evidence forensics.

Based on the raised mobile security issue in usages of smart phones, the purpose of this study is to acquire the evidence smart phone in opened status, by using the Android forensic tools to examine smart phone digital forensics. This study will refer to the United States National Institute of Standards and Technology tool in the smart phone specification [3] and smart phone forensics process in order to make legally binding, and the digital evidence will have evidences ability and credibility.

2 Related Work

Currently, numbers of researches had addressed to the security issues of the smart phone, and developed various technologies for the investigative features. In this chapter, researchers analyzed the definitions of digital Evidence, mobile forensic and smart phone forensic, and also introduced some studies that had down in Android smart phone operating system architectures, and mobile phone forensic tools area.

2.1 Digital Evidence

The digital evidence is a series of binary digit numbers on transmission [4], or stored information files on the electronic device. Moreover, the digital evidence file formats includes audio, video, images, and digital, etc. The digital evidence is not virtual exist, but there are some other features to look for, the digital evidence can be copied with unlimited differences, can be modified easily, hard to be identified the original resource, can be integrated data verification, and cannot be understood directly without technical process.

2.2 Mobile Forensic

With the increased emphasis on social security issue, crime issue is considerable when it comes to the utilization of smart phone technologies, digital forensics provide the technical skills to collect evidences for the court to review and judge cases. Digital equipment has changed daily, people has pervasive use some common digital devices such as computers, Internet, mobile phones, digital cameras, hardware, storage devices, etc. Currently, digital forensics has widely used in the areas of network forensics, mobile forensics, computer forensics, and memory forensics, etc. According to NIST definition of mobile phone forensics process is preservation, acquisition, examination and analysis, and then reporting [5].

2.3 Smart Phone

Due to the advanced technological development, mobile phone's selling was decreased in 2009; smart phones' selling is increased, and the commercial demand cannot be sacrificed by the smart phone. In Table 1 [6] shows definition of smart phone, the various categories of smart phones' forensic, different operating systems and the disordered domestic laws for forensic procedures result in the difficulty of smart phone forensics [7].

Table 1. Definition of Smart Phone

Item	Definition
Capability	With voice and data wireless communication personal management (PIM), such as contacts, calendar, alarm clock, etc.
Input Mode	Common with push-button, voice input, touch and multi-touch
Wireless Transmission	IrDA, Bluetooth and Wi-Fi
Operating System	Symbian, iphone, Windows Mobile, Android, Palm, RIM, etc.
Processor	Embedded multi-task microprocessor

Google Android is an open source smart phone operating system, which is based on Linux [8]. Android system architecture has four main levels, as shown in Figure 1, the lowest level is Linux Kernel, and it implements the use of Linux 2.6 kernel, the second level is Library and Android Runtime, and the third level is the Application framework, which is designed to simplify the reuse of components so that developers have full access to the same framework that APIs used by the core applications. The highest level is the Application [9]. Application level includes a bundle of programs such as the contact manager, web-browser, an email client, calendar, SMS program, etc. which will be shipped as core programs with the handset [10].

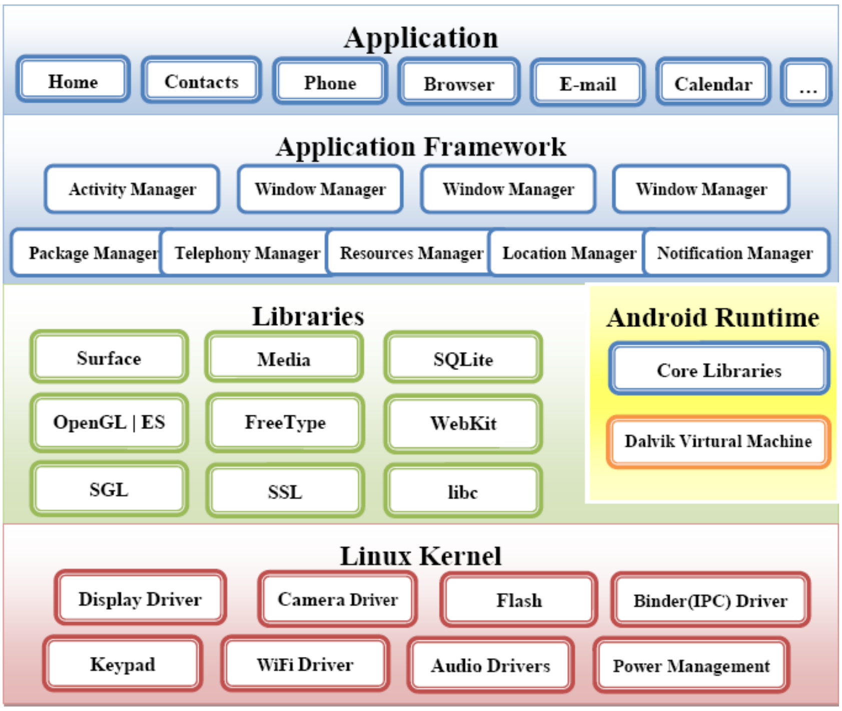


Fig. 1. Android Framework

2.4 Digital Forensics Application

Smart phones forensics tools are divided into software and hardware. Software programs are often seemed Oxygen Forensic Suite [11], MOBILedit! Forensic [12], EnCase®, and Neutrino® [13], etc., and input through the IrDA, Bluetooth, and USB. Through the commercial forensic software, most of the forensic processes are done at the computers to approach the forensic achievements.

Hardware equipments, such as .XRY [14], store all kinds of cable kits, empty SIM cards and SIM card readers, etc. in the forensic tool kits for investigators to apply, in order to collect useful evidence at the crime scene.

The difference between our developed forensic system and the Commercial Forensic system is the forensic progress. In this study, the forensic process can be done without a computer, and save the evidence into the forensic SD card. The comparison of the progress between the developed forensic system and the commercial forensic is shown in Table 2.

Table 2. Comparison of Forensic Progress

Forensic Progress	Common Forensic System	Developed Forensic System
Investigation at the Crime Scene	Record the evidence smart phone outside condition, and switch off the power. Place the smart phone into evidence bag, and bring the bag back to the lab.	Record the evidence smart phone outside condition, and unmount user SD card
Collecting Evidences	Connect to the computer, process evidence with forensic software.	Mount the forensic SD card in the smart phone, process evidence with forensic software, save the collected data in the forensic card.
Analysis	Analyze with the computer.	Analyze with the computer.
Report	Report Analysis data with the computer.	Report Analysis data with the computer.

Based on open source Android forensics tools [15], viaForensics has released to a beta version of its open source Android forensics application which supports all Android devices [16]. This application was developed with a generic architecture which allowed other programmers to add supports easily for the new applications and data sources. Currently, program designers pull the following information in the CSV files on SD card: browser, history, call logs, contact methods, organizations, people, and SMS. This study strengths the function of the Android forensics, and to fulfill the needs of investigation. The comparison in function between the Android and research developed forensics system are shown as Table 3.

Table 3. Comparison of Forensic Tool Function

Function		Android Forensics	Research Developed System
System Log	Call log	O	O
	E-mail	O	O
	Browser	O	O
	Contact	O	O
	Organizations	O	O
	People	O	O
	SMS	O	O
Phone Status	IMEI	X	O
	Running processes	X	O
	Battery status	X	O
	Up time	X	O
	Memory Status	X	O
	WiFi Mac address	X	O
SIM Card	SIM card status	X	O
	ICCID	X	O
	SIM card supplier NO.	X	O
	SIM card supplier	X	O
	SIM cards released country	X	O
Manually Input by Investigators	Data and Time	X	O
	Investigator name	X	O
	Note	X	O

3 System Architecture

Figure 2, shows the system architecture that processes the forensics evidence to collect the evidence from the on-powered smart phone.

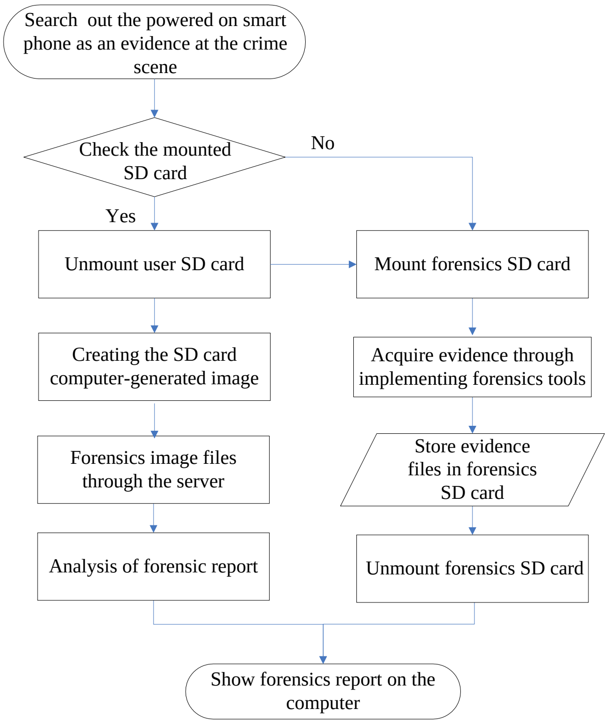
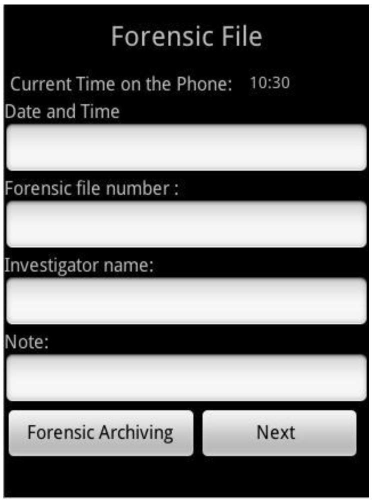

Search out the powered on smart phone as an evidence at the crime scene
Check the mounted SD card
No
Yes
Unmount user SD card
Mount forensics SD card
Creating the SD card computer-generated image
Acquire evidence through implementing forensics tools
Forensics image files through the server
Store evidence files in forensics SD card
Analysis of forensic report
Unmount forensics SD card
Show forensics report on the computer

Fig. 2. System Forensic Flowchart

When the forensic crime scene investigators to detain powered on smart phones from the crime scene, forensics investigators must recorded external appearance state of smart phones at the first step (such as through text, sound recording or taking pictures recorded phone screen state), and then check the mounted SD card in this particular crime scene smart phone by operating the smart phone. If the smart phone was originally mount SD card then select unmount option to process the digital forensic from the computer. The smart phone forensics by using the forensic SD card that mounts on the smart phone when the smart phone didn't mount any original user SD card. When the smart phone had no SD card mounted, the investigators would mount the forensic SD card, in which contained in the forensic tools in the SD card, to collect volatile digital evidence. After the investigation at the crime scene, the collected evidence will be stored in the SD card.

4 System Implementation

This study collect the data from the powered on evidence smart phones at the crime scene, based on the open source forensics tools, Android Forensics, and increase the integrities of the forensics tool to achieve the NIST digital forensics collecting evidence process. By using Java language as the main program creating language, and based on the Android provide API development forensics system, investigators can utilize the created forensic tools to record the evidence from the smart phone in time, in order to avoid the evidence disappear when powered off. After operating the forensics system, the screen will show the forensic system file that contains date and time, file number, investigator's name, and other personnel information or investigation notes, in a created SD card folder, for investigator to input the information, as shown in Figure 3.



Forensic File

Current Time on the Phone: 10:30

Date and Time

Forensic file number :

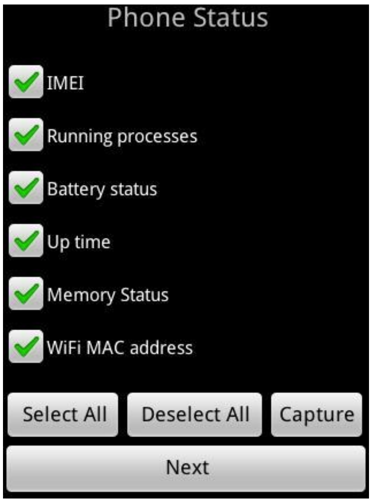
Investigator name:

Note:

Fig. 3. Create Forensics File

In Figure 4, evidence collection from smart phones, includes the current memory status of smart phone, running applications, smart phone battery, up time. This study utilized Java applications through the implementation of Linux shell command, then the phone at the crime scene to the state collecting evidence, evidence collection and executed automatically generate a log file records are maintained in forensic SD card folder.

Using Android API (Application Programming Interface), data collected included SIM card status, SIM card vendors, SIM card number, as shown in Figure 5. The implementation of evidence collection and evidence gathering will be deposited in the forensic SD card folder.



Phone Status

☑ IMEI

☑ Running processes

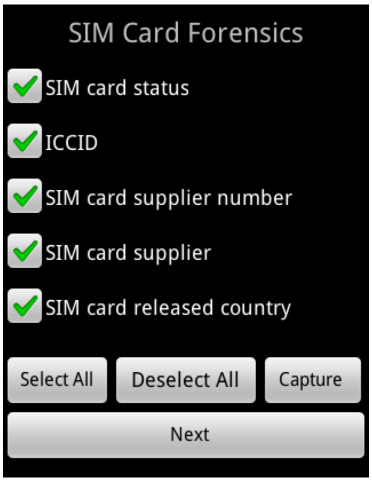
☑ Battery status

☑ Up time

☑ Memory Status

☑ WiFi MAC address

Fig. 4. Smart Phone Evidence Collection



SIM Card Forensics

☑ SIM card status

☑ ICCID

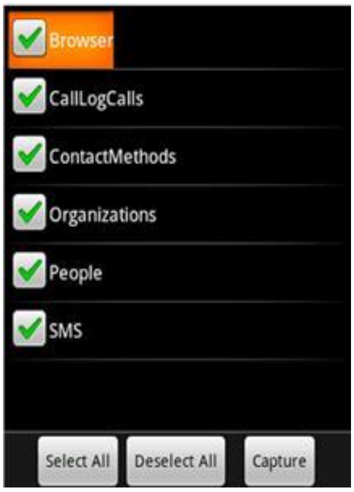
☑ SIM card supplier number

☑ SIM card supplier

☑ SIM card released country

Fig. 5. SIM Card Evidence Collection

In Figure 6, Android forensics tools are based on function check list. Investigators need to select the options of forensic digital evidences and forensic report will be saved to the SD card, such as browser, records, communications records, newsletter, etc. Forensic investigators must returned to forensic lab, and then through process the SD card which stored the forensic evidence collection document file on a Linux computer, in order to inspect the collected evidence statements, as shown in Figure 7.



☑ Browser

☑ CallLogCalls

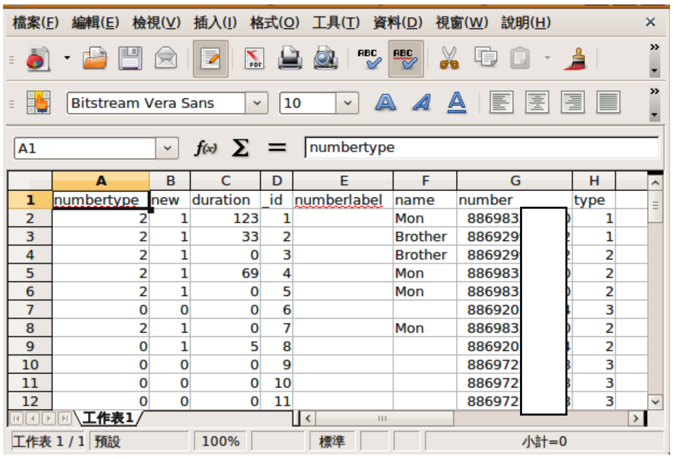
☑ ContactMethods

☑ Organizations

☑ People

☑ SMS

Fig. 6. Android Digital Forensics Application



檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 資料(D) 視窗(W) 說明(H)
Bitstream Vera Sans
10
A1
numbertype
工作表1
工作表 1 / 1
預設
100%
標準
小計=0

	A	B	C	D	E	F	G	H
1	numbertype	new	duration	_id	numberlabel	name	number	type
2	2	1	123	1		Mon	886983[redacted]	1
3	2	1	33	2		Brother	886929[redacted]	1
4	2	1	0	3		Brother	886929[redacted]	2
5	2	1	69	4		Mon	886983[redacted]	2
6	2	1	0	5		Mon	886983[redacted]	2
7	0	0	0	6			886920[redacted]	3
8	2	1	0	7		Mon	886983[redacted]	2
9	0	1	5	8			886920[redacted]	2
10	0	0	0	9			886972[redacted]	3
11	0	0	0	10			886972[redacted]	3
12	0	0	0	11			886972[redacted]	3

Fig. 7. Forensics Report

5 Conclusion

In this study, the forensic tools are based on NIST proposed forensics process to develop the forensic tools. Researchers utilized the Java language as the main approaching language to design the programs for the crime scene forensic investigators on gathering evidence from the smart phone at the crime scene immediately. They can process the forensics without carried the collected smart phone evidence on powered off status back to the lab.

The study result provides additional input functions in Android Forensics tools for the crime scene forensic investigators, and to collect and process smart phone information and status in the crime scene immediately, then saves the evidences in the SD card.

For further study, researchers will not only complete presentation of the evidence collected, but also based on the case or the demand for presented by forensic investigators, to achieve operational efficiency and provide strong evidence to the court review.

ACKNOWLEDGMENTS

This study was supported in part by research grants (NSC 98- 2221-E-017-010-MY3) from the National Science Council of Taiwan.

References

1. Egham: Gartner Says Worldwide Mobile Phone Sales to End Users Grew 8 Per Cent in Fourth Quarter 2009; Market Remained Flat in 2009, http://www.gartner.com/it/page.jsp?id=1306513 (2010)
2. NPD, Android Shakes Up U.S. Smartphone Market, http://ww.npd.com/press/releases/press_100510.html
3. NIST. Smart Phone Tool Specification, Public Draft 2 of Version 1.1 (2009)
4. SWGDE and SWGIT Digital & Multimedia Evidence Glossary, SWGIT Digital & Multimedia Evidence Glossary Version: 2.3 (2009)
5. Jansen, W., Ayers, R.: Guidelines on Cell Phone Forensics, NIST, SP 800-101 (2007)
6. Zhang, Z.H., Luo, H.Y., Chen, L.X., Chen J.Y.: Digital home appliances industry trends, Ministry of Economic Affairs, R.O.C. (in Chinese)(2002)
7. Ayers, R., Jansen, W., Moenner, L., Delaitre A.: Cell Phone Forensic Tools: An Overview and Analysis update, NISTIR 7387 (2007)
8. Yang, W.Z.: Google Android application design and application, Flag Publishing, Taipei (in Chinese)(2009)
9. Android developers, http://developer.android.com/guide/basics/what-is-android.html (2010)
10. Mohindra, D.D.: Android, Incident Response and Forensics (2008)
11. Oxygen Forensic Suite, http://www.oxygen-forensic.com/us/
12. MOBILedit! Forensic, http://www.mobiledit.com/forensic/
13. EnCase®, and Neutrino®, http://www.encaseondemand.com/Home/tabid/632/Default.aspx
14. .XRY, http://www.msab.com/
15. Android Forensics, http://code.google.com/p/android-forensics/
16. NewswireToday, viaForensics Announces Release of Open Source Android Forensics Application, http://www.newswiretoday.com/news/65707/ (2010)