Appl. Math. Inf. Sci. 6 No. 1S pp. 243S-247S (2012)

Applied Mathematics & Information Sciences
An International Journal

Design and Implementation of Forensic Systems for Android Devices based on Cloud Computing

Chung-Huang Yang[1*] and Yen-Ting Lai[1]
[1] National Kaohsiung Normal University, Kaohsiung, Taiwan 802
Email Address: chyang@nknucc.nknu.edu.tw

Received: Received May 02, 2011; Revised July 25, 2011; Accepted September 12, 2011
Published online: 1 January 2012

Abstract: As popularity of the smart phones continues to grow, it changes the way of cyber crime. Number of cyber crime increases dramatically in recent years and investigators have been facing the difficulty of admissibility of digital evidence on smart phones. To solve this problem, we must collect evidence by digital forensics techniques and analyze the digital data, or recover the damaged data in the phones. In this paper, we describe the design and implementation results of forensics software for Android smart phones. Our design is based on guidelines from the National Institute of Standards and Technology for cell phone forensics to ensure the effectiveness of digital evidence and credibility of the evidence on judicial review. In order to minimize the alteration of original evidence source in mobile phones, cloud computing platform is used to flexibly select proper forensic software and store the forensic results.

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

1 Introduction

With the increased emphasis on social security issue, crime issue is considerable when it comes to the utilization of smart phone technologies, digital forensics [6,9,13,20] provide the technical skills to collect evidences for the court to review and judge the case. Digital equipment has changed daily, people has pervasive use some common digital devices such as computers, the 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.

Despite the lagging economy, smart phones remain a hot market. According to Gartner Inc. [10], worldwide smart phone sales will reach 468 million units in 2011, 58% increase from 2010. With the trend, smart phones become very popular in daily life and work, and it has become an indispensable tool. Smart phone has a special feature, the single-user feature. When people decide to take the actions through smart phones, it also raises the security issue. Therefore, smart phones become an important item in digital forensics.

Smart phone forensics acquires digital evidence sources from the SIM cards, smart phone memory, and SD card in smart phones. The purpose of this research is to design and implement a forensic system which acquires the digital evidence of Android smart phones. Our research is based on the National Institute of Standards and Technology guideline for the smart phone forensics [14] in order

* **Corresponding Author: Chung-Huang Yang, chyang@nknucc.nknu.edu.tw**

to make legally binding, so that the digital evidence will have evidences ability and credibility.

2 Digital Forensics

Digital forensics [6,9,13,20] is the science of obtaining, preserving, analyzing, and documenting digital evidence from electronic devices, such as tablet PC, server, digital camera, PDA, fax machine, iPod, smart phone, and various memory storage devices. Generally speaking, the purpose of digital forensic is to investigate the digital evidence which might be involved in computer intrusion, unauthorized access, child pornography, etc. Forensic techniques might be used to attack strong disk encryption systems, such as BitLocker in the popular Windows 7 operating system [11].

Digital forensics can be performed in four distinct phases of collection, preservation, analysis, and presentation [15], illustrated in Figure 1.

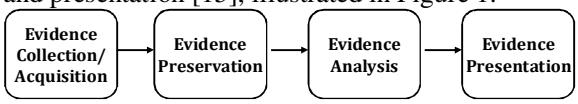

Figure 1: The Phases of Computer Forensics

Here, we give a brief description of these four procedures:

(1) Evidence Collection/Acquisition: This phase involves the collection and acquisition of digital data that could be considered to be of evidential value. For example, we usually used the forensic tools to create an image the disk.

(2) Evidence Preservation: This phase is focus on the preservation of digital evidence in a manner that is reliable and verifiable. This phase usually includes the use of cryptographic hashing, such as SHA-256, to ensure that digital data obtained in a digital crime scene did not alter in the later analysis.

(3) Evidence Analysis: This phase addresses the extraction of digital information that may be of significant to the crime investigation.

(4) Evidence Presentation: The final phase is for documenting the analyzing results for present the digital evidence.

Digital evidence stored in computer can play a major role in a wide range of crimes, including murder, rape, computer intrusions, espionage, and child pornography in proof of a fact about what did or did not happen [6,22]. Digital information is fragile in that it can be easily modified, duplicated, restored or destroyed, etc.

At present, the analysis of digital evidence must depend on the forensics tools such as the Forensic Toolkit (FTK) or EnCase [8]. Most of these tools are commercial software and are too expensive for the small enterprises or individual. In the course of the investigation, the investigator should assure that digital evidence is not modified without proper authorization. The typical goal of an investigation is to collect evidence using generally acceptable methods in order to make the evidence is accepted and admitted on the court. The final forensic report must include [22]:

(1) Where the evidence was stored?

(2) Who had obtained to the evidence?

(3) What had been done to the evidence?

Any step in the process must be carefully recorded in order to prove the electronic records were not altered in the investigation procedure.

Digital forensics can be classified into live-analysis and the dead-analysis [1]. A live analysis occurs when the suspect system is being analyzed while it is running while a dead analysis occurs when a dedicated analysis system is used to examine the data from a suspect system. Currently, many research of digital forensic use the dead-analysis but the way may lose the data due to showdown of machine or removal the plug. For forensic analysis, the collection of volatile information is very important. Volatile information might include hardware information, installed software packages, process states, ..., etc. [19].

Since gathering one evidence on the target system can affect other evidence on the target. In order to produce best quality of the evidence, we shall run known good binaries, hashing all evidence, and gathering data in order of volatility [4].

All digital evidence shall be analyzed to determine the type of information that is stored upon it. In this point, specialty tools are used that can display information in a format useful to investigators. Such forensic tools include [5,8]: FTK, EnCase, SMART, PyFlag and The Sleuth Kit, etc. There are open source tools that can be used for computer forensics, for example, a list is provided by the Digital Forensics Association (http://www.digitalforensicsassociation.org/) which covers about 10 tools. However, these open source tools are seldom used by end-users because they are usually too difficult to install and deploy.

3 Android Forensics

Due to the advanced technological development, mobile phones' selling was decreased in 2010 while smart phones' selling is increased. More and more people today rely heavily on smart phones. However, proprietary operating systems and the disordered domestic laws for forensic procedures result in the difficulty of smart phone forensics. At

present, Android-based devices is the biggest smart phone platform worldwide, according to Garner Inc. [10]. Therefore, this research will focus on the forensics of Android smart phones.

Android [2,7] is an open source operating system for smart phones, which is based on Linux operating system. Android system architecture has four main levels. The lowest level of Android architecture is Linux Kernel, and it implemented the 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. The top-level Application level is shipped as core programs with the Android handset and it includes a bundle of programs such as the contact manager, web-browser, an email client, calendar, SMS program,..., etc. In recent years, several forensic tools [3, 12, 16] for smart phones had been developed. However, technological innovations of smart phones are evolved in a fast-paced matter and new forensics tools are demanded. Smart phones creates significant challenges for forensic researchers.

Digital evidences on (Android) smart phones might come from three area:

(1) SIM (Subscriber Identity Module): a SIM is a special type of removable smart card on most Android smart phones that contains essential information about the subscriber. Forensic tools shall acquire data on SIM, including the International Mobile Subscriber Identity (IMSI), last numbers dialed, or SMS messages.

(2) Memory chip: Detachable (micro-)SD card might be included in the handset to store pictures, music, and applications.

(3) Handset: Android handset provides most valuable source of evidence. The International Mobile Equipment Identifier (IMEI), telephone numbers in the phonebook, geo-referenced data, numbers called, SMS sent, web browser history, ..., etc., might be obtained with the forensic software.

4. Cloud Computing

NIST [17] defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources...". Cloud computing automatically provides service according to user's need while it doesn't require user to know where his/her data stores over cloud platforms.

Cloud computing provides a convenient platform for digital forensics, especially during the phase of digital evidence analysis. Digital forensics with such a cloud hosting [18] will provide a central location to fetch forensic software and store forensic reports. We will use Google Cloud Service as our cloud computing environment, which transmits data by https protocol that supports RSA public key cryptosystem to ensure data security.

5 The Proposed Forensic Systems

Figure 2 shows the proposed three approaches that processes the forensic evidence to collect the evidence from the on-powered smart phone. We have implemented two approaches, one is based on the memory card, the other is based on cloud computing.

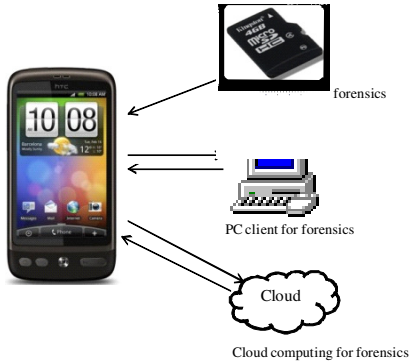

Figure 2: Three approaches for Android forensics

The first approach is to use the detachable memory card, such as SD card or micro-SD card (we will all call it as the SD card in this research), to store the developed forensics tools. Figure 3 illustrates the flowchart of this approach. At crime scene, when forensic investigators detain smart phones, he/she must first record external appearance status of smart phones (such as through text, sound recording or taking pictures recorded phone screen state), and then check whether a SD memory card was mounted in this particular smart phone by operating the phone. If a SD card was originally mounted, then the investigator shall select un-mount option to process the digital forensic of memory card using some computer forensic tools (such as the Autopsy, http://www.sleuthkit.org/autopsy/) on 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.

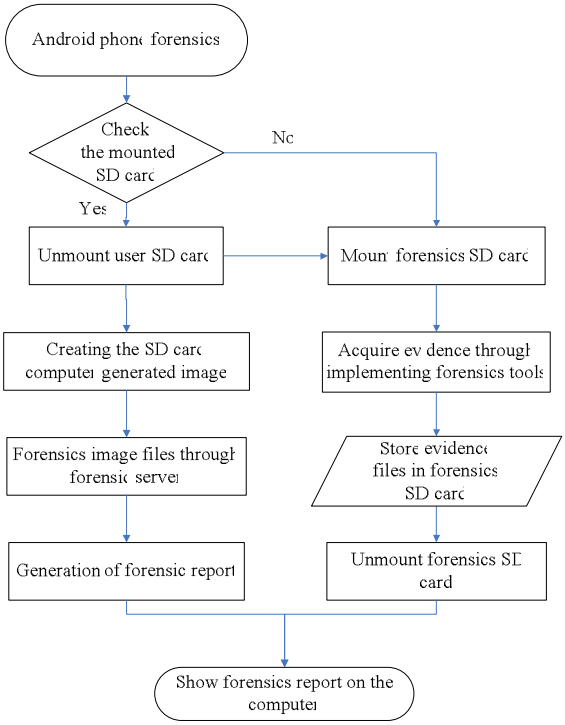

Figure 3: System flowchart of the Android forensics with memory card

Using Android API (Application Programming Interface), the developed forensic software collects digital evidence data included SIM card status, SIM card vendors, SIM card number, as shown in Figure 4. Our forensic software was developed with the Android SDK and tested on the Samsumg Galaxy Tab and HTC Desire devices.

Our 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.

When cloud computing environment is available, we will download forensic software from the Google Cloud Service, without using memory card for fetching software. This will require a network connection from the targeted smart phone to the Google Cloud Service, but it has the benefit of large storage space with high analysis power.

Figure 4: Forensic screens

6 Conclusion

Advanced network functions and computational powers of smart phones create new opportunities for criminals. There are also more and more cases of cyber crime involved smart phones in recent years. Therefore, crime investigator must collect digital evidence of target phones after an incident is occurred. However, most existing phones forensics software are commercial version which are expensive and might not support the latest smart phones.

In this research, we design and implement forensics systems for the Android phones based on memory card or cloud computing. Our design is followed on NIST proposed forensics process and forensic software was written with Java language for the crime scene forensic investigators on gathering evidence from the on-site smart phone. Future research will on creating a better forensic reporting and gather GPS-related data on the smart phone.

Acknowledgements

This study was supported in part by research grants (NSC 98-2221-E-017-010-MY3, 2009-2012) from the National Science Council of Taiwan.

References

[1] F. Adelstein, Live forensics: diagnosing your system without killing it first, Communications of the ACM, **49**(2) (2006), 63-66.

[2] Android developers. http://developer.android.com/.

[3] R. Ayers, W. Jansen, L. Moenner, and A. Delaitre, Cell Phone Forensic Tools: An Overview and Analysis update, NISTIR 7387, 2007.

[4] J. Bates, Fundamentals of computer forensics, Information Security Technical Report, Elsevier, 1998.

[5] B. Carrier, Performing an autopsy examination on FFS and EXT2FS partition images: An introduction to TCTUTILs and the Autopsy Forensic Browser, Proc. SANSFIRE 2001 Conference, 2001.

[6] E. Casey, (ed.) Handbook of Digital Forensics and Investigation, Academic Press, 2010.

[7] S. Conder and L. Darcey. Android Wireless Application Development, Addison Wesley, 2009.

[8] L. Garber, Computer Forensics: High-Tech Law Enforcement, IEEE Computer, **34** (1) (2001), 202-205.

[9] S. Garfinkel, Digital Forensics Research: The Next 10 Years, Digital Investigation, **7** (2010), S64-S73.

[10] Garner, "Sales of Mobile Devices in Second Quarter of 2011 Grew 16.5 Percent Year-on-Year; Smartphone Sales Grew 74 Percent," Gartner, Inc., August 11, 2011.

[11] J. Halderman, S. Schoen, A. Heninger, and E. Felten, Lest We Remember - Cold Boot Attacks on Encryption Keys, Proc. 17th USENIX Security Symposium, 2008.

[12] A. Hoog, Android Forensics: Investigation, Analysis and Mobile Security for Google Android, Elsevier Inc., 2011.

[13] ISO/IEC 27037: Guidelines for identification, collection, acquisition and preservation of digital evidence (DRAFT), 2011.

[14] W. Jansen and R. Ayers, Guidelines on Cell Phone Forensics, NIST SP 800-101, May 2007.

[15] A. Jones and C. Valli C, Building a Digital Forensic Laboratory. Elsevier, Inc., 2009.

[16] NIST, Smart Phone Tool Specification, Version 1.1, April 2010.

[17] P. Mell and T. Grance, The NIST Definition of Cloud Computing, NIST Special Publication 800-145 (Draft), January 2011.

[18] D, Molnar and S. Schechter, "Self Hosting vs. Cloud Hosting: Accounting for the security impact of hosting in the cloud," Proc. 9th Workshop on the Economics of Information Security (WEIS 2010), 2010.

[19] C. Pogue, C. Altheide, and T. Haverkos, UNIX and Linux Forensic Analysis DVD Toolkit, Syngress Publishing, 2008.

[20] SWDGE, Digital & Multimedia Evidence Glossary, Version: 2.2, The Scientific Working Group on Digital Evidence (SWGDE), November 2007.

[21] V. L. L. Thing, K. Y. Ng, and E. C. Chang, Live memory forensics of mobile phones, Digital Investigation, **7** (2010), pp. S74-S82.

[22] L. Volonino, R. Anzaldua, J. Godwin, and G.C. Kessle, Computer Forensics: Principles and Practice, Prentice Hall, 2006.

[23] HwaMin Lee, Min Hong, An Analysis of Learning Effects for Smartphone based Serious Game Applications, *Journal of Future Game Technology*. 1, 1(2011) 1-8.

[24] Changsok Y., Huy K. K., Eunnyeong H., The Economic Value of Online Game Developers in Early Stages, *Journal of Future Game Technology*. 1, 1(2011) 21-34.

Chung-Huang Yang has a Ph.D. degree in computer engineering from the University of Louisiana at Lafayette in 1990. He is currently Professor at the National Kaohsiung Normal University and a Board of Executive Directors member at the Chinese Cryptology and Information Security Association (CCISA), Taiwan. Previously, he was a software engineer at the RSA Data Security, Inc. (Redwood City, USA) in 1991, a postdoctoral fellow at the NTT Network Information Systems Laboratories (Yokosuka, Japan) in 1991-1993, and a project manager of the Information Security and Cryptology Project at the Telecommunication Laboratories, Chunghwa Telecom (Taiwan) in 1995-1997. For more details, please refer to http://security.nknu.edu.tw/.

Yen-Ting Lai received bachelor degree from the Department of Management and Information Technology of Southern Taiwan University of Technology in 2010. Currently he is a graduate student at the Graduate Institute of Information and Computer Education, National Kaohsiung Normal University, Taiwan. His research interests include Digital Forensics and Network Security. Contact him at: f0963217595@hotmail.com.