SCIS 2012 The 29th Symposium on Cryptography and Information Security
Kanazawa, Japan, Jan. 30- Feb. 2, 2012
The Institute of Electronics, Information and Communication Engineers

Design and Implementation of Digital Forensic Systems

楊中皇(Chung-Huang Yang)* 楊波(Bo Yang)†

Abstract: As popularity of the Internet continues to grow, it changes the way of computer crime. Number of computer crime increases dramatically in recent years and investigators have been facing the difficulty of admissibility of digital evidence. To solve this problem, we must collect evidence by digital forensic techniques and analyze the digital evidence. In this research, we design and implement computer forensic systems which integrate several open source digital forensic tools and come with a user-friendly environment for investigators. To avoid evidence loss due to shutdown of target hosts, we use the live analysis technique to collect volatile data with executing commands from an external USB. We also create a live DVD/USB so that target hosts can boot from the DVD/USB which contains a functional operating system with tools for forensic discovery. Finally, we extend our works to create forensic systems for the Android mobile phones.

Keywords: Digital Forensics, Computer Forensics, Digital Evidence, Smartphone Forensics, Cybercrime

1 Introduction

The Internet is the most popular application in modern society. It brings a lot of convenience of communication to human. On the other hand, due to its rapid development and lacking of proper regulations, the Internet happened to be crime breeding. The most serious problem of the Internet is cybercrime. But there are extremely distinct difference between in computer criminal offense and traditional crime action, so the investigator inquiring into computer crime must have the aid of the computer forensics knowledge and techniques.

The digital evidence is a series of binary digit numbers on transmission, or stored information files on the electronic device [5]. Moreover, file formats of digital evidence include audio, video, images, and digital data, 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, and cannot be understood directly without technical process. The four-way linkage theory [14] explains the interrelations between a crime scene, a victim, a suspect, and (digital) evidence, shown in Fig. 1. The more associations (between two or more of these component) established, the greater the probability if successfully solving the (cybercrime) case.

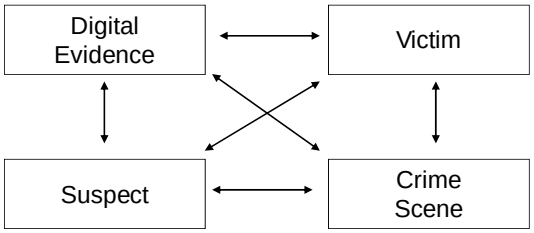

Figure 1: Four-way linkage theory

During an cybercrime investigation, the procedures must be performed according to a scientific procedure in order to have legal effect of digital evidence [9].

* 高雄師範大學 National Kaohsiung Normal University, 116, Ho Ping First Road, Kaohsiung 802, Taiwan. Email: chyang@nknucc.nknu.edu.tw
† School of Computer Science, 陝西師範大學 Shaanxi Normal University, 199 South Chang'an Road, Xi'an, 710062, PR China. Email: byang@snnu.edu.cn

2 Digital Forensics

Digital forensics 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 [5, 10]. 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. Computer Forensics can be performed in six distinct phases of identification, collection, acquisition, preservation, analysis, and presentation [12, 13], illustrated in Figure 2.

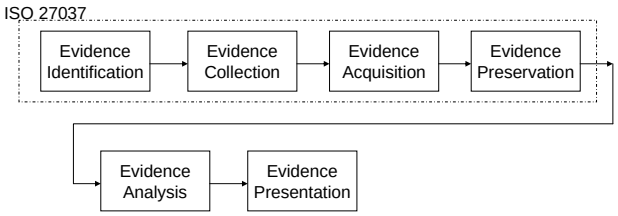

Figure 2: The phases of digital forensics

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

(1) Evidence Identification: This phase searches for the potential digital evidence.

(2) Evidence Collection: This phase involves the gathering the physical items that contain potential digital evidence.

(3) Evidence acquisition: This process involving creating a copy of data within a defined set. For example, we usually used the forensic tools to create an image the disk.

(4) 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 [16], to ensure that digital data obtained in a digital crime scene did not alter in the later analysis.

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

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

Digital evidence is 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 [5, 19]. 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 [9]. Most of these popular 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 [19]:

(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 after the suspect system is shut down. 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. [17].

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].

3 Forensic Tools and Live CDs

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 [6, 9]: FTK, EnCase, SMART, PyFlag and The Sleuth Kit (TSK), etc. There are several 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.

One-way hash function is widely used during preservation of digital evidence. However, as was known recently that the hash function MD5 is insecure and SHA-1 is less secure than was expected [7], this is one of our research motivations to revise the hash function used on forensic tool. Our new forensic tools will come with NIST (National Institute of Standards and Technology) recommended SHA-256 hash function [16].

Live CD is a kind of operation system distribution which can be booting from a read-only medium, such as a CD-ROM or DVD, without actually installing into hard disk[15, 18]. Usually, it was named depending on what media it stores. Consequently, it is named Live DVD because its media is DVD-ROM, and so does Live USB. Currently, there are many Live CD released, such as Knoppix, Fedora Live CD, Tux2live, etc. There are also Live CDs for forensics, such as Helix (http://www.e-fense.com) or caine (http://www.caine-live.net/).

We setup our forensics system into both Live DVD and Live USB so that it becomes portable, and can be easily deployed even moving to different environment, such as Windows-based PCs or Linux-based PCs, etc.

4 The Proposed Computer Forensic System

In this research, we classify the victim machine into two types, one for which the computer system is still functioning while the other has been powered off or cannot reboot. We write a script program and store it on the USB. If the system is still running then we perform the live-analysis with the script program, which will collect the volatile information of system and then store those generated files into the USB disk automatically.

If the target computer is powered off, then we will reboot the machine by the proposed Live DVD/USB and make an image file of disk. Our proprietary Live DVD/USB contains AIR disk image file producer (http://air-imager.sourceforge.net/), The Sleuth Kit forensics program (http://www.sleuthkit.org/), the Autopsy program of graphical interface, etc. System forensics process of the proposed system is shown in Figure 3.

If the target machine is still active when investigator arrived at the crime scene, he/she should collect the volatile information of victim of system rapidly, include which TCP and UDP ports are opened, user login history, services that are activated, etc. These volatile information will be disappeared from target computer after being shut down. The proposed system uses self-developed script program on USB (we will assume that target system is running Linux operating system and has a USB port with proper device driver) to collect volatile information, as illustrated on Figure 3.

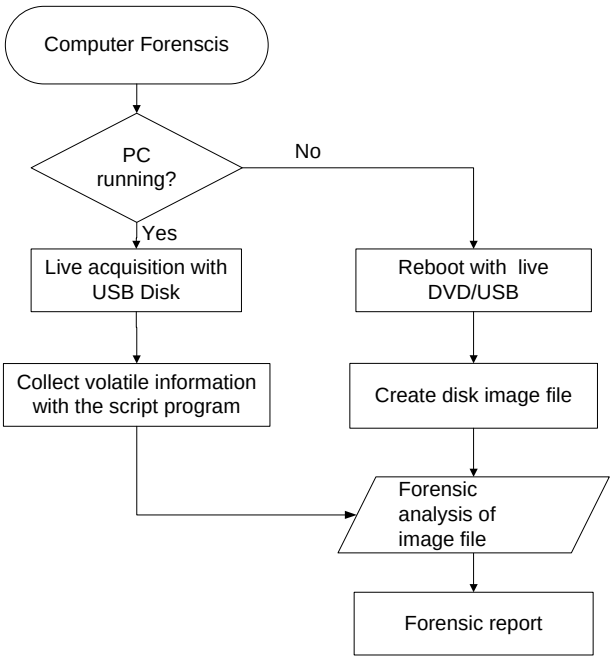

Figure 3: The proposed computer forensics system

Besides a script program to collect volatile information of system on the USB, our system also provides graphical user interface using Xdialog (http://xdialog.free.fr/) to show forensic results. Live-analysis results will provide target machine information of kernel version, CPU type, hostname, date and time. Other volatile information includes recently-executed commands, network connections, current processes, who is logged on, ..., etc.

We reboot target system by Live DVD (or live USB) to perform dead-analysis of digital forensics. The proposed dead analysis forensics system has already made available for public download of DVD image file, http://security.nknu.edu.tw/download/computer_forensics.iso

Our Live DVD/USB includes software of AIR to create an image file of disk and Chinese locale support on The Sleuth Kit (TSK) and Autopsy. An image of disk on target machine can be created by AIR (Automated Image & Restore). It is a GUI front-end to perform linux dd command and can easily

create a forensic disk. Besides AIR, our DVD also contain Guymager (http://guymager.sourceforge.net/) for creating a disk image file, and calculate and verify hash value of the file.

With a disk image, we could then do forensic analysis. Our forensic DVD contains several tools, such as Autopsy (http://www.sleuthkit.org/autopsy/), SFDumper (http://sfdumper.sourceforge.net/), Scalpel (http://www.digitalforensicssolutions.com/Scalpel/), Fundl (http://sfdumper.sourceforge.net/fundl.htm), ddrescure (http://www.gnu.org/software/ddrescue/ddrescue.html), ..., etc.

The forensic analysis of the image disk can be performed by TSK and Autopsy, which provide several analysis functions, including file content, keyword, metadata, file type, etc. Final forensic report of the proposed system is access by using a Web browser.

5 Android Forensics

Android [2, 8] is an open source operating system for smart phones or digital devices, which is based on Linux operating system. In recent years, several forensic tools [3, 11] 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 sources:

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

(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.

The proposed approach 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 4 illustrates the flowchart of our 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 (e.g., Autopsy, http://www.sleuthkit.org/autopsy/) on the computer.

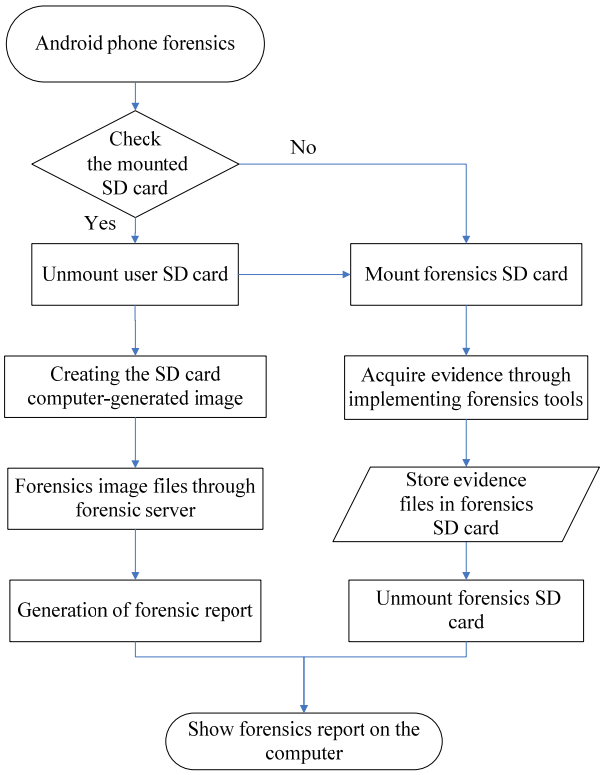

Figure 4: System flowchart of the Android forensics with memory card

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.

Using Android API (Application Programming Interface), we developed forensic software collects digital evidence data included SIM card status, SIM card vendors, SIM card number. Our forensic software was developed with the Android SDK and tested on the 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.

6 Conclusions

In recent years, there are more and more cases of computer crime and the term hacking is no longer a news. Therefore, investigator must collect digital evidence of suspect computer after an incident is occurred. However, most existing digital forensics software are commercial version which are expensive and might not provide up to date forensic software for the fast changing smartphones..

In this research, we developed a new forensic system based on several open source software to reduce cost and we enhance autopsy's graphic interface with the Traditional Chinese language. We created a live DVD/USB for analyzing Microsoft Windows and Unix/Linux file systems (dead analysis). Additionally, we collected the volatile information of system by using live-analysis, which avoid lost of data due to showdown of machine.

We also designed and implemented forensics systems for the Android phones based on memory card. Our design followed on NIST SP 800-101 guidelines on forensics process and our forensic software was written with Java language for gathering evidence from the suspect smart phone.

References

[1] F. Adelstein, "Live forensics: diagnosing your system without killing it first," Communications of the ACM, Vol. 49, No. 2, pp. 63-66, 2006.

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

[6] 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.

[7] Q. Dang, Recommendation for Applications Using Approved Hash Algorithms, NIST Special Publication 800-107, 2009.

[8] L. Darcey and S. Conder, *Sams Teach Yourself Android Application Development in 24 Hours*, Sam Publishing, 2010.

[9] L. Garber, "Computer Forensics: High-Tech Law Enforcement," *IEEE Computer*, Vol. 34, No. 1, pp. 202-205, 2001.

[10] S. Garfinkel, "Digital Forensics Research: The Next 10 Years," *Digital Investigation*, Vol. 7, pp. S64-S73, 2010.

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

[12] ISO/IEC 27037. Guidelines for identification, collection, acquisition and preservation of digital evidence, Draft International Standard, 2011.

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

[14] H. C. Lee, T. Palmbach, and M. T. Miller, *Henry Lee's Crime Scene Handbook*, Academic Press, 2001.

[15] C. Negus, *Live Linux CDs: Building and Customizing Bootable*, Prentice Hall PTR, 2007.

[16] NIST, Secure Hash Standard (SHS), NIST PUB 180-3, October 2008.

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

[18] K. Rankin, *Knoppix Hacks*, O'Reilly, 2004.

[19] L. Volonino, R. Anzaldua, and J. Godwin, *Computer Forensics: Principles and Practice*, Prentice Hall, 2006.