Fast Deployment of Computer Forensics with USBs

Chung-Huang Yang
National Kaohsiung Normal University
Kaohsiung, Taiwan
chyang@computer.org
http://www.crypto.idv.tw/

Pei-Hua Yen
R&D Division
Chimei Innolux Corp.
Jhunan Science Park, Taiwan
amber8520@gmail.com

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 forensics techniques and analyze the digital data, or recover the damaged data.**

In this research, we integrate several open source digital forensics tools and create a graphic user interface to develop 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 USB so that target hosts can boot from the USB which contains a functional operating system with tools for forensic discovery.

Keywords- Digital Forensics, Computer Forensics, Digital Evidence, Live Analysis, Live USB

I. 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.

Digital evidence has the following characteristics [4]: easily to copy or modify, difficult to confirm the source and integrity, and cannot directly to understand its contents, etc. During an investigation, the procedures must be performed according to the International Organization of Computer Evidence (IOCE) Procedure “The Good Practice Guide for Computer-Based Evidence” in order to have legal effect of digital evidence [8].

II. DIGITAL FORENSICS

Digital forensics is the science of obtaining, preserving and documenting evidence from electronic media, such as tablet PC, server, digital camera, PDA, fax machine, iPod, smart phone and various memory storage devices [16]. Generally speaking, the purpose of digital forensic is to investigate the evidence and might include computer intrusion, unauthorized access, child pornography, etc. Fundamentals of computer forensics analysis process as falling into three distinct areas acquisition, analysis, and presentation [2]. We give a brief description of those procedures:

(1) Acquisition Phase: This phase is focus on the obtaining the states of systems that have storage devices and all the digital data for later analysis. We usually used the forensic tools to create an image the disk.

(2) Analysis Phase: Identification of the evidences we have collected, which include file types, contexts of directory and rescue data for find the related between evidence and incident.

(3) Presentation Phase: Documentation of analyzing data for assist the prosecutors to reference.

At present, the analysis of digital evidence must depend on the forensics tools such as Forensic Toolkit (FTK) [6] of EnCase [7]. Most of them are commercial software and are too expensive for the small enterprises or individual.

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 [3, 16]. Digital information is fragile in that it can be easily modified, duplicated, restored or destroyed, etc [10].

In the course of the investigation, the investigator should assure that digital evidence is not modified without proper authorization [9]. 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 [16]:

(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

978-0-7695-4236-2/10 $26.00 © 2010 IEEE
DOI 10.1109/BWCCA.2010.106

might include hardware information, installed software packages, process states, ..., etc [13].

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 [2].

III. Forensic Tools and live CDs

A. Forensic Tools

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, 7, 16]: FTK, EnCase, SMART, PyFlag and The Sleuth Kit, etc.

In Table 1, we give a brief comparison of some of well-known forensic tools. 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-recommended SHA-256 hash function.

TABLE I. Existing Digital Forensic Tools

	EnCase	FTK	TSK
Internationalization	English or Traditional Chinese	English or Simple Chinese	English
User friendliness	Training is needed	Ease of use	Ease of use
Disk Image file	Support	Support	Support
Hash Functions	MD5	MD5	MD5 and SHA-1
Cost	Commercial, Expensive	Commercial, Expensive	Open source software

B. Live CDs

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 [11]. 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 [14], Fedora Live CD [13], Tux2live [15], etc. There are also Live CDs for computer forensics, such as Helix (http://www.e-fense.com) or caine (http://www.caine-live.net/).

We setup our forensics system into Live DVD/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).

IV. The proposed forensic system

A. System Architecture

In this study, we classify the victim machine into two types, one for which the computer system is still functioning while the other has been shut down 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. We show the live-analysis results with Tkinter and Xdioalog.

If the target computer is turned off, then we will reboot the machine by Live DVD/USB and make an image file of disk. Our proprietary Live DVD/USB contains a disk image file producer - AIR (Automated Image and Restore, http://air-imager.sourceforge.net/), a computer forensics program - The Sleuth Kit (TSK, http://www.sleuthkit.org/), Autopsy program of graphical interface, etc. System forensics process of the proposed system is shown in Fig. 1

B. Implementation of Live-Analysis

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 Fig. 2.

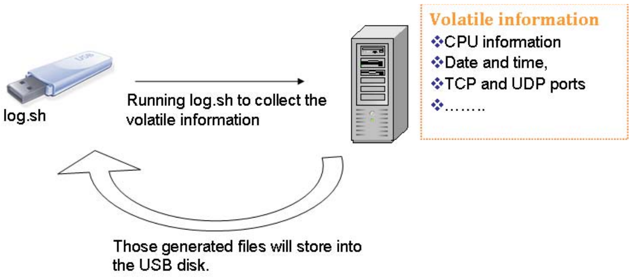
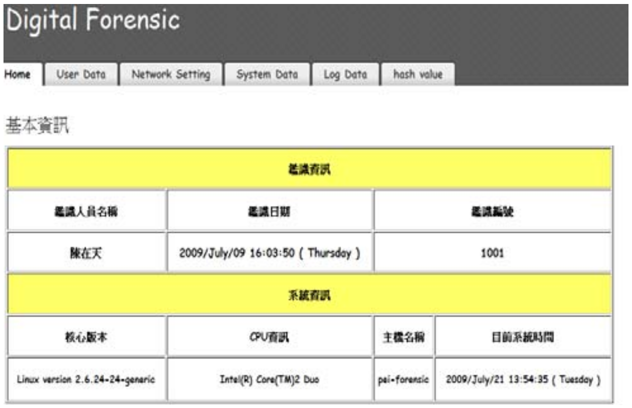

log.sh
Running log.sh to collect the volatile information
Volatile information
❖CPU information
❖Date and time,
❖TCP and UDP ports
❖........
Those generated files will store into the USB disk.

Figure 2. Live-Analysis in the Proposed 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. Fig. 3 shows one of the forensic results on performing Live-analysis, it shows 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.



基本資訊

鑑識資訊			
鑑識人員名稱	鑑識日期	鑑識編號	
陳在天	2009/July/09 16:03:50 (Thursday)	1001	
系統資訊			
核心版本	CPU資訊	主機名稱	目前系統時間
Linux version 2.6.24-24-generic	Intel(R) Core(TM)2 Duo	pei-forensic	2009/July/21 13:54:35 (Tuesday)

Figure 3. Live-Analysis Result

C. Implementation of Dead-Analysis

We reboot target system by Live USB (or live DVD) to perform dead-analysis of digital forensics. Our Live DVD/USB includes software of AIR (Automated Image and Restore) to create an image file of disk and Chinese locale support on TSK and Autopsy.

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

After booting from the DVE, desktop environment is as shown in Fig. 4. Upper right corner is the forensic tools. Investigator could create a disk image of target machine, analyze the disk image, and create a forensic report.

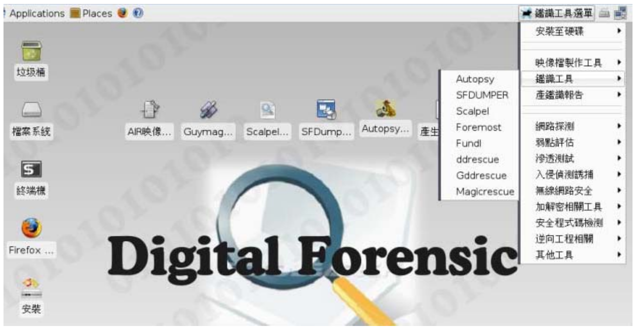
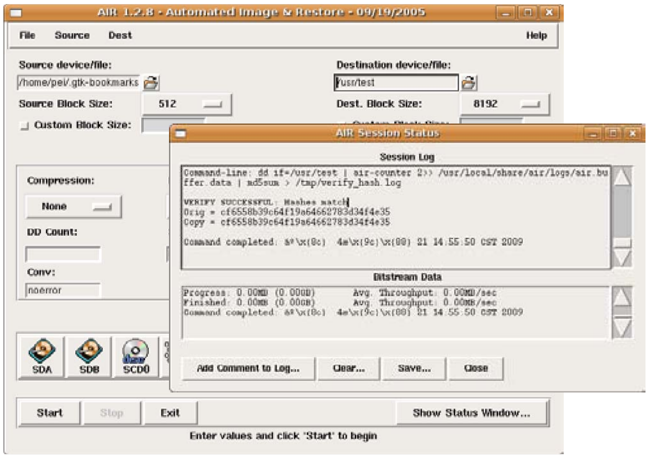


Figure 4. Main Forensic Functions on Dead-Analysis

An image of disk on target machine can be created by AIR (Automated Image & Restore), as shown in Fig. 5. 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 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), ddrescue (http://www.gnu.org/software/ddrescue/ddrescue.html), ..., etc.



Source device/file: /home/pei/.gtk-bookmarks

Destination device/file: /usr/test

Source Block Size: 512

Dest. Block Size: 8192

Compression: None

DD Count:

Conv: noerror

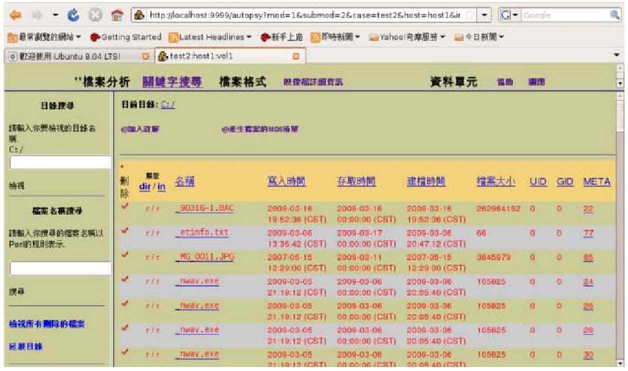
```
Command-line: dd if=/usr/test | air-counter 2>> /usr/local/share/air/logs/air.bu
ffer.data | md5sum > /tmp/verify_hash.log

VERIFY SUCCESSFUL: Hashes match
Orig = cf6558b39c64f19a64662783d34f4e35
Copy = cf6558b39c64f19a64662783d34f4e35

Command completed: 星\x(8c)  4e\x(9c)\x(80) 21 14:55:50 CST 2009
```

```
Progress: 0.00MB (0.000B)        Avg. Throughput: 0.00MB/sec
Finished: 0.00MB (0.00GB)        Avg. Throughput: 0.00MB/sec
Command completed: 星\x(8c)  4e\x(9c)\x(80) 21 14:55:50 CST 2009
```

Figure 5. Live-Analysis Menu

Fig. 6 shows the analysis of the image disk by TSK and Autopsy, which provide several analysis functions, including file content, keyword, metadata, file type, etc.

Final forensic report is access by using a Web browser.



刪除	類型 dir / in	名稱	寫入時間	存取時間	建檔時間	檔案大小	UID	GID	META
✓	r / r	_90316-1.BAC	2009-03-16 19:52:36 (CST)	2009-03-16 00:00:00 (CST)	2009-03-16 19:52:36 (CST)	262984192	0	0	22
✓	r / r	_etinfo.txt	2009-03-06 13:36:42 (CST)	2009-03-17 00:00:00 (CST)	2009-03-06 20:47:12 (CST)	66	0	0	77
✓	r / r	_MG_0011.JPG	2007-05-15 12:29:00 (CST)	2009-03-11 00:00:00 (CST)	2007-05-15 12:29:00 (CST)	3845979	0	0	85
✓	r / r	_nwav.exe	2009-03-05 21:19:12 (CST)	2009-03-06 00:00:00 (CST)	2009-03-06 20:05:40 (CST)	105825	0	0	24
✓	r / r	_nwav.exe	2009-03-05 21:19:12 (CST)	2009-03-06 00:00:00 (CST)	2009-03-06 20:05:40 (CST)	105825	0	0	26
✓	r / r	_nwav.exe	2009-03-05 21:19:12 (CST)	2009-03-06 00:00:00 (CST)	2009-03-06 20:05:40 (CST)	105825	0	0	28
✓	r / r	_nwav.exe	2009-03-05 21:19:12 (CST)	2009-03-06 00:00:00 (CST)	2009-03-06 20:05:40 (CST)	105825	0	0	30

Figure 6. TSK and Autopsy

V. 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 target computer after an incident is occurred. However, most existing digital forensics software are commercial version which are expensive and only support English version.

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.

ACKNOWLEDGMENT

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

REFERENCES

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

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

[3] E. Casey, T. Larson, and M. M. Ferraro, Digital Evidence and Computer Crime, Elsevier Science & Technology Books, 2003.

[4] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computer and the Inter, Academic Press, 2000, pp.41-46.

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

[6] B. Carrier, TSK & Autopsy, http://www.sleuthkit.org/autopsy/

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

[8] L. Garber, “EnCase: A Case Study in Computer-Forensic Technology,” IEEE Computer Magazine, January 2001, pp. 202-205.

[9] IOCE, " Guidelines for Best Practice in the Forensic Examination of Digital Technology ," http://www.ioce.org/fileadmin/user_upload/ 2002/ioce_bp_exam_digit_tech.html

[10] C. E. Landwehr, “Computer security,” International Journal of Information Security, 2001, pp. 3–13.

[11] S. Mocas, "Building theoretical underpinnings for digital forensics research," Digital Investigation, Volume 1, Issue 1, February 2004, pp. 61-68.

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

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

[14] R. Petersen, Fedora Core 7 & Red Hat Enterprise Linux, McGraw-Hill Professional, 2007.

[15] K. Rankin, Knoppix hacks, O’Reilly, 2004.

[16] Tux2live Project, https://tux.nchc.org.tw/trac/tux2live/

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

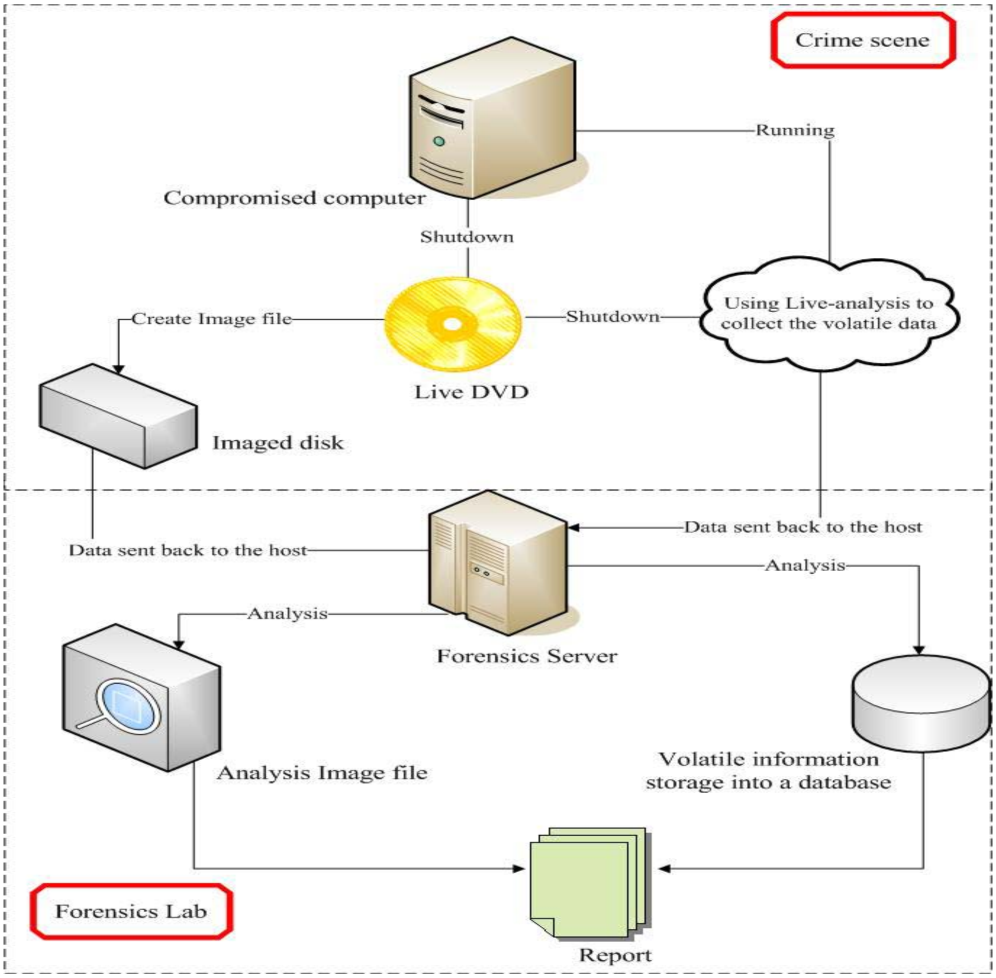


Figure 1. Operations of the Proposed Forensics System.