New Model for Cyber Crime Investigation Procedure

Yong-Dal Shin*

*Dept. of IT & Cyber Police, Youngdong University, Rep. of Korea
ydshin@youngdong.ac.kr
doi:10.4156/jnit.vol2.issue2.1

Abstract

In this paper, we presented a new model for cyber crime investigation procedure which is as follows: readiness phase, consulting with profiler, cyber crime classification and investigation priority decision, damaged cyber crime scene investigation, analysis by crime profiler, suspects tracking, injurer cyber crime scene investigation, suspect summon, cyber crime logical reconstruction, writing report.

Keywords: Computer Forensics, Cyber Investigation, Cyber Crime

1. Introduction

Computer forensics emerged in response to the escalation of crimes committed by the use of computer systems either as an object of crime, an instrument used to commit a crime or a repository of evidence related to a crime. Computer forensics can be traced back to as early as 1984 when the FBI laboratory and order law enforcement agencies begun developing programs to examine computer evidence.

Digital forensics has been defined as the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be crime or helping to anticipate the unauthorized actions shown to be disruptive to planned operations. Digital evidence includes computer evidence, digital audio, digital video, cell phones, digital fax machines etc.

The U.S. Department of Justice published a process model in the Electronic Crime Scene Investigation: A guide to first responders that consists of four phases: collection, examination, analysis, reporting. The analysis phase of this model is improperly defined and ambiguous.


In this paper, we presented a new model for cyber crime investigation procedure. The proposed procedure model is as follows readiness phase, consulting with profiler, cyber crime classification and investigation priority decision, damaged cyber crime scene investigation, analysis by crime profiler, suspects tracking, injurer cyber crime scene investigation, suspect summon, cyber crime logical reconstruction, writing report. This paper presented a new methodology of a digital forensic investigation procedure.

Section 2 shows previous cyber crime investigation model. We present our method for cyber crime investigation procedure model in section 3.

2. Previous cyber crime investigation model

The response procedure of the system and network intrusion incidents was researched by Brian Carrier[5], Chris Prosise [6], electronic crime scene investigation guide [7], J. L. Shin [2], Lee [4], Baryamureeba [17], and Y. D. Shin[18].

Brian Carrier [5] proposed integrated digital investigation process. The paper was consisted of 5 phase like readiness phase, deployment phase, physical crime scene investigation phase, cyber crime
scene investigation phase, review phase. The procedure didn’t include which classifying cyber crime and deciding investigation priority, psychological profiling investigation method, and so on.

3. The proposed a new model for cyber crime investigation procedure

The presented a new model for cyber crime investigation procedure is as follows: readiness phase, consulting with profiler, cyber crime classification and investigation priority decision, damaged cyber crime scene investigation, analysis by crime profiler, suspects tracking, injurer cyber crime scene investigation, suspect summon, cyber crime logical reconstruction, writing report. Figure 1 is a block diagram of the proposed cyber crime investigation procedure model. For more information regarding the investigation procedures are as follows.

3.1. Readiness phase

Cyber crime investigators begin crime investigation, after the incident report received or detected related cyber crime, The goal of the readiness phase is to ensure that the operations and infrastructure are able to fully support an investigation [5]. The readiness phase of the computer forensics can reduce a waste of investigation time and prevent trial and error of crime investigation. The readiness phase becomes important role to investigate systematically.

The operations of this phase provide training and equipment for the personal that will be involved with the incident and its investigation. This includes training the responders, the lab analyst, and staff that will be receiving the initial reports of the incident [5].

3.2. Consulting with crime profiler

Crime profiling is psychological science to know the nature of crime suspects based on information collected from the crime scene. The crime profiler can reduce the cyber investigators' scope of the investigation. Also, the profiler can provide clues for cyber crime. The profiling data can solve a lot of crime, can reduce time and cost of the investigation.

3.3. Cyber crime classification and investigation priority decision

After cyber crime detected or received, the cyber crime investigators refer to crime profiling data and classifying cyber crime as violence or non-violence to consult with victims by the phone and confirmed scene of the cyber crime simply by internet.

3.3.1. Cyber crime classification

In order to investigate the digital-related crime report, we classify by type of cyber crime. We investigate depending on the type of crime. The cyber crime classify as violence and non-violence. The violence crime includes cyber terror, cyber threat, cyber stalking, child pornography. The non-violence crime includes cyber attacks, cyber-theft, cyber scam, internet gambling [16]. The investigators are assigned by classifying cyber crime to fit in investigators’ cyber crime major.

3.3.2. Investigation priority decision

Currently, cyber crimes and digital-related crimes are increasing. Therefore, cyber crime investigators are difficult for the investigation the order in which they are received. We decide investigation priority in order to investigate cyber crime effectively. It reduces investigation personnel, equipment, time and the cost of the investigation.
3.4. Damaged (victim) cyber crime scene investigation

Cyber crime investigators collect digital evidences in the damaged cyber crime scene. Cyber crime investigators investigate in the damaged (victim) cyber crime scene as 3.4.1, 3.4.2, 3.4.3, 3.4.4, 3.4.5, 3.4.6.

3.4.1. Damaged (victim) scene protection using police line
At this stage, cyber crime investigators establish "police line" to protect evidence of damaged cyber crime scene.

3.4.2. Set cyber crime evidence collection equipments
Cyber crime investigators set cyber crime evidences collection equipments such as encase, imaging devices in the victim scenes.
3.4.3. Photo evidences by digital or video camera

Cyber crime investigators photo evidences by digital or video camera to obtain evidences in the victims scenes.

3.4.4. Volatile evidences collection and analysis

Volatile information evidence is recorded in the main memory or temporary file of the hard disk. The volatile evidence will be lost when the damaged computer system is shutdown. Therefore, we must collect volatile evidence using program for examining processes, system state in live computer system [3]. We analyze the collected volatile evidence.

Order of volatile from RFC3227 is as follows: registers, cache, routing table, arp cache, process table, memory, temporary file systems, disk, remote logging and monitoring data that is relevant to the system in question, physical configuration, network topology, archival media [3][9].

We must document and photography to record the evidence of the damaged scene.

There are tools like userdump [8], Encase FIM [13], Encase Enterprise [13], Road Masster III [12] to collect volatile evidence of live computer system.

3.4.5. Obtain the evidences of storage media

Digital evidences of storage media which hard disk, zip disk, floppy disk, USB memory must preserve integrity. Storage media has a threat of evidence modification or deletion, if it was linked to analysis system directly [3]. In order to prevent this threat, we use storage imaging method. The storage imaging method in digital evidence collection process is [3][16]. Disk forensics includes imaging by bit stream clone, creating hash and checksum value, recovering deleted data of storage media, decrypting password of files [1].

There are equipments (tools) for disk forensics which called King Demi AS [11], Encase [13], Road masster III [12].

The investigators seize to examine auxiliary storage media (for example, hard disk, zip disk, floppy disk, USB memory) in depth. They must transfer safely auxiliary storage media which have seized to superior offices to examine evidence deeply.

3.4.6. Obtain the evidences of network [10][15]

Evidence collection of computer network is the act of capturing, recording, analyzing network audit trails in order to discover the source of security breaches or other information assurance problems. Not all the information captured or recorded will be useful for analysis.

Network forensic systems are mainly classified as "Catch it as you can" and "Stop, look and listen" systems. Most network forensic systems are based on audit trails.

Network forensics products are sometimes known as Network Forensic Analysis Tools (NFATs). For example, nstreams, slogdump, tcpflow, chaosreader, dhcpdump, etc.

3.5. Analysis by profiler

Crime profiling is psychological science to know the nature of crime suspects based on information collected from the crime scene. An analysis by crime profiler can reduce the cyber investigators' scope of the investigation. Also, the profiler can provide clues for cyber crime. The profiling data can solve a lot of crime, can reduce time and cost of the crime investigation [16].

3.6. Suspects tracking

The investigators trace to the suspect and crime scene based on the evidence collected from suspect's game ID, E-mail ID, IP address, MAC address which obtained damaged cyber crime scene.
3.7. Injurer cyber crime scene investigation

Injurer cyber crime scene investigation is similar to investigating damaged cyber crime scene. It includes as follows: Investigating injurer cyber crime scene, eye-witness testimony and the evidence capture, and volatile evidence collection and analysis, disk forensic, network forensic, inviting external experts. Cyber crime investigators investigate in the injurer cyber crime scene as 3.7.1, 3.7.2, 3.7.3, 3.7.4, 3.7.5, 3.7.6, 3.7.7.

3.7.1. Injurer scene protection using police line

At this stage, cyber crime investigators establish "police line" to protect evidence of injurer cyber crime scene.

3.7.2. Set cyber crime evidence collection equipments

Cyber crime investigators set cyber crime evidences collection equipments such as encase, imaging devices in the injurer scenes.

3.7.3. Photo evidences by digital or video camera

Cyber crime investigators photo evidences by digital or video camera to obtain evidences in the injurer scenes.

3.7.4. Volatile evidences collection and analysis

Volatile information evidence is recorded in main memory or temporary file on hard disk. The volatile evidence will be lost when the injurer computer system is shutdown. Therefore, we must collect volatile evidence using program for examining processes, system state in live computer system [3]. We analyze the collected volatile evidence.

Order of volatile from RFC3227 is as follows: registers, cache, routing table, arp cache, process table, memory, temporary file systems, disk, remote logging and monitoring data that is relevant to the system in question, physical configuration, network topology, archival media [3][9].

We must document and photographing to record the evidence of the injurer scene.

There are tools like userdump [8], Encase FIM [13], Encase Enterprise [13], Road Masster III [12] to collect volatile evidence of live computer system.

3.7.5. Obtain evidences of storage media

Digital evidences of storage media which hard disk, zip disk, floppy disk, USB memory must preserve integrity. The storage media have threat of evidence modification or deletion, if they were linked to analysis system directly [3]. In order to prevent this threat, we do imaging of the storage media. In the digital evidence collection process, imaging method of the storage media is [3]. Disk forensics include imaging by bit stream clone, creating hash and checksum value, recovering deleted data of storage media, decrypting password of files [1].

There are equipments (tools) for disk forensic which called King Demi AS [11], Encase [13], Road masster III [12].

The investigators seize to examine auxiliary storage media (for example, hard disk, zip disk, floppy disk, USB memory) in depth. They must transfer safely auxiliary storage media which have seized to superior offices to examine evidence deeply.
New Model for Cyber Crime Investigation Procedure

Yong-Dal Shin

Journal of Next Generation Information Technology. Volume 2, Number 2, May 2011

3.7.6. Obtain evidences of the network

Evidence collection of computer network is the act of capturing, recording, analyzing network audit trails in order to discover the source of security breaches.

Network forensics products are sometimes known as Network Forensic Analysis Tools (NFATs). For example, nstreams, slogdump, tcpflow, chaosreader, dhcpdump, etc.

3.7.7. Obtain evidences of printers

There are evidences of the printer in the injurer printer. So, cyber investigators collect evidences of the printers.

3.8. Suspects summon

The investigators summon suspect based on evidence which collected the damaged and injurer cyber crime scene investigation.

3.9. Cyber crime logical reconstruction

Cyber crime investigators reconstruct cyber crime investigation result logically using cyber crime classification and investigation priority decision, damaged cyber crime scene investigation, analysis by crime profiler, suspects tracking, injurer cyber crime scene investigation, suspect summon. The logical reconstruction of the cyber crime can check the result of investigation.

3.10. Writing report

The writing report is the process of submitting case reporting to the court relating to evidence collect, preserve, analyze of the case. The report must write easily, because judges don't know about cyber crime specific digital forensic technique well.

4. Conclusion

In this paper, we presented a new model for cyber crime investigation procedure. The proposed procedure model is as follows: readiness phase, consulting with profiler, cyber crime classification and investigation priority decision, damaged cyber crime scene investigation, analysis by crime profiler, suspects tracking, injurer cyber crime scene investigation, suspect summon, cyber crime logical reconstruction, writing report. This paper presented a new methodology of a cyber crime investigation procedure. If the investigators apply to the actual investigation, the presented procedure will be effective.

5. References