A Stable Evidence Collection Procedure of a Volatile Data in Research

Yong-Ho Kim, Dong Hwi Lee, and Kuinam J. Kim*

Dept. of Information Security Kyonggi University
Porsche0911@paran.com, dhclub@naver.com
harap123@daum.net

Abstract. I would like to explain a method how to get important data from a volatile data securely, when we are not available to use network in computer system by incident. The main idea is that the first investigator who collects a volatile data by applying scripts built in USB media should be in crime scene at the time. In according to volatile data, he generates hash value, and gets witness signature. After that, he analyses the volatile data with authentication in forensics system.

Keywords: Digital Forensics, Digital Evidence, Information Security.

1 Introduction

Although we do not know since when, computers and digital media have been essential parts of daily life.

As technically sophisticated crime that uses digital media increases, procedures that prove integrity of hard disk data or digital evidence from computer systems related to crime and process the data are needed urgently.

In this thesis, cases in procedural law and volatile evidence handling process are examined, and a new alternative plan is presented by analyzing our current volatile evidence handling process and its problems.

2 Related Work

2.1 Definition of Evidence

In SWGDE/IOCE standards, computer crime evidence is classified into three groups as shown in Table 1.

Digital evidence can be divided into original digital evidence and its copies.

Documented evidence can also be divided into demonstrative and documentary evidence.

Demonstrative evidence is evidence needed to rebuild crime scenes or incidents. A jury can rebuild incidents by using various visual data such as graphs, charts, pictures, and models.

* Corresponding author.

O. Gervasi and M. Gavrilova (Eds.): ICCSA 2007, LNCS 4706, Part II, pp. 177–184, 2007.

Table 1. Classification of computer crime evidence

Class	Description
Digital Evidence	Crime information digitally stored or transmitted
Digital Object	Crime information related to physical items
Physical Item	Physical objects that stored or transmitted digital data

Documentary evidence is documents that form evidence. Many law specialists agree that digital evidence is more demonstrative than documentary [2].

It is because that the purpose of computer forensic areas is basically to rebuild crime scenes. However, these classifications depend on types of digital evidence related to specific crime.

Basically, documents to be presented should be intact and original unless there is a special reason. But the federal rules of evidence of the U.S. treat computer evidence differently. According to regulation 1001-3, “if data are stored in a computer or other similar devices, an output of the original data is also original.” The important thing here is that an evidence provider needs to prove his/her copy exactly reflects the original one. The evidence provider should show that the evidence has no error and has not been changed since its confiscation. If he/she cannot do this, the evidence is inadmissible in court

2.2 Evidence Selection Rules

There are some requirements for evidence admissible in court. Evidence should be qualified (reliable), related (able to prove facts of an incident), and material (able to prove subjects related to crime).

Besides, in the U.S., court system, only legally obtained evidence can be used. Therefore, evidence should be collected through search and attachment procedures specified by federal and provincial laws. Although evidence obtained by an illegal search proves that a defendant is guilty, the evidence is inadmissible.

This is called the exclusionary rule.

Precedents in some jurisdictions have established special rules for scientifically valid evidence. According to rule 402 in the federal rules of evidence, relevant evidence is generally admissible if it does not violate the U.S. constitution, statutory law and federal rules of evidence (Evidence obtained by violating a suspect's legal rights, for instance, is inadmissible).

Rule 401 defines relevant evidence as having "any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." This is called the relevancy test. The general acceptance test or Frye standard is anther standard applied to scientific evidence. According to this standard, scientific evidence is admissible at trial only if its scientific techniques are admissible as evidence [2].

3 Preserving Volatile Data

Volatile data is data temporarily stored in a system memory. It is because a memory stores data electrically. If the system's power supply fails, the data stored in the memory will be lost.

"Guidelines for Evidence Collection and Archiving," IEEE internet draft, suggests that the most volatile evidence should be collected first. It is because that the most volatile evidence can be lost most easily. The "volatility order" in the article is as follows [1]:

① Register and cache
② Routing table, ARP cache, process table, kernel statistics
③ System memory contents
④ Temporary file system
⑤ Disk data

Collecting volatile data creates a problem. The problem is that the procedure changes systems' states. Some specialists recommend to capture currently working process, network status, connection information and RAM data 'dump' and to document all the relevant operations and commands of investigators or crime scene technicians. These programs are stored in investigators' special forensic CDs to execute the same commands in a suspect's computer hard disk, and other programs and libraries in the hard disk should not be used.

3.1 Things That Should Be Avoided

Carelessness often damages evidence.

① Do not turn off the system until evidence collection is complete.
It will destroy many evidence materials, and an attacker may have a start/stop script to destroy the evidence.
② Do not trust programs in a system.
Use programs in a device protected for evidence collection (e.g. CD).
③ Do not use a program that changes file access time.

3.2 Chain of Custody

Every procedure to discover and handle evidence should be able to be clearly documented [1].

The following should be documented.

① Evidence is discovered and collected when, where and by whom.
② Evidence is handled and examined when, where, and by whom.
③ Evidence has been managed for what period and by whom and how it has been stored.
④ When the management changed and how it was transferred.

4 Integrity Verification Model for Volatile Evidence Collection

4.1 Problems of the Current Evidence Handling

So far integrity of a hard disk has been proved by creating bit-by-bit images, CRC values, and hash values for disk images or each file to prove the integrity of original data of disk images or individual file. To collect volatile data, we use the method that transmits images of volatile data and original data to a network in normal operation.

The network transmission method in volatile data collection is insufficient to verify if the integrity of volatile data has been kept during the collecting and transmitting processes or if the data has not been changed during transferring and other processes. If these problems occur in the current situation, the results will be disastrous.

The U.S. federal law defines that although evidence provides a fact clear enough to prove the guiltiness at trial, if the integrity or original data of the evidence has been damaged, it is invalid which is emphasizing the importance of data integrity. Even though you have analyzed and recovered data, the data will be invalid if you cannot prove the integrity and lawfulness of the data.

If so, how should we process ever changing network data or volatile data?

To find a solution, in this thesis, data are stored in script CDs or commonly used USB memory devices as files, and the integrity of the data is proved with hash values used as an integrity tool for original data in disk forensic science, and then a method is suggested to prove that evidence has not been changed by transmitting hash values to an authentication server synchronously with evidence collecting and presenting hash values acquired when the volatile data were stored as files.

4.2. Safe Volatile Evidence Collection and Integrity Verification

Impeccable volatile data acquisition procedure in Figure 1.

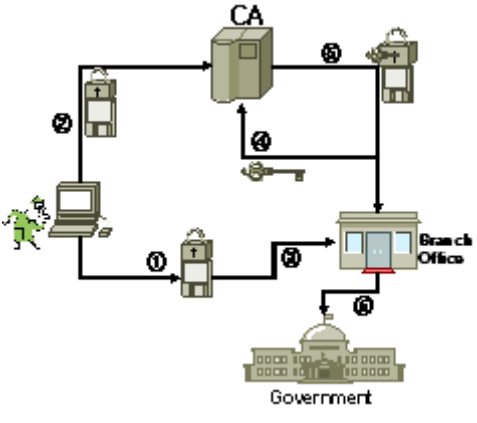

Fig. 1. Volatile data acquisition and verification procedure

An investigator arrives at a crime scene and checks evidence.

① When collecting volatile evidence, obtain commands for automated CD disks. (Create relevant data including the evidence collector name and search time as well as hash values.)

② After collecting volatile data, move to a safe place that offers network services.

③ Transmit the collector's information and hash values to an authentication server.

④ Authenticate the first collector and compare the corresponding hash values. (A certificate issued by an certification authority is used to authenticate a relevant person so that others cannot access the data.)

⑤ If the hash values of the compressed file is the same as the hash values of the presented evidence in integrity verification of the evidence, the integrity of the evidence is proved.

⑥ Present the evidence to a relevant institution

Figure 2 shows the flowchart of a volatile data acquisition procedure done by a scene investigator. The important thing here is to use an automated command CD which consists of scripts that execute commands automatically when you run the CD offering integrity and convenience to prevent errors due to poor initial evidence collection and lack of integrity. If the content of CD seems insufficient, it is

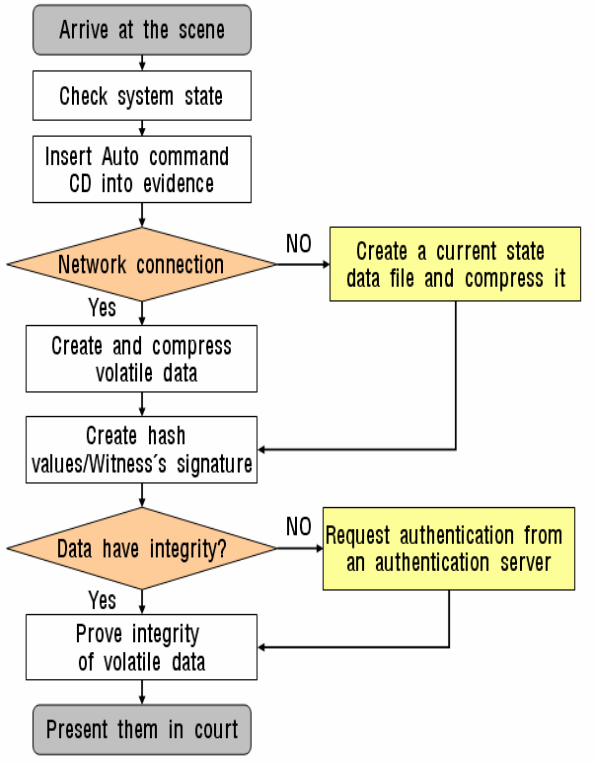

Fig. 2. Volatile data integrity acquisition and verification

recommended to contact a specialist to reproduce it in a CD or USB memory device according to circumstances. It is because it cannot deal with every system and incident although it is useful in many ways.

Floppy disks or USB memory devices can be used to store files created by commands in the CD, but we recommend USB memory types which are commonly used today. Floppy drives are not recommended because PCs in public places and notebook computers generally do not have floppy disk drives, but USB drives are available in most cases as they are mounted on mainboards.

Plus, another important thing to notice in the flowchart is that you should terminate the network connection when it is attacked by a hacker or malicious program. If the connection is terminated, important intrusion information and process data needed in backtracking will be lost. In this case, the first reporter and investigators should terminate the network connection carefully considering if the evidence can be collected only from the affected system or from any other systems.

Fig. 3. Evidence collection and confirmation screen

Figure 3 shows the configuration of results from the CD. Hash values are created automatically with results. We have many compressed files now. Those files should be extracted so that the hash values in them can be used to prepare documents containing creation date and time information of the volatile data, and the documents should be signed by witnesses. Witnesses' signatures are important as they will prove that volatile data were collected safely in CDs in the specified time and places. The documents include acquisition time of files, created hash values, and fields for signatures. They should be signed to prove the originality of data physically and logically and their integrity at the time of creation as well.

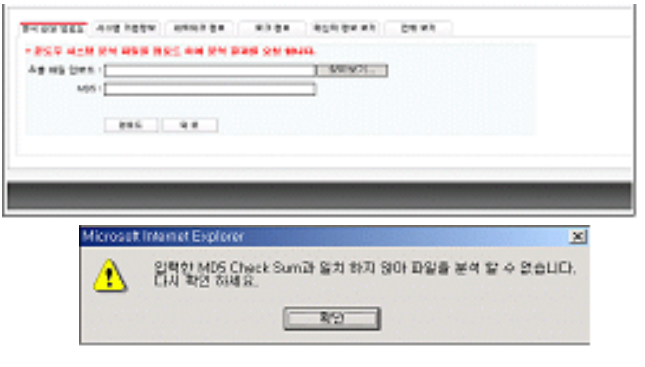

Fig. 4. Hash value authentication error screen of an authentication server

Contents of volatile data collection Although RFC 3227 defines main use of volatile data, there are a variety of scripts to extract exact volatile data for each document. We cannot apply a script to every case, but cannot create one for each case either. Therefore, we need to prepare one or two standard scripts to be used and create other ones for exceptions whenever they occur.

The standard scripts are created for Windows and Linux, and, first, prepare a Windows script as follows:

1. Content of a standard script for Windows

1) Abnormal network check
   ① Abnormal network connection check
   ② Abnormal network and mapping process check
   ③ Abnormal NetBIOS connection check

2) Abnormal process check

3) Abnormal service check

4) Autorun program in registry check

2. Content of a standard script for Linux

1) Collecting important setup file information

2) Collecting file vulnerability information

3) Collecting system log information

4) Collecting system memory information

In addition to these standard scripts, create scripts for other operating systems or special cases. CDs are specially used for command scripts to prevent omissions and errors which can be occurred by operators.

It is also a good idea to create scripts for each organization to deal with infringements not like the example scripts in this thesis. Volatile data should be handled with care as they can easily change, and all the precise data should also be

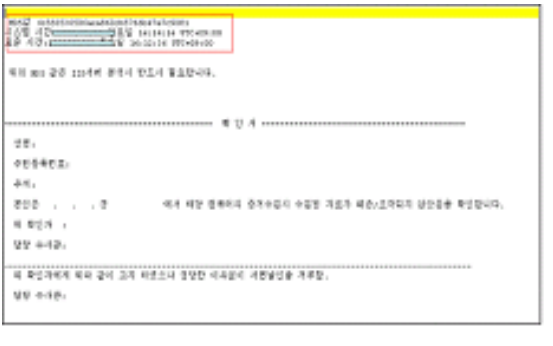

Fig. 5. Witness-form created with volatile data collection

collected at a time as you may not get permission from relevant people everytime you need. After collecting data, store them as compressed files and, along with their creation time, create hash values. Finally, print a one-page document that contains creation time, hash values, and a field, which is needed to be signed by an owner or relevant person. Data collectors should have signatures of relevant people. This document will be useful when court makes a request to prove the integrity of the data.

Figure 5 shows a certificate for a witness's final certification.

5 Conclusions

We have examined safe volatile evidence collection which maintains data integrity, online/offline evidence handling process, and acquisition of reliability. When a system does not provide network services, network transmission and authentication are impossible. In this case, it is needed to get to the source location to collect volatile data, and investigators use a standardized script CD rather than write one directly to acquire reliability and prevent arguments.

Therefore, it is desirable for investigators to collect volatile evidence from affected systems at scenes, and especially, in the case that written documents are considered important like in court, confirmation of owners or managers are required when collecting evidence.

For future work, we need to focus on processes that prove the integrity of volatile evidence and better evidence collection methods. And when creating scripts, active-type selectable scripts should also be considered to deal with various situations, however, law on digital crime should be established first to prevent confusion in investigation.

Acknowledgments. This work was supported by a grant from Security Engineering Research Center of Korea Ministry of Commerce, Industry and Energy.

References

1. RFC 3227 Guidelines for Evidence Collection and Archiving (2002)
2. scene of the cybercrime computer forensics handbook, Debra Littlejohn Shinder Ed tittel
3. Warren, G., Kruse II, J., Heiser, G.: COMPUTER FORENSICS: Incident response Essentials. Addison Wesley, Reading (2001)
4. Mandia, K., prosise, C., Pepe, M.: Incident response and computer forensics, 2nd edn.
5. Park, Y.-S., Oh, S.-M., Choi, Y.-R.: Design of Digital Evidence Collection Model for Integrated Forensics. In: KIAS2005 Conference, vol. 11 (2005)