Digitalevidence Integrated Management System

Hyun-Sang Kim*, Sang-Jin Lee*, Jong-in Lim*
n表彰@cist.korea.ac.kr, sangjin@korea.ac.kr, jilim@korea.ac.kr
*Graduate School of Information Security & Center for Information Security Technology in Korea University

Abstract

The purpose of computer forensic is to make digitalevidence which can be accepted in court using well-organized technic and according to reasonable process in computer crime investigation. Recent forensic technic field is developed every year, however computer crime isn't. Especially, there are lacks of definite procedures such as collection, transfer, analysis of evidence, report evidence to the court by keeping its integrity. In this article, we suppose new digitalevidence management process and digitalevidence integrated management system was realized to three application (digital warrant request & issues system, digitalevidence management module, digitalevidence authentication and tracking system).

Keywords

Digitalevidence, Chain of custody, Digitalevidence authentication, Digital warrant, Computer forensic process

INTRODUCE

It is well-known fact that computer crime is increasing everyday as information of society is developed. So digitalevidence is increasing at not only computer crime but also general crime. Considering of this trend, digitalevidence handling technology and management processing must be reconstructed and developed newly. In this article, we will review the problem of existing management procedure of evidence, and we propose new digitalevidence management process which consists of 3-component(digital warrant request & issue system, digitalevidence management module, digitalevidence authentication and tracking system – Each of system was realized in this research), for improvement and complement of the existing problem.

EXISTING DIGITALEVIDENCE MANAGEMENT PROCESS AND PROBLEMS

Digitalevidence is difficult to treat, because digital information is easy to forge, alter, delete and modify. So, several digitalevidence collection tools and forensic tools are developed. However, there are many problem of composition which is whole due process from evidence collection to submitting to the law court, because we just only focus on the technical developments. In this section, we will review the existing processes of digitalevidence acquisition, management, and dealing. And, also we will look into some problems of those processes.
7. Seized system and storage media are kept and transported.

8. If it require transfer of evidence from someone to the other during storage and transportation, a charge must confirm the state of evidence using his eyes and observe principle of chain of custody (things of confirmation must be recorded in transfer lists)

9. Seized digitalevidences are analysed, and a reported to submit in court is made.

10. The report about Digitalevidence is submitted to a judge, a advocate and jurymen in court.

11. If verification of forgery or alteration for the Digitalevidences is needed, it is verified that hash value gained in the first Digitalevidence is equal to that of evidence submitted.

12. If the trial ends, the Digitalevidences are transported to a depository of evidence.

Problems of existing digitalevidence management process

Occurrence of time cost followed by observance of a lawful process

When digital information is made, it is exposed to deletion, forgery, and alteration. So, quick handling is required to acquire more Digitalevidence and more accurate, from acceptance of incident to seizure of evidences. However, a lawful search warrant for seizure is required in order to seize a suspect's computer. A lawful search warrant for seizure is issued by judge, after judge inspect the proposal of a policeman and a public prosecutor. If it consume the much of time in this process, reliability of digitalevidences will be decreased.

Moreover, digitalevidences exist not only in a suspect's computer but also the various kinds of systems and equipments of the third party connected to the exterior. In order to collect those things, we must ask for the other party's cooperation, or a new warrant must be issued. But in order to ask for the other party's cooperation, it is difficult to prove to others that I make a lawful investigation, because they are far from me. And, much of time and administrative business are required to issue a new warrant.

Problems of digitalevidence certification

In order to preserve contents in hard disk in the process of digitalevidence collection, disk imaging is formed and hash value of the imaging is made. Hash value which was gained in the process of this evidence collection is used to verify integrity of collected data in court. Contents of data are difficult to change because the hash values keep equality due to characteristics of algorithm. The most of forensic tools use a open hash algorithm (Manipulation Detection Code - MDC) such as MD5 and SHA-1 to make hash value. But it has weakness that alters the data, and remake new hash value, and replace existing value to new one (MDC Attack [2]). To prevent this weakness, trusted third party's or suspect's advocate are accompanied by evidence collection process. And they make documentation of digitalevidence. But, there are some problems that require additional human resource and cost of administrative process.

Problems for application of chain of custody [3]

In process of transfer of general tangible evidence, undertake charge and taking over charge confirm the state of evidences using their eyes and follow the chain of custody which consist of the transfer place, the method, and the people and so on.
DIGITALEVIDENCE INTEGRATED MANAGEMENT SYSTEM

Computer forensic needs strict digitalevidence management process, because crime investigation must observe due process. But strict digitalevidence management process decrease investigation efficiency. So we need new digitalevidence management process which is able to observe a due process and have a high efficiency.

We suggest secure and effective computer crime investigation process with 'Digitalevidence Integration Management System' which is made of digital warrant request & issue system, Digitalevidence Management Module, Digitalevidence Authentication and Tracking system.
3. In searching and seizing computer and obtaining digital evidence process, investigator transmits information of digital evidence and digital warrant to authentication center.

4. Authentication center transmits digital evidence authentication number to evidence collector.

5. In transfer process, each charge transmits report to authentication center.

6. Authentication center transmits digital evidence authentication number to charge.

7. Authentication center transmits digital evidence authentication contents and result to the computer crime investigation center.


In next section, we will look into digital signature and verification and describes digital evidence management system’s detail processes, operation method and realize application of each system and module.

**Digital Signature and Verification** [5]

Digital signature is a substitute that creates information by computer in place of conventional pen. Above mentioned ‘By computer’ indicates that after creating message digest of digital document that needed to be transmitted the digested message by sender’s digital signature private keys is encrypted.

Digital Signature’s process

Creating of Digital Signature

1. To use Digital Signature, it is necessary to create public keys and private key pairs.

2. Message digest of digital document is created. If a message gets too long it takes a while to sign in or verify, so summarize message using hash function.

3. Message digest by signing sender’s digital signature is created. In this case, digital signature will be created by algorithm correspond to digital signature.

4. Message to receivers with digital signature is send. If confidentiality is necessary, it is also possible to secure by encryption.

Digital Signature Verification

1. When receiver receives a digital signature message, receiver’s computer restores sender’s original message, using sender’s digital signature verification keys. If restoring is not performed, it is decided that it is not right sender’s signature verification keys.

2. Comparing received message digest and restored message digest, if it turned out to be not the same, message’s integrity is considered to be corrupted.

Authentication Process

Authentication is to prove that someone’s signature verification key is correct whether or not in trusted third...
Digital warrant request & issue system

Digital warrant request & issue system is the web-based system. Purpose of this system is to support request of issue searching/seizure warrant. And the warrant takes the form of paper document and digital document. Specific process is as follows.

Police, prosecutor and judge login digital warrant request & issue system by using their personal certificate. And webpage display the current progress result of requested warrant. If the police and prosecutor want to request new warrant, they fill out warrant in webpage. Police and prosecutor perform digital sign in the warrant request document. Warrant contents and signing values are saved in DB and warrant request document send to judge. Judge verifies police and prosecutor’s signed value. If judge accepts a request then warrant document is made with requested warrant contents. Judge performs a digital signing to the digital warrant file. And he issues paper document warrant and digital warrant. It is sent to the police and prosecutor. If judge dismisses the warrant, then he fills out some comment, and notifies to the prosecutor and police. The digital warrant request & issue process offers three advantages compare with current existing warrant issue process.

First, the whole warrant issue processes are automated with on-line. So it is performed very easily and fast. In this way, it is not necessary visiting several departments to request warrant. And they can recognize current progress anytime, because the whole contents of warrant are geared and stored in DB.

Second, computer crime investigation area can be extended, because the warrant can be made a paper document in hand sign, and a digital document in digital sign. Especially, digital warrant can be used in on-line, so the third party’s cooperation can be requested by on-line.

Third, warrant verifying process is safe and easy. Because the whole processes are based on personal certification and PKI (Public Key Infrastructure). Unauthorized user cannot access or make out document because login or digital signature uses personal certification. Also integrity verifying and non-repudiation of origin functions are supported by PKI.
Above figure 4 shows realize of digital warrant request & issue system. #1 shows current warrant request list, #2 shows display of warrant detail contents in web-browser, #3 shows digital signature verify result.

**Digitalevidence management module**

Digitalevidence management module requests and checks authentication geared with computer forensic tool. Purposes of this system are verification of integrity and realizing of chain of custody. Specific progress is as follows.

Digitalevidence management module acquires investigator’s certificate, digital warrant and evidence information (evidence number, media type, current time, disk image hash and CRC value) from computer forensic tool. So it makes digitalevidence information report and performs digital sign with certification. It transmits digital warrant and evidence information report to authentication center. If authentication is finished, authentication or error number is received from authentication center. Digitalevidence authentication process, using digitalevidence management module, offers three advantages compared with authentication by paper document hand write and verification method.
Above figure 6 shows realize of digitalevidence management module. This module geared with computer forensic tool. We developed computer forensic tool in the last year. It provides digitalevidence collecting, analysis and report with GUI (Graphic User Interface) in Linux or UNIX environment [6]. Investigator can input his certification and digital warrant for digitalevidence authentication.

**Digitalevidence authentication & tracking system**

Digitalevidence authentication & tracking system authenticates the digitalevidence information report and stores the authentication list in database. Purposes of this system are to authenticate digital evidence report and categorize the authenticated information. The categorized authentication result can be use to realize chain of custody and tracking management. Specific progress is as follows.
Therefore, these lists show management history of digitalevidence. Also, it provides integrity verification and non-repudiation of origin functions is supported, because each charge performs digital signature each process.

Second, it is possible to track current digitalevidence charge. Computer crime department of government (Just like Cyber Terror Response Center – Korea [7]) must be able to control several computer crime investigations. If investigation center can access current authentication list of digitalevidence authentication center, then detail information (media type & number, each of hash and CRC value, and so on), current position, charge and integrity maintenance of digitalevidence can be checked in real time. So it is possible to track management of digitalevidence in real time.

![Realize of digitalevidence authentication & tracking system](image)

**Figure 8** Realize of digitalevidence authentication & tracking system

Above figure.8 shows realize of digitalevidence authentication and tracking system. #1 shows each of case (warrant) number, #2 shows each of digitalevidence information (authentication number, authentication time, charge’s name, evidence number, media type, hash and CRC value, comment), #3 shows details of selected digitalevidence information, #4 shows searching function of database.

**CONCLUSION:**

Considering current computer crime investigation trend, integrity of digitalevidence is accepted in court just using hash function provided by forensic tools. However, we describe it is weak from MDC attack. So it is not safe at the cryptography side. In this article, we recommend how to realize the chain of custody that applies the result of authentication and digitalevidence management procedure, using authentication based on PKI. And, we introduce digitalevidence integrated management system which consists of 3- prototype system. But there are many problems on this procedure to apply real law enforcement and investigation. For example, digital warrant request & issue system, it need to construct private network which was connected each others (police, prosecutor, court) to use. And it needs to be supported by law and legal system. Digitalevidence authentication center that police, prosecutor, court and citizen all can trust is about law and legal system rather than technical problem. So, computer forensic researches contain not only technic but also law and legal system. At further research, we must include these facts and develop practically.