International Journal of Advanced Science and Technology
Vol.110 (2018), pp.45-54
http://dx.doi.org/10.14257/ijast.2018.110.05

A Study on the Improvement of Domestic Internal Audit Technique Using Digital Forensics

Eui-San Ahn[1] and Gyu-an Lee[2*]

[1]Department of Science Criminal Investigation, General graduate school. Chungnam National University, (34134) 99, Daehak-ro, Gung-Dong, Yuseong-Gu, Daejeon, South Korea
[2]Department ofConvergence Education, Hoseo Graduate School of venture,(06724) 2497, Nambu-Sunhwan-ro, Seoul, South Korea,
[1]ahn6728@naver.com, [2]leegyuan@hotmail.com

Abstract

All the contents of daily work are being digitalized. In particular, digital information is created and stored in all the works of corporations and national institutions, public institutions. Also, Users are directly or indirectly supporting the creation of digital information. Among these digital informations, digital evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Digital forensics refers to a series of processes submitted to court after digital evidence is collected, analyzed and stored. While the digital forensics method is in the spotlight, the KCS(Korea Customs Service) has introduced the digital forensic investigation technique to track drug trafficking and tax evasion in the direct transaction method using the Internet. Also, local governments have established and operate a digital forensic center to prove network intrusions or illegal acts of employees.

On the other hand, as materialism becomes more widespread, personal injustice, corruption and tax evasion become big issues. Therefore, in this paper, we intend to study domestic internal audit technique that combines digital forensic tracking method. For this purpose, a method for protecting personal information should be studied in advance. In addition, procedures and legal support should be followed to meet the requirements of civil affair process and procedure of criminal cases in the Circumstances with the integrity and reliability of digital forensics. As a result of this study, it is look forward to that a transparent society will be settled by applying the advanced method of domestic internal audit technique using digital forensics.

Keywords*: Digital Forensic, Audit Technique*

1. Introduction

The term inspection refers to the investigation or supervision of public officers' misconduct or delinquency, and the term audit refers to supervision and inspection. In the lexicological sense, both of inspections and audits means to hear and check that the organization's personnel were not negligent or fraudulent. Also, through it, punishing the wrong thing, and doing well means encouraging through case propagation. However, even in the case of public or private companies, the image of inspection or auditing strongly dominates the concept of distrust such as investigation of work. And, in this situation, it is also impossible to exclude the dominant positions of the auditors. If you look at the laws and regulations related to the audit system, the internal auditor conducts periodic audits and irregular audits within the organization, while introducing an external

Received (September 29, 2017), Review Result (December 21, 2017), Accepted (January 8, 2018)
* Corresponding Author

ISSN: 2005-4238 IJAST

audit system in some cases. In the case of internal audits of domestic corporations and public institutions, there are difficulties such as inadequacies in business, problems in appointment of auditors, lack of audit infrastructure, and lack of professional expertise. Especially as the digitization of information is accelerated, the areas of computer analysis, accounting and respect for human rights are more vulnerable. On the other hand, the auditing system of developed countries is changing from the past oriented and formal auditing pointing out the business errors to the role of the passive business partner in the evaluation and improvement of the risk management, internal control, and resource enhancement resource processor. Especially, it is required to analyze the digital evidence and introduce a big data processing system to predict and statistically make the information required for audit in the mass information. In addition, if the real-time audit results using digital forensics are used to ensure the opportunity and conditions to correct mistakes, the new auditing system will be able to break away from the negative image that corporations and institutions view. For to do this, we have divided mobile forensics for analyzing of individual's mobile phones, network forensics for analyzing the flow of payments and funds, and system program forensics for analyzing errors and mistakes and deliberate actions in the work. In this paper, we present the results of this study.

2. The Use of Digital Forensic in Auditing

According to the Administrative Audit Regulations for local governments, audits are divided into government joint audits, comprehensive audits, specific audits, and service audits. Before conducting the audit, it is possible to confirm the data and information related to the audit object in order to confirm the appropriateness of the audit target selection and other problems. At this time, the request for data submission stipulates that the data entered into the computerized information system can be investigated [1]. In this regard, according to the law of external audit of a corporation, an independent external auditor conducts an audit of the corporation to ensure that the accounting is properly performed. In general, audits by government agencies and corporations can be divided into security audits, accounting audits, work audits, and internal audits. The security audit is to investigate and analyze whether the security system is operated safely. And Accounting audit is to investigate and analyze whether management, and other financial information of the enterprise proposed by the management of the enterprise is written in accordance with generally accepted accounting principles. The job audit is to strengthen the competence of the job by examining whether the job is appropriate and unbiased, and whether the workload is appropriate. Internal audits are conducted to confirm whether the user is accessing the network in an unreasonable way or deleting, leaking or modifying information. If the problem is identified through the internal audit as above, the person concerned shall be given appropriate liability and punishment. All of these audits are described in the SOPs, regulations, *etc.* based on the inspection items of Article 24 of the Board of Audit and Inspection Act. According to above Article 25 of the Regulations for Inspection of the Audit and Inspection (hereinafter referred to as the Board of Audit and Inspection), the person who subject to job and accounting audit must be submitted to account books, related documents to the Board of Audit and Inspection [2]. Since most of the information generated by government agencies, local government, and corporations is digitized, it is necessary to extract and analyze only the information for an appropriate auditing in the digitized information for auditing and internal auditing. Therefore, there is a limit to perform correct audit tasks without understanding digital forensic techniques. In particular, because digital data is deliberately easy to delete or change, it should be audited while giving proof of digital evidence. Therefore, it is necessary to consider how to give proof of digital evidence.

2.1. Digital Forensic and Digital Evidence

Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data. In recent years, the increase in the number of smartphones has resulted in the digitalization of most of the information generated worldwide, and the importance of digital forensics, in which digital evidence is adopted as evidence for proving crime, has become more important. This kind of digital forensic classification has been divided into various aspects such as disk forensics, network forensics, database forensics, accounting forensics, mobile forensics, and mobile forensics, depending on researches of investigators and scholars in the field.

2.2. Admissibility of Evidence about Digital Evidence

Conventional evidence documents were easy to read and visibility, but in the case of digital evidence, there is no visibility and readability, so additional programming work must be done to resolve them. Therefore, in order for digital evidence to be recognized as valid evidence in a court of law, it must be proved that it is derived from a scientific analysis and whether it is in conformity with the original through hash value. For reference purposes, a hash value is a combination of letters and numbers that shortens the file characteristics to prove the identity of the digital evidence, leading to a 'fingerprint of digital evidence' during the investigation. In view of the originality of digital evidence, there was a view that digital evidence was original and that the output was a copy. However, in view of the fact that US Federal of Rule 1001-3 and the digital evidence itself is already expected to output, it is a recent view that digital evidence has independent evidence aside after being granted visibility and readability [3].

2.3. Strengthen Methods of Admissibility of Evidence on Digital Evidence

[Supreme Court Dec. 13, 2007, sentencing, Decision 7257, 2007, In Korea]

From now on, I will examine the precedent of the process of adopting digital evidence in the case of Korean spies. In order to use a document output from a digital storage medium as valid evidence, it is necessary to confirmed to match whether the identity of the document stored in the original digital storage medium or not the output document. In particular, in the case of a document output from a "hard copy" or "imaging" medium (that is a copy of original digital storage medium), the identity of the data must be recognized between the original digital storage medium and the medium of "hard copy" or "imaging". In addition, for confirming this process, the operator's professional skill and accuracy must be ensured at each stage of input and processing output, as well as the mechanical accuracy of the computer and the reliability of the program. If a document output from a confiscated digital storage medium is used as a proof of statement, the special law on the truthfulness of the description applies, and in accordance with the provisions of Article 313, paragraph 1 of the Criminal Procedure Act, It can be used as evidence only when the User's authenticity of the establishment is proved [4].

3. The Auditing techniques using Digital Forensics.

3.1. Security Audit using Network Forensics

In national organizations, the security audit refers to the examination of the security management status of personnel, documents, materials, facilities, regional and network equipment that are subject to security. The types of security audit are divided into periodic audit and occasional audit [5]. Especially, in case of leakage of personal information due

to hacking, which is a recent problem, the company may be in great danger due to the class action of the victims against the company that leaked personal information. Let me give you an example of a world-famous corporation's hacking intrusion. It was in 2000 that a youngster gained access to the operating systems of some of the big corporate names like eBay, Amazon and others through his hacking acumen. He repeated the same incident two times in a month. He was later arrested and famously coined with the name “Mafia Boy” by the media. Jailed at the age of 15, his real name is Michael Demon Calce.

However, if there is preemptive security review and supplementation of vulnerabilities before a security incident due to actual hacking occurs, hacking accidents can be prevented. It is not really meaningful to take security measures after a hack has occurred. Therefore, the audit team should construct a security team for packet flow and abnormal IP trace by using WireShark *etc*. and take security measures in advance.

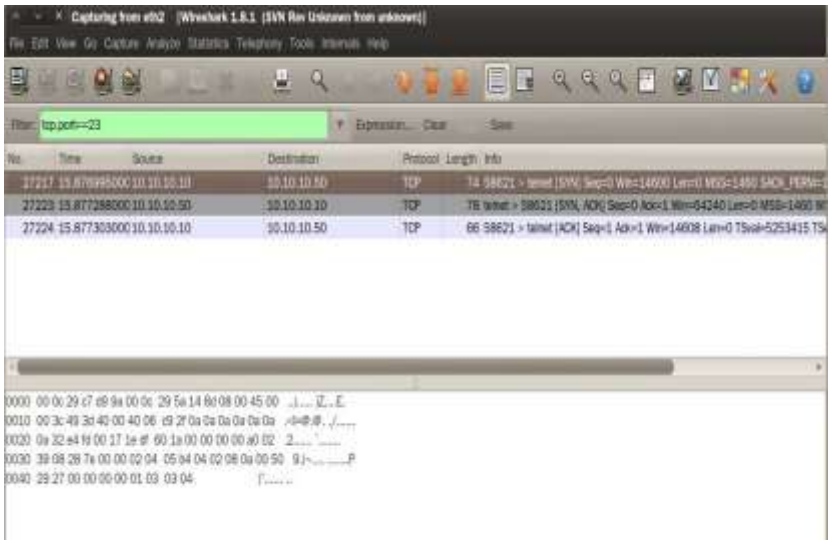

Figure 1. Packet Analysis Using WireShark Tool

3.2. Auditing using Database Forensics

In the event that people became more interested in digital forensics in account auditing, In 2002, it was a scandal(In short, it was an accounting fraud case) involving Enron, WorldCom, Tyco International, Global Crossing, Adelphia. At this time, EnCase Tool(a digital forensic program), proved the reliability and integrity of data that was deleted or analyzed. As a result, the US accelerated the recession and the stock market plunged during the year. In the end, the US government enacted the Corporate Accounting Reform Act in 2002 to prevent corporate accounting fraud, and the Corporate Accounting Supervisory Commission PCAOB) was established. In Korea, there has been a tremendous financial damage caused by Daewoo Shipbuilding. Therefore, database forensic techniques for accounting analysis should be utilized to prevent illegal inheritance of management rights and the formation of slush funds.

3.3. Job Auditing Using Disk Forensic

In the modern era of the fourth generation of the industrial revolution, users use computers and other electronic devices to create, store, and transmit information using networks. All of the day-to-day tasks, such as creating reports, are generated by digital information, such as stored on a computer's hard drive or virtual memory. It is to called digital forensics to collect and analyze digital data. In the past, for your job audit, you must have collected everyday memos, timetables, papers, *etc*. But, in the present, for your job audit, you should acquire electronic logs and electronic files of computers and mobile

devices. Therefore, there is a need for a technique for selectively acquiring and analyzing only necessary data in a digital storage medium.

Figure 2. Stock Market Analysis through Digital Forensic Analysis

3.4. Job Audit Using Mobile Forensics

In the recent workplace life, cell phones have become the most essential thing. Most of daily life uses mobile phone, such as internet ordering, movie watching, file transmission and reception, etc., internationally through direct transactions. As a result, all the activities of the user Is being stored in cell phone. Therefore, for smooth job audit, it will be necessary to collect and analyze appropriate data from such a mobile phone. To the extent that the human rights of an individual are not infringed, it is necessary to technology to select and analyze mobile data related to the job.

Figure 3. Mobile Forensic Using Tool

3.5. Utilization of Digital Forensics in Restructured Companies

As the integration of companies has become more common, private equity firms that have acquired the company are required to apply all the techniques of disk forensics, network forensics, and mobile forensics in order to identify complaints about job neglect. For a private-equity fund that has acquired the company, it is very important to find out and fix any irregularities or illegal practices and to create a new operating-based environment. However, as there is a great deal of risk and cost burden to accommodate all the workforce in accordance with the activities of the union and the conditions of the

takeover, restructuring should be carried out in accordance with the management policy of the new owner. For a restructuring, it is necessary for a company to dismiss some employees or to adjust their departments. At this time, it would be very effective to use job auditing using digital forensics.

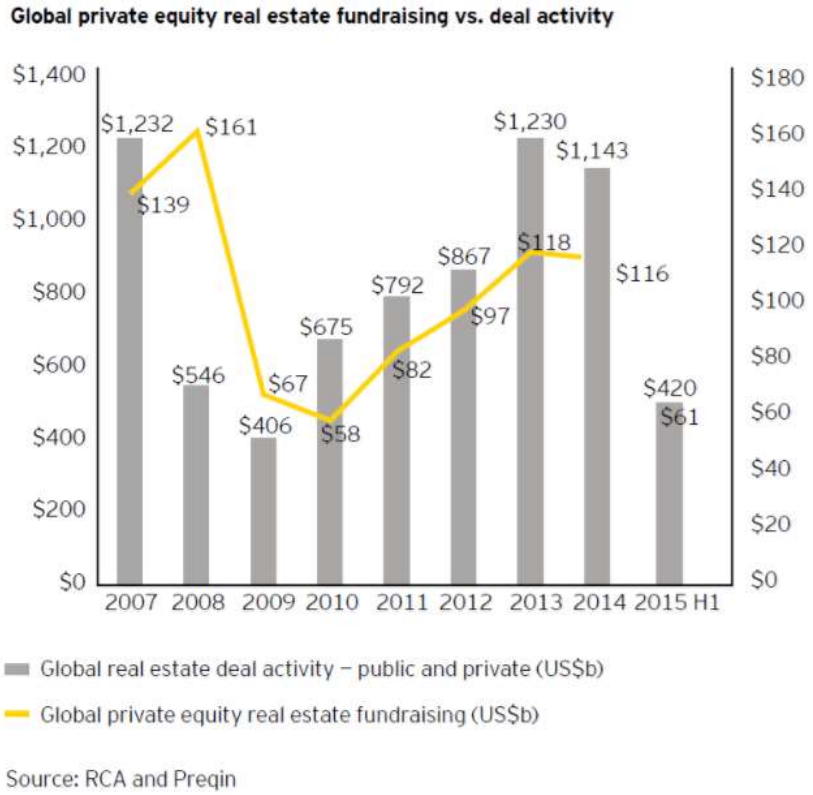

Figure 4. Market Trends of Private Equity Funds

4. Problems of Audit Function and Solution Using Digital Forensics

4.1. Problems of Utilizing Digital Forensics by Audit Agencies

4.1.1. Infringement of Personal Privacy Caused By the Mixture of Digital Information

In most database servers, personal information and institutional information are not separately stored. In addition, according to the Personal Information Protection Act, a public institution encrypts and stores personal information files required for business purposes, but also includes personal privacy information of some users. In such a situation, data collection that is not refined may infringe privacy or human rights of an individual.

Table 1. Major Channels for Intentional and Accidental Data Leaks (Infowatch, 2009)

Leak channel	Intentional leaks		Accidental leaks	
	Amount	%	Amount	%
Mobile computers (notebooks, PDAs)	59	15.7	31	9.7
Mobile data carriers (flash drives, CD, DVD, etc)	8	2.1	24	7.5
Desktop computers, servers, HDD	78	20.8	26	8.1
Internet	67	17.9	63	19.7
Paper hardcopies	27	7.2	115	35.9
Archived media	33	8.8	15	4.7
Email	11	2.9	27	8.4
Other	41	10.9	6	1.9
Unspecified	51	13.6	13	4.1
Total	375	100	320	100

4.1.2. Diversification of Digital Information and Lack of Experts

Digital information is becoming more diversified in recent years. In the case of e-commerce via the Internet, all information such as the purchaser's consumption patterns and the location of the buyer Created and preserved. Also, in recent years, the use of Big Data has been used to digitize and analyze user's movements, Apps that anticipate congestion and provide real-time directions have also appeared.

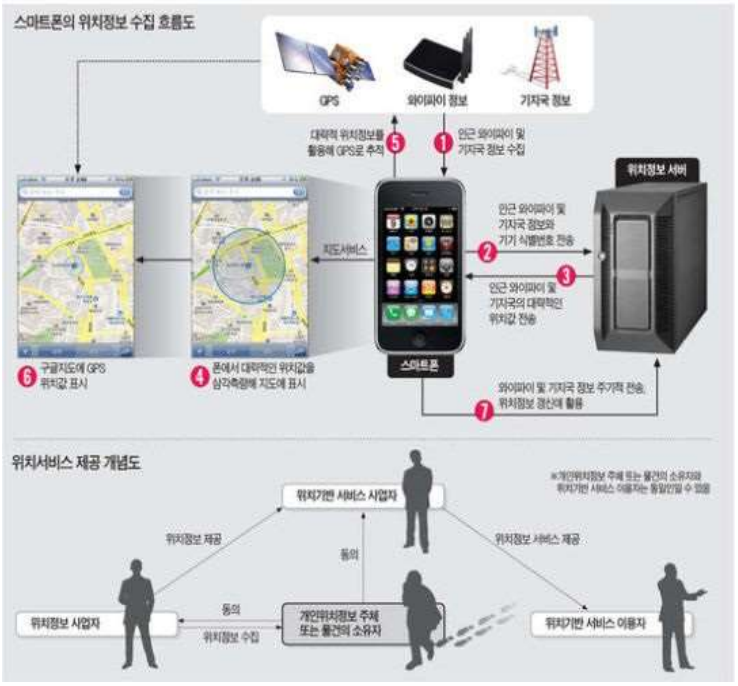

Figure 5. Map of Location Information of Smartphone

4.1.3. Inadequate Development of Domestic Program

An operating system(OS) is system software that manages computer hardware and software resources and provides common services for computer programs. All computer programs, excluding firmware, require an operating system to function. Globally, all countries are working to nationalize the operating system of smartphones. In Korea, Samsung Electronics has focused on development for the 'called ocean' operating system for a considerable period of time, but it is highly suggestive that it has not achieved great results. Among them, Microsoft and Apple are trying not to lose their dominance in the digital world by developing and upgrading a new operating system for their computers. Periodic upgrading of the operating system can be a challenge for auditors seeking to use digital forensics. Existing forensic programs are incompatible with new operating system. Therefore it is requiring periodic purchases or upgrades, and digital forensics using unauthorized programs may not be credible.

4.1.4. Improvement of Laws and Systems

Due to the processing of electronic records and the system related to personal information, and restrictions on the law, the auditing technique using digital forensics requires considerable care and effort. It is necessary to revise the law and system because all the records specified in the Criminal Law & Promotion of Information and Communication Network Utilization and Information Protection Law are digitized.

4.2. Solutions of Problem

Before introducing digital forensics to audit agencies, related laws and systems should be in place. In addition, it is urgent to cultivate relevant experts and to develop reliable programs. Consideration should be given to the application of the digital forensic technique by improving the relevant laws and systems in consideration of the nature, activities and environment of the organization being audited. Experts should be qualified and competent as auditors, so they must master the relevant techniques through training on digital forensics and apply them to their work. In order to do this, constant research and education are needed, such as obtaining a certificate through a national qualification system. The program should use a program that is given the reliability according to the environment of the operating system. Above all, the collection and analysis of unnecessary information should be restricted for the protection of human rights. And Care should be taken to avoid unnecessary administrative waste. By paying attention to these things, improving laws and systems, fostering relevant experts, and developing reliable programs, eventually efficient auditing using digital forensics will be possible.

5. Conclusion

The duties and roles of auditors did not change much, but the environment of auditing changed drastically due to the massive data and digitization of data. In the past, if the auditing method was analog and passive, the advanced auditing technique would be digital and automated. Although the research and analysis so far are not wrong, if the new research environment cannot be met, there is a limit to the ability of auditing. Auditing techniques for corporations and organizations that use digital forensic technology enable efficient collection and analysis of only the data required for auditing in a vast amount of data. Nevertheless, it should be noted that the auditing technique using digital forensics is like a double-edged sword, which is more error-prone than misuse. Because the court does not accept the evidence collected illegally and does not recognize evidence derived from illegally collected evidence, it must also comply with the due process in the collection and acquisition of digital evidence.

In order to selectively collect only the data necessary for auditing in digital storage media, skilled experts in the field of digital forensics must be trained. In particular, accounting audits through database analysis require more specialized personnel. Thus, if domestic internal auditing techniques using digital forensics are applied, it will be possible to motivate employees by punishing employees who committed crimes and by awarding awards to excellent employees. In addition, existing erroneous practices, which give unnecessary administrative burdens to audited institutions and cause considerable time, should be improved.

Ultimately, audit techniques using digital forensics will achieve audit innovation in terms of cost reduction and time saving.

Acknowledgments

"This paper is a revised and expanded version of a paper entitled [Study on the Storage of Digital Photographs by an Investigator] presented at [the 6th International Conference on Next Generation Computer and Information Technology (NGCIT 2017) which was held in Liberty Central Saigon Riverside Hotel, Ho Chi Minh City, Vietnam last August 16-18, 2017]."

References

[1] "Inspection law of municipal corporation", The Legislative Office. http://www.law.go.kr.
[2] "Board of Audit and Inspection Act", Ministry of government Legislation. http://www.moleg.go.kr.
[3] L. Gyu-an, "Digital Forensic for scientific investigation", p.75
[4] [Supreme Court in Korea] Dec. 13, 2007, Sentencing, Decision 7257, **(2007)**.
[5] H. Shin, 8, Police Dictionary, Nov. 2012. BuBmun Co.

Authors

Eui-San Ahn, Department of Science Criminal Investigation, General graduate school. Chungnam National University.

GyuAn Lee, he received his Ph. D of Engineering in SungSil University.

