Advanced Science and Technology Letters
Vol.145 (NGCIT 2017), pp.75-79
http://dx.doi.org/10.14257/astl.2017.145.15

Auditing Techniques using Digital Forensic

Eui-San Ahn[1] and Gyu An Lee[2]

[1] Department of Science Criminal Investigation, Graduate School of Peace & Security Studies. Chungnam National University, (34134) 99, Daehak-ro, Gung-Dong, Yuseong-Gu, Daejeon, South Korea, guidoloveson@hnamail.net (Eui San Ahn: First author)
[2] Department of Convergence Education, Hoseo Graduate School of Venture,(06724) 2497, Nambu-Sunhwan-ro, Seoul, South Korea, leegyuan@hanmail.net (Gyu An Lee : Corresponding author)

Abstract. All the contents of daily work are being digitalized. In particular, digital information is created and stored in all the tasks of companies, including national institutions and public organizations, and users are directly or indirectly supporting the creation of digital information intentionally, arbitrarily or automatically. Among these digital information, proven evidence is called digital evidence, and a series of processes in which digital evidence is collected, analyzed, stored, and brought to court is called digital forensic. While forensic techniques using digital forensics are in the spotlight, the Korea Customs Service has introduced digital forensic investigation techniques to trace drug trafficking and tax evasion in the direct transaction method using the Internet. In this paper, we propose a new method of forensic investigation using digital forensic techniques. The auditor should be able to develop the auditing technique. In order to do this, a method for protecting personal information should be studied, and procedures and legal and institutional support should be followed to meet the requirements of civil and criminal justice while ensuring the integrity and reliability of digital forensics. As a result of this study, we hope to contribute to the development of a transparent society and a society in which people are rewarded through the expansion of auditing techniques using digital forensics.

Keywords: Digital Forensic, Cheating, Inspection, Network Forensic, Truthfulness, Integrity.

1 Introduction

Inspection can be said to investigate or supervise public officials' misconduct and audit is defined as inspection for supervision of doing work. When a terminological dictionary approach is used, both the inspector and the auditor investigate or supervise any work and any other situation that affects development of the business. Even in the case of public or private companies, the image of inspection or audit cannot be ruled out the superiority to the host.

However, if the auditor audits and supervises all the actions using digital forensics, the wrong thing is to guarantee the opportunities and conditions to be corrected, and the good thing is propagated as a best practice, the auditor should be proud of the work. People will be able to resolve their distrust of inspection or auditing. For example,

ISSN: 2287-1233 ASTL

mobile forensics for analyzing mobile phones, network forensics for analyzing the flow of payments and funds, system program forensic analysis of errors and mistakes, and deliberate actions related to personal affairs and capabilities.

As a result of this study, the reliability of the auditing organization will be enhanced along with the transparency of the auditing function.

2 Main Subject

2.1 Security Audit using Network Forensic

In the case of national organizations, the security audit refers to the examination of the adequacy of security management status such as personnel, documents, materials, facilities, regional and network equipment. Types of security audit are divided into regular audit and occasional audit. [2]

Especially, in case of leakage of personal information due to hacking, which is a recent problem, it is necessary to follow up efforts to prevent it from occurring as a security accident threatening the existence of the company through the class action system.

If you look at the cases of personal information leakage caused by hacking, it was revealed that 910,000 users, cell phone numbers and 3.23 million lodging information were infringed by hacking, and the amount of spill damage was worse than originally known.

It is meaningless to consider countermeasures after indidents in spite of possibility preventing if we had made more detailed security review and countermeasures against the vulnerability before the security incident caused by actual hacking.

The audit team should construct a security team for the flow of packets and abnormal IP tracking by using wire shark etc.

2.2 Auditing using Database Forensic

In 2002, the accounting scandal took place such as Enron, WorldCom, Tyco International, Global Crossing, Adelphia, and other large corporations in the US. At this time, EnCase, a digital forensic program, proved the reliability and integrity of the data that was deleted. As a result, the US accelerated the recession and the stock market plummeted during the year. In the end, the US government enacted the Corporate Accounting Reform Act in 2002 to prevent corporate accounting fraud.

In Korea, database forensic techniques for accounting analysis should be utilized to prevent the incident such as Daewoo shipbuilding accounts, the formation of slush funds, and the acquisition of capital.

2.3 Job Audit using Digital Forensic

In the modern era of the 4th generation industrial revolution, users create, store, and transmit information by using various electronic devices including computers. All of the day-to-day tasks, such as job reports, are created on the computer's hard drive or in virtual memory. It is digital forensics to collect and analyze. In the past, collecting everyday memos, calendars, and schedule were for job audits, nowdays collecting computer log records, business activity records, payment documents, payment notes, and special memo stored and transmitted to the computer were job audits. We need techniques that can analyze and prove like that thing.

3 Problems of Utilizing Digital Forensic

3.1 Problems of Utilizing Digital Forensic by Auditors

① Infringement of personal privacy caused by the mixture of digital information

It is hardly possible to categorize and store personal information, government agencies, and corporations. If mobile forensics is used for auditing, private information leakage is hard to avoid.

② Diversification of digital information and lack of experts

Digital information is becoming more diversified in recent years. All information including purchase intention and hobby life is generated and preserved. Due to the use of Big Data, the apps appeared to anticipate the traffic jam and provide guidance.

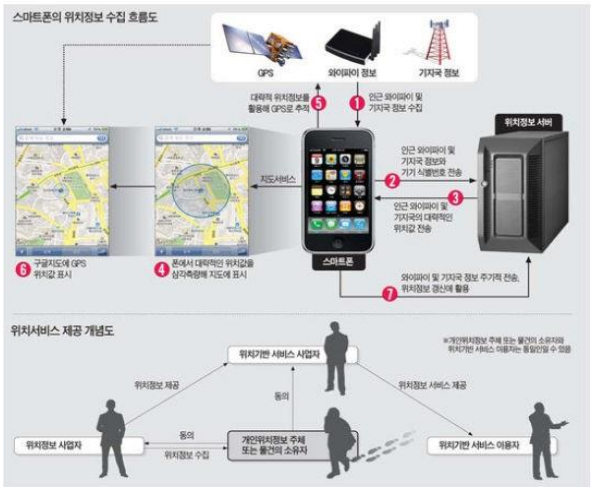

Fig. 1. Map of location information of smart-phone (Korean economy reference)

③ Inadequate development of domestic program

The 21st century is a war of the operating system. The base for utilizing, storing, and using all information is operating system. Because of that reason every nation is trying

to nationalization of the operating system of smartphones. Samsung has focused on the development of the 'Ocean operating system' for a considerable period of time, but it has not achieved the expected results. Microsoft is not trying to lose control of the digital world by developing and upgrading its new operating system.

Upgrading the operating system not only takes the lead in the storage and transmission of necessary information, but also presents many difficulties for auditors to use digital forensics. Older programs are incompatible with new operating systems, requiring periodic purchases or upgrades, and digital forensics using unauthorized programs can be unreliable.

④ Improvement of law and system

The use of digital forensics within the protection line of many laws related to electronic records and personal information requires considerable care and effort. Such as the Law on the Protection of Personal Information of Public Agencies, the Law on the Use and Protection of Credit Information, and the Law on the Public Record Management, are electronically generated and transmitted to digital information. It is necessary to improve the law and system.

3.2 Solutions

The introduction of digital forensics by the auditors should be accompanied by the improvement of laws and systems, the introduction and utilization of experts, reliable programs and tools.

Experts should be qualified and competent as auditors, so they must master techniques and apply them to their work through literacy and education about digital forensics. To achieve this, it is necessary to acquire qualifications through the national qualifications system and to study and educate them constantly. This is a way to train experts who are suitable for the environment where new types of digital information are generated and stored every day. The program must use a program that has been given credibility in accordance with the environment of the operating system, and the related tool should use the authenticated product with authenticity. Above all, the collection and analysis of unnecessary information should be restricted in order to protect human rights. In order to prevent unnecessary administrative waste from being carried out by the detainee and the inmate, the three beats of the tool should be prepared.

4 Conclusion

The duties and roles of auditors have not changed much, but the environment of investigation and analysis should be done in line with the fourth generation industrial revolution. The existing research and analysis is not wrong, but if it fails to respond to the new environment, there is a limit to the ability of auditing.

If the host-audits are suffering from the inconveniences and long preparation time for audit it should be improved.

For this purpose, auditing techniques using digital forensics will achieve auditing innovation by providing reliability, integrity, professionalism, and procedural continuity for digital forensics.

References

1. Board of Audit and Inspection Act, Ministry of government Legislation. https://www.moleg.go.kr. Prosecution Preservation Office Rule, (2017)
2. Shin. H etc 8, Police Dictionary, BuBmun Co. (2012)
3. Yo-gi-e-Tae, Information Leakage of Customer 910000, MoneyToday, (2017)