2017 2(1) 26-31 Submission: 2017/04/30, Peer review: 2017/05/10, Accepted: 2017/06/25, Published: 2017/06/30

International journal of police and policing

Publication state: Japan
ISSN: 2423-8279

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: s092724@naver.com

Peer reviewer
E-mail: editor@j-institute.jp

http://dx.doi.org/10.22471/police.2017.2.1.26

A Study on the Improvement of Digital Forensic Utilization for Cyber CRIMES

Oh Sei-youen

Semyung University, Jecheon, Republic of Korea

Abstract

Cyber-crime refers to the infringement of benefits and protection of laws - socially harmful behaviors - that occurs around cyber-spaces that forms via computer systems connected between information communication network such as the Internet. Such cyber-crimes have characteristics of anonymity, profession, technology and repeatability, hence, are required to be monitored as not only domestic but as an international issue, considering that the cyber-crimes are committed with no spatial and time restriction.

Therefore, This study is about how the government should deal with the rapidly growing and diversifying cyber-crimes, and figure out the policy and the techniques for strengthening in the investigation of cyber-crimes to unite and work towards a common goal. As the perspective of the policy, the government must support the new equipment and the professional manpower to utilize the Digital Forensic system. As the perspective of the technique, the government must construct the integrated system which helps to work with the investigators through the criminal cases. Moreover, this system has to study an analytic plan of the embedded system to use embedded forensic techniques and the basic ontology is important to be in the integrated system. And then in the future, measures to respond to diversified and intellectualized cyber-crimes should be more systemized and be constantly developed with more insightful Digital Forensic analysis than before.

[Keywords] ***Policing, Cyber-Crime, Digital Forensic, Criminal Investigation, Embedded System.***

1. Introduction

Cyber-crime refers to the whole crime actions that occurs in cyber-space including hacking(cracking) which threatens cyber-space security and virus dissemination by attacking the computer systems or information communication that constitutes cyber-space and practicing defamation of character, intimidation, fraud, prostitution and sales of negative images via the Internet[1]. Observing the cyber-crime occurrence trend, it has been increasing more rapidly than conventional crimes, especially within the recent 10 years by more than double. The severity and scale of damages are considerable huge and intensive measures should be prepared by international communities with collaboration among countries. To respond to cyber-crimes, in case of South Korea, a Cyber-crime Response Center is established and has been responding to cyber-crimes. Due to the such cyber-crime occurrence trend and diversified crime-related technologies, highly expert personnels are required, however, not sufficient, and considering the environment is a cyberspace, constant technology development and budget support are in shortage as well, even though utilization methods of Digital Forensic for evidence collection should be actively sought[2].

Therefore, this study proposes a measure to respond to cyber-crimes, from both policy and technological aspects, based on forensic methods via Digital Forensic. To achieve such

a accomplishment, criminal investigation procedures in Digital Forensic, concepts and types of cyber-crimes should be monitored first, then Digital Forensic investigation methods to effectively respond to cyber-crimes and probable problems in the methods should be revised by looking at cyber-crime occurrences by type and state of use of Digital Forensic by the domestic police.

2. Theoretical Background

If an advanced research of Digital Forensic for crime investigation is revised, the study is distinguished into two aspects of policy and technology, involving uses of Digital Forensic ontology, upon concept and procedures of Digital Forensic, human right infringement issue of Digital Forensic-related regulations and ability to collect evidences. Especially, the study is mostly consists of digital data analysis method in terms of Digital Forensic technology, and by using such method, various analytical areas exists – file carving, keyword search, timeline analysis, file-format analysis and code-breaking. In recent times, searches upon tailored analysis methods to each unit and data-type are being processed thanks to popularization of diverse storage such as mobile devices and emergence of virtual systems[3]. When the real conditions of Digital Forensic in Korean police is monitored, the number of requests for digital evidence analysis is increasing, however, equipments and personnels to practice are insufficient and thus, improvement measures are being suggested by the first line investigators, with profession in Digital Forensic ,that there are limitations in performing effective criminal investigation via Digital Forensic based on the types and circumstances of crimes from the aspect of policy[4]. In foreign countries, the application range of Digital Forensic is widely dispersed from terrorism to violent crimes and even economic spy cases, and by establishing Digital Forensic research institute which can deal with such crimes at once, effective criminal investigation is available and being used at suitable time and place, further revising any possible data omissions during investigation procedures[5].

3. Discussion on Cyber Crimes and Digital Forensic with Its Utilization

3.1. Concept of cyber crimes and digital forensic

Although there is no clear academic definition on cyber-crime, it is a general concept, perceived as criminal behaviors which are generally practiced in cyber-spaces that form based on a computer system connecting media such as info-communication network, the Internet[6]. In other terms, the notion of cyber-crime is an undetermined neologism spatializing the cyber-space and further and emphasizing on locations where crimes including school violence, family violence and subway crime, further including a broad range of cyber-crimes when there is any digital evidence to the crime although it does not involve any use of network or computer[7]. For cyber-crime types, the categorized standards by the National Police Agency distinguish into two-cyber-terror crimes such as hacking and virus and general cyber-crimes such as e-commerce fraud, illegal replica, cyber-violence and infringement of private data - according to the purpose of crimes, and features of cyber-crimes are non-face-to-face, anonymity, profession, technology, unconstraint time and space, considerable property damage, rapid propagation and difficulties in detection and inquest, which differ from other existing crimes[8][9].

Digital Forensic refers to a set of detection and inquest processes of a certain behavior based on in-stored digital data in information devices as evidences. That is, through processes of collection, transportation and analysis of a digital evidence, Digital Forensic was first used to capture crime-related data and use it in the court as an evidence of guilt in IACIS(International Association of Computer Specialists) held in Forkland, United States in 1991[10]. As Digital Forensic is accommodated as a part of criminal investigation, the collection of digital evidence involves the same legal procedure as the case of general evidence, hence, additional actions are required to treat the features of digital media. As digital media and data, that become the targets of Digital Forensic, has characteristics

of invisibility, falsification, obviousness of replication and volatility, appropriate measures are needed to each different medium from the initial collection to storage and such conformity of procedures should be reported and be proved by the investigation institution[11].

3.2. Digital forensic process

Digital Forensic process wes suggested from Digital Forensic standard process guideline of National Police Agency Cyber Terror Response Center. That is, investigators are deployed to crime scenes, collect activated data and prove evidences including acquisition of evidences, replicating an image of the evidences and transporting them as well as packaging. Digital Forensic investigation is carried out by completing analysis and investigation by implementing timeline log analysis, data restoration, file and vocabulary research and password decoding of the packaged and transported evidences, and producing a report with expert opinions attached based on the evidence analysis.

3.3. Utilization of digital forensic on cyber crimes

The National Police Agency categorizes cyber-crimes as cyber-terror crimes and general cyber-crimes and associated occurrence and arrest states are the same as <Table 1>[12]. While cyber-crimes rose from 116,961 to 155,366 by 32.8% from 2011 to 2013, arrest decreased from 91,496 to 86,105 by 5.8% from 2011 to 2013, thus it is perceivable that proper arrests are not being performed on the increasing number of cyber-crimes. As characters of cyber-crimes involve aspects of profession and technology, the first line investigating police officers were not professional enough to deal with files and databases, even if they arrived at crime scenes, could not collect digital evidences in a proper way, and possibly resulted in decrease in the number of arrest compared to the number of cyber-crime occurrence state for the reasons.

Table 1. Cyber-crime occurrences and arrested current states (2011-2013).

Type	Total			General cyber crime		
	Occurrences	Arrest		Occurrences	Arrest	
		Number	Personnel		Number	Personnel
2011	116,961	91,496	95,795	103,565	81,197	84,396
2012	108,223	84,932	86,513	98,616	78,56	79,274
2013	155,366	86,105	92,621	144,959	81,573	87,107

<Table 2> is the current analysis state of digital evidences during the past 3 years and the number of occurrences which a digital evidence was analyzed increased from 763 in 2008 to 2,984 in 2011 by 251% on the basis of 2008 and even the number of captured evidences increased from 2,160 in 2008 to 6,632 in 2011 by 207% on the basis of 2008, showing increases in both numbers of cyber-crime occurrences and media for an analysis[8].

Table 2. Digital evidence analysis status (2008-2011).

Analysis status (Evidence analysis)	2008	2009	2010	2011
Case number	763	1,789	2,543	2,984
Evidence number	2,160	4,746	5,476	6,632

<Table 3> is the current status of digital media from 2007 to May 2011, showing an increase by 118% from 2,864 in 2008 to 6,247 in 2010. Among digital media, particularly, the number of smart-phone and mobile-phone analysis increased from 47 in 2008 to 1,611 in 2011, by 3,327% and is perceived to be the most frequently used mean for the support of digital media analysis[8]. Therefore, as cyber-crimes using embedded systems such as smart-phones and mobile-phones are increasing, tailored Forensic investigation processes and analytical methods to each device with different characteristics are required.

Table 3. Digital media types analysis status (2008-2011.5).

Type	Total	PC-note	CCTV / Navigation	Smart-phone / Cellular-phone	Hacking / Password-database
2008	2,864	2,325	51	47	441
2009	5,493	3,820	185	658	828
2010	6,247	3,864	276	1,611	496
2011	2,816	1,394	330	984	108

4. Improvement Measures on the State of Use of Digital Forensic on Cyber Crimes

Knowing from the above current state of domestic cyber-crime occurrences and of Digital Forensic use by the National Police Agency, the number of domestic cyber-crime is constantly increasing, however, due to problems in technological support and policies in investigation processes, arresting practices are not being conducted properly.

Therefore, based on the various problems, a number of application measures of Digital Forensic will be proposed to strengthen responsive actions to cyber-crimes.

First, as Forensic tools are used for an appropriate feature and suitable investigation methods during investigations of cyber-crimes, problems time constraint of cyber-crimes and human right infringement during investigation process may arise. Thus, in order to solve such problems, a Digital Forensic system in an integrated form establishing Digital Forensic ontology and other means should be equipped rather than separated Digital Forensic analysis. Consequently, Digital Forensic system in a form of ontology system should be established.

In addition, for smooth progress and application of Digital Forensic system in a form of ontology system, an appropriate budget, support and training specialized personnels who can utilize them the support should be backed up. As observed above, while the number of digital evidence analysis is increasing by year, the number of personnels who are capable of analytical tasks are only 61 on the basis of 2012 according to the National Police Agency Cyber Terror Response Center, and the number is significantly insufficient to respond to the actual cyber-crime occurrence trend. Furthermore, assuming that acquisition of digital evidences is the most effective and critical proof to prove guilt, strengthening education upon existing professional personnels and training new experts should be implemented in circumstances that profession of the first line investigating police officers are required.

Third, among cyber-crime types, Internet fraud is constantly increasing and the number of conducted analysis on smart-phones and mobile-phones are overwhelmingly increasing, even from monitoring the current state of digital media analysis. Therefore, development of tools is needed so that Digital Forensic can escape from the processes of Forensic collection and analysis of a computer system of a suspect and execute recognition of various embedded systems such as smart-phones and anlaysis of different characteristics of

each device for further establishment of a guideline.

Lastly, future cyber-crimes can be developed even to various cyber-crimes occurring at any place using diverse digital devices including from personal computers to smart-phones, hence, implementation of a scientific investigation method that can respond to the crimes is necessary as well as constant research. In particular, recently, as more diversified cyber-attacks have become available via gaming devices, navigations and mobile devices including smart-phones, PDA, deeper analysis measures for embedded systems should be researched and even Anti-Embedded-Forensic technology should be accommodated into further interest and research from the view of visible function of security.

5. Conclusion and Proposal

Fact that the increasing ratio of cyber-crime has been more dramatic and rapid than the one of other general crimes in modern times was perceivable. Especially, development in IT technology and increased participation of people using the Internet has contributed to the increasing frequency of cyber-crimes.

Hence, the paper investigates the state of use of Digital Forensic and search for new directions to strengthen future responsive measures to cyber-crimes. Indeed, considering the future possible growth and application range of Digital Forensic field, at a point when data collection and analysis via Digital Forensic upon computers of criminals or suspects are required, cyber-crimes using embedded systems including mobile devices such as smart-phones and PDA, navigations, gaming devices are expected to increase, thus, even the embedded systems are recognized as a target of investigation, individually tailored analysis measures for different features of each device are needed and a comprehensively integrated management support system is sincerely needed.

6. References

6.1. Journal articles

[2] Oh SY. The Application of Digital Forensic Investigation for Response of Cyber-crimes. *Journal of Society of Digital Policy & Management*, 13(4), 81-97 (2015).

[3] Lee YH & Park HS. Analysis Strategy of Big Data in Mobile Cloud. *Journal of Communication and Information Science*, 32(7), 57-62 (2015).

[4] Yoo YH & Song BG & Park SJ. The Necessity and Training Plans for Digital Forensic Expertise. *Korean Police Studies Review*, 11(4), 253-284 (2009).

[5] Shin JW. A Study on Digital Forensic Human Training Method. *Journal of the Korea Institute of Information and Communication Engineering*, 18(4), 779-784 (2014).

[6] Kim SW & Jo HB. Prevention Methods of Cyber-crimes Using the Private Security. *The Korea Contents Association*, 13(3), 141-151 (2012).

[7] Meshram BB & Sindhu KK. Digital Forensics and Cyber Crime Datamining. *Journal of Information Security*, 3(3), 169-201 (2015).

[8] Song BG & Chang SH. The Actual Condition of Police Digital Forensic and Its Solutions for Improvement. *Korean Police Studies Review*, 12(2), 115-142 (2013).

[9] Jeong W. The Recent Situation of Cyber Crime and the Legal Measurements. *Hongik University Legal Research Center*, 10(1), 195-224 (2009).

[10] Yun HK & Lee SH. Digital Forensics Ontology for Intelligent Crime Investigation System. *Journal of Korea Society of Computer and Information*, 19(12), 161-169 (2014).

[11] Lim KS & Park JH & Lee SJ. Trends and Challenges of Current Digital Forensics. *Journal of Security Engineering*, 5(6), 461-474 (2008).

6.2. In addition references

[1] www://terms.naver.com (2017).

[12] Korean National Police Agency. Statistical Yearbook of the Police (2013).

Author
Oh Sei-youen / Semyung University Assistant Professor
B.A. Daejeon University
M.A. Dodgkuk University
Ph.D. Dodgkuk University

Research field
- A Study of Park Crime Prevention System Related to IOT and Big Data, Journal of Applied Engineering Research, 10(90) (2015).
- A Study on the Establishment of Policing Governance by Utilizing Big Data Based on Cloud, Indian Journal of Science and Technology, 9(24) (2016).
- A Study on Crime Prevention of Dating Violence Based on IOT, International Journal of Pharma and Bio Sciences, 1 (2017).

Major career
- 2012~present. Korean Association of Addiction Crime, Director.
- 2013~present. Semyung University, Assistant Professor.
- 2014~present. Korean Police Studies Association, Research Director.