International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 4, Issue 9, September 2015 **ISSN 2319 - 4847**

Study on Computer Evidence Forensics

ZHU Zhenfang

School of Information Science and Electric Engineering,Shandong Jiaotong University, 250357,Jinan,China

ABSTRACT

With the continuous development of the computer networking technology, computer technology is playing a more and more essential role in social production and people's lives. Meanwhile, it is surely becoming the nest of criminal activities. In this context, computer forensic technology emerged in response to computer crimes, which has become a hot research field. This paper illustrated the concepts, principles, classifications, procedures as well as tools of the computer forensics. The property of the computer evidence and the anti-forensics were also in presentation. Besides, the current restrictions were discussed and the further developing orientation was prospected.

Keywords: Computer Crime, Static Forensics, Dynamic Forensics, Computer Evidence, Anti-forensics Technology

1. INTRODUCTION

With the popularization of computer and booming development of network, computers play an increasingly important role in daily work, study, and life, and the computer system is also closely related to the business development in government, enterprise, bank, and other industries. However, computers have a lot of effects when bringing convenience to our life. As a new crime form, computer network crime has become more and more popular, crime ways of telecommunication fraud, network attack, etc. emerge in endless to bring huge loss to the country, government, and citizens. In order to bring lawbreakers committing network crime to justice and give tangible proofs for lawful sanction to the court, the interdisciplinary of computer and law, computer evidence forensics merges at the right moment. With the increasing computer crime, computer evidence forensics gradually becomes a hot field drawing focus and study from the society and academics.

2. OVERVIEW OF COMPUTER EVIDENCE FORENSICS

The most opinions show that computer forensics is called as electric forensics [1] and digital forensics which is firstly proposed by International Association of Computer Specialists (IACIS) in the International Computer Specialist Conference held in America in 1991 [2]. In general, computer and all the intelligent electronic equipment with computation and memory function play three roles in computer crime: invasive affected system, tool for criminal purpose, or the storage of crime information [3]. No matter which role the equipment plays, the suspects will always remain a large amount of crime traces. Therefore, computer forensics refers to the process to protect, collect, save, analyze, archive, and submit electronic persuasive and reliable evidence stored in computers and other electric equipment, network, and relevant peripherals to the court with relevant software and hardware technology of computer and network according to laws and regulations [4]. The essence of forensics is the process of detailed and comprehensive information search and crime reconstruction in computer system [5].

3. PRINCIPLES AND STEPS OF COMPUTER FORENSICS

3.1Principles of computer forensics

In order to make evidence collected from computer system be persuasive, acceptable in the court, and legally effective, some operation standards and principles should be followed during computer forensics, and evidence authenticity and integrity should be ensured. The principles in computer forensics are as follows [8]:

(1) Timeliness principle

Because of the imperceptibility and volatility, it is required that staff for forensics should control the intrusive computer system, tool for criminal suspects, and equipment storing potential evidence information to protect the system environment that is, crime scene, extract evidence, and avoid evidence from being destroyed or losing.

(2) Legitimacy principle

Not only should the forensic process and operation conform to laws and regulations, but also should the staff for forensics be equipped with relevant forensics qualification and equipment conform to laws and regulations. Otherwise, the obtained evidence has no legal effectiveness, and previous efforts made for forensics will waste.

(3) Backup principle

Backup principle requires staff for forensics copy all the data in target system into other equipment before obtaining

and analyzing data. It is not allowable to take direct forensics in original system and operate and install any program that may damage the integrity and reliability of original data. Moreover, copy is not only copy operation, but also takes physical mirroring to copy original data. Moreover, multiple backups should be stored in different devices to avoid damage or loss.

(4) Principle of chain of custody

It has to explain the changes of evidence from original acquisition to final submission to the court and provide all the steps for data acquisition and analysis. This is called the chain of custody for evidence.

(5) Supervision principle

Original data has to be supervised by special person. For the operation of original storage and extraction, staff of computer forensics and supervision should be present and give signatures in operation record for approval.

3.2Steps of computer forensics

Generally, computer forensics includes steps of protection of target system, evidence confirmation, acquisition, storage, analysis, and archive. The protection of target system refers to state latch for computer, peripheral, and network system that is, all the feasible measures should be taken before extracting evidence to maintain the operation state when catching and keep detailed record for the state, including system environment and log file. All the records should be under custody of special staff, and both physical environment and system environment should be in safety to avoid hacker or suspect from destroying criminal traces of intrusion, which is similar to the scene blockade by police. The confirmation and acquisition of evidence is to extract potential evidence by means of searching keywords, just like police extract footprint and finger print from the crime scene. Evidence storage refers to storing potential evidence in special forensic devices with backup and the evidence should be separately stored to avoid damage or loss and ensure the legal integrity, reliability, and authenticity. Analysis on evidence refers to analyzing or restoring evidence with various forensic technologies and tools to prove the correlation with the case and further find the relevant suspect. Evidence archive refers to settling the analysis results and conclusion for future testimony.

4. DEVELOPMENT DIRECTION OF COMPUTER FORENSIC TECHNOLOGY

Firstly, tool of computer forensic will develop towards the direction of professionalization, automation, and intelligence, and tools for forensics will become more reliable, safe, and feasible. With the intelligence of tools, manual operation will further reduce during the forensic, but be replaced with software. Secondly, the cultivation of interdisciplinary talents with both computer and law knowledge will become a trend in talent cultivation in computer forensic. Finally, deficiencies in the standard formulation of forensic tools, standard formation of forensic process, qualification of staff for forensics, and authority of institutions will all be solved in the near future.

5. CONCLUSIONS

As a flourishing field, computer forensics has been studied and developed for more than a decade. This work only gives a simple discussion on computer forensics technology, while there are some immature theories in this field. With the increasing development of science and further depth application of computer and network technology, the study on this field will be deeper in the future. It is believed that computer forensics will play an increasingly important role in crime investigation and forensics.

ACKNOWLEDGMENTS

National Natural Science Foundation (61373148), National Social Science Fund (12BXW040); Shandong Province Natural Science Foundation (ZR2012FM038, ZR2011FM030); Shandong Province Outstanding Young Scientist Award Fund (BS2013DX033), Science Foundation of Ministry of Education of China(14YJC860042).

REFERENCE

[1] Ding Liping. Research status of computer forensics analysis of [J]. information network security, 2010 (11): 9-11.
[2] Li Yulong. The study and Research on computer forensics technology [J]. computer security, 2007 (5): 7-9.
[3] Wang Ling, Hua Lin Qian computer forensics technology and development trend of [J]. Journal of software, 2003,14 (9): 1635-1644.
[4] Xing Jun of the [4]. Journal of computer forensics technology and difficulties [J]. Chinese people's Public Security University (NATURAL SCIENCE EDITION), 2003 (6): 38-41.
[5] Zhang Mingwang, Liu Yan. Research on security technology and application of [J]. network by computer forensics technology, 2011 (11): 27-29.
[6] Chen Long, the king of state. The computer forensics technology [J]. Journal of Chongqing College of Post and Telecom (NATURAL SCIENCE EDITION), 2005,17 (6): 736-741.

[7] Ding Liping, Wang Yongji. Research on the legal and technical issues of computer forensics [J]. software, 2005,16 (2): 260-275.
[8] Liu Shuang. On the computer forensics [J]. Heilongjiang science and technology information, 2013 (28): 170
[9] Li Feng, Dynasty. Research on the technology of computer forensics [J]. electronic production, 2014 (1): 82
[10] Zheng Qingan. Application of computer forensics technology for [J]. computer optical disc software and applications, 2014 (6): 47-49.
[11] LAN Li Song. Honeypot technology in Priscilla Chan, Computer Forensics Research and application of [J]. computer programming skills and maintenance, 2013 (8): 8-9.
[12] Yang Jiwu. Some of the computer forensics technology to explore the [J]. manufacturing automation, 2012,34 (3): 67-69,83.
[13] Shandong Research Institute of Computer Crime online forensics system [EB/OL].Http://news.xinhuanet.com/legal/2011-01/12/c_13687726.html
[14] Arsene Azizi, Kudlet Gecity, Wan Joan. Computer forensics technology and limitations [J]. China public security,2011 (4): 122-125.
[15] Su Cheng. Computer forensics and anti-forensics contest [J]. computer security, 2006 (1): 67-68,73.

AUTHOR

ZHU Zhenfang , PhD, lecturer, he was born in 1980, Linyi City, Shandong Province. He obtained Ph.D. in management engineering and industrial engineering at the Shandong Normal University in 2012, his main research fields including the security of network information, network information filtering, information processing etc.. The authors present the lecturer at the Shandong Jiaotong University, published more than 30 papers over the year.