Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 15 (2011) 3663 – 3667

Procedia Engineering

www.elsevier.com/locate/procedia

Advanced in Control Engineeringand Information Science

Computer Forensics Model Based on Evidence Ring and Evidence Chain

Guofu Ma, Zixian Wang, Likun Zou, Qian Zhang a*

The Central Institute for Correctional Police, Baoding Hebei, 071000

Abstract

In recent years, with the development of technology, judicial practice involving electronic crime is frequent. To combat this crime, computer forensics bears the irreplaceable role. This is a combination science of law and computer, but there is a "mismatch" phenomenon exists on the research on computer forensics currently, most of them only study the technical aspects of computer or electronic evidence related to legal issues, the two studies combined less. To solve this problem, in this paper, evidence of the general attributes: objectivity, relevance, legitimacy as a criterion to build a computer forensics model based on ring and chain of evidence. In this model, forensic evidence of links forms a ring, in accordance with the forensic to form chain of evidence. In order to ensure the objectivity, legitimacy of evidence, in building a chain of evidence and evidence ring as well as a supervisory chain in supervision, the final forms a electronic evidence forensics system.

Key words: evidence ring, evidence chain, computer forensics, evidence supervision

1. Introduction

With the development of information technology, especially the development of network technology, the computer has brought the convenience to the people, while it also become a weapon in the hands of criminals. A growing trend in the number and the growing dangers in the hazardous of computer crime have been made against computer crime as the focus of society attention. In this situation, a new field of computer security issues - Computer Forensics produced. Computer forensics is a combination science of law and computer, the computer system is consider as a crime scene, the use of advanced discrimination

* Corresponding author. Tel.: +86-136-7312-3487;
E-mail address: bd_wzx@126.com.

doi:10.1016/j.proeng.2011.08.686

technologies were dissected computer crime, criminal offenders and their search for evidence and confirmation proceedings. It can be said as: In view of computer invasion and crime, the work of computer forensics is to acquit, to preserve, to analyze, and to produce the crime evidence.

As a new type of crime, computer crime has posed a challenge to the judicial practice. Evidence of computer crime in comparison with the traditional evidence of a crime has its characters, such as not easy to gain, to retain with difficulty, the performance shape is diverse, and the content is covert. so in legal proceedings on the use of such evidence is different from the traditional evidence, in addition to the technical to be transformed, but also to obtain evidence in the legal process for the authenticity, legitimacy, capacity of the evidence there any evidence to prove evidence of the use of force size and the accuracy of such issues as the process of making a reasonable explanation.

2. Related Work

Computer forensics is a comprehensive discipline, the research on electronic evidence have different emphasis. One of these is how to deal with the electronic evidence, such research more from angles of the collection of evidence, extraction, preservation, focusing on the computer technical aspects[1]. These studies include: (1) Construction of evidence model; example: In order to protect networks and hosts from attacks, Yan Xiai et al build a virtual environment on the invaders, and then evidence[2]; Liang Changyu et al put forward a types of distributed computer dynamic forensics model, according with this model we can gather evidence in a protected system in real-time[3]; YANG Shumian et al research on how online collection of relevant evidence of multiple computers[4]. (2) Discussion of a detail in computer forensics. For example: Professor Ding Liping, who studied the acquisition and storage of electronic evidence relevant content[5]; Tang Juan, Wang Haiping and other people research on the effectiveness of electronic evidence[6]. However, most of these studies considered purely from the computer technical level, involving little or no knowledge concerning justice, which makes these studies may be used in judicial practice in real time is not necessarily feasible.

In judicial practice, Feng Chunming put forward the conception of evidence ring and evidence chain[7]. According to his opinion, evidence ring is an organic combination of evidence that is collected by the judicial personnel, which has a statutory form and built by judicial persons. It is a platform which can enable the evidence play its proof ability, and it also be an important link in the chain of evidence and the important part. Evidence Chain is a proof system which can prove all the fact of a case.

In this paper, we study the technology of computer forensics and legal issues. And then we put forward a computer forensics model based on evidence ring and evidence chain(EREC Model). In this model, building a complete chain of evidence, on each link in the chain of evidence give matters of attention and find feasible and effective forensic procedures, provide a reference for the forensic department. In order to ensure the electronic evidence objectivity, relevance, completeness, legality and continuity, improve the legal effect of electronic evidence, track the electronic evidence, include identification, preservation, extraction, analysis and presentation which make the whole process are in the custody of the law.

3. EREC Model

3.1. Frame Model

Although electronic evidence is a new type of litigation evidence, it also has something consistent with the traditional evidence that is we can derive a legal fact from each type of evidence (electronic evidence and traditional evidence). Therefore, the electronic evidence need to meet the basic properties of the traditional evidence: relevance, objectivity and legitimacy. Objectivity is the evidence must be objective reality; relevance is the evidence must have some connection with the case, prove the case on the practical significance; legitimacy is the form of evidence is legitimacy and evidence collection procedures must be legal. Based on the above ideas, a computer forensics model based on evidence ring and evidence chain is proposed. The frame model is as follow:

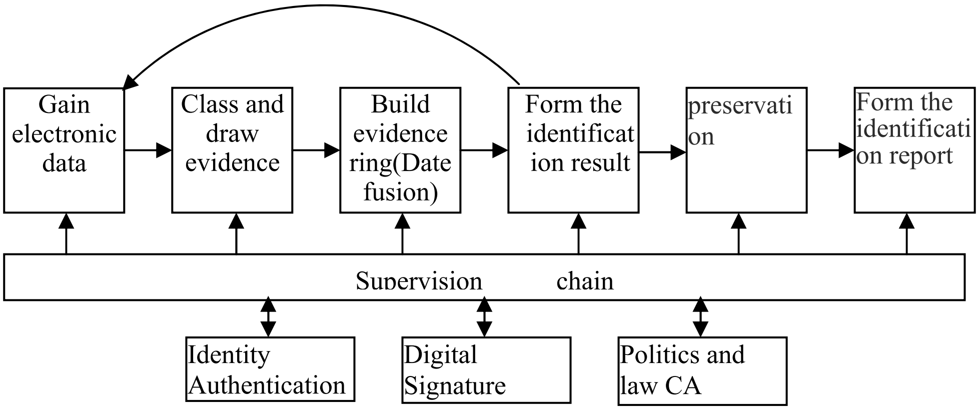

Fig. 1 Computer forensics Model Based on Evidence Ring and Evidence Chain

3.2. Data processing and classification

- Gain electronic evidence and class

Electronic evidence is easy to loss compared to traditional evidence and electronic evidence can not be seen if we don't use the tools. Therefore, in the process of collecting electronic evidence, the original data may result in serious changes. Computer forensics must be fully prepared, including: personnel qualifications for forensic and evidence collection tools to prepare, the licensing laws. Because of the negligence of the work may change or destroy the original, so the first is to do image for the electronic data storage disk, and analysis on the image is more secure than on the original.

- Build evidence ring

Between the evidence and the case there is no definite link can determine a precise objective of support. If there is a connection between the evidence and can confirm each other, then the evidence of support of the case is relatively large. if an evidence is isolation, regardless of their form of expression can not be used alone to prove the facts of the case. In order to give full play to demonstrate the role of evidence, we build the evidence ring. Specifically, this paper adopts the method of data fusion associated with integration of the evidence. The related definitions are as follows:

Def1: Evidence: Here evidence is the people knowledge and an experience that is the conclusion after people's observation and research, which is expressed with the character A.

Def2: Supportability: A digit which constructs in the objective evidence's foundation, with this digit expressed the support degree to a crime fact. It is expressed with the character m.

The relationships between evidence and supportability satisfy the following equations:

$m(\phi)=0$ and $\sum m(A)=1$

Def 3: Recognition frame: Suppose a decision question, all possible results regarding this question we can realize compose a set, this set is called a recognition frame. For example: Regarding a criminal case, the criminal must have the committing a crime motive, the committing a crime time and the committing a crime tool and so on. Then the crime motive, crime time and crime tool compose a recognition frame.

The form of evidence ring is as follow:

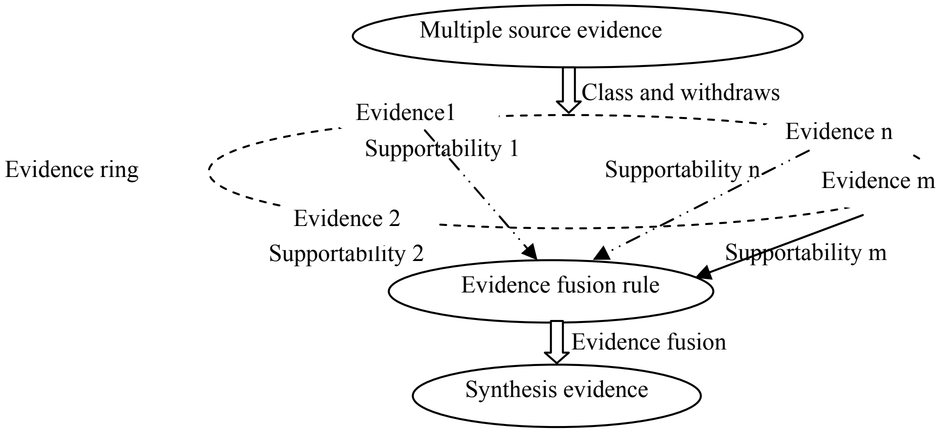

Fig. 2 Form evidence ring (Data fusion)

Dempster synthesis principle reflects evidence joint action. Assigns several supportability to different evidence based on a recognition frame, if these evidences are not conflict completely, then we may calculate a supportability function using the Dempster synthesis principle, this supportability is the comprehensive supportability and these evidence can compose a evidence ring. The initial supportability assigns according to the distribution function based on Dempster synthesis principle.

We regard as the objective existence evidence are the enumeration variables. To a criminal case, there may be some evidence that we express with the characters A1, A2and so on. So the comprehensive supportability (evidence ring supportability) is calculated with the simple match's method. That is how much matched evidence between the electronic evidence we gained and the expert's knowledge and experience (the definition 2). We can calculate it with the equation below:

$$d(I,P)=\sum \frac{m(A_i)}{1} \tag{1}$$

In the equation (1), $d(I,P)$ express supportability that the evidence ring named I to the crimes case named P. $m(A_i)$ is the initial supportability of every existence evidence. In fact, regarding the different case, the role which the evidence plays is also different, to be more nimble we for each evidence supportability establishment weight w. The above formula becomes:

$$d(I,P)=\sum \frac{w_i \times m(A_i)}{1} \tag{2}$$

- Build evidence chain

The evidence chain's formation comes from the evidence rings, therefore evidence chain's proof ability and the certificate strength are decided by the evidence rings' objectivity, valid and the relatedness among these evidence rings. Between evidence chain's each evidence usually was one kind of progressive evolution proof relations, the evidence ring 1 had proven the evidence ring 2 objective existences as well as with its specific relations, finally is proven the fact the existence. The evidence ring is as shown in Figure 3:

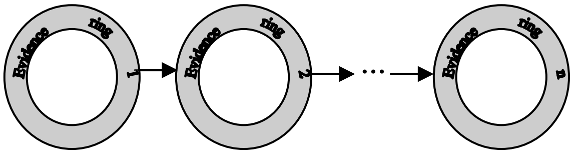

Fig. 3 Evidence chain

The evidence chain's construction, lets the judicial officials stand in the legal commanding point, multi-level, objective, comprehensive, thorough carefully examining and grasps case's fact and the evidence, to the case objective, fair judges.

3.3. Supervision

In order to ensure the validity of the evidence extraction, the objectivity of the evidence and the relatedness between the evidences and the crime case fact, we set supervision module to carry on the entire journey supervision to the evidence collection process. Uses the multi-person digital signature guarantee evidence data integrity which in the surveillance module pokes based on the time; Through the politics and law CA authorized guarantee evidence collection organization as well as the evidence. The process of the supervision can realize the replay of the proces in the whole process, ensure the legitimacy of the electronic evidence, relevance and objectivity.

4. Conclusions

Based on the analysis of the existing forensics model, a computer forecsics model is proposed in this paper. According to the theory of Feng Chunming, the model is based on the evidence ring and evidence chain. By introducing the supervision mechanism, estabilish a supervision chain from forensics to evidence to the whole process of the hall of the electronic evidence, ensuring the legitimacy, objectivity of the evidence. Through the data fusion method for original evidence to set up the evidence ring, further form evidence chain. Evidence ring and evidence chain also ensure the relevance of evidence. The forensics model not only to adapt in obtaining electronic evidence in criminal, civil and admiistrative lawsuit, but also can be used to guide the judicial practice affairs and theory research. The next step will be research on data fusion part of the weight, how to make it more rational, more accurate.

Acknowledgements

This research is supported by general project of The Central Institute for Correctional Police in 2010 (Research on electronic evidence in computer forensics, No:XYY201003).

References

[1]Zhang Kai, Research on Electronic Evidence[D], Beijing: China University of Political Science and Law, 2006.

[2] Yan Xiai, Yang Jinmin, Chang Weidong, Research of Dynamic Computer Forensics System Based on Honeypot[J], Microelectronics & Computer, Vol.27 No.1, Jan 2010, pp:135-140.

[3]Liang Changyu, Wu Qiang, Zeng Qingkai, Distributed and Dynamic Computer Forensic Model[J], Computer Applications, Vol. 25 No.6, June 2005, pp:1290-1293.

[4]Yang Shumian, Liu Jian, Wang Lianhai, Zhou Yang, Online Collection and Analysis Model of Electronic Evidence for Multi-objective Computer[J], Computer Engineering and Design, Vol.32 No.2, 2010, pp:266-269.

[5]Ding Liping, Zhou Bowen, Wang Yongji, Capture and Storage of Digital Evidence Based on Security Operating Syatem[J], Journal of Software, Vol.18,No.7,July 2007, pp:1715-1729.

[6]Tang Juan, Wang Haiping, Sun Guozi, Chen Danwei, Research on Digital Forensics and its Reliability[J], Computer Engineering and Applications, 2006.10

[7]Feng Chunming, Explanation of the criminal evidence[J], Procuratorial theory and practice, No.8, 2004.