The Application Research on Network Forensics

Hu Jingfang* and Li Busheng

School of Information Engineering, Jingdezhen Ceramic Institute, Jiangxi, P.R. China, 333403

Abstract: With the development of network technology, computer crime, network forensics as a kind of active network security defense, has gained widely research and application. This article detailed introduces the concept of network Forensics, Forensics process, Forensics model and some common techniques and methods, the analysis of the Realtime Intrusion Forensics and other four kinds of typical network Forensics system framework on the basis of the Intrusion detection system is discussed combined with network Forensics system, the feasibility of the proposed and analyzed based on Intrusion tolerance, monitoring technologies such as network Forensics system design thought.

Keywords: Computer crimes, network forensics, intrusion tolerance, network monitoring.

1. INTRODUCTION

With the rapid development of network technology, computer crime means enhance unceasingly. Criminals exploit some techniques such as information hiding, network source trackback and the kernel-level rootkit, which has caused enormous harm to the security of computer systems [1]. However, computer crimes cannot be completely eliminated through network security technology, together with which the function of legal punishment and deterrent power should also be used. Network attack and defense have always been contradictory. The appearance and development of the network forensic technology, a mean of active defense in network security aspect, is just under such circumstance.

As the intersection of computer and law area, the research of computer forensic technology has become one of the hotspots in recent years. But so far, the system theories and methods on it have not been established [3]. Some scholars think that forensic analysis is an analysis process of preservation, reconstruction, filing and translation on what happened for the purpose of collecting evidence from a target machine, reconstructing criminal scenes and providing effective and reliable evidence for lawsuit cases. "Digital Forensics" was recommended for describing all the contents of computer forensics technique as a professional term at the first DFRWS(Digital Forensic Research Workshop) annual meeting in 2001,and defined by this statement, 'The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations '.

2. THE BASIC CONCEPT OF NETWORK FORENSICS

2.1. Difference Between Network Forensics and Computer Forensics

Computer Forensics technology related terminology is very mess, from the point of the development of Computer Forensics technology related, have Forensic Computing and Digital Forensics, Electric Forensics, Computer Forensic, Networks Forensics, and Computer Forensics, Internet network Forensics terms such as, the definition of Angle are different [4]. This paper argues that related to computer forensics technology can be divided into three classes of computer forensics, forensics and electronic network forensics.

Computer forensics in the main method of file copy, the recovery of deleted files, buffer content access, system log analysis, etc., is a kind of passive measures, specific to the network environment.

To discriminate between the traditional computer forensics, network forensics which also demand to confirm and obtain potential evidence with legal force detect the intrusion of network system [5], record crime evidence automatically and prevent further invasion mainly through the real-time monitoring and analysis of network data streams, audit trails and the host system log. But viewed from the current research and application, it seems to emphasize the collection of dynamic network information and the active defense of network security. Meanwhile, some methods and techniques of computer forensics should also be applied in network forensics. For instance, if deletion operation on host machine could be tracked dynamically, attacks attempting to clean traces can be detected early enough and perhaps evidence be restored and obtained dynamically, particularly intrusion detection with a function of taking evidence that is often called Intrusion Forensics [6], which has become a development and research hot spot in the intrusion detection technique field at present and is considered equivalent to the term "Network Forensics" sometimes.

*Address correspondence to this author at the School of Information Engineering, Jingdezhen Ceramic Institute, Jiangxi, P.R. China, 333403;
Email: jdzhjf@163.com

1874-4443/13 2013 Bentham Open

Electronic Forensics is the main research in addition to the computer and the network electronic products acquisition, analysis, and display the digital evidence, such as digital cameras, copiers, fax machines, and even a memory storage function of the electrical appliances product, etc. This is not in this paper, the research category, this paper involved in digital forensics will not contain this type of forensic technology.

2.2. Network Forensics Process

Network packet capture is the first step in the process of network forensics, and then the preservation and analysis of captured network data streams in which the network packets are displayed in transmission order and organized to establish connection in the transport layer between two hosts, which is called "Sessionizing" [2-4]. The correlation of network flow -removing irrelevant data with filter as capturing network flow in certain circumstances, the integrality of data-demanding data streams continuously monitored rather than retransmitted with extravagant hopes for network forensics tools, the rate of packet capture, the above are the primary factor considered in network forensics and analysis.

The electronic evidence of network forensics mainly comes from: network data streams; connecting devices(including various kinds of modems, NICs, routers, hubs, switches, netting twines and interfaces, etc) and network security device or software(including IDS, firewall, Net Gap, antivirus software log, network system audit records, network flow monitoring records, etc).

3. THE MODEL OF FORENSICS

3.1. The General Model of Computer Forensics

Since the 1990 s, people have a lot of computer forensics in the model is put forward, mainly including: the basic process model, the incident response process model, the law enforcement process model and abstract model, etc. Brian Carrier and others on the basis of summarizing predecessors' model integrated computer forensics model is put forward. As shown in (Fig. **1**).

The model is divided into five steps:

(1) Readiness Phases: provide personnel and infrastructure to prepare, make sure that when a network event occurs for the investigation.

(2) Deployment Phases: provide investigation and confirmation mechanism, including the investigation and notify, confirmation and authorization.

(3) Physical Crime Scene study Phases: search, collect and analyze Physical evidence and reconstruct criminal behavior.

(4) Digital Crime Scene study Phases: to get the physical evidence for analysis, to obtain the corresponding Digital evidence.

(5) Review Phases: to summarize the whole process of the archive.

3.2. The Model of Network Forensics

Differing from traditional computer forensics, network forensics which is a mean of active defense in network security aspect is a behavior existent before intrusion, but not occurs after intrusion [7-9]. In addition, it analyzes the probability of invasion constantly, acquires evidence and analyzes in a series of attack stages of network intrusion with real-time defense such as sniffer, invasion, damage and hiding invasion footprint. The Network Forensics Model is illustrated in (Fig. **2**).

4. THE BASIC METHOD OF NETWORK FORENSICS

The relevant technology of network forensics involve the techniques of IDS, Honeytrap,, Malicious Code, Intrusion Tolerance, Network Monitoring and Sensor, Agent, SVM, Protocol Analysis and Network Tomography ,etc. The needs of forensics even can be considered to retain information for potential forensics action in the process of protocols design with the development of network forensics technique.

4.1. IDS

It is one of the hot research fields in IDS and new applying way that use IDS collecting electronic evidence while illegal intrusion and malicious behavior was detected. As a tool of forensic and research, IDS was elaborated in detail by Yuill *et al.* in 1999, and Stephenson created "Intrusion Management Model" in 2000, which has made great theoretical contributions to the effective combination of forensics and intrusion detection and considerable effect in the field of network security in which Gross and Monroe and Sommer are also renowned for their contribution [10]. However, the

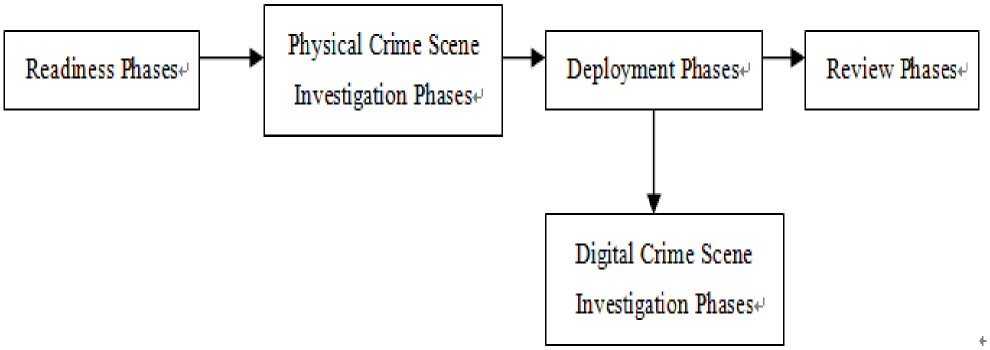
Readiness Phases
Physical Crime Scene Investigation Phases
Deployment Phases
Review Phases
Digital Crime Scene Investigation Phases

Fig. (1). Integrated model of computer forensics.

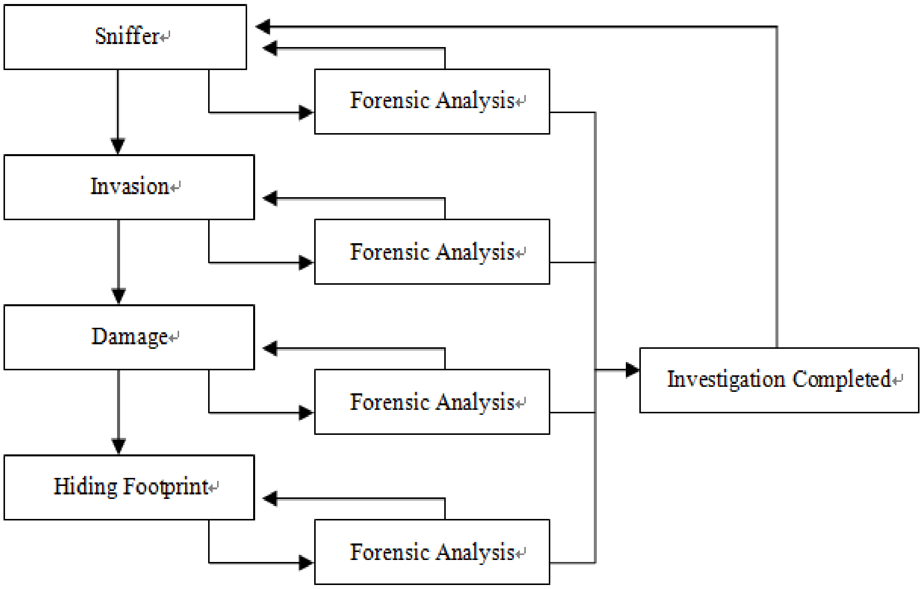

Fig. (2). The Network Forensics.

combinations of the both are still very limited, which provides a broad scope for further research.

The thought to combine electronic evidence collection with system protection produced heated discussions, nevertheless, IDS is certainly the best tool for real-time attack information. Combined with such network security tools or network architectures as intrusion detection for the purpose of dynamic forensics, network forensics will be more systematic, flexible and various with the real-time and intelligent properties, and response quickly.

4.2. Honeytrap

Including such network security techniques as honeypot and honeynet with a core of intrusion deception technique, honeytrap which is a elaborate network trap system monitors the path, tactics, tools and goals of attacker's, and then realizes the function of real-time network forensics by collecting relevant electronic evidence when attacked by hackers [11, 12]. Alec Yasinsac and Yanet Manzano first systematically dissertated the similarity between deception technique and forensics technique and put forward two kinds of honeypot forensics system frameworks-series and parallel, for the purpose of combination of the two. As for intrusion of all this information , whether is it help to bring the criminals to justice, even criminal in itself on account of which being unreal and worthless, yet it is worth our discussion. Besides, honeypot is possible to be turned to the engine of attacking other systems for high-level hackers, which is the risk inherent in this technique.

4.3. Malicious Code Technique

Real-time Forensics techniques often have the interactive problem such as IDS and honey trap. Knowing the network topology structure and layout of security protection [13], the attackers that come from all aspects of interior and exterior of system do anti-forensics activities by the means of interference and infiltration so as to evade accordingly or disturb valid evidence obtained. In order to solve these problems, some scholars advanced and studied a method of concealed forensics using malicious code technique which refers to the evil program with function of concealing in long-term and stealing sensitive information, which is the same principle in forensics.

4.4. Intrusion Tolerance Technique

Firewall technique which is be able to resist the majority of known basic attacks effectively , IDS technology which mainly identifies intrusion behavior from intranet and extranet depending on the known characteristic of intrusion technology-the two are both common network security techniques of attack defense with obvious shortages. Be aimed at ensuring the integrity, authenticity, secrecy of data on the server , the availability of services and the safe operation of system, Intrusion Tolerant System which is a deeper-level anti- attack method referring to the immunogenicity of biology mainly takes into account the system viability in the situation that exists invasion and estimates the impacts caused by invasion rather than analyzes the causes of invasion to solve the current main problems of networks security such as migratory or malicious code, denial of service attacks, internal misuse and malicious behaviors, and faults caused by vulnerabilities in itself. What's more , Intrusion Tolerant System requires the system of attack-resistant operability-the degeneration of system is boundless when it cannot fully-functionally under attack or with unidentified faults, i.e.: the system can maintain limited function rather than completely collapse, and the ability to process dynamic conversion safely, execute and organize under threat. In all, Intrusion Tolerant System process system-infiltrated attack which Firewall and IDS can not effectively resist.

The application of Intrusion Tolerance technique can realize network forensics effectively. Firstly, electronic evidence can be preserved according to the requirement of secrecy of data on the server of Intrusion Tolerant System, which guarantees its legitimacy. Then, the chains of network supervision can be designed according to different running states of the system ,such as normal state, vulnerable state for forensics, degenerative state for Information storage and being -attacked state for forensic analysis. At last, Intrusion Tolerance technique can ensure the validity of real-time forensics of invasion behaviors in the situation that the system doesn't crash and reflect the level of damage by the record of system states.

4.5. Network Monitoring and Sensor Technique

With the capability of data collection and analysis, network transmission content monitoring, website monitoring, real-time monitoring of information on screen and keystrokes analysis and so on, network monitoring system includes such components as host sensor, network sensor and network camera as well as expert system and knowledge base. According to policy setting conditions, it also can trace and alarm in different ways, realize the function of traffic anomaly detection and report on the condition of the systems automatically. The digital information generated by Network monitoring and Sensor can be used as electronic evidence after appropriate chains of network supervision.

4.6. Agent Technique

In recent years, Agent has been widely used in network security fields, especially in multi-agent base intrusion detection in which many research achievements has been made. Distributed real-time active network forensics system based on Agent which has formed a complete forensics system framework by forensics server, forensics database and forensics agent can investigate network intrusion actively and timely and provide adaptive packet acquisition of network traffic as well as the function of data fusion of log system, network traffic and scan investigation, etc. However, this system is imperfect in mechanism of simultaneous collection of host data and network data; in addition, it lacks connection with access control, access authentication, data encryption and some other network security mechanisms.

4.7. SVM Forensics Technique

Generic forensic systems need to preserve all network information, but not all of the information captured or recorded is useful to the analysis [13, 14]. Removing meaningless and useless characteristic points or noise by the discovery of point characteristics of information behavior contributes to the reduction of information storage volume , the enhancement of veracity of detection , the exaltation of computing speed. , which are useful for further analysis , thus the performance of the whole detect mechanism will be improved. Besides, network forensics should be a mean of active defense, which demands not only the detection of known network attack and real-time forensics but also the capability of identification and forensics of unknown network attack or abnormal mode [12-14].

In allusion of them , Mukkamala and H.Sung studied the technique of application of characteristic selection of data packets for forensics, which suggests to be with extend property.

4.8. Protocol Analysis Technique

Network protocol has defined standard and hierarchical network packets in network communication. With the altitudinal regularity of network packets , protocol analysis technique chooses value from set position according to the existing protocol models and then analyzes the protocol in turn thus to compose all the protocols into a protocol tree, of which , a specific protocol is a node and analysis of network packet is a route from boot to leaf.

4.9. Network Tomography Technique

Network Tomography technique works on a similar principle to CT principle in medicine that it acquires network information by statistical inference through a process of sending kinds of probe packets to a specified receiver, observing and analyzing the information obtained by receivers [13]. It is useful to acquire network information that cannot be observed directly, which has been applied to Network Security. For example, it can find the track of DDoS attack form some observing points and ends up finding the attacker. Network forensics based on Network Tomography can trace back intrusion behaviors, tend to form effective chains of network supervision and realize the function of distributed forensics.

5. THE FRAMEWORK OF NETWORK FORENSICS SYSTEM

5.1. Typical Network Forensics System Analysis

Abroad, the study of network forensics system began in the 1990 s, originating in combined with the intrusion detection system, have put forward some preliminary prototype system at home and abroad.

5.1.1. Realtime Intrusion Forensics

Payer's Realtime Intrusion Forensics - (RIF) is the earliest prototype combines Intrusion detection and forensic network Forensics system [7], its implementation is based on a Stack as the core of network Intrusion detection system (NIDS). RIF is the basic thought of the NIDS are integrated into the network operating system of the network Stack, through the Native Stack real-time acquisition packages, and use of state transition, the Memory of the Content [8], the Header Information and Packet Payload simple knowledge of forensic analysis.

Based on this idea, the Payer two prototype system is established, and the intrusion detection mechanism based on the stack are integrated into the network stack, this mechanism can be significant in search mode (Conspicuous Pattern) to make intelligent decisions, the state of the check to track all traverse the network stack each connection.

RIF is available on the host into a "sick" (Pathologic Case) before begin to forensic analysis, and it is worth noting that local stack RIF is the only place to get all the packages.

Redmon introduces a union based on the technology of honey trap trap Network (the Federation of named Decoy Network forensics system framework design, and put forward the evidence to protect the implementation of the mechanism.

5.1.2. Intrusion Forensics Base on the Federation of Decoy Network

A union trap network to provide Production Networks intrusion early warning and legal agent, it is named Decoy Networks, Production network and Cooperative Module and Law Enforcement Networks, through to collecting information from trap network combination, can learn more than the lure of isolation network of knowledge about the attacker intent and ability, can get a global view, the invaders invasion plan and display can be used as evidence in court. Union components in information sharing and collaboration module and collaboration module can feedback the information to law enforcement agents, so that its investigation.

Redmon put forward and discussed about protection and display content of the Retention of the Material problem, points out that the maintenance system in the chain of custody Retention involves technical and legal issues, and discuss mainly for the safety of the electronic evidence, imagine an electronic evidence through the union of Hashing Process.

5.1.3. A Network Forensics System Based on Fuzzy Expert System

FESNF by Kim *et al.* Development of a network forensics system based on fuzzy expert system, this system is a system demonstration, experiment, also didn't have the evidence ability the real-time requirement of network environment. FESNF consists of six components:

(1) Network flow analyzer components: main complete capture and analysis of network flow. It requires to capture all of the network flow, to ensure the integrity of the data.

    Analyzer application rules to capture the network stream to restructure. Packet classification rules are the same as agreement and continuous time. Such as: is the ith a restructuring package Si can be represented as Si Time alpha, Protocol (p), alpha said Time intervals, it is a experience value, p for a deal. It said include protocol packets in alpha p time interval.

(2) Knowledge base components: storage used fuzzy rules, the fuzzy inference engine in the form of:

    IF X1=A1 and X2=A2…and Xn=An THEN Y=Z

    Here, Xi and Y is the semantic variable, Ai and Z is the semantic word, before the IF part is the rule, THEN after a part is rules, FESNF defines five rules to identify the TCP port SCAN, TCP SYN Flooding, ICMPsmurf five intrusion, Land, and the Ping Of Death (Z1~Z5 corresponds with).

(3) Blur components: application for each semantic variable fuzzy set membership function is defined, determining each fuzzy membership degree of the input value.

(4) Fuzzy inference engine components: when all the input values are fuzzy variables into their respective semantics, a fuzzy inference engine access the fuzzy rule base, fuzzy algorithm, derived the semantic value of the variable. In before the rules of "minimum" operation, after using the "largest" calculation.

(5) Inverse blur components: the use of "minimum" largest operation produce output values, as input forensics analyzer.

(6) Forensics analyzer: determine whether capturing packets exist, its main function is to collect data, analyze relevant information, and generate digital evidence. If an obscure component of the output value between 0.9 to 0.1, the forensics analyzer to confirm for the existence of network attacks, and automatically generated from the current restructuring package Si digital evidence.

5.1.4. Almulhem's Network Forensics System

Almulhem etc. Also a prototype network forensics system are presented, its structure as shown in (Fig. **3**), the prototype system consists of three main modules:

1. Tag Module (Marking Module) : a web-based modules, identify and tag suspicious packets.
2. Capture module (the Capture Modules) : based on the host module, installed on all of the host, to collect tag package and transfer them to Logging tool (Logging Facility).
3. Log Module (Logging Module) : data processing activities of Logging tools based on network.

Tag module is the core of the system module, is composed of sensors, watch list with the marker, in its prototype system, is composed of two PC to a network forensics system, a capture as a network, as a Bridge, the Bridge configuration as shown in (Fig. **4**), the sensor USES the Snort.

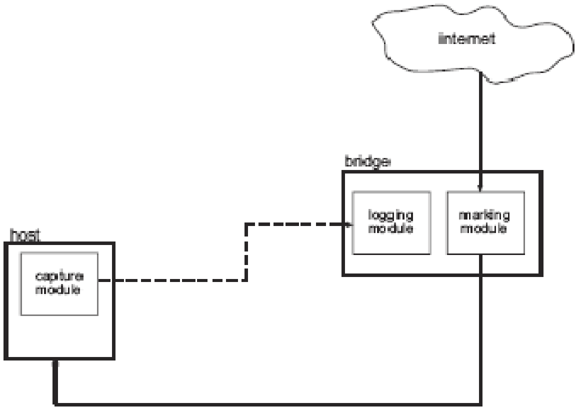

Fig. (3). The overall architecture of the system.

5.2. Network Forensics System Design

Because of the huge number and dynamics of network electronic evidence, forensic analysis depending on artificial alone is not realistic. How to analysis and find the electronic evidence effectively in the massive information is still a problem. In addition, the massive information needs capacious storage media. How to preserve and protect the

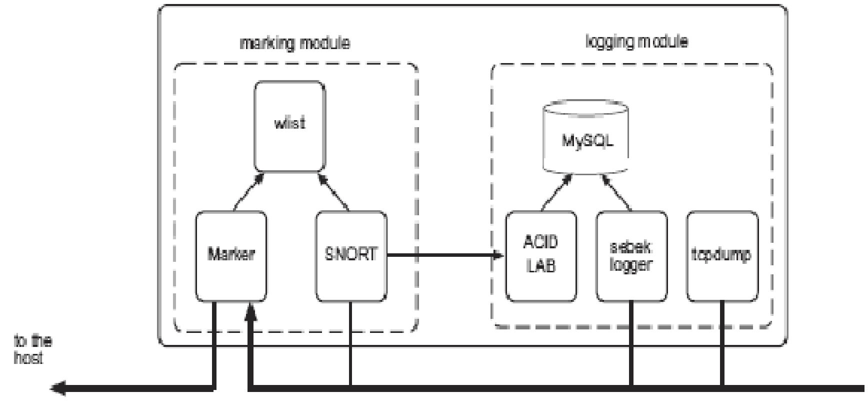

Fig. (4). The bridge Internet.

evidence effectively in the process of the Forensics is an urgent problem. The automatic forensic technology research above the collaborative environment is essential to solve these problems [12]. Since many researchers and computers are involved in those large-scale computer fraud cases, the tracing of the relationship between the object and the criminal evidence turns to be extremely difficult. Correlation analysis is needed so as to track the process of the invasion, then to get the evidence of the crime. The problem is how to make the analytical process automatic and intelligent.

Considering various factors, such as the Internet, the law and the intrusion detection, the design of a network forensics system must contain stored information selection and the design of chain of custody, the ability of invasion tolerance, the positioning capability of attacks, the ability of collaborative forensic analysis, the anti-forensics ability and the standard of information structure. The preservation and analysis of information needs to form the chain of supervision and the evidence must be complete through being collected and being used in the whole process in the court, which the existing design of intrusion detection system hasn't taken into account. To meet users' practical requirement, which is safe and reliable, the three areas: “network", "fault-tolerant” and "security” need cross cooperation [13, 14]. Because the invasion of tolerance is the cross point of the three areas, network forensics system also need to have the ability to tolerate invasion. Network forensics system should have the positioning capability of attacks and meet the forensic needs of law enforcement agencies through the recall and record off attacks. For complex cases, connections between the evidence are considered more legally. The key to successful prosecution of complex invasion also lies in finding out various independent evidences which are relational and confirmed. For network forensics system, since forensics information comes from different network security equipment, the disunity of information structure is hard to analyze the connection between the evidence. Based on the above considerations, network forensics system must have standard format of unified forensics information.

6. FUTURE PROSPECT

Network forensics as an important branch of digital forensics, an emerging discipline has been developed in recent years, there is no formation of the theory, method and system, is not a lot of people are familiar with. Network forensics is introduced in this paper, the relative concepts of computer forensics and digital forensics, the network forensics, electronic evidence and computer forensics made a simple comparison, the basic concept, origin and characteristics of electronic evidence are introduced. Network forensics is to traditional methods and technologies are analyzed, on the basis of comparative analysis of several typical network forensics system, intrusion detection system and network forensics system are discussed combining the feasibility, proposed and analyzed based on intrusion tolerance, monitoring technologies such as network forensics system design thought.

From a technical perspective, the network forensics also lacks the system theory, mainly is the study of the frame structure, it is difficult to meet the needs of the response to the growing Internet crime. We believe that the network forensics will get more and more attention, and will be dealing with Internet crime of last resort.

CONFLICT OF INTEREST

The author(s) confirm that this article content has no conflicts of interest.

ACKNOWLEDGEMENT

Declared none.

REFERENCES

[1] PD Dixon, “An overview of computer forensics”, *IEEE Potentials*, vol. 24, no.5, pp. 7-10, 2005.

[2] Y. Zhihong, L. Zhe and Z. Kuo, “Design and implementation based on dynamic network forensics system”, *Journal of Jilin University (Science Edition),* vol. 46, no.4, pp. 712-720, 2008.

[3] S. Bernato, “The rise of anti-forensics”, [EB/OL] http://www. csoonline.com/article/print/221208.

[4] L. Busheng, “Computer anti-forensics research and implementation based on NTFS file system”, *Computer Engineering*, vol. 20, 2010.

[5] M. Rogers, “Panel session at CERIAS 2006 Information Security Symposium”, Retrieved September 11, 2007, from http:// www. cerias .pursue. edu/symposium/2006/ materials/pdfs/antiforensics. pdf

[6] FORTED, “Richard power. A tour through the realm of anti-forensics”, *Computer Fraud & Security*, vol. 6, pp. 18-20, 2007.

[7] Richard Russon. NTFS Documentation [EB/OJ] .http://www. cribd.com/doc/2187280/NTFS-Documentation.

[8] GRUGQ, "*Digital forensics and the art of anti-forensics*", Germany: Bellua Cyber Security, vol. 2, pp.311-315, 2005.

[9] A. Honingl, "Adaptive model generation: an architecture for deploy of data mining based intrusion detection systems",[EB/OL]. http://citeseer.ist.psu.edu/, [2007-3-2]

[10] U. Payer, "Realtime intrusion-forensics, a first prototype implementation", *TERENA Networking Conference,* pp. 32-36, 2004.

[11] B.J. Redmon, "Maintaining forensic evidence for law enforcement agencies form a federation of decoy networks" [EB/OL]. (CCIPS) http://www.cybercrime.gov/searching.html, [2007-3-2]

[12] J. S Kim., K. Minsoo, B. N. Noth, "*A fuzzy expert system for network forensics*", The 2004 International Conference on Computational Science and Its Applications (ICCSA 2004), Perugia, Italy (LNCS), pp.117-129, 2004.

[13] A. Almulhem, I. Traore, "*Experience with engineering a network forensics system*", Jeju Island, ICOIN (International conference on information networking), vol. 3391, pp. 62-71, 2005.

[14] M. Huang, T.M. Wicks, "A large-scale distributed intrusion detection framework based on attack strategy analysis", *Computer Networks*, pp. 2465-2475, 1999.

Received: August 13, 2013 Revised: August 28, 2013 Accepted: August 28, 2013