International Journal of Grid and Distributed Computing
Vol. 9, No. 12 (2016), pp.75-86
http://dx.doi.org/10.14257/ijgdc.2016.9.12.07

Design and Research of Hybrid Network Electronic Forensics Model Based on Cloud Computing

Tian Junfeng and Li Weiping

School of Computer Science and Technology, HeBei University, Baoding, China
cppsulwp@163.com

Abstract

With the increase of computer network crimes and the changes of the forms, the work of the network electronic forensics is becoming more and more important, and it is required that the technology of electronic forensics should be adapted to the development of complex network crimes. In this paper, the traditional electronic evidence collection technology and the electronic evidence collection method in recent years are studied, and then the hybrid network electronic evidence collection model based on cloud computing environment is proposed, which can work for electronic forensics in dynamic, fast and real-time ways so as to fight against network crimes more effectively.

Keywords*: Electronic Forensics; Cloud Computing; Network Crime; Proxy*

1. Introduction

With the continuous development of computer networks, and the continuous emergence of new protocols, new technologies and new products, the technology of network crime is also more and more complex, with endless performance forms. In order to effectively combat these network crimes and to maintain justice in the virtual environment of computer network, it is necessary to have more powerful and detailed evidence of network crimes, and network electronic forensics is the most effective way to obtain evidence.

Electronic forensics work is a necessary process to prevent and combat computer network crimes and maintain the judicial justice. Especially in the rapid development and application of cloud computing having a profound impact on the social and economic development today, the occurrence of illegal crimes on the cloud computing platform becomes more and more frequent. Beijing Network Security, Beijing Network Security Anti-fraud Alliance and 360 Internet Security Center jointly issued "Report on the Big Data Research of Internet Fraud Crimes in China" showing that in the first three months of 2015, Beijing Network Security Anti-fraud Alliance has received a total of 4920 cases of Internet fraud cases, 1147 cases from 360 mobile phone users, with the per capita loss of 7252 Yuan. For the crimes occurred in the cloud, the traditional method of computer forensics appears to be inadequate. The traditional model of evidence collection is mainly based on static evidence, for the evidence collection and protection of objects, with analysis of evidence in a closed and safe environment so as to obtain forensic results. In addition, the electronic evidence in the cloud is often very large data, which can not be processed online. This requires security storage. The traditional centralized physical storage platform has been difficult to meet the needs of large scale data storage in the process of evidence collection, which has become one of the main reasons for the development of cloud forensics technology. For the storage of electronic evidence in the cloud environment, how to guarantee the origin and integrity of the electronic evidence and to enhance the credibility of electronic evidence has become one of the important research contents of forensic management. In this paper, a new framework of cloud

ISSN: 2005-4262 IJGDC

forensics is proposed which is combined with the theory of dynamic comprehensive forensic technology and TCB trusted computing, not only can effectively extract the dynamic data in the cloud computing, but also guarantee the validity of the evidence.

Problems such as relatively poor effectiveness of traditional method of evidence and the mass storage of electronic evidence have become the focus of further research in the development of modern network.

2. Researches on Electronic Forensics at Home and Abroad

Electronic forensics technology researches based on the cloud computing environment have been put forward at home and abroad. Keyun *et al* listed some of the key issues in the field of cloud forensics, such as what challenges clouds forensics are faced with, what opportunities they have brought, how many valuable research studies there are [1]. Birk *et al* analyzed the technical difficulties faced by the cloud forensics [2], and Reilly *et al*. analyzed the legal obstacles of the cloud forensics technology from the view point of law [3]. Martini and Choo proposed a basic theoretical framework of cloud forensics in 2012, in which the evidence collection process was divided into four basic steps, namely, Evidence Source Identification and Preservation; Collection; Examination and Analysis; Reporting and Presentation [4]. Subsequently, Dr. Zhou Gang from Huazhong University of Science and Technology proposed a method based on field transfer technology, which regarded the virtual machine instance as evidence analysis object [5]. When there was evidence demand, the virtual machine would be transferred to the locality, and the memory mapping, network connection and other volatile data would be preserved in the migration process. Then, the virtual machine instance was loaded in the locality; and finally, some traditional forensic tools were used to carry out the evidence in the virtual machine. Although the method can effectively obtain the evidence from the virtual machine in the normal operation, when the virtual machine instance is not loaded due to malicious damage by the user, the method will fail.

Dynamic forensics is still a relatively new research approach in the field of computer forensics [6]. Dynamic forensics [7] is combination of forensics and intrusion detection, honeypot technology, firewall technology for real-time access to illegal intrusion operating records and intelligent analysis of intrusions, to take appropriate response measures according to the strategy, and to ensure the target host with minimal damage. At the same time, submit and save the obtained evidence. There are some dynamic forensics concept of logs collection and analysis system [8][9][10], Grobler, *et al*. proposed that the dynamic forensics method is still in the development stage, and there is no standard definition and standardized process; at the same time, users should participate in the process of forensic analysis as little as possible. So, they put forward a multi component view of forensics process [11].

Hegarty *et al*. proposed the theoretical framework of dynamic forensic system [12], and described the goal, the realization step and the different dimensions of the dynamic forensics system. The paper also defined three modules of the dynamic forensics system, and discussed the relationship among these modules. The purpose of the framework is to provide some theoretical basis for the implementation of dynamic forensic process in large organizations.

There are also some related references mentioned the relevant theory, principle and design principle of dynamic forensics, such as S Patel R *et al*, put forward the hybrid framework of application and network crime [13]. These literatures provide some good paradigm on the research of the dynamic forensics. However, these documents do not actually implement a dynamic forensic system, or lack experimental data to prove the feasibility of the dynamic forensics system.

Clay *et al*. designed and implemented a dynamic forensic system for file system, which can achieve the purpose of dynamic forensics by monitoring files having been modified,

copied, and deleted [14]. After the implementation of the system, the author has carried on the experiment to the resource consumption of the system. It is found that the dynamic system of the file system is very small, thus it is demonstrated indirectly to be feasible to monitor the dynamic system for other information. In summary, although the dynamic forensics system is not a completely new idea, there is no actual dynamic forensic cloud model that can easily integrate the existing computer forensics tools, and at the same time, there is the lack of experimental data to prove the feasibility of the cloud dynamic forensics model, as well as the assessment and verification for the cloud dynamic forensics system.

This paper presents a hybrid network electronic forensics model in cloud computing environment, which will effectively improve the performance of electronic evidence in real-time, dynamic monitoring, compression and classification, and then improve the real-time requirements of electronic evidence in the current complex network environment, as well as the requirements of mass storage through the strong computing power and mass storage capacity, based on the network behavior and network crime taking the protocol as the main technical means.

3. Hybrid Network Electronic Forensics Model Based on Cloud Computing Environment

As shown in Figure 1, there is a private cloud in the model, which is composed of a large number of high performance computers and network attached storage devices. Each node in the cloud uses a distributed peer-to-peer structure, with the functions of cloud computing and cloud storage, which is an important part of the model. The model is divided into five parts: (1) control center. It is the core of the whole system, connected with the private cloud, to manage all related node in the private cloud in a centralized structure. (2) The operation proxy, which exists in the private cloud in distributed peer-to-peer structure under the management of the control center, mainly responsible for data operation and storage; (3) Additional storage, stored in the private cloud in distributed peer-to-peer structure, which can be directly operated by the control center and the operational proxy, mainly responsible for data storage of electronic forensics. (4) Monitoring proxy, which is located in different protected private networks, are used to dynamically collect electronic evidence from various private networks. (5) Information gathering terminal equipment, such as intrusion detection system, firewall and other security facilities, located in different private networks that are protected. As the private network environment is different, the content is not the same, with the main responsibility for monitoring the network information, to provide electronic evidence for monitoring proxy.

3.1 Control Center

It is a high performance computer, and its functions include: to develop forensics rules, standardize forensic data format, receive the directory index of electronic evidence information from the operation proxy, which is also the important background user interface. When the user needs to call the electronic evidence, it can easily and quickly find the required electronic evidence through classification index of electronic evidence stored in the database by the control center. The host is connected to a directly attached storage device, specifically for its services. Since network electronic evidence is a mass of data, it needs to classify preservation by the network attached storage devices in the private cloud. And the directly attached storage devices connected to the control center is only to store the location of network electronic evidence, like catalogue in the book, so it is used for the specific location of electronic evidence.

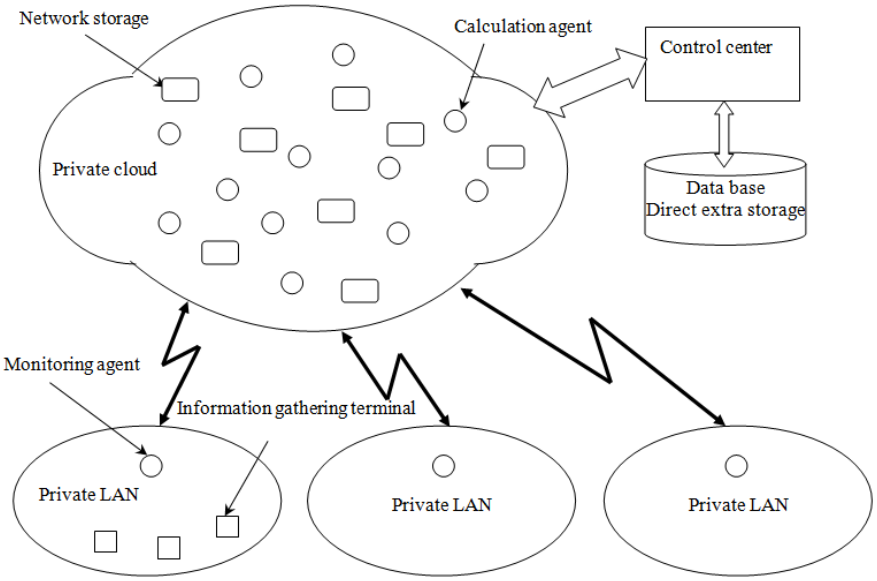

Figure 1. Composite Model of Network Electronic Proof Collection in Cloud Computing

3.2 Operation Proxy

Because they interact directly with the control center, it is called the first level proxy. They are a group of high performance computers in the form of clusters, with the distributed peer-to-peer architecture in the private cloud network. Their main function is to receive the electronic evidence data from the monitoring of the proxy for the audit, specification and analysis, then the structure will be stored in the corresponding network attached storage device, and finally the index of the storage data is uploaded to the control center, for the full preparation of the data. Related electronic evidence is stored in a private cloud storage pool in the form files, and the index is sent as a message to the control center and is written to the database by control center.

3.3 Network Attached Storage

Data storage devices in private cloud, which consist of a large amount of network attached storage devices, exist in the private cloud network in a distributed peer-to-peer way, like a huge data storage pool logically. Its main function is to store network electronic evidence. Because the network electronic evidence has characteristics of huge amount of data, a wide variety and requirements to maintain a long time and so on, a single storage device can not be competent, thus this private cloud storage technology is used. This technology is based on the distributed file system, to form a shared data access storage pool through a highly fault-tolerant technology in the cloud, which is like a huge and high performance data storage devices logically, with features of massive data storage, high reliability, large throughput capacity and so on. They can both be accessed by the operation proxy and be controlled by the control center.

3.4 Monitor Proxy

Because they are indirectly connected to the control center through the operation proxies, they are also known as the second level proxies. They are located in the private local area network which needs the protection and monitoring, such as the campus network, the internal network of business or government departments, *etc*.. The function is to receive the network information and the host logs from the local area network intrusion detection system, honeypot system and firewall and other security transmission

components, then form the preliminary data for electronic evidence and upload to the computing proxy regularly.

3.5 Information Collection Terminal

They are network security components in their own arrangement of private LAN, such as intrusion detection, honeypot, firewall, bastion host. Because of their own characteristics and requirements in the various private LAN, information collected terminal content in each private LAN is not the same. Their main function is to upload a variety of information, including network behaviors from external users and internal users, and the log information of key hosts, to the monitoring proxy with the a regular transmission mode, the transmission cycle differing according to different network characteristics. The transmission cycle is important, for the transmission cycle is too long, and the real-time performance of the electronic evidence will be poor; but if the transmission cycle is too short, it will add unnecessary network overhead, and take up the network bandwidth.

4. Design of Distributed Proxy under Cloud Computing

From Figure 1, we can see that the control center is important, but the characteristics of network electronic evidence are a huge amount of data, the forms of diversification, and the more dispersed sources. Compared with different types of network, the focus and characteristics are also different, so the workload will be very large if these network electronic evidences are described in uniform, and upload to storage devices in dynamic and real-time way. Obviously, single high performance host can not complete such a huge amount of work. So this paper will divide the huge job into several small logically independent contents, and then use different devices to complete these tasks.

From the above analysis, the focus of dynamic network electronic forensics needs to address two aspects: first is to regulate the relative rules of using the electronic evidences with different types, different characteristics and different requirements for the index after storage in order to facilitate the query; secondly, to collect separate electronic evidence of different network for classification and upload. Solid model is used in the form of second proxy to complete these two tasks, close to the control center to be the first proxy (Computing Proxy), downward to be second proxy (Monitoring Proxy). Figure 2 shows the logical relationship of the five major functional components in which proxies are acted as the core.

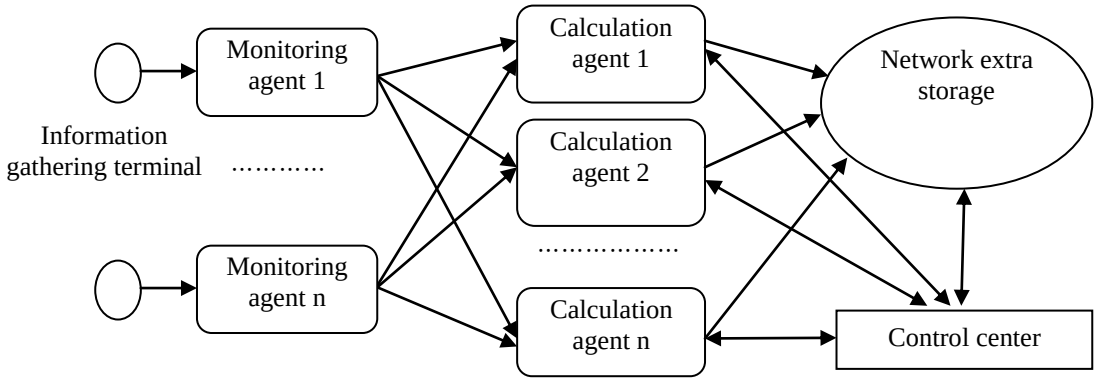

Figure 2. Logical Relationship between Five Functional Modules

In Figure 2, the one-way arrow indicates that the data can only flow along the direction of the arrow, and the two-way arrow indicates that the data can flow with both directions. It should be noted that the monitoring proxy can not directly communicate with the

control center and the network attached storage, but only send data to the operating proxy in one-way direction, so that the data and control center can be protected.

What to solve the first problem is the computing agent in the private cloud. Many high performance computing models are distributed in the cloud, and they are mainly responsible for the conversion and specification of electronic evidence data format, for the storage of the electronic evidence data and index, and upload them to the control center. These hosts also need to be classified for handling different types of network electronic evidences, so that the whole system can also process data orderly. For example, there is much of electronic evidence based on network behaviors, and more numbers of such agents can be deployed; while there are less electronic evidence based on the host, then the agents are less deployed; so that the computing resources in private cloud can be made full use and better complete the task of electronic evidence collection.

The second problem to solve is the monitoring agents in the various private local area networks, which are responsible for collecting electronic evidence from the terminal security device in the local network, and then uploaded to the first-class agent. When the data of electronic evidence is uploaded, two main tasks are **r**equired to solve: (1) to determine the type of electronic evidence, and decide which kind of computing agent to upload. (2) after deciding which type of calculation agent is uploaded, the current workload of the group and a balanced load are determined for the final decision to send to that particular computing agent. These two tasks need two levels of agents to be completed. There is a computational agent information table in each monitoring agent. The main contents of the table are the host address, the type of evidence and the current workload. The initial formation and operation of the information table is that the formation and renewal of the above information is sent by the calculation agent regularly.

5. The Design and Implementation of Data Types and Formats of Electronic Evidence

As the structure, function and characteristics of the private networks are different, the form of network electronic evidence is diverse, but according to the characteristics of network intrusion behavior, these data can be standardized. In this paper, each part of electronic evidence is stored in the form of document. It is divided into two types of content: first is the evidence document composed of original data packet. Because the original data is very large, it is not willing to make a copy of all network data packet. However, since the first 128 bytes of the general packet contains the information of each layer protocol and the front end of data, such as 20 bytes of the IP first protocol, 20 bytes of the TCP first protocol, plus 88 bytes of information of HTTP protocol, therefore, it just needs to copy the first 128 bytes of data packets and produce into the evidence file. When the data packet is less than 128 bytes, it is copied totally, thus the amount of data will be greatly reduced. Secondly, is the description of the behavior or operation of the log file, usually in the form of text file, with the main description of the integrated information of the network or the host operation, such as the addresses of the communicating parties, time, protocol, *etc*.. This kind of file is a comprehensive file, which is analyzed by means of computing agent by summarizing data packets.

5.1 Types of Electronic Evidence Data

From the whole category, it is divided into three major categories: electronic evidence based on the network, electronic evidence based on the host, and electronic evidence based on the protocol. (1) Electronic evidence based on the network: mainly for the visitors to the entire network, such as which network domain to log in and log out, online time, bandwidth taken up the network (the total flow of data packet, the time flow of data packets, the total flow of bytes, and the time flow of the byte unit), *etc*.. (2) Electronic evidence based on the host: mainly for the visitors to a specific server or host, such as time access to the server's, duration, requested services, *etc*.. (3) Electronic evidence based on the protocol: mainly for the visitors to a specific program or service process in the operation, such as the scanning of certain well-known port, the detection for network shared services, *etc*.

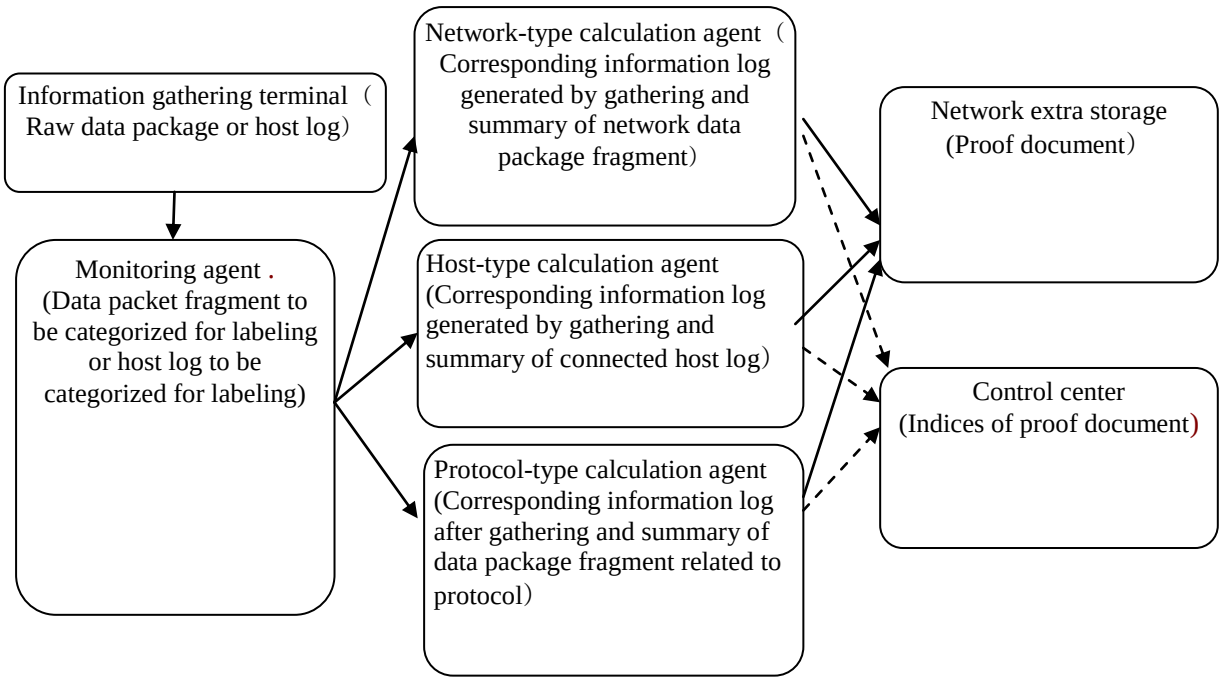

Figure 3. Proof Data Flow Direction and State

Further description and complement should be done after determining the large types, such as the visitor's host address, the destination address, the establishment of the connection, the use of the protocol and port numbers, access time, duration, times, whether it takes CUP, storage devices and printout equipment, and other information on the number of units, such as access to the data traffic and total data traffic. Monitoring proxy will form a file and name the information, and regularly send to the operation proxy, and then after the format conversion, summary, statistical and other processing by the operation agents, a complete electronic evidence is formed combined with the corresponding original data packets, and is stored in the network attached storage; finally they are made into the query index, and uploaded to the control center. Figure 3 shows the flow and the names of the evidence data in each component. The solid line in the diagram refers to the flow direction of evidence, and the dotted line refers to the index information of evidence after file storage.

5.2 Format of Electronic Evidence Data

In this model, the electronic evidence is a form of file, which is divided into three major categories, that is, based on the host, the network and the protocol. The three kinds of network evidence are applicable for different environments, in which network evidence based on the host is mainly applicable for the event that a single server or workstation is directly operated by illegal personnel. The intruder of this kind of event takes the non-authorization operation on the host directly through illegal means, but not through the network. Because of the host logs in the computer operating system record some of the key operations on the host, so the host log file on the server or workstation protected by the electronic evidence based host can be packed and uploaded to the calculation agent in accordance with the upload cycle in time unit. Since the log file of the host is generally small, and the content is also the log record of the host nature, the electronic evidence based on the host only needs to be labeled with the time and the host name or the host address, without other required documentation.

This model focuses on the definition of two types of electronic evidence based on network and on protocol. These two types of electronic evidence from the file forms can again be divided into two types of documents, the first is the original network data file, called the data file for short, and the other is the corresponding summarized information description document file, called the description document for short. The former is the collection of the first 128 bytes of information for each network packet. For the network or key nodes that are protected, if each network packet is recorded and copied, the workload will certainly be extremely large, so it is not feasible whether from the execution time or storage space. Because the first 128 bytes of each packet are basically the main information elements of the packet, the first 128 bytes can be copied and packaged in integration, which will greatly reduce the time and space on the resource consumption, thus to achieve the purpose of effective storage of electronic evidence.

In order to effectively distinguish different electronic evidences, the two important parameters of the relevant host address and the sampling time are taken as the data file names to uniquely identify electronic evidences from various network or key nodes. The corresponding description document has the same root name as the data file, but with different extension names. In this way, a set of electronic evidence will have a unique identity to distinguish it from other electronic evidences. The following will describe the main contents of description documents in the electronic evidence files based on network and on protocol.

(1) Electronic evidence based on network: the application environment of this kind of electronic evidence is mainly based on the whole network as a unit, which mainly records the behavior data of the whole network from users. Table 1 shows the content and description of the record of this description document.

Table 1. Content and Explanation of Description Document based on Network-based Electronic Proof

Content name	Explanation
Identification	Host address of visitor and time of starting visit, same with filename.
Related address	All host addresses related to visitors in the protected network.
Related port	Visited related port number （service） in protected network, should match host address.
Related connection	Concrete information of all connection, including connection times,connection identification and connection time, *etc*.
Total flow of data package	The visitors' occupancy of network traffic flow and other resources, with number of data package as the unit.

Data package flow per second	Correspondence speed rate of the network occupied by visitors, with number of data package / second as the unit.
Total byte flow	Occupancy of network bandwidth and other resources by visitors, with byte as the unit.
Byte flow per second	Correspondence speed rate of the network occupied by visitors, with byte/second as the unit.
Related operation	Related operation content conducted by the visitors to entire network

(2) Electronic evidence based on protocol: the application environment of this kind of electronic evidence is mainly based on the network protocol, which mainly records the behavior data of a specific service process in the host of the protected network. Table 2 gives the content and description of the record of this kind of description document.

Table 2. Content and Explanation of Description Document based on Protocol Electronic Proof

Content name	Explanation
Identification	Address of the server providing service and starting time of visiting, same with filename.
Protocol	The service provided, such as FTP , DNS or SMTP, *etc*.
Command or request	Concrete content of request sent by client to server
Related host address	Address of all clients that visit server
Related connection	Concrete information of all connections related to protocol, including connection times , connection identification and connection time, should match related host address.
Total flow of Data package	The visitors' occupancy of network traffic flow and other resources, with number of data package as the unit.
Data package flow per second	Correspondence speed rate of the network occupied by visitors, with number of data package / second as the unit.
Total byte flow	Occupancy of network bandwidth and other resources by visitors, with byte as unit.
Byte flow per second	Correspondence speed rate of the network occupied by visitors, with byte/second as the unit
Related operation	Concrete operation content of visitors' visiting server, such as which page is visited, which file is downloaded.

5.3 Realization and Description of Electronic Evidence

Figure 4 and figure 5 give a data file of two simple electronic evidence based on the network and on the protocol respectively. As the corresponding description documents have similar contents and description, they will not be given any more.

Time	Source	Destination	Protocol	Info
1 0.000000	192.168.0.2	220.181.27.48	TCP	veracity > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SA
2 0.015173	220.181.27.48	192.168.0.2	TCP	http > veracity [SYN, ACK] Seq=0 Ack=1 Win=2920 Len=0 M
3 0.015202	192.168.0.2	220.181.27.48	TCP	veracity > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
4 0.015533	192.168.0.2	220.181.27.48	HTTP	GET / HTTP/1.1
5 0.038197	220.181.27.48	192.168.0.2	TCP	http > veracity [ACK] Seq=1 Ack=354 Win=2567 Len=0
6 0.039229	220.181.27.48	192.168.0.2	TCP	[TCP segment of a reassembled PDU]
7 0.039254	220.181.27.48	192.168.0.2	TCP	[TCP segment of a reassembled PDU]
8 0.039282	192.168.0.2	220.181.27.48	TCP	veracity > http [ACK] Seq=354 Ack=2841 Win=65535 Len=0
9 0.039609	192.168.0.2	220.181.27.48	TCP	veracity > http [RST] Seq=354 Win=0 Len=0
10 0.048213	192.168.0.2	220.181.27.48	TCP	kyoceranetdev > http [SYN] Seq=0 Win=65535 Len=0 MSS=14
11 0.055106	220.181.27.48	192.168.0.2	HTTP	HTTP/1.1 200 OK (text/html)
12 0.055157	192.168.0.2	220.181.27.48	TCP	veracity > http [RST] Seq=354 Win=0 Len=0
14 0.066796	220.181.27.48	192.168.0.2	TCP	http > kyoceranetdev [SYN, ACK] Seq=0 Ack=1 Win=2920 Le
15 0.066839	192.168.0.2	220.181.27.48	TCP	kyoceranetdev > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
17 0.089890	192.168.0.2	220.181.3.25	TCP	syscomlan > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 S
18 0.090123	192.168.0.2	220.181.27.48	HTTP	GET /img/logo.gif HTTP/1.1
19 0.109199	220.181.27.48	192.168.0.2	TCP	http > kyoceranetdev [ACK] Seq=1 Ack=398 Win=2523 Len=(
20 0.110753	220.181.27.48	192.168.0.2	TCP	[TCP segment of a reassembled PDU]
21 0.111831	220.181.27.48	192.168.0.2	HTTP	HTTP/1.1 200 OK (GIF89a)
22 0.111883	192.168.0.2	220.181.27.48	TCP	kyoceranetdev > http [ACK] Seq=398 Ack=1874 Win=65535 L
23 0.113969	220.181.3.25	192.168.0.2	TCP	http > syscomlan [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
24 0.114010	192.168.0.2	220.181.3.25	TCP	syscomlan > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
25 0.114784	192.168.0.2	220.181.3.25	HTTP	GET /img/gs.gif HTTP/1.1
26 0.136508	220.181.3.25	192.168.0.2	TCP	http > syscomlan [ACK] Seq=1 Ack=396 Win=6432 Len=0
27 0.137560	220.181.3.25	192.168.0.2	HTTP	HTTP/1.1 200 OK (GIF89a)
28 0.137585	220.181.3.25	192.168.0.2	TCP	http > syscomlan [FIN, ACK] Seq=422 Ack=396 Win=6432 Le
29 0.137620	192.168.0.2	220.181.3.25	TCP	syscomlan > http [ACK] Seq=396 Ack=423 Win=65114 Len=0
30 0.138002	192.168.0.2	220.181.3.25	TCP	syscomlan > http [FIN, ACK] Seq=396 Ack=423 Win=65114 L
31 0.159804	220.181.3.25	192.168.0.2	TCP	http > syscomlan [ACK] Seq=423 Ack=397 Win=6432 Len=0

Figure 4. Network-based Electronic Proof

From the electronic evidence given by Figure 4, it can be seen that the host 192.168.0.2 has accessed to the two hosts of 220.181.0.0 network, namely, 220.181.27.48 and 220.181.3.25 respectively, with the number of connections twice, for the duration of 55.1 milliseconds and 111.6 milliseconds; and the request to download two graphics files of logi.gif and gs.gif, of which the total amount of the data packet is 31, packet flow rate of 193.99 per second, with the total byte flow of 8548 bytes, byte flow rate of 53490.5 bytes per second.

Time	Source	Destination	Protocol	Info
1 0.000000	192.168.0.1	192.168.0.2	TCP	imyx > ftp [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
2 0.000071	192.168.0.2	192.168.0.1	TCP	ftp > imyx [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PE
3 0.000236	192.168.0.1	192.168.0.2	TCP	imyx > ftp [ACK] Seq=1 Ack=1 Win=65535 Len=0
4 0.001293	192.168.0.2	192.168.0.1	FTP	Response: 220 Serv-U FTP Server v6.0 for WinSock ready...
5 0.010602	192.168.0.1	192.168.0.2	FTP	Request: USER tcpip2004
6 0.011098	192.168.0.2	192.168.0.1	FTP	Response: 331 User name okay, need password.
7 0.015919	192.168.0.1	192.168.0.2	FTP	Request: PASS ftp_test
8 0.016777	192.168.0.2	192.168.0.1	FTP	Response: 230 User logged in, proceed.
9 0.021170	192.168.0.1	192.168.0.2	FTP	Request: SYST
10 0.021412	192.168.0.2	192.168.0.1	FTP	Response: 215 UNIX Type: L8
11 0.027196	192.168.0.1	192.168.0.2	FTP	Request: REST 100
12 0.027427	192.168.0.2	192.168.0.1	FTP	Response: 350 Restarting at 100. Send STORE or RETRIEVE.
13 0.033111	192.168.0.1	192.168.0.2	FTP	Request: REST 0
14 0.033326	192.168.0.2	192.168.0.1	FTP	Response: 350 Restarting at 0. Send STORE or RETRIEVE.
15 0.038842	192.168.0.1	192.168.0.2	FTP	Request: PWD
16 0.039029	192.168.0.2	192.168.0.1	FTP	Response: 257 "/" is current directory.
17 0.051168	192.168.0.1	192.168.0.2	FTP	Request: TYPE A
18 0.051380	192.168.0.2	192.168.0.1	FTP	Response: 200 Type set to A.
19 0.069902	192.168.0.1	192.168.0.2	FTP	Request: PORT 192,168,0,1,19,137
20 0.070168	192.168.0.2	192.168.0.1	FTP	Response: 200 PORT Command successful.
21 0.075424	192.168.0.1	192.168.0.2	FTP	Request: LIST
22 0.076391	192.168.0.2	192.168.0.1	TCP	ftp-data > commplex-link [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
23 0.076558	192.168.0.2	192.168.0.1	FTP	Response: 150 Opening ASCII mode data connection for /bin/ls.
24 0.076662	192.168.0.1	192.168.0.2	TCP	commplex-link > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS
25 0.076683	192.168.0.2	192.168.0.1	TCP	ftp-data > commplex-link [ACK] Seq=1 Ack=1 Win=64240 Len=0
26 0.076989	192.168.0.2	192.168.0.1	FTP-DA	FTP Data: 1460 bytes
27 0.077020	192.168.0.2	192.168.0.1	FTP-DA	FTP Data: 389 bytes
28 0.077105	192.168.0.2	192.168.0.1	TCP	ftp-data > commplex-link [FIN, ACK] Seq=1850 Ack=1 Win=64240 Len=0
29 0.077376	192.168.0.1	192.168.0.2	TCP	commplex-link > ftp-data [ACK] Seq=1 Ack=1850 Win=65535 Len=0
30 0.077390	192.168.0.1	192.168.0.2	TCP	commplex-link > ftp-data [ACK] Seq=1 Ack=1851 Win=65535 Len=0
31 0.092493	192.168.0.1	192.168.0.2	TCP	commplex-link > ftp-data [FIN, ACK] Seq=1 Ack=1851 Win=65535 Len=0
32 0.092507	192.168.0.2	192.168.0.1	TCP	ftp-data > commplex-link [ACK] Seq=1851 Ack=2 Win=64240 Len=0

Figure 5. Protocol-based Electronic Proof

From the electronic evidence given by Figure 5, it can be seen that this is a FTP based network communication process. The host 192.168.0.1 as a client has accessed to the FTP server 192.168.0.2, its login name is tcpip2004, and login password is ftp_test. After logging, the LIST command is used to display the contents of the root directory in the list;

the connection number is 2, the first connection is not closed; the second establishment time of connection is 16.1 millisecond; the total amount of data packet is 32; packet flow rate of 345.92; with the total byte flow of 30194 bytes, byte flow rate of 326446.3 bytes per second.

6. Conclusion

Along with the development and improvement of the network, the modern electronic evidence collection is characterized by huge amount of data, a wide variety of types and complex evidence collecting process. In these characteristics, there is a lot of technical limitations and lag for the traditional forensics, which is more and more difficult to adapt to the requirements of modern forensics. In this paper, a hybrid electronic forensics model based on cloud computing is designed, and is studied and discussed in depth. The hybrid model combined with distributed computing, storage and centralized management will realize convenient and efficient forensic query, which makes users find the required electronic evidence effectively.

This model uses two-level agents to differentiate the complex network electronic forensics, which assigns logically independent operation, transmission and monitoring functions to each agent with different functions for their own responsibilities, thus it has solved the technical problems such as diversification of the electronic evidence data and complexity of process. The use of powerful computation ability of cloud computing has realized the efficiency of the forensic work. The network attached storage devices in a private cloud have provided massive data storage capacity, and solved the problem of huge data of electronic evidence. The standardization of electronic evidence data format also makes electronic evidence have the characteristics of portability.

In short, the improvement of computer network is becoming faster and faster, and the traditional forensic methods have been unable to do so, which need a variety of new forensic methods for supplement and improvement. The forensic model presented in this paper is started from this point of view, and strives to explore a faster and more effective method of electronic forensics.

Acknowledgements

This work is supported by the Natural Science Foundation of Hebei province (F2016201244) , the Natural Science Foundation of Hebei institution (ZD2015088)and the National Natural Science Foundation of China (Grant No. 61379116).

References

[1] L. De Marco, F. Ferrucci and T. Kechadi, “Reference Architecture for a Cloud Forensic Readiness System”, **(2014)**.
[2] B. Martini and K. K. R. Choo, “Cloud forensic technical challenges and solutions: a snapshot”, IEEE Cloud Computing, vol. 4, **(2014)**, pp. 20-25.
[3] S. Simou, C. Kalloniatis and E. Kavakli, “Cloud Forensics: Identifying the Major Issues and Challenges”, Advanced Information Systems Engineering, Springer International Publishing, **(2014)**.
[4] D. Quick and K. K. R. Choo, “Cloud storage forensics ownCloud as a case study”, Digital Investigation, vol. 10, **(2013)**, pp. 287–299.
[5] Z. Gang, “Research on Scene Migration of Computer Forensics Cloud Computing Environment”, Wuhan: Huazhong University of Science and Technology, **(2011)**.
[6] M. Bashir, J. A. Applequist and R. H. Campbell, “Development and Dissemination of a New Multidisciplinary Undergraduate Curriculumin Digital Forensics”, Proceedings of the Conference on Digital Forensics, Security and Law, **(2014)**.
[7] P. Zhu, Y.-H. Du, “Research on APT-Trojan Forensics based on Virtual Machine and API Monitor”, Netinfo Security, vol. 4, **(2014)**, pp. 78-81.
[8] B. Fu and Y. Xiao, “Accountability and Q-Accountable Logging in Wireless Networks”, Wireless Personal Communications, vol. 75, no. 3, **(2014)**, pp. 1715-1746.
[9] S. Simou, C. Kalloniatis and E. Kavakli, “Cloud Forensics Solutions: A Review”, Advanced Information Systems Engineering Workshops, Springer International Publishing, **(2014)**, pp. 299-309.
[10] P. Khandelwal, “Forensic Model to Classify”, Frontier in Technology, vol. 1, no. 1, **(2014)**, pp. 23-28.

[11] R. C. Hegarty, D. J. Lamb and A. Attwood, "Digital Evidence Challenges in the Internet of Things", Proceedings of the Tenth International Network Conference (INC), Lulu.com, **(2014)**.
[12] R. C. Hegarty, D. J. Lamb and A. Attwood, "Digital Evidence Challenges in the Internet of Things", Proceedings of the Tenth International Network Conference (INC), Lulu.com, **(2014)**.
[13] S. R. Patel and D. Kathiriya, "Heterogeneous Framework for Indian Cybercrime Cases", IJRCCT, vol. 2, no. 8, **(2013)**, pp. 639-643.
[14] S. R. Selamat, S. Sahib and N. Hafeizah, "A Forensic Traceability Index in Digital Forensic Investigation", **(2013)**.

Authors

Tian Junfeng
(1965-), Male, hebei province, Hebei University professor. network security

Li Weiping
(1988-), Male, hebei province, Doctor degree, network security

