The Design of Electronic Data Evidence Collection System Based on C/S Structure

Honghui GONG[1, a], Yanwei XU[2], Ting ZHANG [3]

[1,2,3] Jiangxi Police College, Nanchang 330200, China

[a]gonghonghui@126.com

Keywords: C/S Structure; Electronic Data; Electronic Evidence Forensic

Abstract. In the computer network crime and network security means defense technology escalating the situation, a growing number of technical and legal experts come to realize, is completely dependent on network security technology to combat computer-related crime can not be very effective, it must apply the law deterrent sanctions and technical preparedness to jointly curb cybercrime, Network Forensic technology is in this situation and developed, it belongs to an active network security defenses. But whether it is the concept of network forensics technology or greater extension of the scope of Computer Forensic technology, it has not yet formed the theory, method and system of systems. Computer forensics technology has become a hot research topic in recent years, the field of computer science and law intersect, this paper presents a study on electronic data forensics system based on C/S structure.

Introduction

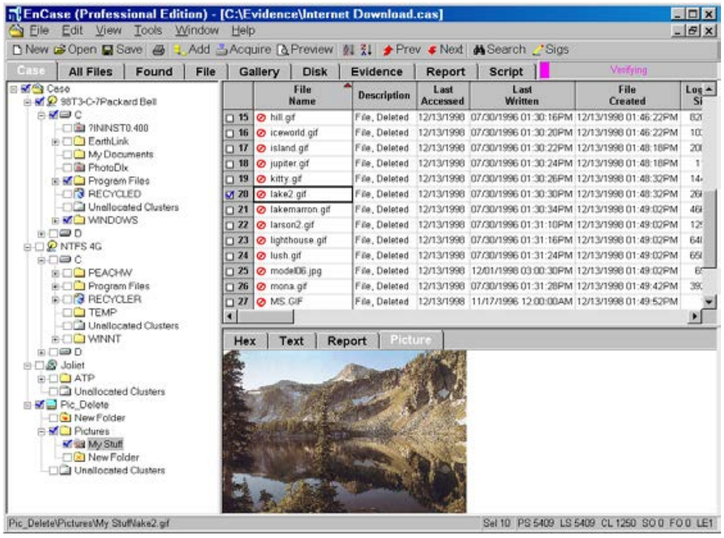
The emergence and development of the Internet, is a profound revolution in human society is and will proceed. Network technology in society brought infinite wealth, but also to the traditional rules of conduct and social order caused a strong impact. Use networking tools and therefore lead to all kinds of disputes and even illegal, a crime against our laws posed a severe challenge. Among them, a key question is whether the electronic evidence and established or not [1-2].

Electronic evidence is in the form of a data message is stored in the computer parts, or because the computer system is running to generate corresponding data message, which includes information and procedures for the process of running a computer program processed. Computer systems for objects and tools of all kinds of new criminal activities have become increasingly rampant, various types of computer crimes that seriously endanger the country's development and stability, the fight against and prevention of computer crime has become a national judiciary to be addressed a major problem [3]. The key is how to combat computer crime perpetrators will remain in the computer system "marks" as a valid evidence provided to the court proceedings, which involves technology is computer forensics technology is people study and attention.

Characteristics of electronic evidence

Computer forensics is mainly to expand work around the computer evidence, the purpose is to reflect offenders stored in a computer and related equipment information becomes effective criminal proceedings the evidence provided to the court. Computer evidence refers to the computer or computer system is running generated electromagnetic record its content to prove the facts of the matter, also known as electronic evidence [4].

Like with traditional evidence, electronic evidence must be credible, accurate, complete, consistent with the laws and regulations, to the court accepted. In accordance with relevant evidence theory, electronic evidence as part of the original scope of the evidence and circumstantial evidence theory. Electronic data forensics examples shown in Figure 1.



	File Name	Description	Last Accessed	Last Written	File Created	Log Si
□ 15	hill.gif	File, Deleted	12/13/1998	07/30/1996 01:30:16PM	12/13/1998 01:46:22PM	82
□ 16	iceworld.gif	File, Deleted	12/13/1998	07/30/1996 01:30:20PM	12/13/1998 01:46:22PM	10
□ 17	island.gif	File, Deleted	12/13/1998	07/30/1996 01:30:22PM	12/13/1998 01:48:18PM	20
□ 18	jupiter.gif	File, Deleted	12/13/1998	07/30/1996 01:30:24PM	12/13/1998 01:48:18PM	1
□ 19	kitty.gif	File, Deleted	12/13/1998	07/30/1996 01:30:26PM	12/13/1998 01:48:32PM	14
☑ 20	lake2.gif	File, Deleted	12/13/1998	07/30/1996 01:30:30PM	12/13/1998 01:48:32PM	26
□ 21	lakemarron.gif	File, Deleted	12/13/1998	07/30/1996 01:30:34PM	12/13/1998 01:49:02PM	46
□ 22	larson2.gif	File, Deleted	12/13/1998	07/30/1996 01:31:10PM	12/13/1998 01:49:02PM	12
□ 23	lighthouse.gif	File, Deleted	12/13/1998	07/30/1996 01:31:16PM	12/13/1998 01:49:02PM	64
□ 24	lush.gif	File, Deleted	12/13/1998	07/30/1996 01:31:24PM	12/13/1998 01:49:02PM	65
□ 25	model06.jpg	File, Deleted	12/13/1998	12/01/1998 03:00:30PM	12/13/1998 01:49:02PM	6
□ 26	mona.gif	File, Deleted	12/13/1998	07/30/1996 01:31:28PM	12/13/1998 01:49:42PM	39
□ 27	MS.GIF	File, Deleted	12/13/1998	11/17/1996 12:00:00AM	12/13/1998 01:49:52PM	

Figure 1 .The case study of electronic data evidence collection

Characteristics of electronic evidence embodied in:

1) Not easy to be found easily be changed or deleted, and changed. Transfer digital evidence and the evidence of different traditions, they are mostly magnetic media as the carrier. Because magnetic media content stored data can be altered, and are not easily leave marks. Therefore doubt the authenticity of digital evidence and security, once a dispute arises, the digital evidence can hardly be accepted as evidence in legal proceedings or arbitration.

2) A variety of storage formats. Digital evidence in a computer as a carrier, and its essence is to store a certain format on a hard disk, floppy disk or storage media of first-class binary code, its formation and reduction should be the use of computer equipment. In addition, with the advent of multimedia technology, digital evidence that mix text, graphics, images, animation, audio and video and other media information, this electronic evidence in multimedia form of covering almost all the traditional types of evidence.

3) Mutilating. Computer information are ultimately represented by binary numbers, in the manner of the presence of a digital signal, and the digital signal is non-continuous, so the reception of digital evidence, listening, abridged, editing and other operations, from an intuitive sense cannot be identified.

4) The high-tech nature. Electronic evidence can accurately store and reflect circumstances of the case, is less affected by subjective factors, which determines the accuracy of electronic evidence it has strong evidence. The collection and review of electronic evidence judgment, often requires a certain science and technology, and even cutting-edge science and technology, and science and technology with the development process will be constantly updated, changed.

5) The transfer process and other extraneous information generally shared channel. Electronic evidence stored on a computer in essence, a computer system generated electromagnetic record was part of its transmission, it is often associated with the flow of information during transmission systems other applications simultaneously. Therefore, when necessary, and these need to be electronic evidence irrelevant information separate, and to ensure this separation process is non-destructive electronic evidence itself.

Electronic data forensics based on C/S architecture technology

The traditional method of electronic evidence is insufficient to meet the rapid development of computer network technology, so that criminals take advantage of, so investigation in trouble. To solve this problem, to explore new electronic forensics Method C/S structure is the inevitable trend of development of great significance. Specific approach is to forensics and electronic discovery software C/S structure environment combined aim is to solve the traditional forensic methods manifested evidence is incomplete, inadequate, use of evidence, not high. In the implementation process should pay attention to three issues - Identify sources of data and evidence collection, evidence clearly the scope and purpose, to ensure the reliability of the evidence. In the computing environment of electronic evidence, many sources of data, different sources of data and evidence collection objects are also different. Client forensics object is a client's file; Supplier forensics objects are smaller memory; forensics object database is relatively large memory. Therefore, to determine in advance forensic data sources is necessary, you can narrow the scope of evidence, save time, and then the opportunity to obtain the best evidence, arrested criminals as soon as possible. The scope and purpose is clear evidence of electronic evidence collection process is the most critical step is to determine the precise scope of the meaning associated with evidence taken of the case, due to be taken to eliminate irrelevant evidence and wasting time phenomenon. In this context, but also to ensure the evidence is true, legitimate, only to extract real and effective evidence, the court will adopt. On the basis of the previous two questions specifically, to ensure the reliability of the evidence taken is also critical, which is the use of C/S structure platform can do, but also to ensure that the evidence must be complete, fully foolproof. Logo C/S structure shown in Figure 2.

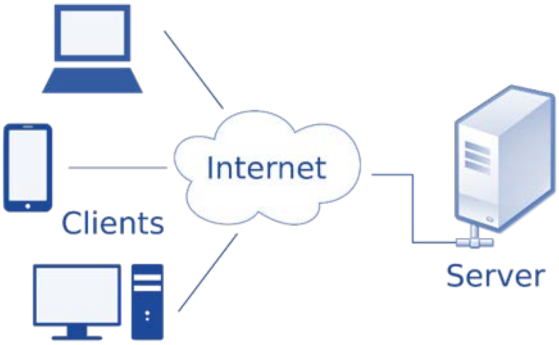


Figure 2. Architecture of the C/S architecture technology

Database application C/S architecture consists of two parts, namely the client application and the database server program. Both may be referred to the foreground program and daemon. The machine running the database server program, called the application server, once the server program is started, it is ready to wait for a response sent to the client request; client program running on the user's own computer, which corresponds to the server computer, the client computer can be called. When the need for data in the database to any operation, the client program will automatically search for the server program, and to its request, the server program to make a response in accordance with a predetermined rule, returned results [5]. C/S structure of the application into two parts, the server is responsible for data management, client interaction with the user to complete the task. But with the growing scale of business, the complexity of applications continues to increase, gradually also exposed its own problems, such as client maintenance of large, complex software upgrade procedure, special network requirements, long development cycle.

The overall design of electronic evidence forensic system

The electronic data forensics analysis is made up of a series of forensic analysis and processing module, interface module and high speed storage server. On the network, the analysis workstation can share these high speed and large capacity server resources. Forensic analysis of the network in the station, you can analyze the same evidence file, you can also analyze different evidence file, at this time, only the evidence file and working space mapped to the machine. The electronic evidence forensic system work flow shown in Figure 3

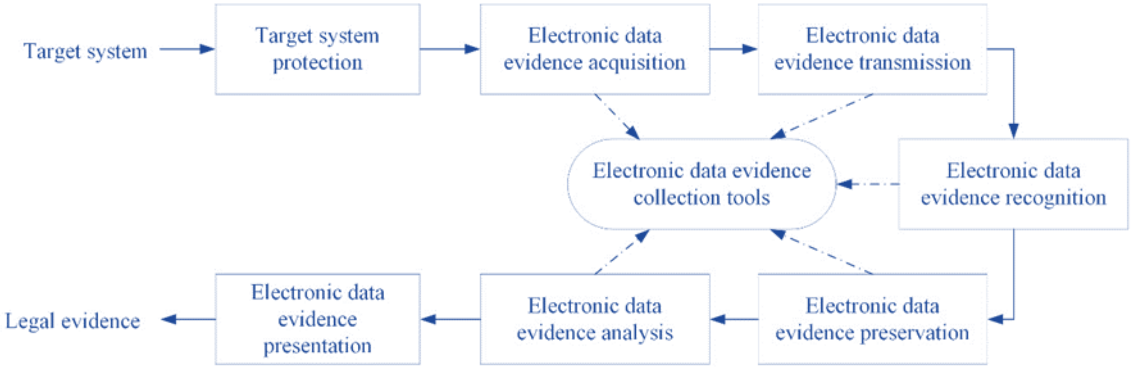

Target system
Target system protection
Electronic data evidence acquisition
Electronic data evidence transmission
Electronic data evidence collection tools
Electronic data evidence recognition
Legal evidence
Electronic data evidence presentation
Electronic data evidence analysis
Electronic data evidence preservation

Figure 3. Electronic forensics workflow

Through research, development and integration of existing mature technology, we developed a set of electronic evidence recovery, search, extraction, preservation and other available and practical tools and software, the development of the program in addition to having the characteristics of a good graphical user interface and ease of operation outside , but also to deal with the scope and content of the evidence, cross-platform electronic evidence described in the development of uniform standards and so on, as much as possible to reduce human intervention in evidence collection process, reduce the purpose of the technical requirements of the user, so that the grass-roots public security organs in the computer technician is missing situation, can grasp and become proficient in the application, and quickly play a role in combat. From the perspective of operational status and operating mode of the computer to analyze electronic evidence can be extracted into the online and off-line analysis and extraction analysis and extraction. Online analytical processing and data analysis to extract refers to in the original machines running state and extraction of off-line analysis and extraction means after the original hard disk clone, clone disk-based data analysis and extraction targeted. Overall design structure of electronic evidence forensic system based on C/S architecture is shown in figure 4.

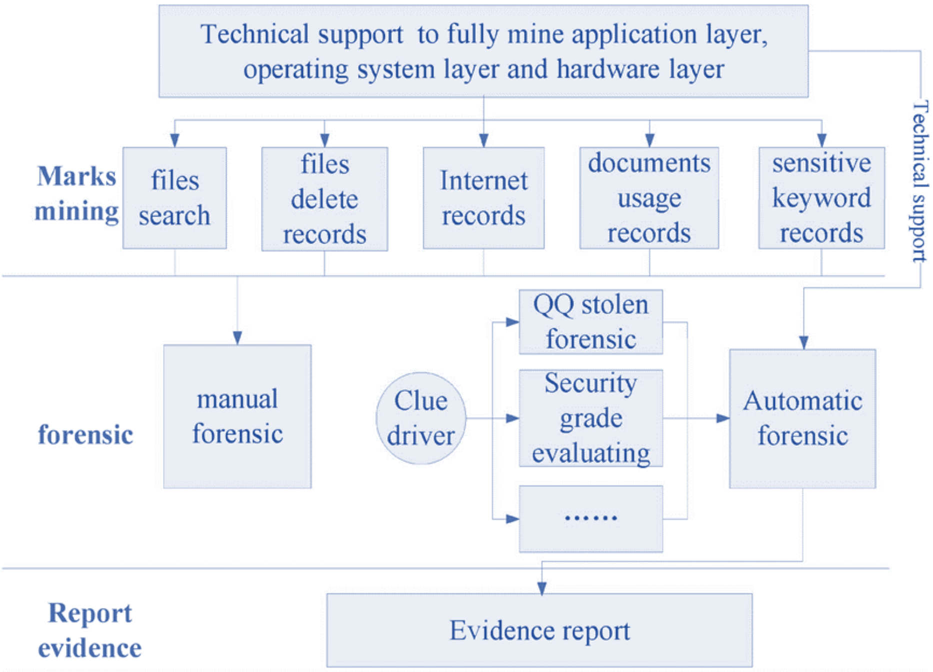


Figure 4. Overall design structure of electronic evidence forensic system based on C/S

Conclusion

With the rapid development of computer technology and the popularity of information technology, people derive a lot of convenience, but at the same time computer crimes are increasing. How electronic evidence obtained through the use of computer forensics to combat computer crime, has become a focus of attention. Most traditional computer forensics is still evidence, so by evidence obtained data is likely to have been damaged. Based on this problem, we designed a dynamic forensics system C/S model, the system enables proactive, real-time forensics, effectively overcome the shortcomings of traditional methods.

This article discusses based on C/S structure system of electronic data takes from the use of standard electronic data forensics technology, standardized electronic data forensics processes and practical methods to start electronic data forensics, forensic work to establish a scientific, standard system mode as the starting point, in summary, sorting a common electronic data base case used in forensics technology methods, scientific systems theory as a guide, according to the legal requirements of work processes to achieve a practical system of electronic data forensics . The system design relies on international common C/S structure of the electronic data forensics tools platform, comply with the standardized forensic tools, full use of the C/S structure of sophisticated electronic data forensics methods, making electronic evidence obtained through this system to become more scientific, credible. The system conforms to the current forensic technology development trend of international electronic data, the overall design from the electronic data forensics actual work, is engaged in electronic data forensics staff a good helper. We believe that both the initial technical staff and senior technical staff, either using the system or carry out more in-depth development of this system, based on the development of this system will play its due role.

Reference

[1] Dykstra J, Riehl D. Forensic collection of electronic evidence from infrastructure-as-a-service cloud computing[J]. Rich. JL & Tech., 2012, 19: 1.

[2] Poisel R, Tjoa S. Forensics investigations of multimedia data: A review of the state-of-the-art[C]//IT Security Incident Management and IT Forensics (IMF), 2011 Sixth International Conference on. IEEE, 2011: 48-61.

[3] Giova G. Improving chain of custody in forensic investigation of electronic digital systems[J]. International Journal of Computer Science and Network Security, 2011, 11(1): 1-9.

[4] Turnbull B, Taylor Sr R, Blundell Sr B. The anatomy of electronic evidence–Quantitative analysis of police e-crime data[C]//Availability, Reliability and Security, 2009. ARES'09. International Conference on. IEEE, 2009: 143-149.

[5] Quick D, Choo K K R. Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?[J]. Digital Investigation, 2013, 10(3): 266-277.