Research on the Application of Computer Network in my country's Crime Investigation

Wenfu Yang  
1College of Internet of Things, Jiangxi Teachers College, JTC, Yingtan, 335000, China  
*Corresponding author e-mail: ywf0701@jxsfgz.com

Abstract. With the development of information technology, more and more computers are used in our daily work and life, it has become an indispensable helper around us. Computer network technology has also effectively improved our country’s criminal investigation technology, this also makes our country gain more criminal investigation methods. This paper mainly analyzes and summarizes the computer network investigation technology.

Keywords: Network Investigation Technology, Data Recovery, Data mining

1. Introduction
The rapid development of network technology allows computers to connect to different networks for interconnection and information sharing. It provides high work efficiency in our country. However, many criminals also use network information technology to commit more secret crimes, or use computer technology to cover up their criminal behaviors. In order to combat criminal acts, we must obtain these important traces in time after committing criminal acts. These are effective evidence against perpetrators of computer crimes.

2. Cybercrime Investigation Technology
Investigation technology is the general term for the specialized techniques used by investigative agencies to discover, record, extract, identify, and appraise various clues and evidence related to the case in accordance with the provisions of the law and the use of modern scientific and technological theories and methods in investigative activities. Investigation technology is an important part of investigation work and determines the progress of investigation work. Network investigation technology is a science and technology that uses computer, network, communication and other high-tech open technologies to form relevant technologies and methods to combat cybercrimes in a targeted manner [1].

2.1. Log analysis technology
A log refers to a record that is generated during the operation of a service or program and can explain the status information of the service or program. The log includes normal and incorrect status parameters. It often appears as a text file in the form of "time + record". There are many logs related to
computer information systems. From the source, they can be divided into service logs such as web site logs, system logs, VPNs, etc. The format of these logs is not uniform, and the amount of data needs to be analyzed with special tools. In addition, logs are mainly based on time. Recording the operating conditions involved in the corresponding services in sequence, generally only reflects the operating conditions of certain specific events, and cannot fully reflect the entire activity of a certain system or user. Therefore, it is relatively single and one-sided, which requires the various types of multiple systems. Logs are combined for analysis to better reflect user activity [2].

Extracting and analyzing logs quickly and accurately is an important factor in determining the efficiency of case investigation. Faced with logs with various formats and huge data, investigators need to have a clear analysis method to analyze the logs.

2.2. Data packet sniffing technology

In the network, thousands of problems may occur every day. All network problems basically originate from the data packet level. They may seem to be applications with beautiful appearances, but in essence they are "except for gold and jade. "Among them", with bad design and useless realization, may also seem to be trustworthy, but it is actually malicious behavior. But at the data packet level, it is impossible to have real secrets unless the communication is encrypted. Therefore, the more research at the data packet level, the better you can understand and control network data. Let investigators better and faster grasp the "essence" of data packets. Therefore, a thorough analysis of data packets is essential.

Data packet analysis technology can be used to understand the characteristics of the network, query the communication subjects on the network, identify possible malicious activities or attacks, network bandwidth usage, and find insecure and Applications that abuse network resources. The packet sniffer is used to analyze data packets to capture and analyze the process of transmitting data on the network. Data packet sniffing technology is a kind of cybercrime investigation technology commonly used by investigators. The collection of information is mainly done by using sniffer. However, if you want to analyze the information further and want to obtain the information needed for the investigation, you may also It is necessary to combine other programs and technical means to filter the data, and then analyze the suspicious data after filtering out [3]. The specific application of packet sniffing technology often requires the support and cooperation of communication operators. Communication operators provide data packet sniffing technology interfaces at the gateway’s population to facilitate relevant law enforcement agencies in cases where the procedures need to be legal. In the case of data packet sniffing technology can be used to intercept related or suspicious data packets.

2.3. Data recovery technology

Data recovery refers to the use of certain technical means to store lost data on electronic devices such as server hard drives, desktop hard drives, laptop hard drives, mobile hard drives, storage tape libraries, U disks, MP3s, digital memory cards, etc. Techniques for rescue and recovery. The reason why data can be restored is determined by the structure of the storage medium and the way the data is stored. For example, after a file on the hard disk is deleted, the file data is not erased from the hard disk, but only the code in the file header is modified to Shows the deletion mark, the real data still remains on the hard disk, which provides an opportunity to recover the data. Therefore, when the storage medium with important evidence is damaged and the data cannot be found, cannot be read or even lost, investigators can use data recovery technology to read through special technical means that it is invisible and invisible under normal conditions. Readable and unreadable data to provide strong evidence for the case [4].

(1) Objects and results

In computer forensics, deleted application files, log files, exchange files, or fragments of a historical file will be important clues to the case. These are the data to be recovered, and the recovery in daily computer use is only for application files. Recovery and recovery effect must achieve "the file is usable". The scope of forensic recovery is not only application files but also system files, and the
recovery results may not be complete or usable. Instead, analysis techniques are used to "reproduce the original data form" and obtain clues or evidence that are beneficial to the case. Even a time, a certain piece of data, or a few bytes may be crucial to the capture of criminals.

(2) Legality

In our country, electronic data evidence can appear in court as legal evidence only for nearly 10 years. At present, my country does not have a specialized electronic data forensics institution, nor has it implemented the certification of electronic data forensics personnel, and in view of the characteristics of electronic data that are easy to modify without leaving traces and the results of the environmental impact are relatively different, whether the forensic process is consistent Procedures and evidence collection tools will affect the legal effect of evidence. Therefore, data recovery should be studied from the perspective of evidence, and the process of obtaining evidence must comply with legal norms to ensure that the evidence obtained has legal effect. Evidence collection should be carried out in accordance with standards, and evidence collection tools certified by relevant departments should be used [5].

(3) Primitiveness

The method of data recovery in the forensic process is different from the traditional data recovery. The data recovery in the forensic process must maintain the originality of the evidence as much as possible. For example, after the hard disk partition table is damaged, the MBR can be repaired by searching for the logical partition and the extended partition. The FAT1 of the FAT partition is damaged and the FAT2 can be overwritten with FAT1 when the FAT2 is normal, but the data recovery in the crime forensics cannot do this. Forensic tools should adopt virtual technology to establish virtual disk to ensure that the forensic object will not be changed. Traditional data recovery is mainly aimed at the availability of data recovery results, while computer forensics is a reconstruction process of computer crime scenes, which aims to discover and extract original evidence.

(4) Trace historical traces

From the perspective of computer forensics, the extraction of trace features should further expand the concept of data recovery. It is necessary to study trace features on storage media to reflect the historical status of data changes as much as possible. After the hard disk is repartitioned, there will still be traces of the original partition, and the logical disk will also leave some traces on the original volume after being reformatted. Especially important is the file operation. The addition, deletion, and modification of files will generate many temporary files and intermediate files in the system, which are very useful traces. According to these trace characteristics, recover the file content or part of the data, which will become a kind of meaningful data. For example, after a file is deleted, although the original storage area of the file is re-allocated, and the file's directory data may still exist, the file's directory data, name, and time attributes may be used as important clues in case investigation or become evidence. According to the above characteristics, the difficulty of computer forensics is far greater than that of general computer data restoration, and its technical requirements are higher than computer data restoration [6]. Computer data repair is only for the data itself. Repairing data is mainly caused by accidents. The data recovery in the computer forensics process is aimed at the evidence of the destruction of criminal suspects. The difficulty of obtaining evidence increases with the improvement of the suspect's computer level. This requires computer data recovery to be researched and developed in accordance with these technical characteristics of electronic forensics.

2.4. Social network packet capture and analysis technology

1) Principle of proxy capture

In network protocol packet capture and analysis technology, network packet capture is the premise and the key. According to the different principles of packet capture, packet capture methods can be divided into two categories: proxy capture and monitor capture.

1. The so-called proxy-type packet capture refers to forwarding between the client and the server through the proxy server. All client requests are first sent to the proxy server, and the proxy server
submits to the remote server [7]. The response from the remote server is first sent to the proxy server and then forwarded to the client. The principle is shown in Figure 1.

![Figure 1. Schematic diagram of proxy packet capture](image)

2. The so-called snooping packet capture means that the packet capture software directly calls the packet capture library to monitor the data traffic from the network card at the data link layer, and then decapsulates and recombines the network protocol layer by layer, and finally provides the user for analysis. Its principle block diagram is shown as in Fig. 2.

![Figure 2. Listening packet capture method](image)

2) Technical process

Network data packet capture and analysis technology means to find out the working principle and workflow of illegal APP/software equipment through the steps of establishing the investigation experiment environment, data packet capture and filtering, data analysis and research and judgment, and continuous tracking of key information. Criminal methods, server interface URLs, number of servers, server IP addresses and locations, users or victims location and other intelligence information, and finally achieve a technology for the purpose of finding criminal suspects. The specific process of technical operation is shown in Figure 3 [8].

![Figure 3. Network protocol data analysis technical process](image)

2.5. Data mining technology

Data mining (Data) refers to searching for the valuable information hidden in a large amount of data through algorithms. Data mining is an interdisciplinary subject, involving artificial intelligence, statistical analysis, information retrieval, machine learning, pattern recognition, etc. Commonly used data mining techniques include decision tree methods, association analysis, cluster analysis, neural networks, etc., and corresponding methods are adopted for different data objects and different mining purposes.

With the advent of the network society, especially the arrival of the Internet + and the era of big data, our lives have truly entered a series of new generation information technologies such as the Internet of Things, smart cities, cloud computing, big data, mobile Internet, and smart manufacturing. As the carrier, the wave of big data has swept across. Massive data has nurtured huge commercial interests, and some criminal groups have been stealing it for a long time. People use the network system to collect, process, store, and retrieve information, and then transmit the information, and ultimately achieve the purpose of resource sharing. In this process, the stronger the dependence on the
network, the more the network system is violated. Its destructive power is greater, its scope is wider, and its social harm is more serious [9].

Therefore, in the face of massive amounts of data, it is necessary to use data mining technology to find the clues of cybercrime in time to carry out effective prevention and investigation. Jack Ma once said that achieving "pre-existing Zhuge Liang" is the most important thing in the entire data era, that is, there must be a preventive mechanism. In the past, the thief was caught by the anti-picking police who physically tracked him day by day, but once he used electronic payment, the police only had to analyze his payment records, and found that the person actually took 50 different buses in a day. Go, compare with ordinary people's usual travel records, then this person may be suspicious. In the investigation of cybercrime cases, the technical means, time of committing the crime, social accounts and content information used in cybercrime against criminal suspects can all be analyzed by association rules to analyze the logical relationship between them, and further narrow the scope. Identify the target

2.6. protocol stack fingerprint technology
The protocol stack fingerprint recognition technology can quickly determine the version of the operating system with a high probability. Although the definition of TCP/IP protocol stack has become a standard, various manufacturers have made different interpretations when writing their own TCP/IP protocol stack. These explanations are called "fingerprints" because of their unique characteristics. Through these subtle differences, investigators can accurately determine the version of the operating system and can further analyze various data packets sent by the system [10].

3. Conclusion
With the development of computer networks, computer network investigation technology is more widely used in criminal investigation. Therefore, our country pays more attention to computer network investigation technology. It can obtain criminal traces more efficiently. I believe that with the development of network technology, computer network investigation technology will be more efficiently applied in criminal investigation.

References
[1] WANG Bao-yong, SONG Bin. Discussion on Electronic Forensics in Computer Network Crime Investigation [J]. Digital Technology and Application, 2010:87.
[2] Su Zhe. Computer Search and Detention and Acquisition of Electronic Evidence in Criminal Investigation [J]. Journal of Jiangsu Police College, 2007:172-172.
[3] Jiang Hanqiu. Investigation and Evidence Collection Path Analysis of Electronic Evidence in Cybercrime [J]. Journal of Anhui Police Vocational College, 2016
[4] Jiang Hanqiu. Investigation and Evidence Collection Path Analysis of Electronic Evidence in Cybercrime [J]. Journal of Anhui Police Vocational College, 2016
[5] Wang Chunliu, Yu Peng. Application of Electronic Data Forensics in the Investigation of Cybercrime Cases [J]. Legal Expo, 2016
[6] Xing Fei. Discussion on the Application of Mobile Phone Forensics in the Investigation of Duty Crime [J]. Shang, 2015:222.
[7] He Yifeng. Application of computer network forensics technology in cracking down on network crime [J]. China Science and Technology Exhibition, 2014:240.
[8] Penmen. Network criminal electronic evidence investigation and protection [J]. Journal of chongqing institute of technology (social science edition), 2012-35-36 + 47.
[9] Penmen. Network criminal electronic evidence investigation and protection [J]. Journal of chongqing institute of technology (social science edition), 2012-35-36 + 47.
[10] Xu Teng. Research on Electronic Evidence in Computer Crime Forensics [J]. Automation & Instrumentation, 2011:178-179+182.