Research on investigation and evidence collection of cybercrime Cases

Yanbo Wu, Dawei Xiang*, JiangMing Gao and Yun Wu
Hubei University of Police Wuhan, China
*Corresponding author Email: 240325743@qq.com

Abstract. Based on the actual data, cases of cyber crimes and the author's experience of attending crime investigation, this article analyzes the characteristics and tendency of new cybercrimes, talks about the requirements of cybercrime prevention and control, and shows us the problems of cybercrime investigation for obtaining evidence. The investigation department should improve the ability to investigate and collect evidence from the material evidence to the electronic evidence. There're some problems that must be paid attention in the process of electronic evidence collection. The readers will get to know the techniques and methods of cybercrime scene protection, site investigation and online tracking in the investigation of cybercrime cases. The basic principles of extracting electronic evidence are expounded. The cybercrime investigation process is refined. The model of cybercrime investigation and evidence collection is constructed.

1. Introduction
As computer crimes have become increasingly rampant, it challenges the cyber police seriously in many countries around the world. According to the survey of various major cybercrime cases in China in the past three years and the author's experience of attending crime investigation, it can be found that the following eight important characteristics of cybercrimes are increasingly highlighted, such as diversification of criminal phenomena, concealment of criminal processes, modernization of criminal methods, the intelligence of criminal organizations, the rejuvenation of criminal subjects, the unbounded criminal groups and regions, the serious consequences of crimes, and the difficulty in investigation and evidence collection.

All of this makes cybercrime cases clearly different from traditional criminal cases in finding clues, filing for investigation, identifying and protecting the sites, collecting and fixing evidence, analyzing evidence and judicial identification, and judicial proceedings, etc. How can we choose the corresponding investigation strategy and investigation method after filing a case? Is there any information involved in the computer system? Can this information be effectively fixed and completely extracted? Whether the case involving cybercrime can be successfully detected... There is no doubt that cybercrime investigation will be a breakthrough to solve all these problems.

2. Overview of cybercrime investigation
The characteristics of cybercrime make cybercrime cases clearly different from traditional criminal cases in terms of law enforcement basis, clue discovery, filing investigation, on-site determination and
protection, evidence collection and fixation, evidence analysis and judicial identification, and litigation procedures. Network detection technology is a frontier and brand-new professional technology in China and even in the world. It has high requirements for the professional knowledge, practical experience and comprehensive quality of investigators. Investigators need a solid foundation of computer science and technology, keep track of the development of network technology, update and improve the knowledge structure in a timely manner, and need to repeatedly participate in investigation and practice, constantly enrich the actual combat experience and improve the level of technology and tactics. Cybercrime investigation specifically refers to public security, judicial, state security organs and other administrative agencies that have authorized the criminal investigation and law enforcement authority to conduct authorized criminal investigations on cybercrime, through the entire process of filing, cracking, and selling cases, including screening clues. Secret investigation, site investigation, arrest and trial, judicial identification, trial and transfer.

Effectively prevent and control cybercrime, there are three main requirements in the investigation.

Requirements for the construction of the investigation agency itself. Since cybercrime is a highly intelligent and high-tech crime, it is necessary to have high-tech detection techniques corresponding to such high-smart crimes as the investigation agencies at all levels to detect such crimes, and to continuously carry out skills training. Strengthen the self-cultivation of investigators. In addition, the investigative agency needs to continuously upgrade its own investigative equipment to adapt it to the requirements of technical investigation.

Requirements for the cybercrime investigation mode. The investigation mode is the idea or routine on which the investigating subject is based in detecting the case. Because cybercrime is different from traditional crime, the detection mode of cybercrime is also very different from the traditional investigation mode. Therefore, we need to study and summarize the cybercrime investigation mode, and gradually form a set of network for the current network. A new type of investigation that is criminal and can effectively detect cybercrime.

Requirements for cybercrime investigation measures. Investigative measures refer to specific means of investigation. Because cybercrime is difficult to find, difficult to obtain evidence, and difficult to arrest, the conviction rate of cybercrime cases is extremely low. Therefore, combining with the characteristics and laws of cybercrime cases, summarizing and improving investigation techniques and methods It is the key to detecting such cases.

3. Detection methods for cyber crime cases

3.1 Cyber crime scene protection

The quality of crime scene protection will have a major impact on whether criminal evidence can be collected, whether the crime fact can be determined and then solved in time. Cybercrime is larger than the time and space of traditional crimes. Sometimes it can be free from geographical restrictions, and even it can be committed across borders. It is difficult to determine the scene. Moreover, because the criminal target is intangible electronic data, the computer system, especially the network system, has a complicated structure, and the forensic work is technically strong, and inadvertent operation may lead to the destruction of evidence. The specific methods for determining the cybercrime scene are as follows:

3.1.1 The case of destroying the physical characteristics of the computer system is obvious, that is, the computer itself and its space.

3.1.2 Based on the information of the case, from the analysis of the criminal suspect's motives, means, computer professional knowledge level, knowledge level, etc., analyze the possible perpetrators and computer for crime, and then determine the scene of the crime.

3.1.3 The crime scene is found according to the contents of the system log or audit record of the computer information system.

3.1.4 Determine the crime scene according to the type, nature and means of crime of different cases.
Focus on the computer that discovered the problem, radiate to other places and equipments connected to the network, and determine the crime scene based on the circumstances of the case.

In addition to hacking cases, most of the cybercriminal murders are internal personnel (sometimes even those who assist in the investigation). Therefore, it is possible to conduct investigations based on computer operators and related business personnel in the victim units. The person, then the person to the scene to determine the crime scene.

3.2 Cyber crime scene investigation

The investigation of cybercrime scene is an activity in which the judicial organ observes, inspects and inspects the crime scene according to law to understand the circumstances of the case and collect relevant evidence. General survey methods for cybercrime scenes:

3.2.1 Study the case, observe and inspect the site, and determine the site and scope of the survey.
3.2.2 Determine the survey sequence according to the site environment and the circumstances of the case. Generally, the computer is used as the center to survey the periphery. For larger sites, the methods of fragmentation, segmentation, stratification, and partitioning can be simultaneously performed.
3.2.3 Record the original scene by means of photography, video recording, drawing, transcript, etc. to "fix" it, and use a scale and a chart to illustrate. For the fleeting images and text on the screen of the monitor, it is necessary to use the method of photography and video to obtain evidence.
3.2.4 Detailed investigation and collection of various evidence. Under the premise of ensuring that the computer information is not destroyed, the suspicious traces of the crimes related to the crime, such as fingerprints, footprints, tool marks, ink, grease, dust, dirt, hair, fibers, etc., are found. Pay attention to various physical evidence, especially various documents such as system manuals, computer operating records, computer printed forms, stock invoices, shipping orders, deposit slips, and burnt or burnt paper, recorded fragments, wiped or Modified records, etc. Extract various magnetic storages that may contain criminal information, mainly mobile hard disks, USB flash drives, magnetic tapes, magnetic disks, optical disks, mobile phones, and the like. If the project is unwilling to surrender, it can be copied and the victim will use the copy. The investigator must pay attention to the original, which is a requirement for evidence.

3.3 Cyber Crime Online Tracking

The investigation of online criminal activities is usually carried out through Internet access IP addresses, Internet access accounts, and Internet access. For network intrusion cases, if a strong Intrusion Detection System (IDS) is installed, it is very beneficial to prevent and track intrusions regardless of whether the user installs a Unix system or a Windows system.

When the IDS system detects an unexpected event, that is, if the network system is suspected of being invaded, it must be checked and judged in time:
3.3.1 First, disconnect the system from the network. Because the network administrator needs to control the environment before making a judgment. More importantly: if the intruder is still online, he will continue to disrupt the work of the network administrator.
3.3.2 Copy all the registration files, including the log file of IDS itself and the event log file (windows NT system) or SYS file (UNIX system) of the network system. Of course, there is a potential problem with this approach, that is, sophisticated intruders can easily cover up their tracks by destroying log files. In addition, it is good to find independent and obvious information in the log information of a large number of log files.
3.3.3 Check the time of the last access to the privileged account (in the Windows NT administrator directory or the UNIX root directory), compare it with the log file saved by the network administrator, and check the command usage record of the account
3.3.4 Find and analyze suspicious circumstances:
Check the latest modification date of the system device file and check if the "password" or "su" binary file has been violated. If you keep a record of these system devices, you need to compare them carefully with the current results. Check the copy of the system management file on the user directory. For UNIX systems, run the "find" command and check the binary file "password" or "su" in the user partition. If you find such files, record the users who own them, the size of the files, and the date of modification, compare them with tools under /bin or /usr/sbin.

Check for the latest changes to the password and user authorization files to find out if there are any abnormal additions or deletions, and whether the user group or user ID number has been changed.

Scan the progress table for activity with or without exceptions. If you find a suspicious process, pay attention to the owner, size, and time of the processor, and try to identify the resources currently being used by the process, such as files and pipes. Scan all open TCP/UDP service ports on the host. Check if the network's daemon is plugged into a Trojan horse by an intruder.

Record the process and content of the above inspection work in words, including the date, host name, user name, and the names of other people present.

3.4 Tracking the trail of intruders
There are also traces of hackers who are looking for it. Here are a few ways to trace the trail of potential intruders:

3.4.1 The intruder will try repeatedly. What the intruder needs to do at the beginning is to collect information about the server in order to discover the details that can be exploited, and then gradually carry out deep intrusions. For example: For the first time, when the network administrator browsed the IDS log, he found that a hacker was scanning the mail server and looking for an open FCD and UDP port. Second, the intruder's IP address appeared again, but this time his target Concentrated on the open port; the third time, maybe a few more hours, the intruder will enter the SMTP command sequence through port 25.

3.4.2 The intruder's access pattern can provide very important clues such as geographic location, occupation, and age. Most hackers tend to move between 9 pm and 3 am, and if the hack happens only between 9 am and 5 pm on weekdays, then the hacker may be attacked at their workplace. The steps of the intrusion process can reflect the skill level of the intruder. A seasoned intruder does not waste time on grammatical errors and repetitive trials; hackers attempting to enter SMTP commands through the NNTP port of the Network News Transfer Protocol are usually a beginner. If the system log is checked in time after the intrusion, you may find that the command log file in the root account directory has disappeared. These signs indicate that it is a skilled hacker attack. He carefully deleted the records of all activities and even fooled the IDS alarm. Mechanism, this is like a spy stealing secrets and then erasing fingerprints. One way to prevent this is to save the log files in several places, and preferably one is stored on a removable medium such as a floppy disk; you must also back up the log files while you are backing up the system data.

3.4.3 Make good use of IDS. The rapid growth of Internet technology has led to the emergence of new attack methods, and IDS developers can only update their products with these changes. In other words, the content that IDS can check and record is based on the methods obtained from past intrusions, but it is difficult to find out for new network attack methods. In addition, even the most sophisticated probing tools are no substitute for manual analysis of intrusion events because automated tools do not have the ability to synthesize information from disparate events. Therefore, for network administrators, the main role of adopting IDS is to filter out irrelevant information in order to concentrate on dealing with really serious network attacks.

4. Cyber crime case investigation procedures
The whole process of cybercrime investigation, including screening, secret investigation, on-site investigation, arrest, trial, judicial identification, trial and transfer, is carried out as the end of cybercrime investigation activities. Common methods include: methods for obtaining case clues, methods for analyzing and characterization of cases, methods for finding breakthroughs in cases, categorization and statistical methods of data information, and correlation analysis methods for case
clues. See Figure 1 for the investigation of cybercrime cases. This paper focuses on on-site protection, site investigation, electronic evidence collection and extraction of cybercrime cases.

5. Collection and extraction of electronic evidence

5.1 Collection of evidence of cybercrime

In the process of detecting cybercrime. It is very important to correctly implement computer forensics and fix evidence of crime. In order to ensure the authenticity of electronic evidence, four issues should be paid attention to in the collection of electronic evidence in cybercrime: collect strictly according to law, collect electronic evidence comprehensively, invite electronic experts to participate, and ensure the privacy rights of the parties.

5.2 Extraction of electronic evidence

Since the main carrier of electronic evidence is on computer media, the extraction of computer evidence, also known as computer media analysis, is the process of finding valuable data from computers and information systems. The principle of computer evidence extraction:

5.2.1 Maintain the originality of the data. That is, the forensic analysis of the data is a copy of the original bitstream of the data on the analyzed machine, which we usually call a clone.

5.2.2 Ensure the continuity of evidence. That is, when the evidence is formally submitted to the court, it must be able to explain any change in the evidence from the initial state of acquisition to the state of appearance in court. Of course, there is preferably no change.

5.2.3 Maintain the integrity of the data during analysis and delivery. That is, analyzing the software and hardware environment does not change the analyzed data, and the data does not change during the data transfer process.

5.2.4 The accreditation of the forensic process. That is, the process of obtaining evidence must be supervised. In other words, all investigation and evidence collection work done by experts appointed by the plaintiff should be supervised by experts appointed by other parties.

5.2.5 Timeliness of evidence collection. It is necessary to restore the destroyed and deleted electronic data in a timely and accurate manner.

6. Construction of cybercrime investigation and evidence collection model

Cyber crime cases are characterized by strong concealment and virtual reality. In addition to the investigation methods of traditional crimes, the investigation should also change the investigation ideas, explore new investigation modes, and adopt new investigation measures based on the network.

The Multi-Dimension Forensics Model (MDFM) reflects the deepening of the forensic process over time. At any time, digital forensics can be cycled back to the state of any node, in line with the real forensic process; The object-oriented concept proposes that the forensic process needs to select the “forensics strategy” and the definition of “knowledge base” according to the “forensic needs”; more rarely, the forensic process is divided into evidence supervision layer, evidence acquisition layer and basic data. The three parts of the layer, in which the data and knowledge base are in the basic position, the evidence acquisition is the main work, and the supervision mechanism at the highest point runs
through, ensuring the integrity of the evidence chain and greatly improving the reliability and legitimacy of the digital evidence.

![Diagram](image)

**Figure 2.** Multi-dimensional investigation and evidence collection model.

**Acknowledgments**
This work was obtained from the mobile intelligent terminal security analysis and evidence collection research of the scientific research program of Hubei provincial department of education (B2016253). The scientific research project of Hubei police college is "research on Internet user data collection and analysis method", and the general teaching and research project of Hubei police college is funded by the fund of "cultivation of students' network intelligence acquisition and analysis ability in public security colleges". At the same time, this paper is funded by Hubei collaborative innovation center for electronic forensics and trusted applications.

**References**
[1] Weibing Wang, Hao Qin. Application of network packet catching and analysis technology in the investigation of network crimes [J]. Journal of People's public security university of China: natural science edition
[2] Shisheng Yang. Countermeasures and Suggestions for the difficulty in investigation and evidence collection of network crime cases [J]. Employee legal world: under,2014,0(9):38-38.
[3] Ting Chen, Yongzhao xie. Evidence collection, review difficulties and countermeasures of electronic data in cybercrime cases [J]. Journal of public security: journal of Zhejiang police college,2016,0(3):31-35
[4] Corey Vicka, Peterman Charles, Shearins Sybil, Greenberg ichael s., Van Bokkelen James. Network Forensics Analys IEEE Computer Society, 6(6): 60-66
[5] Statistical report on the development of Internet in China (the 40th) August 4, 2017, page 2-3, Beijing, China Internet network information center (CNNIC)
[6] Yonghao Mai, Guozi Sun, Rongsheng Xu, Shijian Dai. Computer forensics and judicial expertise [M]. Beijing: tsinghua university press,2009:281.
[7] Linsong Qian, Bo Long, Yonghao Mai. Research on the influence and countermeasures of CSDN user information leakage event [J]. China information security,2012,25(1):78-80
[8] Xiaosheng Tan. Security and risk analysis under the situation of "Internet +" [J]. China information security,2015,66(6):49-51