Application research of electronic forensics technology in internet pornography cases

Dawei Xiang, Yanbo Wu*, Min Jiang
Hubei University of Police, Wuhan, China

*Corresponding author Email: wuyanbo687@126.com

Abstract. Studying cybercrime investigation and evidence collection has important practical significance for improving the detection rate of network cases and curbing cybercrime. The article expounds the objectives, basic processes and key technologies of electronic forensics. Through a real case, it analyzes the principles and conditions of remote access to the records in the database, and proposes a method for remotely obtaining data to verify the electronic forensics technology in the case of “cyber pornography”. The actual forensic process. Finally, the countermeasures and suggestions for the investigation and evidence collection of cybercrime cases are put forward.

1. Introduction
With the rapid development of China's economy and the increasing openness of the market, domestic lawless elements are constantly learning and exploring the fresh experience of international cybercrime groups, using the latest network technology to evade attacks, such as using virtual hosts and hosting hosts to build websites. Some countries or regions in the country, or through the overseas service agencies that provide agency services, publish websites, and then use these websites as a platform to conduct remote command and control of agents at all levels, and to recruit members in the territory through the establishment of information websites and advertisements throughout the network. During the organization of criminal activities, the network address and domain name were continuously changed dynamically, and the investigation and attack by the public security organs were evaded, which led to the continuous increase of the investigation costs of the public security organs and the increasing difficulty in handling cases. How to effectively combat cybercrime has become an urgent need for public security organs and the whole society to ponder and urgently solved problems. It is extremely urgent to take decisive and effective measures to curb cybercrime.

2. Electronic forensics overview
The direct application of electronic forensics technology is mainly reflected in the actual combat of public security, judicial practice and national security[1]. The goal of e-discovery generally refers to solving these five problems through digital forensics methods and means: “find who (who), when (when), where (where), by what method (how to “What is the criminal activity”, referred to as “five W”[2]. Of course, the specific objectives should be determined before the start of the forensic activities, based on the needs of the case and the clues that have been discovered. On the one hand, the
case can be ascertained through the digital forensics process, and serious crimes can be brought to
court to crack down on criminals. On the other hand, The electronic forensics process restores the truth,
clarifies the facts, and the suspects are innocent[3].

At present, China does not form a unified standard for forensic work processes. Under normal
circumstances, the electronic forensic process is carried out in accordance with the following four
steps[4]. The evidence collection process is shown in Figure 1.

```
Figure 1. Forensic process.
```

Prepare for evidence, objectively analyze the object of evidence collection, select appropriate
forensic tools, and develop a plan for evidence collection.

The evidence is fixed, the original evidence is legally fixed, and a copy of the original data is made.

Data analysis and evidence extraction, analysis and processing of the obtained data copies, search
and extract data related to the case and able to prove the facts of the crime.

Evidence is presented and the electronic evidence obtained is submitted in a court-approved form.

3. "Network porn" case study

3.1 Basic case

In June 2017, a network supervision system of a city network received a report from the masses: found
a pornographic website on the Internet. After receiving the telephone instructions from the political
supervision committee of the network supervision detachment, the author immediately began to
investigate pornographic websites and conduct online forensics. The results of previous investigations
show that this is not an ordinary cyber porn site, but a network alliance that provides a large number of
child pornography materials and multiple related sites. After discussion by all the police officers of the
investigation team, the following conclusions were drawn:

3.1.1 These websites are all released by overseas ip (United States). It is difficult to trace them. There
are few successful precedents in China, but most of the websites are domestic netizens, and the impact
is very bad.

3.1.2 According to the same characteristics of the website and certain posting contents, it is suspected
that the website manager is the same group and should be in the territory at present;

3.1.3 The affiliate website is not a pornographic website. It mainly publishes child pornography. This
not only violates the laws of our country, but also violates the laws of most countries in the world,
because the publication of adult pornography websites is not illegal in many countries. Behavior, but
the publication of child pornography has been a serious crime by most countries in the world.

3.1.4 Due to the above reasons, the case can be smoothly applied for Interpol to conduct an
investigation, and the overseas judicial institution can be reasonably required to close the website.

After careful consideration, the network supervisors finally decided to make a case investigation on
this extremely difficult case. After special investigation methods (this content is confidential, it is not
disclosed here) and the investigators' selfless work, in mid-August, Wang, the main administrator of
the website alliance, was arrested in a coastal city, but Wang and his "boss" (Gao) contact with a single-line, never met, and after Wang was arrested for 3 days, the user password of the remote login website server operating system was changed by Gao, and some of the contents involved in the website were deleted, making forensic and tracking work impossible. Afterwards, the case was deadlocked.

Fortunately, the investigators skillfully used the web backup files on the laptop of the suspect Wang, crossed the operating system of the overseas server, and successfully obtained the database records on the US server remotely, and finally completed the forensic work and succeeded. Traced to the exact location of Gao, the case was successfully detected.

3.2 Forensics process
In the face of new types of online fraud crime cases, the public security organs handling cases must first make a record of the case in daily work, analyze and contrast the methods of committing crimes and the law of crime in many online fraud cases[5]. Judging the criminal dynamics by sorting out and analyzing the statistics of various cases. Secondly, it is necessary to actively collect information on fraudulent scams (such as QQ group and WeChat group) in the network environment within the jurisdiction, and keep abreast of criminal trends. At the same time, the public security intelligence information system is used to analyze and lock the clues of the ID card number, mobile phone number, online record, accommodation record, flight record and train record of the person involved[5].

Conducting cybercrime investigation and evidence extraction requires specialized electronic equipment and a complete set of statutory procedures, which can only be carried out by people who are familiar with the appropriate technology and have the appropriate law enforcement qualifications[6]. In the process of data collection, the case should be correctly classified and appropriate investigation ideas and modes should be selected[7]. A timely summary of the investigation process is a problem and new inspiration. For cybercrime, investigation and evidence collection should be as pre-positioned as possible, especially online forensics and remote forensics activities. Otherwise, once the criminals destroy the evidence in advance, it is very likely that the case-handling personnel will return without success and ride the tiger.

After the network case occurred, the investigators collected network information and evidence of crime through remote forensics techniques in order to ascertain the facts of cybercrime[8].

3.2.1 Website data protection. Dynamic websites and static websites can be used as a fundamental distinguishing mark by whether or not there is back-end database support. Generally speaking, criminal suspects making pornographic websites are basically dynamic, and definitely have back-end database support. Generally, a specific script file (asp, php, etc.) is used to connect to the database, and then access, extract, add, modify, delete, and back up the recorded data through the database. In order to ensure the security of the data on the website, the current common practice is to use the DAC control method. In layman's terms, at least two passwords must be set:

The first password is the password that enters the operating system. It constitutes the first protection for the data on the operating system. If the password of the operating system is obtained, the remote login operating system can directly access all the webpage code stored in the hard disk of the computer. And database files.

The second password is the password to enter the database management system. Currently, most relational databases support this function to meet international standards (SQL92 or SQL99). It constitutes the second protection for the records in the database, can be associated with the password of the operating system, or can be set independently. If the suspect sets a separate password, even if we obtain the password of the first operating system, at best, Obtaining a complete database file, but
because the database content is encrypted by the second password, the specific record content in the database file cannot be read. To obtain the specific record, a large amount of decryption work is performed on the second password.

3.2.2 Remote acquisition of records in the database. During the investigation of the case, we obtained the system remote login password of the US server by interrogating the captured suspect and found that its associates have modified the system password of the overseas server, so that we cannot directly log in to the server remotely. It is also impossible to directly obtain any data in the database from the operating system of the overseas server, and the investigation work is blocked. In the past, the investigation work will stop here, and it is difficult to continue tracking down from this line.

Fortunately, we found a backup of all the webpage code of a child pornography website on the suspect’s laptop. This backup is exactly the same as the webpage code of the suspect’s website on the overseas website. In the script file that connects the PHP web page and the back-end database, the PHP web page connects to the database script generally requires 4 parameters:

```
$sql_server_name="localhost"; /* database server name */
$sql_username="******"; /* Connect to the database username */
$sql_password="******"; /* Connect to the database password */
$sql_database="******" ; /* The name of the database */
```

These parameters represent the database server's name or ip address, database user name, database password, and database name. If the PHP web page and the database are placed on the same server, the database address will be filled in as localhost by default. If the web page and the database are not in the same server, the ip address of the server where the database is located must be filled in the relevant code of the web page. Implement the connection, for example:

```
$conn=sql_connect("127.0.0.1","root","123456");
```

The first field is the ip address of the database server, and the last two quotation marks are the username and password. The username to connect to the database is in the trusted state. By default, the "root" user is used, which is the root user. As mentioned earlier, the password of the database can be set separately or not. By default, the database considers the operating system to be secure and trustworthy. Generally, the password is not set separately. At this time, the password of the database is the same as the operating system password. This is also a mistake that database beginners can easily make, but in general, it will only bring security risks to the database.

The investigators use the same PHP webpage code on the suspect's laptop and on the foreign server to build a website on their own machine that is identical to the one on the overseas server. The website and the website on the overseas server use the database in the US server as the back-end database. The only difference is that the $sql_server_name parameter on the overseas website is filled with "localhost", indicating that the database is local, and the website made by the investigator fills in the IP address of the foreign server on the $sql_server_name parameter.

The sly fox can’t escape the good hunter. The criminal suspect Gao is a hundred secrets, only changed the login password of the operating system, but forgot to change the login password of the background database. Therefore, the investigator successfully crossed the operating system of the overseas server and directly connected the background database, thus remotely. Obtained evidence of crime and data of great value for further investigation of the case.

4. Methods and techniques for extracting computer evidence

4.1 On-site system inspection

Try to get as much volatile data as possible before taking evidence collection steps on a running
computer system, such as: data in registers and caches; data in memory; network connection status; status of running processes, etc. Table 1 lists the steps to obtain these data and the commands to implement them[9].

Table 1. steps and commands.

| step                                      | command |
|-------------------------------------------|---------|
| Create a new shell                        | cmd.exe |
| Record system date and time               | date,time |
| Determine the login person                | loggedon |
| Record open sockets                       | netstat |
| List the process of opening a socket       | fport   |
| List the currently running processes      | pslist  |
| List recently connected systems           | nbtstat |
| Record system time                        | date,time |
| Record the steps taken                    | doskey  |

When checking the running system, it must be recorded. Because the commands are executed on the victim computer and the environment is changed, the investigation records determine the system changes caused by these behaviors later.

4.2 Mirror backup of the production evidence

In the evidence investigation, the first consideration is to follow all the rules of evidence. The best option is to protect the original drive from making a valid evidence mirror backup. When making an evidence mirror backup, first check the low-level system configuration BIOS to determine the drive geometry of the evidence medium and the boot order of the system.

First of all, to create a boot disk, be sure to avoid booting from the evidence drive, and make sure that the DRIVE.BIN driver file is not loaded. At the same time, write lock technology is used to intercept any write request to the evidence driver.

4.3 Analysis of log files

Log files are often the main object of network detection and the main form of electronic evidence. The understanding of the location distribution of computer system log files is conducive to the smooth progress of the investigation process, and helps to quickly and accurately collect log files[10].

The Windows operating system maintains three separate log files: the system log (sysevent.evt), the application log (appenent.evt), and the security log (seeevent.evt). System logging records system process and device driver activity. Windows audited system events include device drivers that fail to start, hardware errors, duplicate IP addresses, and start, pause, and stop of services; application logs include information about user programs and The activities of commercial general purpose applications. The application log can include events audited by Performance Monitor, such as the number of failed logins, disk usage, and other important metrics; system auditing and security processing used by Windows can be found in the security log[11].

Security events audited by Windows include changes in user privileges, changes in audit policies, changes in audit policies, file and directory access, print activity, and system login and logout.

The following information can be obtained by examining these logs:
- Identify users accessing specific files;
- Identify users who successfully logged into the system or attempted to log in to the system.
but did not succeed;
- Track the use of specific applications;
- Track changes to the audit policy.

In actual cybercrime cases, criminal actors often use the characteristics of electronic evidence to create falsehoods, conceal or destroy evidence, making it more difficult for us to obtain electronic evidence. At the same time, we should also examine and judge the evidence throughout the entire process of forensics, properly preserve the electronic evidence, and make all relevant records so that the electronic evidence we obtain is legal and effective.

5. Countermeasures for the investigation and evidence collection of cybercrime cases

Due to the openness, randomness, internationality, non-distance, degeneration, and intelligence of the Internet, cybercrime has become increasingly rampant[12]. The author believes that in the case of cybercrime cases, it is necessary to adhere to the method of fighting against each other in order to receive the effect of treating both the symptoms and the root causes. The so-called "hit" is to strictly use various networks to engage in illegal and criminal activities, so that they do not dare to do it. Among them, electronic forensics is one of the means to effectively combat cybercrime; "defense" means to prevent the work technically. So that it can't be. The "defense" in thought is to raise awareness, actively carry out online struggles, strengthen ideological and cultural education, and vigorously popularize scientific and cultural knowledge. Especially in the aspect of technical prevention and control, we must strengthen network construction and network management, improve network blocking technology, and conduct network security research[13].

Electronic forensics technology has been applied in the fight against crimes and has played an active role, but there are also deficiencies in the actual application process. With the rapid spread of mobile Internet and the characteristics of networked crimes, a single static forensic model can no longer meet the actual needs of combating crime. Dynamic forensics technology needs to be applied to the electronic forensics process of criminal cases[14].

China's public security organs should absorb all kinds of fresh experiences in the special action of abduction and combat telecommunication fraud activities, and change the ideas and strategies for managing illegal crimes on the Internet as soon as possible[15]: on the one hand, we must change from passive to active, and then engage in passive evidence collection to network information and personnel dynamics. Carry out active evidence collection to realize the transformation of post-attack and banned to early warning and comprehensive defense; on the other hand, we must pay attention to the unilateral action to domestic and foreign, domestic and foreign action or even multi-party linkage, and seek cooperation and stability through various diplomatic platforms. The mutually beneficial and win-win international police cooperation mode not only achieves the concentrated strike effect of various short-term special actions, but also realizes the favorable situation of long-term effective system control and comprehensive management.

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] Junbo Fu. Analysis on the Development Trend of Electronic Data Forensics Technology[J]. Information and Computer, 2016(2): 68-69
[2] Yanbo Wu, Dawei Xiang , Yonghao Mai. Application Research of Electronic Forensics Technology in "Falungong" Cases [J]. Police technology. 2015,(4):48
[3] Chao Xu. Discussion on the Standardization of Electronic Data Forensics in Cyber Crime[J]. Information Network Security, 2014(9): 157-160, [15]
[4] Yonghao Mai, Sun Guozhen, Xu Yusheng. Computer Forensics and Judicial Identification (2nd Edition). Beijing: Tsinghua University Press, 2013.
[5] Xueguang Wang. Research on Digital Forensics and Related Legal Issues [J]. Computer Science, 2014.10: 110.
[6] Xiaosheng Tan. Security and Risk Analysis under the Situation of “Internet +”[J]. China Information Security, 2015, 66(6): 49-51
[7] Zhonghong Ma. Research on the New Difficulties and Countermeasures of Cyber Crime Representation Based on Telecom Fraud—Based on the Investigation of W Province[J], Journal of Chinese People's Public Security University: Social Science Edition, 2018, (3): 78- 86
[8] Linsong Qing, LONG Bo, MA Yonghao. Research on the Impact and Countermeasures of CSDN User Information Leakage Events[J]. China Information Security, 2012, 25(1): 78-80
[9] Yonghao Mai, Guozhen Sun, Yusheng Xu, Shijian Dai. Computer Forensics and Judicial Identification [M]. Beijing: Tsinghua University Press, 2009: 281
[10] Wenhua Luo. Reviewing the game between the prosecution and the defense of the new Internet crime case from the fast broadcast court[J]. Journal of China Criminal Police College, 2017(2): 111-115
[11] Jizhen Zou, Yiheng Gao. Discussion on the method of investigation and experiment in cyber crime[J]. Network ecurity technology and application,2017(4):187-187,189
[12] Casein He. Application Analysis of Electronic Data Forensics Technology [J]. Information and Communication, 2016(5): 146-147
[13] Shisheng Yang. Countermeasures and Countermeasures for the Difficulties in the Investigation and Obtaining of Cyber Crime Cases[J]. Employee Law and Law: Xia, 2014, 0(9): 38-38
[14] Sen Wen. Application of Electronic Forensics Technology in Drug Crime Cases [D]. [Master thesis] Lanzhou University of Technology, 2014
[15] Ting Chen, Yongzhao Xie. Difficulties in the collection and review of electronic data in cybercrime cases and countermeasures[J]. Journal of Public Security: Journal of Zhejiang Police College, 2016, 0(3): 31-35