Research on Computer Forensics Technology based on Data Recovery

Duan Ruibo[1] and Zhang Xiong[2]

1Yunnan College of Foreign Affairs & Foreign Language, China,651700

2Songming County Public Security Bureau, China,651700

Keywords: computer forensics technology; data recovery; computer crime

Abstract: With the rapid development of information technology, fundamental changes have taken place in the way people work. However, computer crime has also become the main type of cases in the Internet era. Therefore, computer forensics technology has become an important research content of computer crime evidence collection. Firstly, this paper analyzes the relationship between computer forensics and data recovery. Then, this paper analyzes the steps of computer forensics. Finally, this paper analyzes the application of anti-forensics technology and computer forensics technology.

1. Introduction

With the popularization of information technology, computer network high-tech crime has become a new cancer, which has seriously threatened people's life and property security. At present, the means of crime has become more and more high-end, which has many characteristics, such as concealment, high intelligence, complexity, degree and so on. However, in order to cover up the fact of cyber crime, criminals will destroy the data and electronic evidence involved in the case, which can effectively help them escape the risk of law. In computer crime cases, it is difficult for us to take incomplete electronic evidence as effective evidence, which will increase our workload seriously. Therefore, we must recover data through computer forensics technology, which will better complete the collection and solidification of electronic evidence. In March 2012, the eighth amendment of the Criminal Procedure Law (Draft) was adopted, which states that "all the materials that can be used to prove the facts of a case are evidences." Therefore, cases involving electronic forensics have become evidence, such as corruption, gambling, SMS fraud, network number theft, network e-mlm, software infringement, etc.

2. Connection and Process of Computer Forensics and Data Recovery

2.1 Relationship between computer forensics and data recovery

There are many similarities between computer forensics and data recovery, and there are many similarities in technology. However, there are still some differences between the two. The main purposes of data recovery are as follows. Through technical means, we can recover the deleted data or data files. When the data is restored, the technician does not know its purpose. However, the computer forensics technology takes the recovered data as the legal basis. Therefore, the data recovery of computer forensics is a proof document with legal effect. Data recovery is an important part of computer forensics, which can effectively obtain electronic evidence. Therefore, computer forensics technology has become a link of public prosecution department and legal department, which can help them solve, judge and try cases more effectively.

2.2 General steps of computer forensics

At present, computer forensics technology is constantly changing, which is totally different from passive defense technology, such as firewall, intrusion detection, VPN and so on. With the development of hacker attack technology, computer forensics has become a complex system

  DOI: 10.25236/icme.2019.085

engineering. At present, the law enforcement department has not formed a unified standard of evidence collection, which has seriously affected the efficiency of judicial evidence collection. For traditional computer forensics, this paper develops a framework model, as shown in Figure 1.

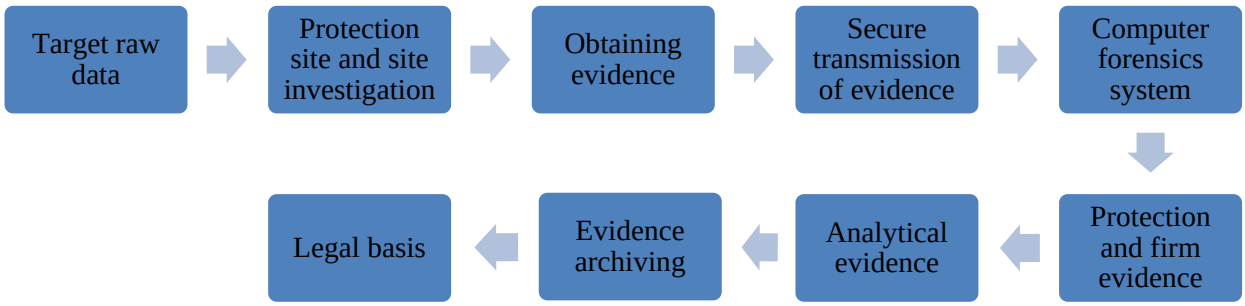

Figure 1: General steps of computer forensics

3 Anti-forensics Technology

Anti-forensics technology can be roughly divided into three categories, which can be jointly applied. It greatly improves the difficulty and accuracy of forensics. The classification of anti-forensics technology is shown in Figure 2.

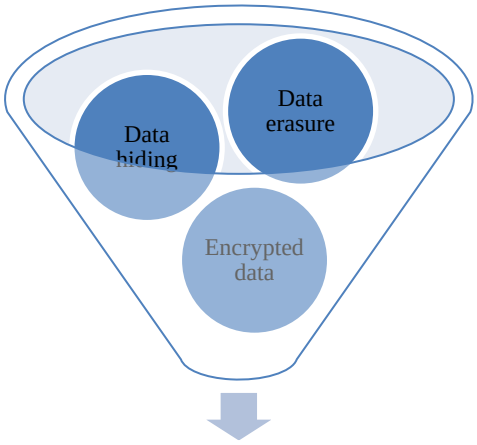

Figure 2: The classification of anti-forensics technology

3.1 Data erasure

Data erasure is the best anti-forensics technology, which can remove any potential evidence, including index, directory, block data and other original data. When the original data can't be obtained, the computer forensics work is not lack of normal development. At present, there are two tools for data clearing in the anti-forensics Toolkit (TDT), namely Necrofile and Klismafile. Necrofile is mainly used to clear file information and data. By occupying the tools in TCT index nodes, we can overwrite the index nodes in TCT, which will randomly rewrite the relevant data blocks.

3.2 Data hiding

When the criminal destroys the evidence, the criminal may only delete the data, which does not disguise the source file, such as hiding in the hidden space of graphics, images, music and disks. Runefs is a common anti-forensics tool for data hiding, which can mark criminal data or files as bad

blocks. In this way, criminals can escape from obtaining evidence, because TCT is unable to check the disk damage.

3.3 Encrypted data

Encrypting data files has become a common tool. When the intruded computer runs programs that can't be hidden, and the intruder wants to escape the evidence collection, the forensics personnel can obtain the functions of these programs by the way of reverse analysis. The methods and basic principles of file encryption are consistent. At the beginning of software operation, we can decrypt the encrypted code through the text decryption program. Among them, the decrypted code may be hacker programs, other decryption programs, and other programs.

4. Application of Computer Forensics Technology

Data recovery technology usually includes two levels. One is hardware based data recovery, which is mainly caused by hardware problems. The other is data recovery based on software, which is mainly caused by human factors, such as format, file deletion, partition table information damage, boot sector information damage, etc. The application of computer forensics technology is shown in Figure 3.

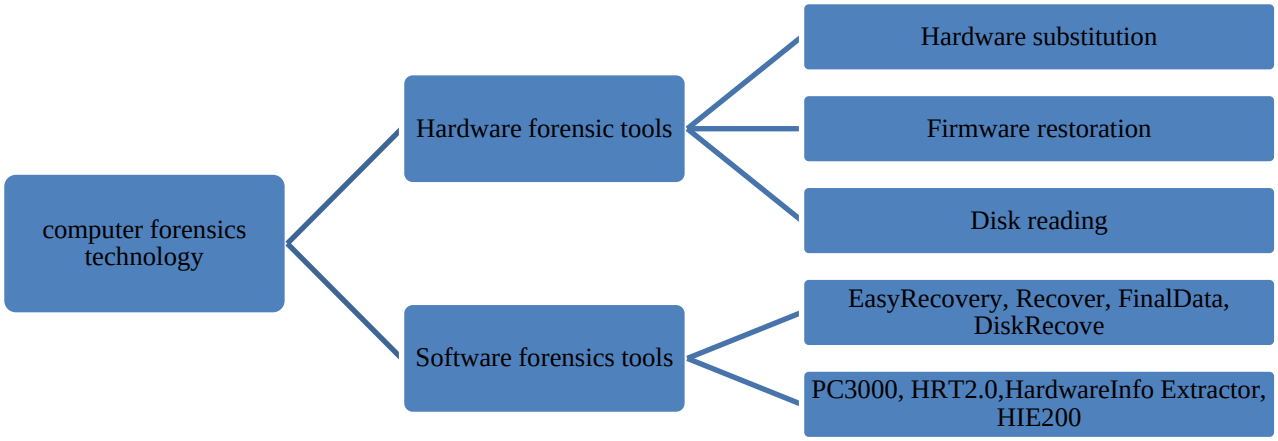

Figure 3: The application of computer forensics technology

4.1 Hardware forensic tools

Hardware based data recovery has many ways, such as hardware replacement, firmware repair, disk reading. Among them, the hardware alternative data recovery method is as follows. By replacing bad hardware with good hardware of the same model, we will achieve data recovery, such as hard disk circuit board replacement, flash disk control chip replacement, etc. Among them, the recovery method of firmware repair data is as follows. Through the special hard disk repair tool, we can repair the hard disk firmware, which will recover the hard disk data, such as pc3000. Among them, the disk reading data recovery method is as follows. In the super clean workshop of level 100, we can open the hard disk. After taking out the disk, we can scan through the special data recovery device, which will read out the data on the disk.

4.2 Software forensics tools

There are many kinds of software for software based data recovery, such as easyrecovery, recover, finaldata, diskrecover, etc. Through software data recovery, we can recover various forms of data, such as error deletion, error formatting, partition table corruption, etc. At present, the traditional single data recovery software can't meet the needs of the society. Some enterprises have

researched and sold various professional finished software, such as Pc3000, Hrt2.0, Hardwareinfo Extractor, Hie200 and so on. These software can repair the bad sector of the hard disk.

Conclusions

At present, computer illegal crime has become the main way of illegal crime, which can destroy criminal evidence in the process of crime. However, with the development of forensics technology, computer forensics provides sufficient evidence for solving cases. Therefore, data recovery plays an important role in computer forensics, which can provide strong data support for dealing with computer criminal activities. Therefore, the computer forensics technology based on data recovery has become a link of the public prosecution and law departments, which can help them to solve, judge and judge cases more effectively.

References

[1] Wang Qin, research and Analysis on Key Technologies of data recovery in computer forensics [J]. China management informatization, 2008,11 (8): 72-76.

[2] Wu Wei. Fraud in enterprise information system and countermeasures [J]. Digital communication world, 2018, 4 (1): 65-69.

[3] Li Fulin. Research and implementation of computer forensics technology based on flash data recovery [J]. Information system engineering, 2018, 5 (11): 78-82.

[4] Chu Hongbo. Computer forensics technology and its development trend [J]. Nanfang agricultural machinery, 2018, 3 (12): 172-176.

[5] Li Yaxuan. Research on manual recovery technology of master partition table in electronic forensics [J]. Network security technology and application, 2018, 3 (6): 112-116.

[6] Chen Chao. Research on the improvement of network forensics technology under the information police mode [J]. Police technology, 2012, 1 (3): 172-176.