

# Improvement of Corrupt Path Recovery Algorithm in Software Network

Wang Junhai<sup>1,a</sup>, Li Tianxiang<sup>2,\*</sup>

<sup>1</sup>City College, Southwest University of Science and Technology, Mianyang, Sichuan, 621000, China

<sup>2</sup>Sichuan Changjiang Vocational College, Chengdu, Sichuan, 610106, China

<sup>a</sup> email: giswjh@163.com

\*corresponding author

**Keywords:** Data Security, Path Recovery, Algorithm Improvement

**Abstract:** The traces of computer use include the operation records and criminal evidence of computer users. Extracting and recovering these data is an important part of the computer investigation and verification process. Based on the analysis of Windows Platform file system, a network trace recovery algorithm based on the minimum content feature is proposed, which is used to recover and extract the online records of computer users. This algorithm is based on the characteristics of the smallest element content source of index.dat file, how to match the network information and decide whether to extract. The experimental results show that all the remaining data can be recovered, USCIS can be set immediately, then split, split or re install the system, and the field of computer information forensics can play a huge role.

## 1. Introduction

Informationization brings all kinds of convenience to human beings. Intangible conditions also create conditions for criminals to use computers or networks to commit crimes. It is necessary to find strong evidence from these evidences to fight against computer crime. The concept of computer debating was first proposed at the International Conference of computer experts held in the United States in 1991. That is, the use of computer identification technology can analyze criminals and determine computer evidence of computer crime, and bring a lawsuit against them. As one of the most important aspects of computer accommodation[1], this paper focuses on the process of extracting, analyzing and confirming the data stored in the subsequent storage medium, and analyzing it as appropriate evidence.

When the user uses the computer, the system records the user's use track, such as the history of automatic access to the network. In addition, some wrong operations, or illegal acts of concealing criminal facts, are the reasons for the loss of track data. Therefore, data recovery, that is, the recovery of deleted data, is a powerful supplement to the static fault tolerance work.

Traditional data recovery technology focuses on the detection and recovery of data structures at the file system level, such as file records. For example, the most popular data recovery products in the industry are simple recovery, final data, and d-recovery. These products often have defects that are difficult to prevent file system corruption. At the same time, they lack the ability to restore confidential data in the field of debating.

In order to make up for these shortcomings, a deep recovery algorithm for user network speed under Windows operating system is proposed. This is, after the operation computer of the disk of the damaged file system such as copyright encounters, all the remaining network drawings can be recovered, the minimum information feature of index. Dat file, and the ideological basis of Grace's data recovery. Through experimental comparison and analysis, the algorithm has good performance. Compared with products with similar functions, it has certain advantages in scanning rate and data recovery success rate.

## 2. Technical Introduction

## 2.1. Online Transaction Documents

There are multiple hidden files index.dat in the windows operating system. Even if the history is cleared by ie, the record in the index.dat file still exists. These functions of index.dat file are very helpful for computer fault tolerance. As shown in Figure 1[2].

Windows 95/98/ME	\Windows\Temporary Internet Files\Content.IE5\ \Windows\Cookies\ Windows\History\History.IE5\
Windows 2000/XP/7	\Documents and Settings\<>username>\Cookies\ \Documents and Settings\<>username>\Local Settings\History\History.IE5\ \Documents and Settings\<>username>\Local Settings\

Figure 1 Index. Dat file distribution

By analyzing the configuration of index. Dat file, the network trace can be extracted. On the contrary, as long as the index. Dat file is completely cleared, the network traceability can be prevented. A more extreme approach is to do something similar to formatting. As a result, all old index. DAT files will be lost and invisible.

## 2.2. File System and Traditional Data Recovery

When obtaining the index. Dat file, only data recovery technology can be used. Data recovery refers to the recovery of data lost in all computer related storage devices[3].

Recovery refers to extracting target data that the operating system cannot see so that it can be seen. A file is a horn for data. The operating system uses the file system to manage files. If you understand the management organization of the file system, you can recover the data normally. Fat 32-year-old and 7-year-old file systems are NTFS. Files under fat 32-year-old, entry record file directory, empty space, file, chain memory device determine file distribution table and NTFS data attributes, including file records. Through such a complex data structure of data management. When receiving the command to delete a file, considering the performance, the file system does not clear everything. Instead, it simply marks the file control structure that indicates the file has been deleted. The area occupied by the file can be reused, and the data of the file remains the same [4]. Therefore, when the file control structure and data are not covered, the success rate and accuracy of file recovery are 100%.

As mentioned above, the traditional data recovery technology achieves the purpose of data recovery by extracting and determining the control structure of the file and extracting the content of the file according to the rules of the file system. They are limited by traditional data recovery technologies at the file project and file record levels. This type of technology focuses on the recovery of the entire file. If the file system is damaged and the data is overwritten, the recovery of the file will be incomplete and the data will be incorrect. Using traditional data recovery technology to recover network traceability by recovering index. DAT files will greatly affect the reliability and accuracy of network traceability information debate.

## 3. Reply Based on Minimum Content Feature

The type of file is the start and end of fixed content, such as a collection of independent data organization methods. Therefore, the "algorithm of minimum information function" is the practice of organizing feature information of index. Dat file content and using network data recovery to realize matching extraction and Analysis on computer floppy disk. The main steps are as follows.

After confirming that the network traceability information comes from the index. Dat file, analyze the content structure of the file, and obtain the content of the file in the form of structure.

Analyze and build some feature information that can directly identify single network tracking record, such as data header, data block, data tail control information, etc[5].

The characteristic information is determined as a pattern string, which is used to match and retrieve the byte stream of small depth (sector, etc.) on the whole disk or partition. According to the needs, the data are extracted directly in the same place and analyzed into the network trace records required by the computer forensic science.

The characteristics of the algorithm refer to the unique characteristics. The function of directly identifying network trajectory can distinguish these data from irrelevant data, and directly extract target data from the nearest location. The smallest feature is that it can determine the feature of network track record. AMCF algorithm restores the analysis object to a single network trace record, avoids the defects of traditional file system level data recovery technology, and reduces the complexity of data recovery level and structure. Through fine-grained matching in the smallest cell, all the remaining network trace information on the computer can be detected correctly, which increases the possibility of completely recoverable data. Storage technologies such as formatting operation and paging file of operating system copy a large number of data, extend to disk, and even become unmanageable wild data. AMCF algorithm uses the idea of deep scan fine-grained to ignore these changes. The fine-grained view data is larger and more scattered, and the possibility of data being overwritten and cleared is smaller, even invisible. Or, the algorithm can collect more network tracks. To be more specific, the debate on network traceability information should be conducted[6].

#### **4. Shortest Path Ray Tracing Algorithm**

The shortest route tracking algorithm of dynamic network can solve two problems of the original LTI algorithm, but its computational efficiency is low. According to the law of wave propagation, in order to improve the shortest path of dynamic network, an improved shortest path tracking algorithm of dynamic network is proposed. Ray tracing algorithm calculates the efficiency of calculating the minimum travel time of the nodes ahead. However, the improved post tracking method is also used in the shortest path tracking algorithm of dynamic network, and the calculation efficiency is still very low. Compared with the shortest path of dynamic network, the post tracking method in the transmission algorithm has the problem of low efficiency [7]. The improved method is put forward. First of all, in the step of calculating the minimum running time of forward nodes, not only the minimum running time of each node is calculated, but also the time of each node is recorded. Then, when tracking the receiver's ray path, the algorithm is improved by using the secondary source's position information of each node and the law of wave propagation to reduce the calculation amount and improve the calculation efficiency.

In the dynamic network shortest path tracking algorithm, the original LTI algorithm has disadvantages in the rear tracking process and improves the ray tracing path of the original receiving signal point. In the first LTI algorithm, the total travel time of the receiving original viewing point is the travel time of each node and the calculation of the node. Secondly, the minimum travel time and the corresponding node selection. Finally, use the segment containing the node as a possible area for the secondary source of receiver [8]. In fact, the secondary source of the receiver is not necessarily these fragments. In addition, when the original LTI algorithm determines the possible area of the secondary source of the receiver, the segment of the receiver is not excluded, and the algorithm can fall into an infinite loop. The moving time of the receiving point obtained by linear interpolation of the segment can be less than that obtained by other segments of the unit [9].

#### **5. Conclusion**

In the process of computer tracking, as much as possible as user information is important to me. By analyzing the content structure and characteristics of index. Dat file, online records can be extracted accordingly. According to the summary of existing data recovery technology, the problem of extracting network from accidental or man-made damage starts to trace the source. In the face of this problem, the network drawing based on the minimum information characteristics proposes the

recovery algorithm. In addition to the network tracking data visible in the current system, the algorithm can also recover the network tracking information, such as deleting, formatting disks and re dividing, and carry out strict operations. The experimental results show that, under the condition of ensuring extremely high results and efficiency, the algorithms such as scanning speed and scanning compatibility have excellent performance, and have quite high practical value[10].

At the same time, the algorithm is limited. This algorithm is only suitable for special purposes. A type of file cannot be recovered because the focus level of the algorithm is lower than that of the file system. In addition, it is necessary to improve the algorithm. For example, this algorithm uses the principle of depth scanning. Instead of byte stream matching algorithm, it can match according to the offset of the feature content on the disc. Most URL entries have a sector offset of 16 times. The algorithm only supports the recovery of network drawing, based on the characteristics of file content. The algorithm, registry, log, image, cash and all types of files like other files, may be applicable in theory. The next goal of this paper is to use AMCF algorithm to recover more types of sensitive data and play a greater role in the field of computer information debate.

## References

- [1] Sedef Savas, Massimo Tornatore, Ferhat Dikbiyik. (2018). RASCAR: Recovery-Aware Switch-Controller Assignment and Routing in SDN. *IEEE Transactions on Network and Service Management*, no. 99, pp. 1-1.
- [2] Thang Manh Hoang, Hoang Xuan Thanh. (2017). Cryptanalysis and security improvement for a symmetric color image encryption algorithm. *Optik - International Journal for Light and Electron Optics*, vol. 155.
- [3] Huang Rui, Zhang Hongqi, Chang Dexian. (2018). A Backup and Recovery Mechanism for Security Service Chain Fault in Network Function Virtualization Environment.
- [4] Li, X. Yang. (2017). Optimized Multipath Routing Algorithm for MANET Based on Reliable Stability Estimation, vol. 39, no. 3, pp. 605-612.
- [5] Shen Z, Shu J, Fu Y. (2017). Seek-Efficient I/O Optimization in Single Failure Recovery for XOR-coded Storage Systems, vol. 28, no. 3, pp. 877-890.
- [6] Chantasiriwan S, Charoenvai S. (2018). Using Superheated Steam Dryer for Cogeneration System Improvement and Water Recovery.
- [7] Evgeny Nuger, Beno Benhabib. (2018). Multi-Camera Active-Vision for Markerless Shape Recovery of Unknown Deforming Objects. *Journal of Intelligent & Robotic Systems*, vol. 92, no. 3, pp. 1-42.
- [8] Se-Hoon Jung, Jong-Chan Kim. (2019). C k LR Algorithm for Improvement of Data Prediction and Accuracy Based on Clustering Data. *International Journal of Software Engineering and Knowledge Engineering*, vol. 29, no. 5, pp. 631-652.
- [9] Jiying Liu. (2018). On the recovery conditions for practical ghost imaging with AMP algorithm. *Optics Express*, vol. 26, no. 16, pp. 20519.
- [10] Xin H, Wang F, Li Y, et al. (2017). Secondary release of exosomes from astrocytes contributes to the increase in neural plasticity and improvement of functional recovery after stroke in rats treated with exosomes harvested from microRNA 133b-overexpressed multipotent mesenchymal stromal cell, vol. 26, no. 2, pp. 243.