Research on NTFS File Anti-Delete Forensic Technology

Weimin Wu, Gang Zhao[a], Wenxin Lai and Jiongjiang Lan

School of Guangdong University of Technology, Guangzhou 510000, China.

[a]zhaog.0539@qq.com

Keywords: NTFS, File Record, Anti-delete, Forensic.

Abstract The deleting mechanism of file is summarized by means of research on NTFS structure and management mechanism. After analysis on the deleted leftover, valuable information included in it was acquired. A method is proposed for anti-delete forensic based on traversing free file record. Software named *AntiD Forensics* is designed and implemented, as well as verifying that anti-delete forensic technology for NTFS has great application value in computer forensics.

1. Introduction

Information technology has penetrated into all fields of society, and information security issues are also facing a great threat and challenge[1]. The field of computer forensics has a history of 30 years, and the use of electronic evidence becomes more and more common. But criminals are increasingly cunning, trying to remove the evidence of the crime to cover up the crime, which bring great difficulties to forensics.So the research on the anti-delete technology is imminent. A number of excellent forensic tools were developed at present,for example *Winhex* and *EnCase*[2]. The domestic has made a number of research results in the legislation, the framework of the computer forensics, cloud forensics, smart phone forensics, and so on.[3,4,5,6]. Generally speaking, The domestic focus on theoretical research of computer forensics, the use of the forensics software are imported from abroad majority, with less products which own independent intellectual property rights.

On the basis of previous studies, a methods are proposed for anti-delete forensic based on traversing free file record, and the realization of the concrete technology is given, whitch can be applied to the field of NTFS electronic forensics.

2. MFT Structures in NTFS

The file record(FR) is used for treatmenting file by NTFS, File name, build time, access time, modify time, file size, file storage location and other information are stored as attributes in FR, and all the file records are stored in master file table(MFT).

Some important system data are also recorded in MFT, Which are called “Metafile”,including the data structure of file location and data recovery, and guide the program data, the partition of the allocation of bitmap and other information. Metafile occupied first 16 records of MFT, and record of root dictory is stored at No. 6 record.

3. Research on Anti-delete Forensic Technology

Through the analysis of the NTFS file deletion mechanism, this paper discusses the implementation of the anti-delete technology based on NTFS file record.And the feasibility of the mothed is verified by experiments.

3.1 NTFS File Deletion Mechanism

The data associated with the file in NTFS mainly has the following parts:FR, file index entry, number of cluster in $BitMap. After file or folder are deleted, NTFS did not wipe out related information completely in order to juggle efficiency of CPU and hard disk reading and writing, just to change the data of the particular field. change law of NTFS when file are deleted:

（1）Field of deleted mark(offset 0x16) in FR is set to 00H;

（2）The cluster number of file contents is set to 00H in $BitMap, which means those clusters is available;

（3）Other changes: index entry is covered, FR sequence number plus 1, etc. But these changes are not significant for the anti-delete forensics.

According to the law (1) can be known, FR still record all the attributes information after the file is deleted, and information can be extract by traverse those type of FR,and extract file contents by judging recoverable property based on law (2).

3.2 Technology Realization of Anti-delete Forensics

In order to obtain the evidence information, first of all, the free FR is retrieved, and valuable FR need be filtered out,then relevant information are extracted. Technology of anti-delete forensics can be divided into two steps to achieve。

3.2.1 FR Preprocess

The $BITMAP attribute of MFT record the status of every FR,though which all free FR can be positioned.Free FR is very much,however, not all of the free FR have the value of evidence. The valueable FR can be extracted by testing the integrity and condition filtering, and saved into the buffer preprocess. The process can be illustrated as shown in Figure 1.

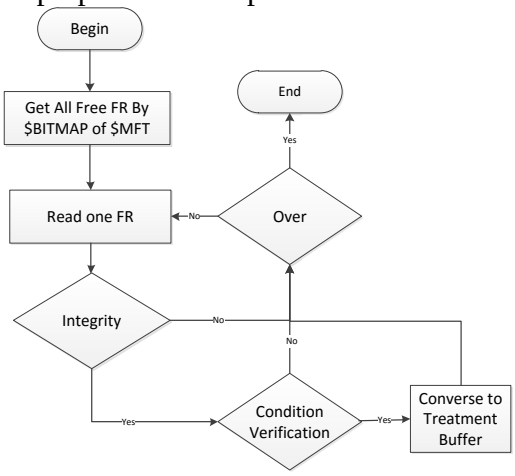

Fig. 1 FR Preprocess

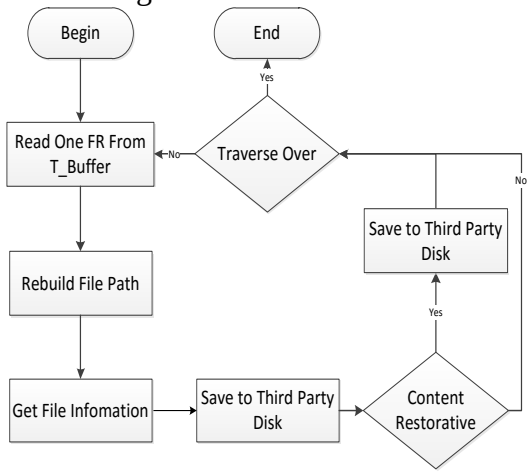

Fig. 3 Infomation Extract

Integrity verify whether basic attribute are stored in FR, These attributes include $STANDARD_INFORMATION,$FILE_NAME, $DATA attribute.Not all of free FR contain these attribute,we found those free FR do not contain thoes basic attribute after partition is formatted completely by experiment as be shown in Figure 2.

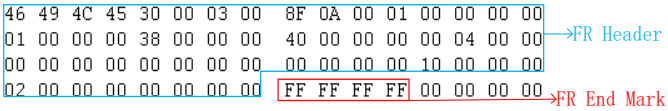

Fig. 2 FR without Basic Attribute

Condition Verification allows forensic personnel to set filter conditions which has been mastered,including: key words of file name, file suffix, file build time, file modify time, file last read time, file size and file path. Only conditions are satisfied, the FR will be saved into treatment buffer. The more specific the conditions are set, the more accurate the evidence is.

3.2.2 Information Extraction

After the valueable FR is written to the buffer, information should be extracted. The process of extracting information can be illustrated as shown in Figure 3.

Firstly, the path of file can be rebuild by analysis of $STANDARD_INFORMATION attribute of file infomation can be extracted directly, and some common infomation of file can be extracted from FR which including file name, file build time ,file modify time, file access time ,traditional attribute and file size. The information as be shown in in figure 4.

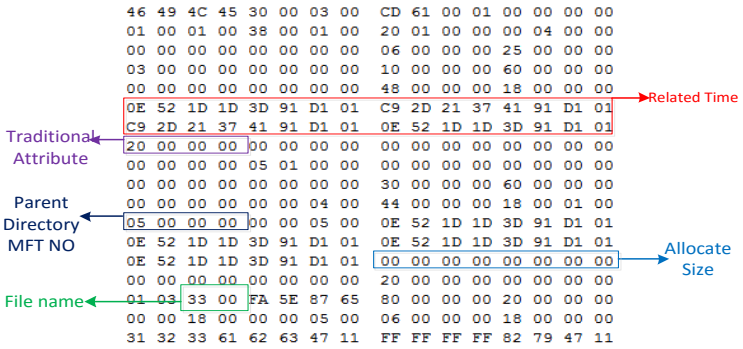

Fig. 4 Information in FR

Recoverable property of file contents shold be judged by two situation:

（1）If the $DATA attribute is resident, file contents can be acquired from FR directly,as the figure 5 shows;

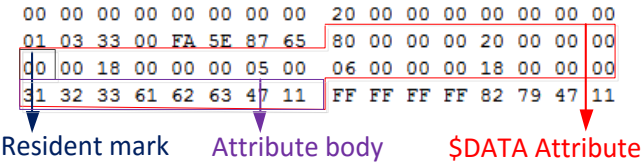

Fig. 5 Rensident $Data Attribute in FR.

（2）If the $DATA attribute is non-resident, Recoverable property of file can be judged by analysing usability of clusters which were used by file once from $Bitmap. If those clusters is available, which means file content has ben coverd,the file contents can not be recover.if not, the file contents can be recover.Non-resident $DATA attrbute is shown in figure 6.

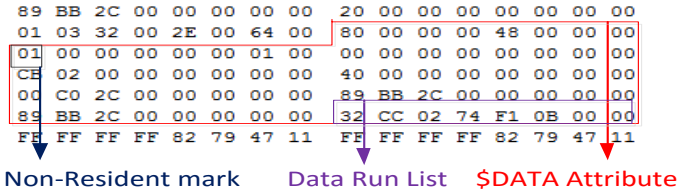

Fig. 6 Non-rensident $Data Attribute in FR

4. Experiment

4.1 Experimental Process

The Forensics tool *AntiD Forensics* is designed based on the above analysis. Then the tool was compared with the existing forensic software *finalforensicsV3.1* and *X-Way forensics* by *experiment.*These conditions of file were set up to extract file infomation：

Last read time of file:2016/02/20　08:00:00;

File suffix:.exe;

File size:0-1024000000B.

Experimental Environment 1:

OS:Windows7_x64 Ultimate[6.1.7600: Service Pack1]; Memory:KingSton 8GB DDR3 1600 KVR16N11; CPU:AMD x3 400.

The result of Experiment is shown in table 1.

Table 1 Compariton of Experimental Result

Tool	Count of Recovery	Time/s
AntiD Forensics	78	22.6
finalforensicsV3.1	76	24.0
X-Way forensics	78	23.5

Experimental Environment 2:

OS:Windows7_x86 [7601:Service Pack 1]; Memory:Samsung 4GB DDR3L 1600; CPU:Intel

Core i5 4590.

The result of Experiment is shown in table 2.

Table 2 Compariton of Experimental Result

Tool	Count of Recovery	Time/s
AntiD Forensics	66	20.2
finalforensicsV3.1	66	20.5
X-Way forensics	59	21.4

Experimental Environment 3:

OS:WindowsXP_x86 [5.1.2600:Service Pack 3]; Memory:SKingSton 2GB DDR2 800; CPU:Intel Pentium G3258.

The result of Experiment is shown in table 3.

Table 3 Compariton of Experimental Result

Tool	Count of Recovery	Time/s
AntiD Forensics	28	28.4
finalforensicsV3.1	26	292
X-Way forensics	26	28.6

The tool *AntiD Forensics* has more advantages than *finalforensicV3.1* and *X-Way forensics* on the count of recovery file and efficiency,which can be seen through the experimental result.

5. Evidence Analysis

The evidence can be acquired by analysising the file information which has been extracted: （1）verify weather the last access time of the file is consistent with the time of the crime; （2）Run the file in order to verify whether the mechanism of file is consistent with the criminal behavior.

6. Summary

Through analysing NTFS structure and file management mechanism r, a mothed of anti-delete forensics which based on analysing free FR, is proposed in this pape.A forensic tool named "*AntiD Forensics*" was designed based on the above mothed. Experiment shows that the *AntiD Forensic* has more advantages than other forensic tools, and the feasibility of the scheme is verified. This method has a certain application value for today's computer forensics.

References

[1]. .Liao Hui, Lin Jie. Design and Implementation of Network Terminal Security Assessment Index System. Journal of Guangdong University of Technology. Vol. 27 (2010) No. 2, p. 84-88.

[2]. Long chen, Guoying Wang. Survey of computer forensics. Journal of Chongqing University of Posts and Telecommunications, Vol. 17 (2005), No. 6, p. 736-742.

[3]. Shuai Wang. Introduction to ComputerForensicsTechnology in Cloud Computing Environment. Computer Science. Vol 41 (2014) No. B10, p. 90-91.

[4]. Yan Cheng. Research on Digital Forensic of Cloud Crime. Computer Science. Vol 41 (2014) No. B10, p. 74-78.

[5]. Xueguang Wang. Research on Digital Forensics and its Relevant Problems of Law. Computer Science. Vol 41 (2014) No. B10, p108-113.

[6]. Jun Zhang, Lina Wang. An Integrated Open Forensic Environment for Digital Evidence Investigation. Wuhan University Journal of Natural Sciences. Vol. 17 (2012) No. 6, p. 511-515.