Research on Computer System Information Hiding Anti-Forensic Technology

Jing Leng[1, a] and Tonghong LI [2, *]

[1,2] Department of Information Technology, Hubei University of Police, Wuhan 430034, China;

[a]daleng0127@sina.com

* The Corresponding Author

Keywords: Information hiding; Anti-forensic; NTFS file system

Abstract. This paper studies various possible ways of information hiding in modern computer systems, analyzes the data hiding of disk drive, and emphatically analyzes various information hiding methods of NTFS file system and the possible detection methods of various methods. Also, this paper discusses the great influence of various hidden techniques as the computer anti-forensic means on computer forensics.

Introduction

With the development of computer forensics technology, computer anti-forensic technology is also quietly rising. Anti-forensics destroys the investigation, protection, collection, analysis and court litigation of electronic evidence against all stages of the computer forensics process, reduces the amount and the quality of evidence obtained. This has formed a severe challenge to the development of forensic technology.

The common anti-forensics techniques are: data erasure, data hiding, data encryption, network source anti-tracking, kernel-level Rootkit, attacking computer forensics tools and other technical means. Among them, data hiding is one of the most important means of computer anti-forensics. Data hiding is usually divided into non-physical forms of data hiding and physical forms of data hiding. Non-physical form of data hiding is the usual meaning of information hiding, including: data encryption, steganography and digital watermarking. The physical form of data hiding is primarily a data hiding related to computer storage and operating system. Here we mainly discuss the physical form of data hiding.

This paper mainly studies various data hiding methods and strategies in modern computer systems and the impact of data hiding anti-forensics technology on computer forensics.

Computer Hardware Information Hiding

HPA and DCO Data Hiding

Host Protection Area HPA. After the ATA-5 protocol has been established, the hard disk has introduced the host protection area technology. By using the ATA command to directly protect an area behind the hard disk for storing data and configuration files, neither the operating system nor the BIOS can read the area. The unprotected area of the hard disk can be read, written, partitioned and formatted normally without any impact on the data in the "hidden protected area". However, there are tools that make changes to the HPA for data hiding. Once entering into these protected areas, large amounts of data can be hidden. These areas will not be taken seriously by forensic analysts. Some forensics software can not effectively get the hidden data in the area.

Device Configuration Overlay DCO. Device configuration overlay is another hidden area of the hard disk drive (HDD), first introduced in the ATA-6 standard. DCO has a stronger ability to hide data than HPA. The DCO was designed to allow system vendors to buy hard drives from different vendors,

possibly different sizes, and then configure all hard drives to have the same number of sectors.

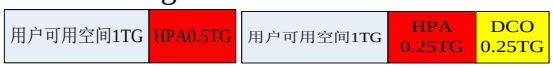

Figure 1. A disk drive with only HPA or with HPA/DCO at the same time

If the hard disk drive supports HPA / DCO, then the two can exist alone or in parallel, as shown in Figure 1. 1.5TG disk drive, HPA 500G, or 1.5TG disk drive, HPA and DCO each 250G.

Data Hiding Analysis . We can use tools to create and modify hard disk drives HPA / DCO, such as HDAT2, SETMAX, Feature Tool, MHDD and so on, as shown in Figure 2. We can use a MHDD to change a 200G Seagate drive to 100G.

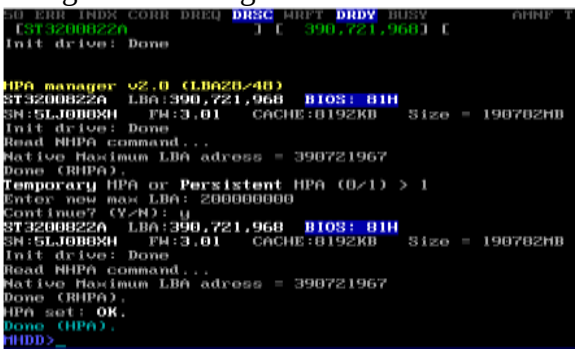

Figure 2. The creation of HPA

Figure 3. Hiding a partition and viewing it with encase analysis

The steps to create or control an HPA / DCO hiding data are as follows: First, use the disk editing tools to copy the files that need to be hidden to the end of the disk partition. Second, create an HPA in the area where you need to hide the file, the size of the space can be arbitrarily determined as needed. Finally, eliminate references to new file spaces in the source file space so that you can have a hidden file on your disk drive. This file will not be found if you do not have specialized software or hardware tools for the HPA zone. There are many forensics tools for implementing data hiding using HPA / DCO, such as the Sleuth Kit, the ATA Forensics Tool, EnCase software tools, as well as hardware tools such as Forensic, Ultradock v4,Forensic RTX and so on.

Hidden Partitions

Hidden partitions, that is, in general conditions, do not display the part of the hard disk that can not be used directly, and generally cannot be accessed. Some brands, such as Lenovo's notebook, default to the factory to set up a hidden partition for themselves, so as to store some system startup or similar key recovery main files, and provide the start entry. When the Windows7 operation system is newly installed or partitioned, it will also reserve a certain space as a partition to start the boot file. The partition is a hidden partition.

In addition, you can also use the relevant tools to set up the hidden partition. For example, DiskGenius can implement partition hiding and hiding partition analysis. The author conceals a partition of a disk and verifies the hidden files by encase analysis, as shown in Fig.3.

If the data is hidden in the hidden partition by means of technical means, it will be an effective counterproof method. Therefore, the forensics analysts need to use a variety of means to take full consideration of the comprehensiveness and integrity of evidence acquisition in the analysis of forensics.

The Information Hiding of Slack Space

The slack space on the disk mainly includes volume slack and file system slack. Volume slack is the partition where the file system resides, between the end of the file system and the end of the partition. File system slack is the end of the file system and does not have unused space allocated to any cluster.

The appearing reason for volume slack and file system slack is that partitions are not an integer multiple of clusters. For example, in a partition with 10001 sectors, the first 10000 sectors are divided into 2500 clusters, each cluster has four sectors, and then the last sector is left and becomes the file system slack.

The amount of data hidden in the volume slack is unrestricted, so the suspect can simply modify the size of volume slack to hide more data. In file slack, the hidden data is limited by the size of the cluster. For example, a file system has eight sectors in a cluster. The largest volume of data hidden in the file system slack is the capacity of 7 sectors.

The hidden data in slack space is the product of the storage capacity of the file system and the whole computer system. Slack space data hiding technology makes full use of the physical properties of the formatted storage medium to hide the data. The application of this technology to data hiding has dual advantages: the host or the carrier file is not affected by any influence, and does not affect the normal operation of the whole digital system. The reason is that the hidden data is transparent to the operating system and the file manager. Writing data to slack space to implement data hiding is also one of the important means of anti-forensics technology. Criminals can hide various kinds of information to the area, such as various viruses, Trojans and criminal software tools.

If you want to detect hidden data in slack space, the simple way is to use the Windows command line tool chkdsk to analyze the file system. Complex methods require the use of specialized tools such as Guidance's Encase software and NTI's GetSlack software to support the collection and analysis of evidence for these spaces.

Data hiding of Computer NTFS File System

The NTFS file system is the standard file system of the current Microsoft operating system, and there are many methods to hide the data in the NTFS file system. In this part, we mainly discuss the common data hiding methods and the detection methods of hidden data.

NTFS Data Hiding Standard

From the suspect’s point of view, a good NTFS data hiding technology should meet the following criteria: First, the normal system tools (such as chkdsk, etc.) do not check any errors. Second, the hidden data cannot be rewritten or the possibility is very low. Third, the normal user can not find the hidden data. Fourth, the technology can store a certain amount of hidden data.

Information hiding of labled bad clusters

In a hard disk, the sector that cannot be normally accessed or not properly read and written is called a bad sector. In the Master File Tab (NTFS), there is a bad cluster list file ($ BadClus) that records all the corrupted cluster numbers in the volume on the disk, preventing it from the use of the distribution system. Cluster the hidden documents into bad clusters, that is, to add the “pointer” of these clusters to the data running list of $BadClus, so that we can hide the file. The size of the data hidden in this method is unrestricted. The suspect can simply assign more clusters to $BadClus, use it to hide the data, without having to worry about the destruction of data hiding.

Information Hiding for the Extra Cluster of Files

The method of hiding information is to hide the data by using the extra clusters assigned to the file. For example, a file has 10752 bits, and the NTFS file system needs to allocate 3 clusters to each cluster of 8 sectors, but the suspect can assign more clusters to the file to achieve the purpose of data hiding. It is not limited to hide the size of the data in this way, because the suspects can be assigned to the redundant clusters of files according to their needs. One disadvantage of using this way of hiding is that the size of stored files can not be changed. Once the capacity of files is increased, the hidden data will be covered or lost. Maintaining the stability of the stored files is the prerequisite for maintaining this information hiding.

The detection of this data hiding method can be analyzed using the Windows command line tool

chkdsk. There is currently no dedicated tool for this automated inspection process.

Information Hiding for File Slack Space

File Slack space is the end of the file valid data to the end of the last data block between the end of the storage space. Windows file systems use fixed-size clusters. The size of our common cluster is usually 4KB, 8KB, 16KB, 32KB, 64KB, 128KB. After determining the size of the cluster, all the reading and writing of the files are distributed according to the cluster. For example, the cluster size of a partition is 32KB, for a 15KB file, the system will allocate 32KB of space to it, but in this 32KB space, the real used space is only 15KB, the remaining 17KB can not be assigned to other documents. This part of the space is the so-called file slack space.

There are two types of file slack, one is ram slack, the other is the drive slack. Ram slack is from the end of the file to the end of the last sector, while the drive slack is from the beginning of the next sector to the end of the last cluster of the cluster where the file is located, as shown in Figure 4.

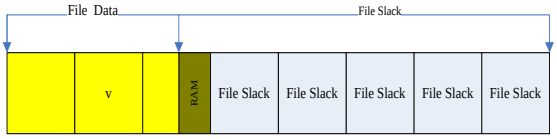

Figure 4 The diagram of file Slack structure

Since Windows ignores the information stored in the driver slack, the data stored in the slack will not be detected by the operating system itself. Ram slack can also store hidden data, but because space is too small, it is often not an ideal storage option.

Here is an example of writing data to the file's Slack space using the Slacker.exe tool. Slacker.exe is a tool that writes data to the file's slack space on the NTFS file system for data hiding. Write the file test.txt (9 bytes) into the picture file ptest.jpg with Slacker.exe, as shown in Figure 5.

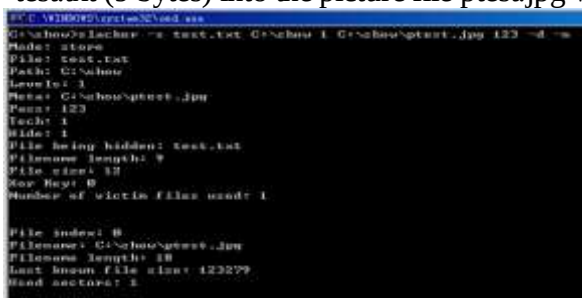

Figure 5. Writing a text file to a picture file

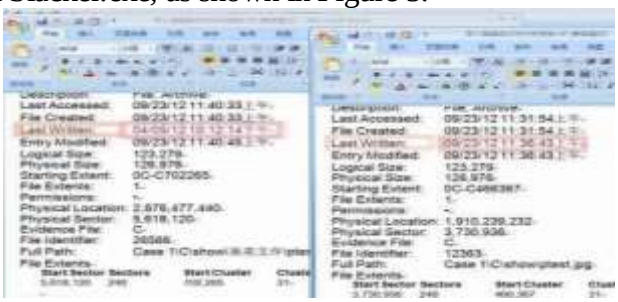

Figure 6. Comparing the changes in the picture file after the file is written

After writing the data successfully, encase is used to analyze and compare Ptest.jpg files before and after writing. The file size is not changed, but the final writing time has changed. At the same time, the other properties of the file have also changed a lot, as shown in Figure 6.

Information hiding of Alternate Data Stream

Alternate Data Stream (ADS) is a feature of the NTFS file system. It does not need to rebuild the file system, you can add additional attributes or information to the file mechanism. Allow the existence of a separate data stream file, and also allow a file to attach to multiple data streams, that is, in addition to the main file stream, it also allows many non main file streams to be parasitic in the main file stream. By this simple file stream, we can implement file hiding.

There are many forensic analysis tools for ADS, and the robustness of ADS data hiding method is poor, so when the files with ADS files are copied to non NTFS partitions, the file stream will be deleted

automatically. It's extremely unreliable to implement file hiding with the ADS stream.

NTFS Data Hiding Analysis and Detection

Analysis of NTFS data hiding is generally difficult, because the file system is very flexible, and can support various operating systems, so there will be many data hiding methods. In addition, the complete file of windows NTFS file system is confidential and not public. Therefore, sometimes it is impossible to determine which combinations of values in the file system data structure are reasonable and which are unreasonable.

Usually, checking and analyzing the hidden data of NTFS file system can be divided into three stages: checking to determine whether any abnormal data is hidden, extracting hidden data, and covering hidden data.

If there is data hidden in the NTFS file system, the necessary analysis should be carried out in every computer forensic process. Generally speaking, it can be considered from the following aspects. First of all, before the computer forensics analysis to integrity check for the NTFS file system, such as using the CHKDSK command-line tool to check, if there is any error, the file system may be possible to be manipulated, and is in an unstable state. Second, check the size of the cluster to which the file is allocated, and the size of the file cluster (which is determined by the size of the file) by default. Once it is found that the user modifies the default cluster size of the file, it indicates that the cluster is in an abnormal phenomenon, it is very possible that someone modifies the default cluster's size to hide the data. The third is to search for data hiding tools in the file system. The fourth is to use the Microsoft OEM tool NFI to examine metadata files. NFI.EXE is Microsoft's OEM tool that allows you to dump important metadata files from the NTFS master tables as well as check for any anomalies in the metadata files.

Conclusions

Data hiding technology has always been one of the important technologies of computer forensics. All the hidden data or the means and technologies for protecting data through covert means can be regarded as counter-evidence collection methods. The hidden technology of computer system discussed in this paper is only a part of the possible methods of data hiding. With the development of technology and the emergence of new systems, more and more data hiding methods will emerge. The artistic charm of hidden data mainly depends on technical hobby or suspect's creativity. More data hiding technology creation and discovery can effectively promote the development of computer forensics technology.

Acknowledgements

This work is partially supported by the MOE (Ministry of Education in China) Planning Project of Humanities and Social Sciences (17YJAZH043) .

References

[1] Ewa Huebner. Data Hiding in the NTFS File Syste-m [EB/OL], http://www.ise.pw.edu.pl/Security/szkolenia/Huebner-Hiding_Data_in_the_NTFS_File_System-19Oct.pdf.

[2] Cheong Kai-Wee. Analysis of hidden data in NTFS file system [EB/OL] , http://www.forensicfocus.com/hidden-data-analysis-ntfs.

[3] DaeMin Shin, Yeog Kim, KeunDuck Byun.Data Hi-ding in Windows Executable Files [J], Australian Digital Forensics Conference,2008

[4] Li Busheng,Computer Anti-forensic Research and Implementation Based on NTFS[J].Computer Engineering,Vol.36 No.19,2010.10,274-276.

[5] Mayank R.Gupta,Michael D.Hoeschele, M.K.R., Hid-den disk areas: Hpa and dco [J]. International Journal of Digital Evidence 5 Issue 1(2006).
[6] Peng L. Individual Vision and Peak Distribution in Collective Actions [J]. Communications in Nonlinear Science and Numerical Simulation. 2017, 47: 238-252.
[7] Alexander Krenhuber, Andreas Niederschick. Forens-ic and Anti-Forensic on modern Computer Systems[EB/OL].http://www.fim.uni-linz.ac.at/lva/SE_Netzwerke_und_Sicherheit_Comm_Infrastructure/forensic.pdf.