International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

Computer Forensics: An Analysis on Windows and Unix from data recovery perspective

Palwinder Singh[1] , Amarbir Singh[2]

[12]Assistant Professor, Department Of Computer Science ,GNDU, Amritsar,India

Abstract - *Computer Forensics is a research hot topic in the field of computer security with the recent increases in illegal accesses to computer system. According to the procedure of computer forensics, this paper presents procedure of computer forensics, analyses of source of digital evidence on windows and unix. The paper gives a quick glance of various methods used by culprits to destroy the information in the electronic storage media and their corresponding forensic approach done by the computer forensic experts in the perspective of recovery.*

Key Words: Computer forensics; Analysis; digital evidence; Windows; Unix.

1. INTRODUCTION

With the rapid development of information technology, the computer continuously spread to people's work and life, it brings more and more for the convenience of the people at the same time, also becomes a powerful tool for criminals. A presence on the computer and related peripheral devices has become a new form of digital evidence. Digital evidence in itself has many characteristics different from traditional physical evidence. From the computer system to extract the required data as evidence in court has raised new challenges to the law and computer science. "Computer forensics" the term comes from the IACIS (International Association of Computer Specialists) the International Conference which was first held in 1991, and it was called at the time the main topic at the annual meeting of the 13 session of the International FIRST (Forum of Incident Response and Security Teams) in 2001. As the computer field and legal field of an interdisciplinary science, computer forensics is gradually becoming the focus of research and attention. This paper includes the (a) computer forensics technology, (b) Forensic analysis on Windows (c) Forensic analysis on Unix. The basic method of preserving, detecting and obtaining the electronic evidences was described in [1][2]. A working definition of

Computer Forensics can be formulated as the pursuit of knowledge by uncovering elemental evidence extracted from a computer in a manner suitable for court proceedings [3]. The term elemental implies operations on a fundamental level; such as the microscopic elements of the medium or the bits and bytes of an individual sector. The term uncover refers to the presentation of some aspect of evidence not available through simple observation.

2. COMPUTER FORENSICS

We define computer forensics as the discipline that combines Elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.

A. Computer Forensic technology

SANS article gives an overview of the following definition [4]: Computer forensics makes use of software and tools, according to some pre-defined procedures, comprehensive examination of computer systems to extract and protect computer-related crime evidence. Computer forensics must follow certain criteria in order to ensure the authenticity, comprehensiveness and objectivity of the evidence to the maximum extent. Computer evidence compared with the traditional evidence, has the following characteristics :

1) Computer evidence has a high precision, vulnerability and perishability.

2) Computer evidence has a strong hidden.

3) Computer evidence with multimedia-based.

4) Computer evidence is gathered quickly, stored easily, takes up less space. It also has capacity, transportation convenience, and can be repeated.

According to the characteristics of evidence, computer forensics can be divided into static and dynamic forensics evidence. Static evidence is stored in the computer system with not running or independent disks and other storage media. It is the later evidence. In the case of the invasion, it analyses computer systems which have been attacked using a variety of technologies and methods, and can obtain evidence of the attackers. It detects running computer or

network to obtain evidence. With intrusion detection, honey pot and trap technology, it dynamically analyses the intruder's attempt to obtain real-time digital data.

B. Procedure Of Computer Forensics

Computer Forensics is a four step process

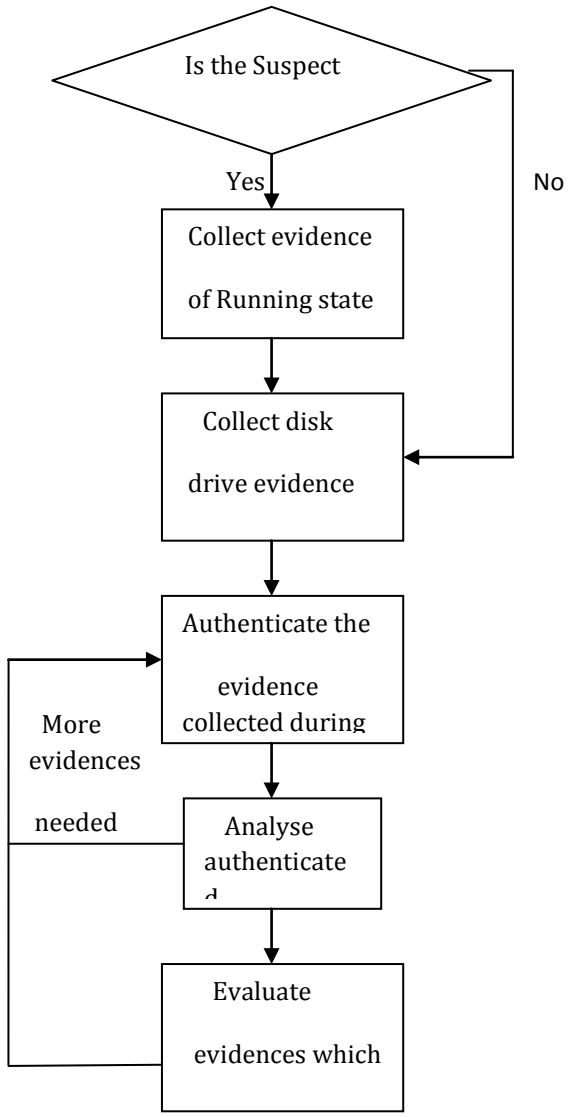

FIG.1 COMPUTER FORENSIC PROCESS

- **Acquisition**

Physically or remotely obtaining possession of the computer, all network mappings from the system, and external physical storage devices

- **Authentication**

The authentication of the evidence is the process of ensuring that the evidence has not been altered during the acquisition process. In other words, authentication shows that the no changes to the evidence occurred during the course of the investigation. Any changes to the evidence will render the evidence inadmissible in a court. Investigators authenticate the hard drive evidence by generating a checksum of the contents of the hard drive. The algorithms most commonly used to generate these checksums are MD5 and SHA.

- **Analysis**

The most time consuming step in computer forensics investigation is the analysis of the evidence. It is in the analysis phase that evidence of wrongdoing is uncovered by the investigator.

- **Evaluation**

Evaluating the information/data recovered to determine if and how it could be used again the suspect for employment termination or prosecution in court

3. THE SOURCE OF DIGITAL EVIDENCE

Digital Evidences come from the target system host data and network data. The main information on a host of evidence comes from some cases as follows [5].

- System log files
- Data and program files
- Swap files
- Temp files
- Free disk space and system buffers.

Evidence on the network data from some cases as follows.

- Firewall Logs
- Intrusion Detection System logs
- Network communication link records
- Information on network devices

4. FORENSIC ANALYSIS

Analysis of the data is the most important part of the investigation since this is where incriminating evidence may be found. Ideally, the forensic analysis is not done directly on the suspects computer but on a copy instead. This is done to prevent tampering and alteration of the suspect's data on the hard drive. The contents of the hard drive are copied on one or more hard drives that the investigator will use to conduct the investigation. These

copies, or images, are obtained by coping bit by bit from the suspect's hard drive to another hard drive or disk. The hard drive containing the image of the suspects hard drive obtained in this manner is called a bit-stream backup. The reason why hard drives must be copied bit by bit is because doing so ensures that all the contents of the hard drive will be copied to the other. Otherwise, unallocated data (such as deleted files), swap space, bad sectors, and slack space will not be copied. A goldmine of evidence may be potentially held in these unusual spaces on the hard drive [6]. The main aspects of forensic analysis are tracking the hacking activities, recovering the data sent through internet and data recovery from target machine. But in this paper our main focus is on data recovery from target machine. Data on the disk can be damaged by following ways.

- Physically destroying the drive, rendering it unusable.
- Destroying files through erasing.
- Overwriting the drive's data so that it cannot be recovered.
- Degaussing the drive to randomize the magnetic domains-most likely rendering the drive unusable in the process.

Because of the differences between Windows-based operating systems and UNIX, analysis of the data on these two systems is presented separately.

A. Forensic Analysis On Windows

Despite the unreliability and propensity to crash, Windows remains the most widely used operating system in people's computers. Investigators must be familiar with how Windows work and the idiosyncrasies associated with Windows in order to conduct a thorough and fruitful investigation. An intimate knowledge of file allocation and deletion in Windows file systems is needed to recover deleted files. For this paper, we will be focusing on NTFS, the file system used in Windows NT and Windows 2000 and above. But many of the techniques mentioned in this section could be used in earlier versions of Windows with few, if any, modifications. NTFS stores attributes of files and folders in a system file called the Master File Table or MFT [7]. The attributes in the MFT of most interest to the forensic analyst are the filename, MAC times (the date and time of a files last modification, last access, and creation), and the data (if the file is small enough) or the location of the data on the disk. With folders, additional attributes of interest are the index entries in the MFT of the files for that folder or, if the MFT cannot hold the entire folders entries, the location of these entries in an index buffer (an allocated space outside the MFT to hold these index entries). NTFS writes data to the disk in whole chunks called clusters. The size of the cluster varies depending on the size of the disk partition and the Windows version. NTFS uses another system file $BITMAP to keep track of what clusters have been allocated on the disk. In the $BITMAP file, a single bit is used to indicate to if the cluster has been allocated or not. So when a file is allocated the bit for the assigned cluster of that file must be set in the $BITFILE file, a record must created in the MFT, an index entry must be created in the folders MFT record or index buffer, and addresses of any clusters used to hold file information must be added to the MFT record. When a file is deleted the bit of the clusters of that file is set to zero in the $BITMAP file, the MFT record is marked for deletion and the index entry is deleted (by moving up the entries below it and thus, overwriting it). However, if the index entry is the last one for that folder, the entry remains visible and thus the attributes are recoverable; useful evidence like file access times can be found. NTFS overwrites the MFT records marked for deletion when creating a new record in the MFT. If no new records have been created in the MFT, the records marked for deletion are not overwritten and useful file attributes and possibly data (if it fit in the record) can be recovered as well [7]. But it is possible to recover deleted files even after its record is overwritten in the MFT and index entry of its parent folder. If the file data was large enough, the data would have resided in some clusters on the disk instead of the MFT itself. Clusters holding data of deleted files compose part of the unallocated space on the disk, so a simple listing of the file directory's contents will not show the deleted files. Because the forensic analyst has all the contents of the suspects hard drive, the analyst could search for a deleted files contents on the disk using a hex editor or other forensic tools. Unallocated space is a huge source of information for analysts because deleted file data residing there may not have been overwritten yet. Unallocated space also contains contents of the index buffers of deleted folder entries. Moving and renaming a file creates entries in the MFT that have the same MAC times, starting clusters and file sizes. Forensic analysts can examine the record allocated renamed file in the MFT with the deleted file in the unallocated space to compare if they are indeed the same. If they are the same, this can establish proof that a suspect had knowledge of the files existence since the suspect moved it (if only the suspect had access to the computer). MAC times also can help prove the suspect's

knowledge of a file and its contents as they show the time it was created, last modified, and last accessed. For example, if the file was last accessed at a time much later than the creation time, the investigator could show that the suspect knowingly used the file, as shown in a court case involving child pornography in which the defendant had claimed he simply downloaded files of unknown content and forwarded them to others without viewing them. The forensic investigator had evidence of the MAC times of the files in question and that many of the files had access times far later than the creation times. The defendant pled guilty as a result. Analysts can also inspect the contents of the Recycle Bin that holds files that are deleted by the user. When a file is deleted it is moved to the Recycle Bin where a record is created in a system file of the Recycle Bin (named INFO) for that particular file. The entry contains useful information for the analyst such as the files location before it was deleted, the files original name and path, and the date of the deletion. These pieces of information can show that the suspect did create and knew the location of a file and knowingly deleted it. When the user empties the Recycle Bin, Windows deletes the entries in the INFO file. If it is not completely overwritten, the deleted INFO file entry can still be examined. As stated before, deleted file data and attributes may reside in the unallocated space. Another area of the disk that may hold deleted file attributes is the file slack. File slack refers to the space between the end of a file and the cluster it resides in. It is often the case that a file does not fit into an exact multiple of clusters. So the space remaining is called file slack and it may contain data from previously deleted files[7]. In addition data may be found in the swap space. If the RAM is full, the OS writes some of the data to a special place on the disk called the swap space. This is the concept behind virtual memory. The swap space may contain the remnants of these deleted files if they were deleted very recently. Shortcut files in Windows provide analysts with another source of information about files. Shortcut files contain MAC time of the files that they refer to and the full paths to the referred files. Remnants of deleted shortcut files, like other files, can be searched in the unallocated space, slack space, and swap space of the disk. Investigators can also examine the Internet files that are cached by Internet Explorer. These files are named Index.DAT and they contain the URL, date last modified by the server and the date last accessed by the user. These caches may be deleted by the user but again, like deleted files and shortcuts, these deleted cached files may be recovered in the spaces of the disk mentioned above. These temporary files are used to spool print jobs in order for the application program to continue to be interactive with the user. The temporary files include the data itself and the full path, potentially useful to the forensic examiner. When the printing job is finished, these temporary files are deleted and may be recovered in unallocated space or the swap file. The forensic analyst may look at Windows registry to find information about hardware and software used. The registry contains the configuration information for the hardware and software and may also contain information about recently used programs and files. Proof that a suspect had installed a program or application may be found in the registry. Another source to recover files and find evidence is the NTFS $LOGFILE. The $LOGFILE records all transactions done on the NTFS. The $LOGFILE is used to restore the NTFS if (or more appropriately, when) the system crashes. The NTFS is then able to undo or redo transactions. The $LOGFILE may contain index entries for folders, a copy of a MFT record (including MAC times), index buffers, and other potentially useful information that the examiner can use. For example, evidence of a filename may only exist in the $LOGFILE and nowhere else (if it had been overwritten).Windows systems give the forensic analyst plenty of sources of useful information. The places mentioned in this paper are just some of the areas that the investigator can search for evidence against the suspect.

B. Tools To Recover Data On Windows

- **Drivespy**

It is a forensic DOS shell. It is designed to emulate and extend the capabilities of DOS to meet forensic needs. It includes A built in Sector (and Cluster) Hex Viewer which can be used to examine DOS and Non-DOS partitions.

- **Encase**

It is a computer forensics product which is used to analyze digital media (for example in civil/criminal investigations, network investigations, data compliance and electronic discovery). The software is available to law enforcement agencies and corporations. It includes tools for data acquisition, file recovery, indexing/search and file parsing. Special training is usually required to operate the software.

- **Ilook**

The ILook Investigator Forensic Software is a comprehensive suite of computer forensics tools used to acquire and analyze digital media. It provides the list of allocated and unallocated files and works with compressed zip files.

C. Forensic Analysis On Unix

Conducting an investigation on Unix systems is very similar to conducting one on Windows systems. The forensic analyst must understand how Unix allocates and deletes files in order to know where to look for the contents and attributes of files that exist (and potentially hidden) and are deleted. But the idiosyncrasies of Unix provide the investigator with different approaches to analyzing the data on Unix systems versus windows systems. Unix and Windows view files very differently. Unix uses the concept of inodes (index nodes) to represent files. Each inode contains the pointers to the actual data on the disk as well as file attributes useful to the investigator; these include the owner ID, access Permissions (read, write, execute), the number of links (number of directories referencing the file), the MAC times which are the last modification, access, and change of status (change of owner, permission or number of links), and file size. Note that the filename is not included with the inode. Instead the file name is stored as an entry in the directory structure along with the location of the actual inode. Like the NTFS on a Windows system, the Unix file system allocates data in fixed sized pieces called blocks. This is analogous to the clusters used by the NTFS. Therefore, file slack, the space between the end of a file and the end of the cluster, is also found on unix systems as well as Windows systems because not all files fit exactly into the blocks on the disk. Forensic analysts can examine the file slack for remnants of deleted files and attributes. File deletion in Unix involves marking the directory entry for that file name to marked as unused, resulting in the disconnection of the file name with the actual file data and attributes. The inode of the file is marked as unused and some but not all of attribute information is lost. The file data blocks are marked as unused according to the creators of the Unix forensics toolkit, The Coroner's Toolkit (TCT), the deleted file data and attributes remain for long periods of time such as hundreds of days for heavily used systems because Unix has good file system locality files tend to be clustered together instead of randomly space apart. Unix file systems avoid fragmentation as much as possible to achieve this locality, allowing deleted files and attributes to remain much longer on the disk since chances are slim that the new files to be written to the disk are the same size as these deleted files. So, deleted files may be easier to recover on Unix systems than on Windows. The Coroner's Toolkit is widely used to examine Unix systems and contains many useful utilities for forensic analysts. One such tool is the unrm, a tool that un deletes files. Deleted file attributes can be recovered using the ils tool in the TCT. Remember that file attributes are very important to investigators, especially the MAC times. Even TCT includes a tool called mactime that neatly displays the MAC times of a file. Everything in Unix is a file. So any transactions done within Unix will leave evidence of that the transaction occurred because the MAC times for the associated files will be altered. Analysts can examine the MAC times of files in Unix like the MAC times of files in Windows to show that the suspect had knowledge of the existence and contents of a file. However, skilled hackers can alter the MAC times to hide their tracks within the file system since inode information is stored in the file system. So investigators should not completely trust the MAC times of files. Unix tools can be used to examine the contents of the hard drive. Commonly used commands include find, grep, and strings. Analysts can use these tools to form keywords to search for a specific piece of data like an email or pornography. The TCT includes a tool called lazarus that attempts to classify the blocks of data as text files or binaries. With text files, lazarus checks for the keywords that the analyst has requested in the form of regular expressions. Places on the hard drive that the analyst could look for remnants of files are nearly the same as those on Windows systems. In addition to the file slack mentioned earlier, investigators can search through the Unix swap file (similar to the Windows swap file), and of course, the unallocated space occupied by unused and deleted files. In addition, for each user in Unix there is a directory named /tmp that holds temporary application files. This is similar to the situation in Windows with temporary application files being created; the contents of these temporary files may still exist in the /tmp directory at the time of the investigation and may be used as evidence against the suspect. Unix gives the users the ability to repeat commands used in previous sessions. In order to do this, the commands are saved in a shell history file. Thus the shell history file can be examined to trace the steps of a hacker or to show that the suspect knowingly created, modified, accessed, and/or deleted a specific file. However, a user (or hacker) can clean out the shell history file to cover his tracks. So, the shell history file can be useful only some of the time, especially if no attempt has been made at modifying it.

Forensic analysis of a Unix system shares some characteristics with that of a Windows system. The search for deleted data involves looking in the same kinds of spaces like the unallocated space, file slack, and swap space. But investigation of Unix systems can involve the use of Unix tools that help in the search for certain patterns among the contents of the disk. In addition, unix forensics

toolkits such as the Coroner's Toolkit enormously aid in the examination of Unix systems.

D. Tools To Recover Data On Unix

- ***The Coroner' Tool Kit*:**

A coroner's means government official who Investigates human death or determines cause of death. The Coroner's Toolkit is a set of tools for post-mortem analysis of a UNIX system [8]. It is designed to discover data or programs which may not be visible to the operating system through the normal file interfaces

- **The Sleuth Kit**

The Sleuth Kit (TSK) is a library and collection of Unix and Windows-based tools and utilities to allow for the forensic analysis of computer systems. The seulth kit's tools allow us to examine the layout of disks and other media [8]. It supports DOS partitions, BSD partitions (disk labels), Mac partitions, Sun slices (Volume Table of Contents), and GPT disks. With these tools, you can identify where partitions are located and extract them so that they can be analyzed with file system analysis tools.

5. CONCLUSION:

Many criminal investigations in today's technology rich society will involve some aspect of computer forensics discussed in this paper. Any person undertaking to investigate such a case should be familiar with the basic technologies involved in gathering the information, how to properly gather the data, and how to ensure that the information will be valid as evidence during trial. In particular, it is important to be able to acquire, authenticate and analyze data stored in electronic devices, whether they run Unix or Microsoft operating systems. Furthermore, a competent investigator should understand the technologies involved in tracing and detecting the actions of a specific computer user. In the above pages, we have given an overview and brief introduction of each of these important aspects of computer forensics. In future we shall proceed towards Web forensics which includes tracking the hacking activities. Our purpose in compiling this paper was to bring together the different perspectives of computer forensics in one place, but it is not meant to be a complete description of the field.

REFERENCES

[1] Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section (CCIPS) July-2002. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] Thomas Welch, "Handbook of information Security Management ", CRC Press LLC, 1999.

[3] G.Shpantzer and T.Ipsen, "Law Enforcement Challenges in Digital Forensics." Proc. 6th National Colloquium Information System Security Education. NCISSE Colloquium press, 2002.

[4] Lunn D A. An overview of computer forensics. http // www. sans.Org/ in forsecFAQ/ incident/ forensics. html.

[5] Zhang Yan, Lin Ying "research on the key technology of Secure Computer forensics" Third International Symposium on Intelligent Information Technology and Security Informatics

[6] Warren G. Kruse II and Jay G. Heiser. Computer orensics: Incident Response Essentials. Addison Wesley, Boston 2001, p. 2.

[7] Bob Sheldon. .Forensic Analysis of Windows Systems, from Handbook of Computer Crime investigation:Forensic Tools and Techniques, 137-139.

[8] Wietse Venema, "File recovery Techniques",Dr.Dobb's Journal, december 2000. [cited may 21,2003].