ISSN No:-2456-2165

Computer Forensics: Data Recovery Perspective over Windows and Unix

Kaustubh Aggarwal* , Dr. Shravan Kumar Garg**
*M.TECH Scholar, CSE department, S.I.T.E, Swami Vivekanand Subharti University, Meerut, India **Professor, CSE department, S.I.T.E, Swami Vivekanand Subharti University, Meerut, India

Abstract:- Now a days, illegal access to computer systems are increasing rapidly, that's why need of computer security has been increased. It gave birth to the need of Computer Forensics to get the evidences of those attacks. Analyzing the digital evidences on Windows and Unix platform is presented in this paper. Various methodology used by digital hackers to wipe out the information in e – storage media and its corresponding ways of recover taken by the forensic experts are being discussed in this paper.

I. INTRODUCTION

Due to rapid development in information technology, computer became a powerful mechanism as it brings convenience not only for common people but also for criminals. Comparing traditional and digital evidence, digital evidence has differed properties. Extraction of evidences in the form of data from computer system has now raised new provocations to laws and information technology. The term "Computer forensics" was introduced in IACIS (International Association of Computer Specialists), the first International Conference held in 1991. For the first time, it was the main theme at the annual meeting of 13th session of International FIRST (Forum of Incident Response and Security Teams) held in 2001. Afterwards, Computer forensics became the hot topic for research. This paper incorporate following – (a) computer forensics (b) Forensic analysis on Windows (c) Forensic analysis on Unix. The definition of Computer forensics can be expressed as the discipline that amalgamates computer science and elements of evidence that are extracted from computer for further court proceedings. The term essential suggests procedure on a principal level; like the tiny components of the medium or the pieces and bytes of an individual area. The term uncover alludes to the introduction of some part of evidence not accessible through basic perception.

II. COMPUTER FORENSICS

The definition of Computer forensics can be expressed as the discipline that amalgamates computer science and elements of evidence that are extracted from computer, networks, storage devices, wireless communications in such a way that it proves to be evidences in the court proceedings.

A. Computer Forensic technology

SANS article gives an overview of the following definition[1]: 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 investigation should follow certain measures to guarantee the validness, extensiveness and objectivity of the proof to the greatest degree. Computer Evidence has the accompanying attributes in contrast with the traditional evidence:

(i) Computer evidence is extremely vulnerable, perishable and précised.
(ii) The evidence is intensively hidden.
(iii) Multimedia based computer evidences.
(iv) The evidence is collected swiftly, easily stored and occupies less room. Also, it is effortlessly transported and can be repeated.

The division of computer forensics is into two types – static and dynamic forensic evidences, it is according to the trait of forensic evidence. Static evidence remains in the hard disk or any other storage media, known to be later evidence. After any invasion, the system is analyzed using different technologies and methodologies to acquire evidences of the attack. To obtain evidence, running system or networks are being detected. Dynamic analysis is processed in case of intrusion detection, honey pot and trap technology. The real time digital data is obtained after such analysis.

B. Course of Action of Computer Forensics

A four step process is being followed for Computer Forensics –

- **Acquisition:**

Getting the access of the computer either physically or remotely and mapping the networks and external storage devices from the system.

- **Authentication:**

While acquiring evidences, it has to be taken care of that the evidence should not be modified. Or, we can say that, authentication ensures that the evidence has not been modified throughout the investigation. If the evidence is altered, then it is not accepted by the court of law. Investigators authenticate the evidence by the generation of checksum. This checksum is usually generated using most commonly used algorithm – MD5, SHA.

- **Analysis:**

Analysis of evidences is the most tedious step in the investigation of computer forensics. It is that phase of investigation where all the crimes are unfolded by the investigator.

- **Evaluation**:

The recovered information is being determined so that it can be used against the suspect for the prosecution in court.

III. ORIGIN OF DIGITAL EVIDENCE

Digital evidence is sourced from the targeted system host and network data. The crucial information extracted from the host is as follows:

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

Information obtained from network data is as follows:

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

IV. FORENSIC ANALYSIS

The collection and analysis of data is the foremost part of any investigation. By this, we can get the accusing evidence. Forensic analysis is executed on a copy instead of the suspect's computer. It is done to prevent damaging and alteration of data on the hard drive of suspect's system. The data of hard drive is copied to another one and is used for further investigation. Images or copies are extracted by copying bit by bit from the suspected hard drive to the other storage device. This process of copying is and containing images is known as bit- stream backup. Copying data bit by bit is done to ensure that whole content is copied. Otherwise, unallocated data (such as deleted files), swap space, bad sectors, and slack space will not be copied [2]. A goldmine of evidence may be potentially held in these unusual spaces on the hard drive [3]. The main facet of forensic analysis is to track the hacking activities, recovery of data shared using internet and data recovery from target machine. In this paper, our main highlight is on the data recovery from target system. Following are the techniques that can be used for destroying data –

- Damaging the disk in such a way that it can't be used again.
- Deletion of data.
- Superimposing the data making it unrecoverable.
- Demagnetizing the drive making it of no use.

Analyzing data on Windows and UNIX is quite different. So, it's presented separately.

A. Window based forensic analysis

Windows is the most extensively used operating system despite of being unreliable and crashing propensity. In order to execute a fruitful investigation, investigators must know about Windows and its behavior. Knowledge of file allocation and deletion is needed for the recovery of data. Our centre of attention is on the file system used in Windows 2000 and above for this paper. NTFS stores attributes of files and folders in a system file called the Master File Table or MFT[4]. For a Forensic analyst, most interesting trait of MFT is – filename, MAC times (date and time of last modification, access and creation of a file) and the location of data. Apart from folders, index entries are the additional attributes which attracts the interest of the forensic analyst. These are the entries in MFT of files for the particular folder and if information of folder is not in present then it can be found in an index buffer (outside MFT, an unallocated space to hold index entries). Data written on the disk by NTFS is in whole chunks known to be Clusters. To maintain a track of cluster allocation on the disk, system file $BITMAP is being used by NTFS. Single bit is used to indicate for the allocation of the file in the $BITMAP file. Following the trend of $BITMAP file, after the allocation of bit a record is created and in MFT record an index entry is being created. Clusters are being used to keep the track record of that file and it must be affixed in MFT records. After the deletion of a file, the $BITMAP file is set to zero and MFT record is also marked as deleted. But, if the deleted file marks the last entry of MFT record, then it remains visible and can be recoverable. Creation of a new record makes the NTFS to overwrite the deleted MFT records. 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 [4]. Even after the records are overwritten in MFT, recovery of the file deleted is attainable. Some residues must have left in the clusters if the file data is large. As the forensic analyst is having wholesome data of suspect's hard drive, using hex editor or some other forensic tool, analyst can search for the data. Examination of allocated renamed file with the deleted on in the unallocated space can be done by the forensic analyst by their comparison. If the files compared are found to be same, then it will act a proof against the suspect. Using MAC times, it will be helpful in proving that suspect had the knowledge of the file. Inspection of Recycle Bin can also be executed by the forensic analyst as it contain the files deleted by the user. File moved to Recycle Bin holds the record that when was it created, when was it modified and the destination from where is it deleted. Such information is helpful in proving suspect's guilt. And, if the user deletes the file from Recycle Bin then its information is stored in INFO file. Deleted INFO file can be inspected if it's not overwritten. File slack is another area of disk from where deleted data can be retrieved. Space between end of a file and the cluster where it is resided can be termed as file slack. Apart from this, if RAM is not empty, then OS write down the data in a different place known as Swap Space. It is the space where residues of recently deleted files can be found. Investigation of cached files which are formed during internet access on Internet Explorer can also be executed by the analyst. These files are stored as Index.DAT containing the information of URL, last accessed by the suspect. Another source from where evidence can be extracted is the NTFS $LOGFILE. All the transactions that are carried out on the NTFS are recorded in $LOGFILE. In this paper, the sources mentioned from where the investigator can collect evidences are just some of them.

B. Recovery tools used in Windows OS

- **Drivespy –**

Drivespy is built to improve the forensic analysis over DOS. It includes A built in Sector (and Cluster) Hex Viewer which can be used to examine DOS and Non-DOS partitions [2].

- **Encase –**

For analyzing digital media, a forensic tool was developed named as Encase. For investigating civil crimes, network related crimes and many more, encase is used. This software is designed for acquisition, recovery of data and file parsing. To operate this, distinctive training is required.

- **Ilook –**

This software is designed to acquire and analyze the digital media for the forensic analysis. It works with unallocated and allocated files by providing them to the investigator and also, analyzing the compressed files.

C. Unix based Forensic Analysis

Executing an investigation over Unix operating system is quite similar to the Windows one. The investigator just needs to know the allocation and deletion of files done in Unix. The content and attributes of file that are potentially hidden is found and how to access them, is to be known by the forensic analyst. Different behavior of Unix operating system provides the analyst with differentiated approach. Viewing files in Unix is distinct in comparison to the Windows operating system. Concept of Index Nodes (Inodes) is utilized by Unix for the presentation of files. Pointers are present in each inode which is very useful for the investigator. These pointers include owner ID, MAC status, number of directories referring to file, permissions to read, write, execute and file size too. It should be kept in mind that filename is not there with the inode. In fact, along with location of the file, the file name is saved in a directory like structure. In Unix file system, data allocation is into fixed size of pieces known as blocks. Just like Windows, file slacks are also found in Unix because every file can't be fitted into blocks. Residues can be investigated in the file slack as executed in the Windows OS. When a file is deleted in Unix system, the directory entry marks the file name as unused which results in detachment of the file name with the actual one. Most widely used software for forensic investigation of Unix system is 'The Coroner's Toolkit'. One of it's tool called as Unrm is extensively used for restoring the files which have been deleted by the user. Each file attribute is very crucial in the investigation process as it has the MAC times. By analyzing the MAC times of files, each and every transaction can be investigated. Moreover, analysts must remember that users or hackers can modify the MAC times of the file to hide the information of their tracks. To represent the blocks of data as text files or binaries, TCT has a tool known as Lazarus. Using this tool, investigator checks the file by requesting keywords in the form of regular expressions. The forensic toolkits are extensively used in examination of Unix OS.

D. Recovery tools used in Unix OS

- **The Coroner's Tool Kit –**

The term 'Coroner's' meant the government official who executes post mortem of the dead body after crime. Similarly, The Coroner's Toolkit is a set of tools for post-mortem analysis of a Unix system [5]. It is designed and developed to locate the data that is not visible normally.

- **The Slueth Kit –**

The Slueth Kit (TSK) can be used in both Windows and Unix based operating system. It is a library and collection of tools to be used in investigation of any crime in both Windows and Unix platform. The Slueth Kit's tools allow us to examine the layout of disks and other media [5]. It is helpful in locating and extracting the partitions so that the evidences can be collected.

V. CONCLUSION

In today's era, as the technology is getting smarter, digital thieves are also getting smarter. It's very important to protect our private information from such people. That's why it is necessary for everyone to know about the computer forensics. Through this paper, we have given a basic overview of Computer Forensics which will be helpful for those who are undertaking such investigations. Our main motto for the compilation of this paper was to bring the different perspectives of Computer Forensics into the limelight, but it's not a complete description, just an overview.

REFERENCES

[1]. http//www.sans.Org/inforsecFAQ/incident/forensics.html.

[2]. Palwinder Singh, Amarbir Singh "Computer Forensics: An Analysis on Windows and Unix from data recovery perspective", IRJET, [cited April 2016]

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

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

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