Extraction of Persistence and Volatile Forensics Evidences from Computer System

Esan P. Panchal
Department of Computer Science,
IT Systems and Network Security,
Gujarat Technological University,
India

***Abstract*- Forensic Investigations are carried out in order to find who committed a crime, from where and how using a computer system. Consider a scenario that in an organization an employee might have disclosed company's private data through the organization's computer. This would result in financial as well as reputation loss. Forensic Investigators need to get an access of all the computers, say, 100 computers throughout the organization. The normal procedure carried out by forensic investigators in order to collect the Evidences is Hard Disk Imaging and further analyzing it in a laboratory. This involves extraction of Persistent and Volatile Data from the Windows Registry as well as the slack space and allocated space.This involves doing the Live Analysis, Dead Analysis or Postmortem for finding the hidden and deleted files from the clusters. This investigation becomes a tedious task when Investigators have to take images of hundreds of hard disks and each of 1 TB. There are many disadvantages of performing this task in terms of time, money and resources. Even there are issues as to where to securely store 100 TB data? All these questions would make an investigator's task very complex and time consuming. If this time is reduced to half then it would be beneficial to investigators as well as the organizations. Current techniques perform the analysis of a computer systems and help to find evidences but leads to time constraints for any entity. Henceforth, there should be a technique which saves time, money and resources for the organizations and make the job of the investigators easy and less laborious.**

***Keywords*- Forensic Investigations, Hard Disk Imaging, Evidences, Persistent Data, Volatile Data, Slack Space, Allocated Space, Windows Registry, Live Analysis, Dead Analysis, Postmortem.**

I. INTRODUCTION

Computer forensics (sometimes known as computer forensic science) is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media[1].

Digital Evidence – encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator [2].
Finding digital evidences from a computer system requires few techniques to be used. But problems arise when there are junks of data to analyze and hundreds of computer hard disks to take evidences from. In order to solve the problems of wastage of different resources, we just focus only on those areas of the computer system from where all the digital evidences can be found and analyze most probable areas where can find forensics evidences. So, instead of whole disk duplication, we just analyze the data where there are probabilities of crime or attack occurrences in computer system.

II. MOST PROBABLE AREAS OF COMPUTER SYSTEM FOR GETTING DIGITAL EVIDENCES

Getting persistent and volatile data would make the investigators work easy for performing analysis. The investigators don't need to extract all the data from all the computer systems. They focus and collect on the relevant part which gives them evidences. These evidences can be found by collecting information from persistent and volatile storage devices. They need not collect all data but get metadata. Persistent and Volatile memory help in order to accomplish these tasks.

III. WHAT SHOULD BE ANALYZED FROM A COMPUTER?

Computer Forensics is the specialized practice of investigating computermedia for the purpose of discovering and analyzing available, deleted, or "hidden" information that may serve as useful evidence in a legal matter.Computer forensics can be used to uncover potential evidence in many types of cases including, for exampleCopyright infringement, Industrial espionage, Money laundering, Piracy, Sexual harassment, Child pornography, Theft of intellectual property, Unauthorized access to confidential information, Blackmail, Corruption, Decryption, Destruction of information, Fraud, Illegal duplication of software, Unauthorized use of a computer etc.

How is it possible to retrieve deleted evidence? A computer's operating system utilizes a directory that contains the name and placement of each file on the drive. When a file is deleted, several events take place on the computer. A file status marker is set to show that the file has been deleted. A disk status marker is set to show that the space is now available for another use. While the user can no longer see the file listed in any directory, nothing has been done to the file itself! This newly available space is called free or unallocated space and until the free space is overwritten by another file, the forensic specialist can retrieve the file in its entirety. Overwriting might be caused by a variety of user activities, such as adding a new program or creating new documents that happen to be

written to the space where the "deleted" files exist. It is only when the data is overwritten by new data that part or all of the files are no longer retrievable through forensic techniques

The useable space on computer hard drives is divided into sectors of equal size. When a user needs to store information, the computer's operating system automatically determines which sectors will be used to perform the task. In many instances the information being stored will not use up all of the space available in the designated sector(s). When this happens, information that was previously stored on the hard drive remains in the unused part of the designated sector, in what is called slack space. This means that even if part of the drive has been overwritten with new data, chances are that some implicating evidence will remain in the slack space. Critical data contained in slack space is also recoverable using forensic techniques.

- Login Activity
- Examination of Internet Activity
- Computer usage history
- Uninstalled/Installed Programs
- Violation of rules of an Organization
- Deleted Files
- Currently logged on user / user accounts
- Current executing processes and services
- Windows registry

IV. Analysing Computer for getting digital evidences

The impact forensic science has had on countless criminal investigations and trials make it a crucial part of law enforcement. Therefore, it is necessary to continue advancing the forensic science to meet the increasing demand of law enforcement against cyber-crime. In cyber-crime investigations, the crime scene can consist of one or more computers perhaps spanning one or more computer networks. A cyber-criminal may affect a system locally or remotely. A local attacker may leave physical evidence at the scene such as witnesses or fingerprints in addition to electronic evidence. Via the Internet, a remote attacker can penetrate other systems connected to the Internet from anywhere in the world, leaving only electronic evidence. In either case, digital forensic evidence can be gathered from the criminal's computer, the victim's computer, or both. This digital evidence can be broadly categorized in two ways, non-volatile and volatile.

A. Non-Volatile Digital Evidence

Non-volatile electronic evidence can be recovered after a system is powered down and is found on hard drives, USB flash drives, and floppy disks. It is in non-volatile memory where most of the electronic evidence originates. System logs, network logs, malicious code, corrupted files, emails, internet browser cached files and history, and deleted files are all forensic evidence stored in non-volatile memory. Network logs may contain TCP session logs indicating the source IP address from where the attack originated. The malicious code may be analyzed to determine exactly what the attacker did to the system. Emails may contain incriminating records of criminal activity and possibly reveal accomplices. Analysis of the disk drive's file system can lead to therecovery of deleted files, which may contain further evidence. Electronic evidence gathered from non-volatile memory can be used to determine how and when a system was infiltrated, what files were corrupted and how, and how much damage, if any, was done to the system. For the criminal's computer, email and browser history and cache can prove the criminal's intent, expose any accomplices, and even give further evidence of how an attack, if any, occurred . However, a careful cyber-criminal may have permanently erased any incriminating evidence from non-volatile memory, thereby making its recovery impossible. In the case of an infiltrated computer running malicious code, there is other evidence that can be useful.

B. Volatile Digital Evidence

The other type of electronic evidence is in volatile memory. Unlike data stored on hard drives, electronic evidence found in main memory disappears once power is removed from the system. Information about each running process, such as create times, exit times, open files, executing code, and child process are stored in main memory. This type of evidence is useful if a malicious program is running or another program has been corrupted on a live system. Unlike the non-volatile memory, this evidence cannot be erased from memory as long as malicious code is running. Additionally, trusted programs may be used to gather data from a live system such as open network ports, established network connections, logged on users, and list of running processes [11].

V. Importance of Memory Forensics

Memory forensics is important in order to do forensic investigations. Data from memory is captured and further analyzed. Using traditional analysis, data is captured and further analyzed in forensic laboratory. But there are some limitations of traditional analysis as, if data is encrypted then investigator cannot access that data unless it has been cracked or recover the key to decrypt data. As keys and passwords are rarely stored in hard disk. It just loaded into a memory when user types in their password, or when data is going to be decrypted. The passwords and keys are necessarily loaded into and stored in memory; analysis of that memory can allow the Techniques and Tools for Recovering and Analyzing Data from Volatile Memory analyst to recover them. Another limitation of traditional analysis is that the inability of the physical disk to reveal information about processes that were running in memory, which denies the investigator insight into how applications were being used on the system at the time of the attack. It is also possible for a suspect to hide data in memory, or for a remote attacker who has compromised a

system to tore tools, data, and other artifacts there rather than on the system's drive [12].

- Attackers who write viruses, Trojans and Worms that reside only in memory not in hard disk. So, Forensics investigation might be tough because these kind of malicious activities could not be caught.
- All of the above forensics evidences are found in computer memory. It would reside in persistent or volatile memory.
- Login Activity, Examination of Internet Activity, Computer usage history, Uninstalled/Installed Programs, Deleted Files can be found in persistent memory.
- Currently logged on user / user accounts, Current executing processes and services, Network connections can be found in volatile memory.

A. Persistent Data: Persistent data is the data that is stored on a local hard drive or another medium and is preserved when the computer is turned off [3]. Persistent data should be collected when it is clear that evidence related to the computer security incident resides in the persistent storage areas.

B. Volatile Data: Volatile data resides in registries, cache, and random access memory (RAM). Since volatile data is ephemeral, it is essential an investigator knows reliable ways to capture it.Volatile data generally resides in RAM which would be lost if computer is turned off or rebooted. Volatile data should be collected if you are not sure why a computer is acting abnormally.If you notice suspicious user activity or if you have been alerted that a rule or policy has been violated.

VI. TECHNIQUES FOR FORENSIC ANALYSIS

In order to perform above task we need to use some techniques of forensics analysis.

A. Live Analysis: Analyzing a system while it is alive. Leaving the box up and running, and performing an acquisition and analysis without touching the box in any way. Turning off box may alert attacker.

B. Dead Analysis:System is already been shut down or powered off and performing analysis against the physical drive itself. When system is off dead analysis is takes place. So, persistent data would be captured for analysis. This will help investigators to find more evidences by analyzing disk. Like in NTFS file can be hide inside other file. This kind of malicious activities could be caught by dead analysis.

C. Post-Mortem Analysis:Forensics can be applied to "post-mortem" analysis as well. In the case of a computer "crash", analysis can determine whether the event was the result of innocent user error, a computer virus, hardware failure, or a malicious attack. Recovery of important files can be a big part of the preservation aspect of the investigation [4].

By performing above techniques different evidences can be found. From which it is easy to be find suspicious computer. Consider in an organization opening social networking site are not allowed, still if that is to be found means that computer is to be suspicious. So finding most probable computer from bunch of computers is most important task to minimize time to investigate. For example, fromwindows registry extracting visited URLs by an user might tell that user had tried to breach the security or policy violated etc.
There are so many other areas of computer from which investigator can find forensics data which is further used to find most probable computer which is to be suspected.

VII. AREAS FROM WHICH FORENSICS EVIDENCES CAN BE FOUND

1. **HKEY_CURRENT_USER/Software/Microsoft/Internet Explorer/TypedURLs**
   Typed URLs typed by an user in Microsoft Internet Explorer

2. **HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU**
   MRU is the abbreviation for most-recently-used. This key maintains a list of recently opened or saved files via typical Windows Explorer-style common dialog boxes (i.e. Open dialog box and Save dialog box) (Microsoft, 2002). For instance, files (e.g. .txt, .pdf, htm, .jpg) that are recently opened or saved files from within a web browser (including IE and Firefox) are maintained. However, documents that are opened or saved via Microsoft Office programs are not maintained. Subkey * contains the full file path to the 10 most recently opened/saved files. Other subkeys in OpenSaveMRU contain far more entries related to previously opened or saved files (including the 10 most recent ones), which are grouped accordingly to file extension.

3. **HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs**
   Maintains list of files recently executed or opened through Windows Explorer.

4. **HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon**
   This key contains the last logon information

5. **HKLM\SYSTEM\CurrentControlSet\Enum\USB STOR**
   This key contains addition information about list of mounted USB storage devices, including external memory cards.

6. **HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU**
   Maintains a list of entries (e.g. full file path or commands like cmd, regedit, compmgmt.msc) executed using the Start>Run commands.The MRUList value maintains a list of alphabets which refer to the respective values. The alphabets are arranged according to the order the entries is being added.

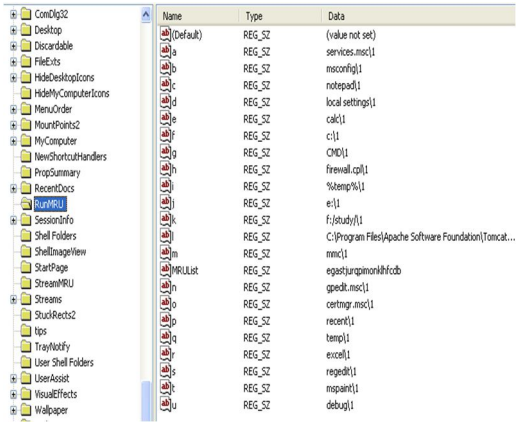

Fig 1. Content of RunMRU Key

7. **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall**
   Getting details of uninstalled programs by user. All programs listed in Control Panel>Add/Remove Programs correspond to one of the listed subkeys. However, they are other installed programs (e.g. device driver, Windows patch) that are not listed in Add/Remove Programs.

8. **Doskey /history**
   Getting previously typed command using command prompt

By using above techniques it would be easy for an investigator to make decision on specific computer to be investigated.

VIII. TOOLS FOR WINDOWS REGISTRY ANALYSIS

A. RegRipper - RegRipper is an open source forensic software application developed by Harlan Carvey. RegRipper, written in Perl, is a Windows Registry data extraction tool.

B. RegFileExport - RegFileExport is a small console application that allows you to easily extract data from offline Registry file located on another disk drive. RegFileExport read the Registry file, ananlyze it, and then export the Registry data into a standard .reg file of Windows. You can export the entire Registry file, or only a specific Registry key.

C. python-registry - A forensic investigator who wanted to access the contents of the Windows Registry from his Linux laptop.python-registry currently provides read-only access to Windows Registry files, such as NTUSER.DAT, userdiff, and SOFTWARE. The interface is two-fold: a high-level interface suitable for most tasks, and a low level set of parsing objects and methods which may be used for advanced study of the Windows Registry. python-registry is written in pure Python, making it portable across all major platforms [13].

IX. TOOLS FOR VOLATILE MEMORY ANALYSIS

A. The Volatility Framework - The Volatility Framework is a completely open collection of tools, implemented in Python under the GNU General Public License, for the extraction of digital artifacts from volatile memory (RAM) samples. The extraction techniques are performed completely independent of the system being investigated but offer unprecedented visibility into the runtime state of the system. The framework is intended to introduce people to the techniques and complexities associated with extracting digital artifacts from volatile memory samples and provide a platform for further work into this exciting area of research.

B. Foriana - It is tool for extraction of information such as the process and modules lists from a RAM image.

C. Draugr - It is a Linux memory forensics tool written in Python.

D. Volatilitux – It is another Linux memory forensics tool written in Python.

X. TOOLS FOR GETTING PERSISTENT DATA

A. DD - Disk imaging tool

B. EnCase (only for Windows) - EnCase is a family of all-in-one computer forensics suites.

C. FTK - It scans a hard drive looking for various information.

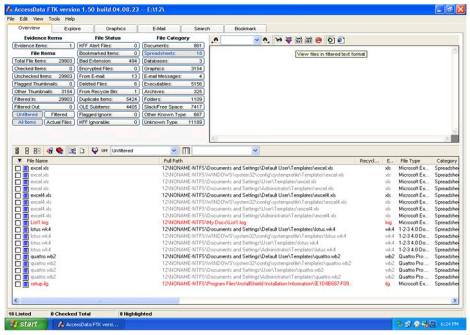

Fig – 2 AccessData FTK version 1.50

fig-2 shows that all spreadsheets are captured using FTK tool. And can collect data from slack space as well. So deleted files can also be recovered by using this tool.

Analyzing persistent and volatile information from a computer system helps forensics investigators to find suspicious computer from a bunch of computers. This will help investigators to save their resources like time, money and manpower.

XI. FUTURE WORK

- Extracting persistent and volatile information from a computer system in forensic point of view.
- Finding most probable areas of computer system from which evidence of crime can be easily caught.
- Automating the forensics tasks like live analysis or dead analysis.
- Aim: Just not to waste the time of investigators.

XII. CONCLUSION

Gathering and collecting the evidences should be done in a systematic manner so that there is no loss of integrity of evidences. The evidences should be stored in form of images and investigations should be carried out properly through standard problem-solving techniques with the tools and applications available.

Effective collection and analysis of digital evidence is a tedious task. This can be done through the Live and dead analysis and evidence collection through imaging the disk drives. In recent years the investigator had to use many forensics tools to perform this task. Integration of all types of forensics tools is a major challenge.

ACKNOWLEDGEMENT

REFERENCES

[1] http://en.wikipedia.org/wiki/Computer_forensics

[2] http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Presentations/DigitalEvidence.pdf

[3] http://www.us-cert.gov/reading_room/forensics.pdf

[4] http://www.windowmeister.com/computer_forensics.htm

[5] B. Carrier: File system forensic analysis, Addison-Wesley Professional, USA, (2008).C. V. Marsico and M. K. Rogers, “ipod forensics,” *International Journalof Digital Evidence*, vol. 4, no. 2, 2005.

[6] M. Kiley, T. Shinbara, and M. K. Rogers, “ipod forensics update,”*International Journal of Digital Evidence*, vol. 6, no. 1, 2007.

[7] S. Willassen, “Forensic analysis of mobile phone internal memory,” in*Advances in Digital Forensics*, 2005, pp. 191–204.

[8] J. Sammes, Anthony and B. Jenkinson, “The treatment of pcs,” in*Forensic Computing*. London: Springer, 2007, pp. 277–299.

[9] W. H. Allen, “Computer forensics,” *Security & Privacy, IEEE*, vol. 3,no. 4, pp. 59–62, 2005.

[10] Forensic Analysis of the Windows Registry by LihWernWong

[11] OFFLINE FORENSIC ANALYSIS OF MICROSOFT® WINDOWS® XP PHYSICAL MEMORY by John S. Schultz

[12] Techniques and Tools for Recovering and Analyzing Data from Volatile Memory by Kristine Amari

[13] http://www.williballenthin.com/registry/index.html