THINK INDIA JOURNAL ISSN: 0971-1260

Vol-22-Issue-16-August-2019

Interpretation of Cyber Forensics Methodologies and Tools

Aswin Thotapalli [1], *Deepak Prashar[2], Awadhesk Kumar Shukla[3]

Research Scholar, Department of CSE, LPU, ashuaswin93@gmail.com

Associate Professor, Department of CSE, LPU, Deepak.prashar@lpu.co.in

Assistant Professor, Department of CSE, LPU, awadhesh.23866@lpu.co.in

Corresponding Author: - Deepak Prashar

Abstract- Forensics in the field of computer science is called by a lot of names, cyber forensics, digital forensics or even computer forensics. Cyber crimes these days are happening at a breathtaking speed and the investigators need to be on par with the criminals to be able identified and apprehend them. Computers are used in almost every task like in IoT to automation in today applications rather than in the beginning times and thus it leads to higher rate of cyber crimes. It leads to the emergence of cyber forensic investigators who have the role of protecting from the various threats and vulnerabilities. This is achieved through the usage of some innovative tools and techniques as represented in this paper. This paper describes the methodologies, tools and techniques used in a digital forensic investigation and provide the insights of the best alternatives for the different situations in hand.

Keywords- Cyber, Forensics, Digital, Forensic tools, Forensic techniques

1. INTRODUCTION

One of the biggest threats facing businesses and corporations is cyber-attacks and threats. Data breaches are one of the most devastating cyber-crimes. Forensics means using an established scientific process for analyzing, collecting and presenting of evidence or data. Cyber forensics is an over-arching field which deals with the forensics for not just the data but the system or hardware as well. Forensic investigators have a pre described set of rules they adhere to every time an investigation is carried out. They also have proprietary tools and software's used to access, retrieve and document the evidence. Database forensics comes under the branch of digital forensics which deals with metadata, memory data, database content and log files to form a timeline. In the late 1970s with the advent of the first personal computers intended for public, users in their personal interests began the process of computerization and informative society, and with the development of public internet networks in the early 1990s there has been increase in the number of cybercrimes crimes carried out using personal computer.

And so, with the rise of the cyber-crimes there was a need for an established law and investigation procedure. This arrived in 1984 with the first such assistance given to the Federal Bureau of Investigation by CART [1]. This led more and more investigative agencies to look at computers as evidence, nowadays any and every electronic item is considered as a source of evidence. Cyber-crimes started exploding in 2000 and this led to the standardization and globalization of the investigation tools and techniques used today in digital forensic investigation. Organizing an incident response team requires establishing, among other aspects, some procedures and methods of analysis that allow us to identify, recover, rebuild and analyze

evidence of what happened. One of the sciences that cover these needs is the Forensic Science, it gives us the techniques and principles necessary to perform our investigation, whether criminal or not. If we take forensic science to the level of computer systems, then we talk about computer forensics or digital forensics.

In a more formal way, we can define Digital Forensic Analysis (DFA) as a set of principles and techniques that comprise the process of acquisition, conservation, documentation, analysis and presentation of digital evidence. Digital evidence means the data set in binary format, that is, it includes the files, their content or references to them (meta- data) found in the physical or logical media of the attacked system. Within the DFA, we can highlight the following the phases:

- Incident identification.
- Collection of evidence.
- Preservation of evidence.
- Analysis of the evidence.
- Documentation and presentation of the results.

Most of the incidents that occur in reality can be framed in several of the above categories, so a good way to identify them is by the mechanism of transmission used. For example, a virus that creates a back door in the system should be handled as a malicious code incident and not as an unauthorized access incident since the virus is the transmission mechanism.

2. SYSTEM ATTACK PREVENTION

This is to detect an attack on your computer systems before it occurs, or at worst when the attack begins. It will always be better to prevent the attack than having to recover the system using its backups. A computer system can prevent attacks by the following:

A. Management: It has proper management of patches and updates to the hardware and software, since many of the attacks are based on exploiting a small number of vulnerabilities in systems and applications.

B. Security: Secure servers based on the concept of minimum privilege, that is, configure them to provide a limited number of services and with a level of restricted access according to the type of user.

In addition, default configurations should be avoided, such as predefined keys, etc. It would also be better to send notification to the administrator when accessing privileged levels which are not authorized.

C. Maintenance: Maintaining network security by setting a perimeter filter in secure mode that is denying any type of access not expressly authorized and having only the traffic necessary for normal daily activity. This will include installing-Firewall, intruder detectors

ISSN: 0971-1260

Vol-22-Issue-16-August-2019

(IDS), network monitors, use of virtual private networks (VPNs), use of secure protocols (IPSec, SSL).

D. Prevention: Prevent the execution of malicious code (malware), using antivirus programs able to stop this type of code like viruses, Trojan horses and worms.

2. PHASES OF DIGITAL FORENSIC ANALYSIS

The whole process of digital forensic is divided in to four phases as described below along with the various activities that are associated with it.

1. Incident Identification
2. Preservation of Evidence
3. Analysis of Evidence
4. Documentation of the Incident

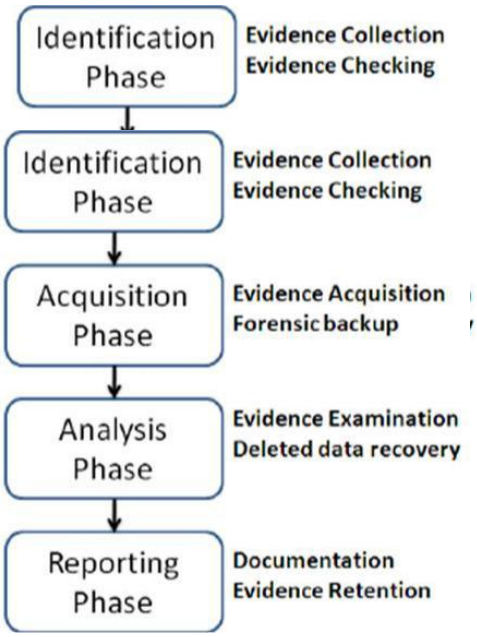

Fig.1 Phases of digital forensic process

There are some major outcomes at the end of the process like it list the system's IP addresses and map the physical address assignment MAC with these IPs (ipconfig, arp, netstat, net). Search hidden or deleted files (hfind, unrm, lazarus). Display system logs and user logs (reg, dumpel) and display system security settings (auditpol). It also generates hash functions of files (sah1sum, md5sum). At the end make bit-by-bit copies of hard drives and partitions (dd, safeback) and

analyze network traffic (tcpdump, windump). After these queries or steps the investigators go on to the log files. They go through the system logs and user logs in search of entries and warnings about installation failures, accesses not authorized, wrong or failed connections, etc. Depending on the platform of the victim these files are found in different locations.

3. ROLE OF OPERATING SYSTEM IN FORENSICS

3.1 Microsoft Windows

This operating system provides the investigators with an environment to perform these inquiries in a number of places, namely, in the Administrative Tools menu, the Event Viewer, the Services Viewer or the the local security directive. Another place where a lot of information is hidden but accessed by the investigators is the Windows registry. The application of the system regedit.exe can help them with this task, but if for some reason they don't trust it, they use their own tools such as reg (allows you to query the registry without modification), or regdmp (exports the record in plain text format .txt) and save it for later querying. In these files they will have to look for a needle in a haystack, due to the huge amount of information that is stored and mixed. A starting point could be to search the registry keys Run, RunOnce, RunOnceEx, RunServices, RunServicesOnce, Winlogon, because under these keys are the services, programs and applications to be loaded at system startup.

3.2 UNIX/Linux

In this type of systems, a series of log files are available (logs), which can usually be found under the /var/log directory. Some of the most important ones are detailed below:[2]

1. /var/log/messages: Contains the general system messages.
2. /var/log/secure: Contains information related to authentication of users and authorization privileges given to them.
3. /var/log/wtmp: Contains a history of all login and logouts.
4. /var/run/utmp: Contains a dynamic list of who has started the session.
5. /var/log/btmp: Contains any failed login attempts on the system.

In addition to these log files, the files may also contain clues of keys, users and groups, they can be found in /etc/passwd, /etc/shadow, /etc/group. The investigators could also find signs of anomalous activity in /root/.bash_history that contains the commands executed by the user and/or the hacker. For the initial purpose of confirming the attack or compromise of the system these first inquiries will be sufficient.

4. EVIDENCE COLLECTION

Usually a detailed forensic investigation is carried out as any other action will tamper with the existing state of the system and causes all the evidence to be corrupted. Now they will have to follow a series of steps in order to gather evidence that allows the investigators to determine the method of entry to the system, the activity of the intruders, their identity and origin, duration of

the crime and all this while taking precautions to avoid altering the evidence during the collection process.

The investigators are meticulous on data collection, taking pictures of the equipment and of the environment because they never know if they will have to deal with the attackers in a trial and all evidence is required.

Next, they have to decide if they want to start taking samples on a "live" or "dead" system. There will be hidden evidence with different levels of volatility, such as procedural records, data structures in RAM or cache memory, active network connections, current users and processes, file system, etc. It will be very difficult to gather all this information at the same time and much of it will be lost if the investigators decide to turn off the computer, Also, if the attacker is still online, he can detect their activity and act with an evasive or, worse, destructive action eliminating all the information. Dead system is only chosen in a handful of cases. For example, if the system is infected with a replicating virus which is causing all the files to be deleted the longer the system stays active.

Evidence collection following the order of highest to lowest volatility.

1. Records and contents of the cache.
2. Memory contents.
3. Status of network connections, route tables.
4. Status of the processes in execution.
5. Content of the file system and hard drives.
6. Content of other storage devices.

The first four forms represent volatile forms of data. Within the volatile evidence the investigators recover the following system data in real time:

1. Date and time.
2. Active processes.
3. Network connections.
4. Open TCP / UDP ports and associated applications “listening”.
5. Users connected remotely and locally.

The outputs of some of these commands take up little space but others can generate a huge amount of information with considerable capacity (from hundreds of MB to hundreds of GB). An interesting option would be to use external USB drives, very economic and that allow great flexibility of handling and transport of large quantities of information. Another option is to use data transmission tools over the network (netcat), which would allow them to send all the

information collected to a secure system, such as for example a device connected in the same network or a laptop connected directly to the affected system.

As soon as they have obtained all the volatile information of the system, they will have to collect the information contained on hard drives, taking into account that these devices not only contain partitions, files, directories, etc. But it also contains other types of data that refer to the files themselves, metadata. It is the metadata that will be of great importance in forensic analysis. Simply copying the hard disk into another hard disk will not copy all the data, specifically hidden data. So, the investigators make an image of the disk, they create bit-by-bit copy of the original disk preserving all the information it contains, including the blocks of the deleted files, free space after each block, inodes or index node (metadata), etc. As a general rule they will always obtain images of hard drives for post collection analysis and always on read-only media. One of the most used tools in UNIX/Linux environments is dd, this allows the investigators to create bit-by-bit images of disks, in addition to offering other options such as obtaining the hash MD5 of the copy, etc. They also combineit with the netcat tool to transfer the complete images through the network.

5. PRESERVATION OF EVIDENCE AND ANALYSIS

It is essential to define appropriate methods for the storage and labeling of the evidence. The first step they do is to make two copies of the evidence obtained, generate a checksum of the integrity of each copy by using hash functions such as MD5 or SHA1, Include these signatures on the label of each copy of the evidence on the CD/DVD or flash drive itself and include the date and time of creation of the copy and name of each copy.

If they also decide to remove the hard drives from the system to use as evidence, they must follow the same procedure, place on them the label “EVIDENCE ORIGINAL ”, also include the corresponding hash amounts date and time of the extraction of the equipment, data of the person who performed the operation, date, time and place where it was stored. This process is known as the chain of custody, where the records of each of the people who manipulate the evidence are recorded. The investigators prepare a document in which the personal data of all those involved in the process of handling the evidence from the time they were taken until storage is recorded.

They keep a record of:

1. Where, when and who handled or examined the evidence, including their name, their identification number, dates and times, etc.

2. Who was guarding the evidence, for how long and where it was stored.

3. When changing custody of the evidence, when and how the transfer occurred and who transported it.

ISSN: 0971-1260

Vol-22-Issue-16-August-2019

All these measures will make access to evidence very restrictive and remain clearly documented, making it possible to detect and ask for handling responsibilities in case of unauthorized access attempts.

Determination of how the attack was carried out: Once they have the chain of events that have occurred they determine which was the way of entering the system, finding out what vulnerability or failure of administration caused the security hole and what tools the attacker used to access the system. These data, as in the previous case, must be obtained in methodical manner using a combination of log file queries, registry, keys, user accounts, etc. A good starting point is to review the services and open processes that it collected as Volatile evidence, as well as TCP / UDP ports and connections that were open when the system was still alive.

6. TOOLS USED FOR DIGITAL FORENSIC ANALYSIS

As seen above in the digital forensics analysis phases, investigators use a plethora of tools to achieve their outcomes. Some of them are described and analyzed based on their characteristics below:

6.1 SANS SIFT[6]

The SIFT Workstation is a forensic tool which was released in December of 2008 by the company SANS

SIFT stands for SANS Investigative Forensic Toolkit. It is a program developed for Ubuntu OS. SIFT is an advanced forensic tool with provides the investigators with a huge variety of forensic tools and incident response tools like Evidence Imaging, Threat Hunting, Malware Analysis, Memory Analysis, Timeline Generation, Image Retention, Autopsy and so on.

Fig 2. SANS SIFT terminal and working space

6.2 Pro Discover Forensic[7]

ISSN: 0971-1260

Vol-22-Issue-16-August-2019

Technology Pathways is an organization which specializes in creating forensic tools. It was founded in 2001. One of the most famous and widely used tool created by them is the ProDiscover Forensic. The Forensic is an advanced data recovery and management tool that can recover files without changing any of the metadata of the file. It can do this because it recovers data at a sector level. It has capabilities such as Text Search Engine, Hash Comparison, Registry Viewer, Event Log Viewer and so on. It is supported on a wide range of Operating Systems including Windows, Mac and Ubuntu.

Fig 3. Pro Discovers forensics working space

6.3 Volatility Framework [8]

The Volatility Foundation is an Independent and Non profit foundation that created the Volatility Framework. It was created in Python under the General Public License. Volatility Framework is used to extract data from RAM Dumps or the volatile memory. Volatility Framework is modular in design and can run on practically any operating system.

```
E:\>"E:\volatility_2.4.win.standalone\volatility-2.4.standalone.exe" imageinfo -f memdump3.raw
Volatility Foundation Volatility Framework 2.4
Determining profile based on KDBG search...

          Suggested Profile(s) : Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (E:\memdump3.raw)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82935c28L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82936c00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2014-03-13 13:31:20 UTC+0000
     Image local date and time : 2014-03-13 16:31:20 +0300
```

Fig 4. Volatility framework workspace

ISSN: 0971-1260

Vol-22-Issue-16-August-2019

6.4 CAINE[10]

CAINE stands for Computer Aided Investigation Environment. It is a Linux Distro developed specifically for cyber forensics. As it is an entire distribution of linux it provides a full fledged environment with GUI. It has a lot of tools pre built like Autopsy, Guymager, Caja web manager and so on. It can be used for Mobile Forensics, Analysis, Script Analysis, Network and Memory Forensics and so on. It is also helpful in automating the compilation of reports to a certain extent.

Fig 5. CAINE framework working space

6.5 Xplico[11]

Xplico is a network analyzer. It is used in forensic investigation to trace out the data packets sent and received on a system. Xplico was developed by Gianluca Costa & Andrea de Franceschi and it is written in C, Python and PHP.

Fig 6. Xplico framework working space

6.6 Forensic Toolkit [13]

This is a collection of forensic tools for Windows platforms, created by the Access Data. This ToolKit will allow the investigators to collect information about the attack, and it consists of a series of command line applications which allows generating of various reports and statistics of the file system to analyze

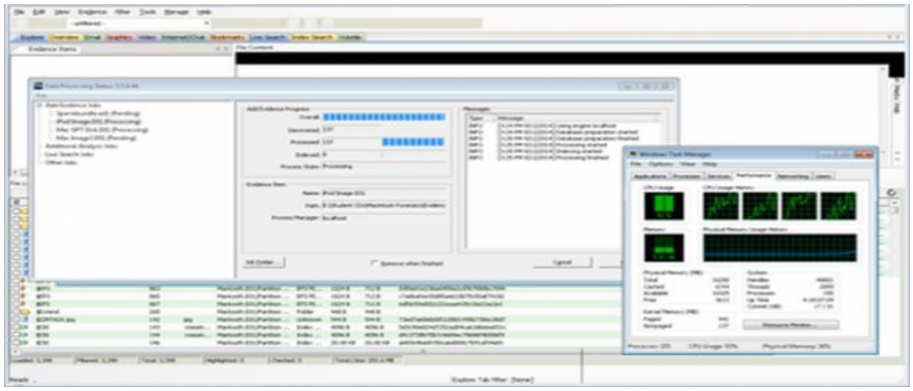

Fig 7. Forensic toolkit framework working space

7. CONCLUSION

In the present era of cyber world, the rate at which cyber crimes are increasing is exponential. With this there is a demand of some tools and techniques by which their effects can be mitigated and in this direction cyber forensics is one of the promising measures. There are various steps in the forensics analysis like identification, preservation of evidence, analysis which is followed by documentation. But the same task is become easier and more precise by using the tools developed in the course of time and research. In this paper extensive review is done of the various tools that look very promising for the forensic investigation.

REFRENCES

[1] Xu, Maochao, et al. "Modeling and predicting cyber hacking breaches." *IEEE Transactions on Information Forensics and Security* 13.11 (2018): 2856-2871.

[2] Chhetri, Sujit Rokka, Sina Faezi, and Mohammad Abdullah Al Faruque. "Information leakage-aware computer-aided cyber-physical manufacturing." *IEEE Transactions on Information Forensics and Security* 13.9 (2018): 2333-2344.

[3] Koroniotis, Nickolaos, Nour Moustafa, and Elena Sitnikova. "Forensics and Deep Learning Mechanisms for Botnets in Internet of Things: A Survey of Challenges and Solutions." *IEEE Access* 7 (2019): 61764-61785.

[4] Prasanthi, B. V. "Cyber forensic tools: a review." *International Journal of Engineering Trends and Technology (IJETT)* 41.5 (2016): 266-271.

[5] Zhan, Zhenxin, Maochao Xu, and Shouhuai Xu. "Characterizing honeypot-captured cyber attacks: Statistical framework and case study." *IEEE Transactions on Information Forensics and Security* 8.11 (2013): 1775-1789.

[6] Al-Dhaqm, Arafat, et al. "CDBFIP: Common database forensic investigation processes for internet of things." *IEEE Access* 5 (2017): 24401-24416.

[7] Kaur, Mandeep, Navreet Kaur, and Suman Khurana. "A literature review on cyber forensic and its analysis tools." *International Journal of Advanced Research in Computer and Communication Engineering* 5.1 (2016): 23-28.

[8] Roman, Rodrigo Fernando Morocho, et al. "Digital forensics tools." *International Journal of Applied Engineering Research* 11.19 (2016): 9754-9762.

[9] Vanlalsiama, B., and Nitesh Jha. "Cyber Forensic: Introducing A New Approach to Studying Cyber Forensic and Various Tools to Prevent Cybercrimes." *IITM Journal of Management and IT* 6.1 (2015): 123-128.

[10] Balon, Nathan, R. Stovall, and T. Scaria. "Computer Intrusion Forensics." (2003).

[11] Dimpe, Precilla M., and Okuthe P. Kogeda. "Impact of Using Unreliable Digital Forensic Tools." *Proceedings of the World Congress on Engineering and Computer Science*. Vol. 1. 2017.

