IJETMR
International Journal of Engineering Technologies and Management Research
A Knowledge Repository

MEMORY FORENSIC: ACQUISITION AND ANALYSIS OF MEMORY AND ITS TOOLS COMPARISON

Mital Parekh [1], Snehal Jani [*2]
[1] Student in M.Tech, Department of Cyber Security, Raksha Shakti University, Ahmedabad, Gujarat, India
[*2] Assistant Professor, Amity School of Applied Sciences, Amity University Madhya Pradesh, Gwalior, India

Abstract:
The enhancement of technology has led to a considerable amount of growth in number of cases pertaining to cyber-crime and has raised an enormous challenge to tackle it effectively. There are various cyber forensic techniques and tools used to recover data from the devices to tackle cyber-crime. Present research paper focuses on performing memory forensic and analyzes the memory which contains many pieces of information relevant to forensic investigation, such as username, password, cryptographic keys, deleted files, deleted logs, running processes; that can be helpful to investigate the cyber-crime pining down the accused. The three main steps followed in memory forensic are acquiring, analyzing and recovering. Recovery of the evidences of crime from the volatile memory can be possible with the knowledge of different tools and techniques used in memory forensic. However, it is always tough to analyze volatile memory as it stays for a very short period. Not all tools can be used for memory forensic in every situation and therefore, it is important to have the knowledge of tools before applying to solve a particular cyber-crime. It is yet to establish on using a single tool for complete investigation, however, most of the tools used are successful in providing reasonable evidences. The present research paper provides an insight on analyzing the memory that stores relevant data, collection of evidences from the device(s), extraction of essential data using different memory forensic tools, tools useful for various purposes and the best suited tool for a particular situation.

Keywords: *Memory Forensic; Digital Forensics; Volatile Memory; Memory Forensic Tools.*

Cite This Article: Mital Parekh, Snehal Jani. (2018). "MEMORY FORENSIC: ACQUISITION AND ANALYSIS OF MEMORY AND ITS TOOLS COMPARISON." *International Journal of Engineering Technologies and Management Research,* 5(2:SE), 90-95. DOI: 10.5281/zenodo.1198968.

1. Introduction

Memory forensic is successful realm which recovers and analysis evidence in the memory of the digital devices by using various tools. The advancement of technology has increased the rates of cybercrime related cases and in order to curb such cases memory forensic has emerged as a potential tool in recent years.[1] Memory forensic is helpful to analyze physical memory, RAM,

to collect the evidence by recovering the data from the seized device that was used during the crime. Memory forensic is also helpful to provide visibility into the runtime state of the system, and, the memory (RAM) must be analyzed for forensic information.[2] Each and every function performed by an application or operating system results in a special kind of change to the random access memory. The research paper focuses on use of memory forensic to recover the data from the devices. As mentioned above there are various tools used in memory forensic and the paper is about using various tools and its suitability for specific purpose. Also, a comparison of various different tools and its uses has been presented. The tools studied in this research paper for memory forensic are RAM Dump, Registry Dump, and Autopsy tool.

2. Background

Depending on the situation, upon arriving on crime scene, an investigator is left with two options: either interact with the system or pull the plug. On one side, it has been known for some time that normal user interaction is undesirable, even performing a clean shutdown would destroy potential evidence by changing timestamps and potentially overwriting information. Following this train of thought, it was suggested that pulling the plug of a machine will leave it in a more preserved state than powering it down gracefully. [3] On the other side, while pulling the plug does preserve the current contents of the hard disk drive, RAM it allows little or no insight into what operations the system was performing at the time when the power was removed. In light of this lack of knowledge, others have provided incident response steps to perform in order to gain insight about the state of the system.[4] Neither of the options works if the contents of RAM is of concern as pulling the plug clears the contents of RAM, while performing many incident response action overwrites potential evidence in memory akin to create new files on a suspects hard disk.

When concerned with the contents of RAM, neither choice is adequate. Simply, pulling the plug can clear the contents of RAM (in most cases), and performing many incident response actions overwrites potential evidence in memory akin to creating new files on a suspect hard disk drive. Two additional concepts need to be introduced into acquisition and analysis stages in order to take advantage of RAM contents: the acquisition of RAM, and the extraction of information from the RAM duplicate.

3. Literature Review

Memory forensics involves analyzing the data stored in the physical memory at operating system runtime. Its primary application is in the investigation of advanced computer attacks which are quiet enough to avoid leaving data on the computer hard drive. Consequently, the memory (RAM) must be analyzed for forensic information. Each and every function performed by an application or operating system results in a special kind of change to the random access memory. These changes often stay for a long time after completion of the operation, significantly storing them, memory forensics provides extraordinary visibility into the runtime state of the system, such as which processes were running, open network connections, and recently executed commands. Individuals can perform an extraction of these artifacts that is totally independent of the machine being investigated.[5] Critical data may exist exclusively in memory, such as unencrypted e-mail messages, disk encryption keys, non-cacheable internet history records, off

the record chat messages and memory-resident injected code fragments. Memory forensics is forensic analysis of a computer's memory dump. Its primary application is investigation of advanced computer attacks which are stealthy enough to avoid leaving data on the computer's hard drive. Consequently, the memory (RAM) must be analyzed for forensic information.

4. Memory Forensics

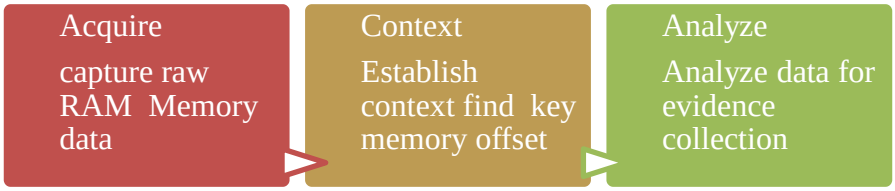

Figure 1: Acquisition and Analysis of Memory

Memory forensic is about capturing the memory contents which is a great tool for incident response, malware analysis, and digital forensics capabilities. Vital information can be retrieved through assessment of network packet captures and hard disk, however, it is the matter of computer memory that enables the investigative agency to reconstruct the entire event of past, present and future happenings after inducing malware or an intrusion by advance risk factors. Even a small part of information stored in RAM may help to associate typical forensic artifact that may appear different and allow for an integration which could otherwise remain unnoticed. There are three reasons for gathering and analyzing the data contained in the physical memory. The physical memory contains real-time data related to the operating system environment, such as the currently mounted file system and the list of processes being operated. Even the encrypted data is generally decrypted when it is stored in the physical memory. Therefore, significant information can be obtained if analysis is performed effectively on the physical memory. The different types of information that can be extracted from memory include processes, dynamic link libraries (dll), process memory, image identification, kernel memory and objects, networking, registry, malware.

5. Acquisition and Analysis of Memory

Volatile and Non-volatile memory are the two types of memory available in the system. Volatile memory stores data temporarily and non-volatile data is stored permanently in the system. Memory stores current working of processes, registers, stack of processes, deleted files, and encrypted data. Volatile memory or Random Access Memory (RAM) only maintains its data while the computer or device is powered on. Non-volatile Memory, or NVRAM, is for longer-term storage. When a computer is powered off, evidence in RAM is lost and normally cannot be recovered, however, the data in NVRAM often remains after the system is powered off and can be analyzed after the fact. [6]

Acquisition is done with two different approaches. 1) Live System/device 2) Dead System/Device. When system is live it uses different technique to retrieve data from the system than dead system.[7] Farada bag is used to collect device and then forensic is proceeded.
Acquisition is a technique in which collection of evidence is carried out from the seized device through which a crime is committed. A write blocker is attached with the seized device to

collect the data, so that there is no change in the evidence and hash value can be calculated after which RAM and Registry is Dump with the use of RAM Dump memory forensic tool which collects all the data from the RAM and generate the reg.mem file which collects all the data from RAM and then this file is analyzed in Encase tools and report is generated. If the retrieved data matches with the original one then accused can be convicted on the basis of this.

6. Tools and Techniques

The study focuses in two phases of memory analysis: acquisition of the data and analysis of the collected data. Collection of evidence focuses in obtaining digital evidence in an acceptable form. There are mainly two approaches for acquire physical memory images: Hardware based tools and Software based tools. [8] In this paper the focus is on the software based tools.

6.1. Volatility

Volatility is an open source memory forensics framework for incident response and malware analysis. It is written in Python and supports Microsoft Windows, Mac OS Xand Linux.

Volatility is one of the best open source software programs for analyzing RAM in 32 bit/64 bit systems. It can analyze raw dumps, crash dumps, VMware dumps (.vmem), virtual box dumps, and many others. [9] Volatility tool is used for analyzing RAM from which the data can be recovered. Volatility tool is used for analyzing RAM from which the data can be recovered. The hash value of the collected evidences from stored files, deleted files, encrypted emails, password protected files can calculated with the help of HashCalc and it is compared with the retrieved files.

6.2. Autopsy

Autopsy is a GUI-based open source digital forensic program to analyze hard drives and smart phones effectively. [10] Autopsy is used by thousands of users worldwide to investigate what actually happened in the computer. It's widely used by corporate examiners, military to investigate and some of the features are.

- File type detection
- Media playback
- Registry analysis
- Photos recovery from memory card
- Extract geo-location and camera information from JPEG
- Extract web activity from browser
- Show system events in graphical interface
- Timeline analysis
- Extract data from Android – SMS, call logs, contacts, etc
- It has extensive reporting to generate in HTML, XLS file
- Format Alphabetical Memory forensics tools are used to acquire and/or analyze a computer's volatile memory (RAM).

6.3. MANDIANT Memoryze

MANDIANT Memoryze, formerly known as MANDIANT Free Agent, is a memory analysis tool. Memoryze can not only acquire the physical memory from a Windows system but it can also perform advanced analysis of live memory while the computer is running. All analysis can be done either against an acquired image or a live system. [11]

6.4. Belkasoft Evidence Center

Belkasoft Evidence Center makes it easy for an investigator to acquire, search, analyze, store and share digital evidence found inside computer and mobile devices. The toolkit will quickly extract digital evidence from multiple sources by analyzing hard drives, drive images, memory dumps, iOS, Blackberry and Android backups and chip-off dumps. Evidence Center will automatically analyze the data source and lay out the most forensically important artifacts for investigator to review, examine more closely or add to report. [12]

6.5. WxHexEditor

WxHexEditor is an open source cross-platform hex editor written in C++ and wxWidgets. It uses 64 bit file descriptors (supports files or devices up to 264 bytes). It does not copy the whole file to your RAM. This makes it faster and lets it open very large files. Some of the features are; you can copy/edit your Disks, HDD Sectors with it. (Useful for rescue files/partitions by hand.)

6.6. HELIX3

This tool can collect data from physical memory, network connections, user accounts, executing processes and services, scheduled jobs, Windows Registry, chat logs, screen captures, applications, drivers, environment variables and Internet history. And then data is analyzed on the basis of that report is generated.

7. Memory Forensic Tools and Comparison

Table1: Memory Forensics Tools and comparison

Tool	Autopsy	MANDIANT Memorize	Belkasoft Evidence	WxHexEditor	Xplico	HELIX3
Features						
1.Easy to use	Yes	Yes	Yes	Yes	Yes	Yes
2.Support Computer	Yes	Yes	Yes	Yes	Yes	Yes
3.Support smart phone	Yes	No	No	Yes	Yes	No
4.Information Security	Yes	Yes	Yes	Yes	No	Yes
5.Support Image Format	Yes	Yes	Yes	Yes	Yes	Yes
6.Memory Acquisition	Yes	Yes	Yes	Yes	Yes	Yes
7.Memory Analysis	Yes	Yes	Yes	Yes	Yes	Yes

8.Fast Operation	Yes	Yes	Yes	Yes	Yes	Yes
9.Cost Effective	Yes	Yes	Yes	Yes	Yes	Yes

8. Conclusions

Memory Forensic is widely used to analyze, acquire, report generation of memory. Memory Forensic tools are useful to fetch memory from RAM, Physical Memory of seized device; when device is seized and it will connect with block writer so that there is no any change in evidence. We have used RAM Dump and Autopsy to collect data. It will recover all the data which may be deleted files, deleted logs, and running processes from Physical memory, RAM, Registry with the use of RAM Dump, Registry Dump, Autopsy, Volatility tools which are used to backup files, and help to generate the forensic report. Although there are so many different tools are used for memory forensic each and every tools have different purposes and different types of data collection methods. Six tools are investigated depending on their features two tools Autopsy and Belkasoft Evidence Center fulfill most of the requirement.

References

[1] Reith M, Carr C, Gunsch G. (2002). An examination of Digital Forensics Models. International Journal of Digital Evidence.1, 3, p1–12.
[2] Pooja Salave, Atisha Wakdikar (2017). Memory Forensics: Tools Comparison. International Journal of Science and Research (IJSR). 6, 6, p5-8.
[3] Timothy Vidas (2007). The Acquisition and Analysis of Random Access Memory. Journal of Digital Forensic Practice. 1, 4, p315-p323.
[4] Richard Nolan, Colin O'Sullivan, Jake Branson, Cal Waits (2005). First Responders Guide to Computer Forensics, Carnegie Mellon University.
[5] Dr. Hardik Gohel, Dr. Himanshu Upadhyay (2017). Design of Advanced Cyber Threat Analysis Framework for Memory Forensics. International Journal of Innovative Research in Computer and Communication Engineering. 5, 2, p132-137.
[6] Berning, T., Dreseler, M., Faust, M., Plattner, H., & Schwalb, D. (2015). nvm malloc: Memory Allocation for NVRAM. ADMS@VLDB.
[7] Mahesh Kolhe et al, (2017). Live Vs Dead Computer Forensic Image Acquisition. International Journal of Computer Science and Information Technologies, 8, 3, p 455-457.
[8] Divyang Rahevar. (2013) Study on Live analysis of Windows Physical Memory. Journal of Computer Engineering (IOSR-JCE). 15, 4, p76-80.
[9] Rui YANG, Jiang-chun REN*, Shuai BAI and Tian TANG. (2017). A Digital Forensic Framework for Cloud Based on VMI, 2nd International Conference on Computer Science and Technology (CST 2017) ISBN: 978-1-60595-461-5.
[10] Neelam Maurya, Jyoti Awasti, Ragvendra Pratap Singh, Dr. Abhishek Vaish. (2015). Analysis of Open Source and Proprietary Source Digital Forensic Tools. International Journal of Advanced Engineering and Global Technology.3, 7, p 916 – 922.
[11] User Guide MANDIANT Memoryze™ Version 3.0.0 https://www.fireeye.fr/content/dam/fireeye-www/services/freeware/ug-memoryze.pdf.
[12] Belkasoft Evidence Center 2018. https://belkasoft.com/ec.

*Corresponding author.
E-mail address: scjani@ gwa.amity.edu