Asif *et al. (IJECI)* 2023

(IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

International Journal for
Electronic Crime Investigation

DOI: https://doi.org/10.54692/ijeci.2023.0704169

Research Article

Vol. 7 issue 4 Oct-Dec 2023

Volatile Data Acquisition and Analysis by Using Memory Forensics Techniques

Rabia Mehmood
Department of Computer Sciences, COMSATS University, Lahore
Corresponding author: rabiamehmoodciit@gmail.com

Received: September 30, 2023; Accepted: November 29, 2023; Published: December 22, 2023

ABSTRACT

Memory forensics is a vital component of digital investigations, involving the analysis of volatile memory (RAM) in computer systems to gather evidence, identify malicious activities, and reconstruct cybercrime incidents. This paper provides an overview of memory forensics, highlighting its definition, importance, purpose, and scope. It explores the evolution and significance of memory forensics in response to increasingly complex cyber threats. The memory forensics process is discussed, covering memory acquisition and analysis. Legal and ethical considerations related to the admissibility of memory evidence and privacy protection are examined. The paper also discusses the types of memory, including physical and virtual memory, and their characteristics and significance in memory forensics. Furthermore, it explores the memory acquisition process, different methods, tools, and techniques used, as well as the importance of preserving evidence integrity. Finally, the paper introduces various tools for memory analysis, such as Volatility, Volatility Workbench, FTK Imager, Encase, Hibernation Recon, and Xplico, and highlights their role in extracting valuable evidence from memory dumps.

Keyword: Memory forensics, volatile memory, digital investigations, evidence, malicious activity, cybercraime.

1. INTRODUCTION

Memory forensics is the investigation and examination of volatile memory (RAM) in computer systems in order to gather data, spot malicious activity, and reconstruct instances involving cybercrime. It is essential for gathering information, recognizing malicious activity, and looking into cybercrime incidents. Memory analysis is crucial since traditional disk-based forensics may not be able to capture all pertinent data on their own. Memory forensics can provide information about current system activity, encryption keys, network connections, and more [1].

Examining and analyzing a computer's volatile memory is a part of memory forensics. The operating system and any open apps keep their active data and code in volatile memory. Memory forensics are crucial because they give investigators access to data that might not be saved on disc, like passwords, encryption keys, network connections, and active processes. Reconstructing the sequence of events during an incident and determining the existence of malware or unauthorized activity both benefit from this knowledge. Extraction of useful data from a system's volatile memory is the main goal of memory forensics. Investigators can find information on cyberattacks, data breaches, system intrusions, and other security problems by looking into memory. Memory forensics aids in retracing the timeline of events, spotting malicious activity, and comprehending the offenders' actions. Due to the present cyber threats' increasing complexity, memory forensics has quickly developed. Traditional disk-based forensics by themselves would not be able to paint a complete picture of the occurrence due to the increasing sophistication of malware and advanced persistent threats (APTs). Memory analysis adds to disk-based forensics by providing details on the system's configuration at the time of the incident, including loaded drivers, active network connections, and in-memory artifacts. Memory forensics has evolved into a crucial investigative tool for cybercrime, inspiring the creation of specialized tools and procedures [2].

2. MEMORY FORENSICS PROCESS

2.1. Acquisition of Memory

The target system's memory must be acquired as the initial stage in memory forensics. Memory acquisition can be accomplished by a number of techniques, such as physical acquisition and live acquisition. The target system's memory modules are taken out and imaged using specialized hardware during physical acquisition. Contrarily, live acquisition is removing memory from a functioning system without shutting it down [3].

2.2. Memory Analysis

The next stage is to analyze the memory to draw out important information after it has been acquired. The process of extracting, decoding, and interpreting data from images of memories that have been acquired is known as memory analysis. To recognize active user sessions, open network connections, and operating processes, many strategies can be employed. Data structures including process lists, file handles, registry hives, and kernel objects are also examined as part of memory analysis to look for signs of malicious activity [2].

3. LEGAL AND ETHICAL CONSIDERATIONS

3.1. Admissibility of Memory Evidence

The admissibility of volatile memory evidence in court proceedings is one of the difficulties in memory forensics. The brittleness of memory raises concerns about its dependability and vulnerability to manipulation. Memory forensics findings have, however, successfully been admitted as evidence in the past. Memory analysis, for instance, was essential in locating encrypted data and supplying proof of criminal activity in the United States v. Stewart case. Courts are setting standards for the admission of memory forensics findings as they increasingly recognize the significance of memory forensics in locating crucial evidence [4].

3.2. Privacy and Data Protection

Memory forensics investigations entail accessing and examining private data kept in a system's volatile memory. During these investigations, it is crucial to make sure that privacy rules and data protection laws are being followed. Investigators must take reasonable efforts to preserve the privacy of those concerned and handle sensitive material discovered during memory analysis responsibly. This entails putting appropriate data anonymization procedures into place and making sure that only authorized individuals have access to the data gleaned via memory forensics. Proper handling of privacy and data protection issues is crucial to maintain the integrity of the investigation and avoid potential legal and ethical complications. Investigators should follow established guidelines and best practices for conducting memory forensics to protect the rights and privacy of individuals involved while still obtaining valuable evidence. It is crucial for investigators to keep up with the most recent methods, devices, and regulatory requirements as memory forensics develops. Memory forensics can be effectively used to obtain important evidence and advance the area of digital forensics by adhering to suitable protocols and best practices [3].

4. TYPES OF MEMORY

4.1. PHYSICAL MEMORY

4.1.1. Definition and Characteristics

RAM (Random Access Memory), another name for physical memory, is the actual memory modules that are installed in a computer system. Its job is to keep track of the information that the system is currently using. Performance of the system is impacted by physical memory's unique properties, including capacity, speed, and access time [5].

4.1.2. Memory Organization

A computer system's memory components are arranged hierarchically as part of memory organization. It covers all memory types, including cache memory, main memory (RAM), and virtual memory. A memory hierarchy that maximizes data access and storage efficiency is created by the different capacities, speeds, and costs at each level [5].

4.1.3. Volatility and Data Persistence

Physical memory is volatile, meaning its contents are lost when the power is turned off. This characteristic poses challenges for memory forensics investigations, where investigators analyze memory contents for evidence or artifacts. To preserve data during system shutdown or when physical memory is insufficient, data persistence mechanisms such as hibernation files and page files come into play [6].

5. VIRTUAL MEMORY

5.1. Introduction and Purpose

Modern operating systems use the memory management method known as virtual memory. In situations where physical memory is insufficient to support all current processes, it enables the system to utilize disc space as an extension of that memory. Programs won't run out of memory because to virtual memory's wider accessible memory area and efficient memory allocation [5].

5.2. Address Translation

Address translation is a critical process in virtual memory management. It involves mapping virtual addresses used by processes to physical addresses in the underlying physical memory. This mapping is typically maintained through page tables. Analyzing virtual memory mappings is crucial in memory forensics investigations to understand the memory layout and locate specific data or artifacts [7].

5.3. Page File Analysis

The page file, also known as the swap file, is a file used by operating systems to store pages of memory that are not actively being used. During memory forensics investigations, analyzing the page file can provide valuable insights and potential artifacts. Investigators examine the page file contents to reconstruct system activities, identify relevant evidence, and gain a deeper understanding of the system's state at a given time [7].

6. MEMORY ACQUISITION

It is an important component of digital forensics, and it comprises the process of obtaining data from a computer system's volatile memory. Memory acquisition provides vital information about a system's state, including active processes, network connections, and system configurations in digital forensics investigations. This information can be used to investigate security incidents, detect malware, and detect harmful activities on a system.

The memory forensics acquisition process can be divided into the following steps:

- Identify the system: The first step is to identify the system that will be acquired. This involves identifying the operating system, hardware configuration and any installed security software.
- Prepare the acquisition media: The next step is to get the acquisition media prepared. This media must be large enough to hold the memory dump and forensically sound.
- Acquire the memory dump: A variety of tools can be used to obtain the memory dump. These tools can be used to acquire the entire system's memory or to acquire a particular portion of memory.
- Verify the acquisition: After acquiring the memory dump, it should be verified to ensure that it is complete and accurate.

The primary goal of memory acquisition is to collect the state of the system at a certain point in time. There are two distinct methods of memory acquisition: live acquisition and dead acquisition [8].

6.1. Live Acquisition

The process of acquiring memory data while the system is still running is known as live acquisition. This method can offer real-time information on the current state of the system, such as active processes, network connections, and system configuration. Live acquisition is beneficial in instances where the system's current status must be captured, such as when an incident is ongoing [7].

6.2. Dead acquisition

It is the collection of memory data after the system has been shut down. This method is useful when live acquisition is not available, for as when a system is not responding or has been turned off. Dead acquisition can also be beneficial in situations where the system state must be preserved, such as in cybercrime investigations or when dealing with sensitive systems that must not be disturbed [8].

6.3. Hardware-based tools

It include physically removing memory chips from the system and reading the memory contents with specialized hardware devices. This method is usually more difficult and requires higher levels of expertise than software-based memory acquisition methods. However, it may be more dependable than software-based methods since it is less susceptible to interference from running processes or malware. Magnet AXIOM Live and Access Data FTK Imager are a few common hardware-based tools for live memory acquisition [9].

6.4. Software-based tools

Running software on the system to capture memory contents and save them to a file for later analysis acts as what software-based tools do. The Sleuth Kit, X-Ways Forensics, Volatility, Rekall, and Redline are some notable software-based methods for live memory acquisition. These tools scan the system's memory for specified data structures or patterns, and then copy the relevant data to a file for further analysis [8].

6.5. Hybrid memory acquisition tools

It combine hardware and software-based methodologies to provide a more efficient and eliminated approach. Hybrid tools often involve connecting a hardware device to the system and then running software to retrieve the contents of the memory. As the hardware device may provide direct access to the memory, this method may be more efficient and reliable than software-based methods. Magnet AXIOM, Cellebrite UFED Cloud, and Access Data FTK Imager Enterprise are some popular Hybrid acquisition solutions that combine the features of hardware-based and software-based tools. To protect the integrity and admissibility of evidence, certain processes must be followed when undertaking memory acquisition. This includes documenting the acquisition process, verifying the memory image's integrity, and securely storing and transporting the evidence. Documentation should include information regarding the system being analysed, the date and time of the acquisition, the method utilised for acquiring memory, and any pertinent acquisition process details [9].

6.6. Verifying the memory images integrity

It entails comparing the acquired memory data to a known good copy of the system's memory. This is referred to as validation, and it ensures that the acquired data is correct and has not been manipulated. One typical method for validation is to create a digital fingerprint of the memory image using a hash algorithm. To confirm that the obtained data has not been altered or changed, this fingerprint can be compared to the hash value of a known good copy of the memory. Secure evidence storage and transport are critical to ensuring that the memory image is not compromised during the investigation. To safeguard against unauthorized access, memory images should be kept in a secure environment. It is also critical to preserve the memory image during transport, which can be accomplished through the use of encryption or other secure transfer methods. It is critical to follow the chain of custody procedures while transporting evidence to ensure that the evidence is not corrupted or altered during transit. Memory forensics is an important part of computer forensics investigations. Memory acquisition enables investigators to gain access to crucial information about the state of a system, such as active processes, network connections, and system settings. To maintain the integrity and admissibility of evidence, proper procedures, including documentation, validation, and secure storage and transit of evidence, must be followed [10].

6.7. Analyzing

So, whenever we start analyzing the memory forensics, we have different option and different tools for analyzing its content A Memory image is basically a dump of RAM i.e., volatile memory and contain the information of processes and different sectors of computer. The analysis part of memory is crucial as every single artifact has its important in a case for this section, we are using different variety of tools to analyze a basic memory image from a victim’s hard drive as an example. And see how to recover most of the evidence from the memory sample the The memory sample using in this case is downloaded from an online website:https://github.com/volatilityfoundation/volatility/wiki/2.6-Win-Profiles [7].

6.8. Tools

The tools require for the analysis of memory forensics are given below:

- Volatility
- Volatility workbench
- Ftk imager
- Encase
- Hibernation recon
- Xplico

We are using some of the tools mentioned above for analysis purpose [8].

6.9. Volatility

The volatility framework is an open-source collection of different tools. This framework is written in python language and it is under the License of GNU General Public License

This tool was used by mostly forensic examiner to examine the memory analysis Dump Lets start the Analysis part

The volatility framework official link is: https://github.com/volatilityfoundation/volatility

So, the volatility framework comes with different profile options for every type of Operating System e.g., for window it has a Win profile same for mac and Linux Systems. The command for checking the OS profile is:

vol.py -f (location of the dump) image info

Basically, this is used to determine whether we are working on a right System or not As the profile is confirmed we move to the different option for Analysis (Depending on the case) Mostly the other option used are:

amcache - Print AmCache information

cmdscan - Extract command history by scanning for COMMAND_HISTORY

dlldump - Dump DLLs from a process address space

evtlogs - Extract Windows Event Logs (XP/2003 only)

filescan -Pool scanner for file objects

netscan -Scan a Vista (or later) image for connections and sockets

pslist - Print all running processes by following the EPROCESS lists

These are the options that are mostly used in the analysis part and most of the time we can see the malicious activity from the output of these commands

Now move to the next tool i.e., volatility workbench. The volatility workbench is also a part of volatility framework but has A GUI Framework. The volatility workbench is used as it is fast and has a GUI interface and easy to use. The volatility workbench can be downloaded from the given link https://www.osforensics.com/tools/volatility-workbench.html.

Now we move to the other tools i.e., hibernation recon. The memory dump is not a little piece of evidence. It has a variety of different artifact inside of it some of them includes:

- Hiberfill.sys
- Pagefile.sys
- Swapfill.sys

Every .sys file has his importance in the analysis. The hiberfill.sys file contains all the information when a computer goes in the hibernation state. Basically, when a person wants to go somewhere and he doesn't want to shut down his system and close their apps and website he use this method. The advantages of using this method are that it saves all the running processes into memory and when we back and power on the computer we have the same screen as we left off. Mostly people use this method to save their battery life of laptops as in hibernation mode the system go in sleep but doesn't use power. During the analysis this file help us a lot if some attacker hibernates their PC and go somewhere we can extract the information of their PC by analyzing this file [12].

6.10. RECOVERY

The practice of recovering erased or concealed data from the volatile memory (RAM) of electronic devices, particularly computers, is known as memory forensics recovery. This feature of memory forensics is essential because it allows access to data that would not be available using conventional disk-based forensic techniques. Data recovery in memory forensics involves extracting and reconstructing obscured or deleted data from the volatile memory (RAM) of electronic devices. This can be done using software-based or hardware-based methods and tools. In this paper, software-based tools are the main topic [9].

6.10.1. Volatility

Volatility is an open-source memory forensics framework for malware analysis and incident response. Microsoft Windows, Mac OS X, and Linux are all supported by this Python-written program. One of the best open-source software tools for 32-bit and 64-bit systems to analyze RAM is Volatility. It has the ability to examine a variety of dump types, including raw dumps, crash dumps, VMware dumps (.vmem), virtual box dumps, and more. [13] The RAM from which the data can be recovered is examined using a volatility tool. With the aid of HashCalc, the hash value of the gathered evidence from stored files, deleted files, encrypted emails, and password-protected files can be calculated. This value is then compared with the files that were successfully retrieved [8].

6.10.2. Autopsy

A GUI-based open-source digital forensic program called Autopsy can efficiently analyze hard drives and mobile devices. Thousands of users all over the world use autopsy to determine what actually transpired in the computer. Military investigators and corporate examiners both frequently use it because of some of its features:

a) File type detection

b) Media playback

c) Registry analysis

d) Photos recovery from memory card

e) Extract geo-location and camera information from JPEG

f) Extract web activity from browser

g) Show system events in graphical interface

h) Timeline analysis

i) Extract data from Android – SMS, call logs, contacts, etc

j) It has extensive reporting to generate in HTML, XLS file

k) Format Alphabetical Memory forensics tools are used to acquire and/or analyze a computer's volatile memory (RAM) [9].

6.10.3. MANDIANT Memoryze

A memory analysis tool is MANDIANT Memoryze, formerly MANDIANT Free Agent. Memoryze is able to analyze live memory while a computer is running in addition to acquiring the physical memory from a Windows system. Any analysis can be performed on a live system or an acquired image [8].

6.10.4. Belka soft Evidence Center

An investigator can easily gather, search, analyze, store, and share digital evidence from computers and mobile devices using Belkasoft Evidence Centre. The toolkit analyses hard drives, drive images, memory dumps, iOS, Blackberry, and Android backups, as well as chip-off dumps, to quickly extract digital evidence from a variety of sources. The most crucial forensically significant artefacts are automatically analyzed by the Evidence Centre and presented for review, closer inspection, or addition to the report [9].

6.10.5. WxHex Editor

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 [8].

6.10.6. 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 [10].

7. REPORTING

In the discipline of memory forensics, reporting entails making the findings and conclusions that result from the analysis of memory data explicit and understandable, particularly for non-technical people [15]. The main goal is to give a succinct overview of the investigation's findings so that someone who might not have a strong technical background can easily grasp it. The report serves as a tool for bridging the communication gap between the technical analysis and the intended audience by streamlining the findings' presentation. It uses plain English rather than technical jargon to efficiently communicate the main points. The focus is on presenting important findings, such as suspicious activity, proof of unauthorized access, and potential security flaws, without getting bogged down in complex technical details unless absolutely necessary for understanding. The study also describes how these conclusions can affect the concerned organization or people. It is significant to note that the report preserves the correctness and integrity of the findings and conclusions obtained from the memory analysis despite being aimed at a non-technical audience [9].

7.1. Purpose of the Report

This report's objective is to describe the results and recommendations of the memory forensics investigation done in connection with the XYZ case. We sought to find any malicious activity, find possible security holes, and make suggestions for increasing system security by examining the memory image obtained from the compromised machine [7].

7.2. Executive Summary

Memory forensic analysis revealed several important findings. First, several instances of suspicious processes were identified, indicating the presence of malware in the system. These processes were found communicating with external IP addresses, suggesting an unauthorized network connection. Additionally, the analysis uncovered evidence of file tampering and attempts to cover up malicious activity. Based on these findings, we recommend immediate incident response actions to mitigate the potential risks associated with a compromise [6].

7.3. Case Background

A security incident involving unauthorized access to the company's network was reported in the XYZ case. To ascertain the scope of the compromise, track down the attacker, and evaluate the effect on the organization's systems and data, a memory forensics investigation was started. Utilizing best practices, the analysis was done on a memory image that was taken from a compromised server [12]

7.4. Methodology and Tools

The memory forensic analysis was conducted with tried-and-true methods and tools. To ensure proof integrity, the memory image was acquired using a hardware-based write blocker. The volatility framework, a popular open-source memory forensics tool, was then used to process and analyze the acquired memory image. Additionally, thorough analysis and the extraction of pertinent artifacts were done using the Rekall framework [11].

7.5. Finding and Analysis

Several patterns were discovered during the memory analysis, which gave important information about the attacker's activities. Malicious software is present on the system if suspicious processes like "backdoor.exe" and "malware.exe" are present. These processes' network connections revealed communication with well-known command and control servers connected to malware campaigns. Additionally, a sophisticated attack intended to avoid detection was revealed by the analysis of memory structures, which revealed attempts to alter crucial system files. These results strongly support the need for a focused intervention [13].

7.6. Interpretation and Conclusions

The XYZ system has been infected by sophisticated malware, according to the findings of the memory forensic analysis. In order to maintain persistence, the attacker set up command and control channels, modified system files, and gained unauthorized access using sophisticated methods. The confidentiality, integrity, and availability of data within an organization are seriously at risk from a compromise. It is advised to take immediate corrective action to stop the breach, get rid of the malware, and secure the compromised system [14].

8. CONCLUSION

Several suggestions are made to improve the security posture and stop upcoming incidents in light of the analysis's findings.To stop further communication with the command-and-control infrastructure, isolate and disconnect the compromised system from the network. To comprehend the capabilities and potential effects of the identified malware, conduct a thorough malware analysis. In order to fix flaws that an attacker has exploited, all software and operating systems should be updated and patched. For the purpose of quickly identifying and responding to similar incidents, enhance network monitoring and intrusion detection capabilities. Enhance user education and training initiatives to inform staff about typical attack vectors, phishing attempts, and social engineering strategies.

REFERENCES

[1] E. Casey, A. Richard, and J. M. James, "Handbook of digital forensics and investigation," Academic Press, 2014.

[2] H. Carvey, "Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 8," Elsevier, 2014.

[3] A. Marshall, E. Casey, and T. Mørk, "Digital forensics: digital evidence in criminal investigations," John Wiley & Sons, 2014.

[4] J. Schatz and T. Yu, "Memory forensics using volatility framework in a virtual environment," Digital Investigation, vol. 10, no. 4, pp. 326-335, 2013.

[5] I. Ghafir, "The legal admissibility of memory forensics: An overview," in International Conference on Information Networking (ICOIN), pp. 628-633, 2018.

[6] H. Richardson, D. O'Sullivan, and N. A. Le-Khac, "A framework for the forensic investigation of live systems," Digital Investigation, vol. 9, no. 1-2, pp. 32-41, 2012.

[7] S. Silberschatz, P. B. Galvin, and G. Gagne, "Virtual Memory: An Overview," in Operating System Concepts, 9th ed. Wiley, 2013.

[8] B. Carrier and E. H. Spafford, "Forensic Analysis of Volatile System Memory," Digital Investigation Journal, 2011.

[9] A. Walters, "Memory Analysis and the Windows Page Cache," Digital Investigation, vol. 13, no. Suppl. 1, pp. S55-S64, 2015.

[10] G. Soghoian, "Analyzing the Windows Page File and Memory," IEEE Security & Privacy, vol. 12, no. 3, pp. 72-75, 2014.

[11] A. A. Lin, Y. N. Liu, and Y. H. Hu, "Memory Analysis and Reconstruction Techniques for Virtual Machine Forensics," in Proceedings of the 2012 International Symposium on Information Technologies in Medicine and Education, pp. 24-27, 2012.

[12] D. Rahevar, "Study on Live analysis of Windows Physical Memory," Journal of Computer Engineering (IOSR-JCE), vol. 15, no. 4, pp. 76-80, 2013.

[13] R. Yang, J.-c. Ren, S. Bai, and T. Tang, "A Digital Forensic Framework for Cloud Based on VMI," in "2nd International Conference on Computer Science and Technology (CST 2017)," 2017, ISBN: 978-1-60595-461-5

[14] N. Maurya, J. Awasti, R. P. Singh, and A. Vaish, "Analysis of Open Source and Proprietary Source Digital Forensic Tools," International Journal of Advanced Engineering and Global Technology, vol. 3, no. 7, pp. 916-922, 2015.

[15] E. Casey, "Digital evidence and computer crime: Forensic science, computers, and the internet," 3rd ed., Academic Press, 2011.

[16] E. Casey, "Digital Evidence and Computer Crime," Academic Press, 2014.

[17] R. Pal, "Memory Forensics in Digital Forensics," International Journal of Computer Science and Information Security, vol. 15, no. 2, pp. 180-188, 2017.

[18] NIST, "Guidelines on Electronic Evidence Collection and Preservation," NIST Special Publication, 80-86, 2014.