Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 07 Issue 02
2024

Research Article
https://doi.org/10.56979/702/2024

Forensic Strategies for Revealing Memory Artifacts in IoT Devices

Hafiz Ahmad Mujtaba[1], Gohar Mumtaz[1*], Muhammad Haroon Ahmad[2], and Mudassar Rehman[3]

[1]Faculty of Computer Science and Information Technology, Superior University, Lahore, 54000, Pakistan.
[2]Riphah International University, Lahore, 54000, Pakistan.
[3]Riphah International University, Sahiwal, 57000, Pakistan.
[*]Corresponding Author: Gohar Mumtaz. Email: gohar.m@superior.edu.pk

Received: March 11, 2024 **Accepted:** July 23, 2024 **Published:** September 01, 2024

Abstract: Forensics of Ram plays an important role when used in the field of digital forensics, during the examination of Memory to identify signs of unauthorized or unusual activities within computer systems. This area has gained significant attention because it allows for the recovery of fleeting data that typically disappears when a system is powered down, thus helping investigators piece together the sequence of events that led to security breaches. Recent developments in memory forensics have focused on improving the methods used for acquiring and analyzing memory. This paper seeks to assess the effectiveness of different memory forensic tools and techniques, particularly in their application to malware detection and the extraction of evidence. It wraps up by proposing a framework aimed at enhancing memory forensic practices, addressing current shortcomings in the field, and outlining potential research avenues to strengthen memory analysis in increasingly complex digital landscapes.

Keywords: Digital Memory Forensics; Volatile Memory Analysis; Digital Forensics: Malware Detection; Evidence Extraction.

1. Introduction

RAM forensics is now a critical aspect of forensics because now in most cases it is admissible as evidence, to uncover the signs of suspicious activities, system anomalies. Unlike traditional forensic methods that rely on non-volatile data, memory forensics captures the processes state whether they are running or stopped so, investigators retrieve crucial information that may not be available through other means.

Now during the capturing of memory, we have several processes that are in running state some are making the internet connections while some are completing their jobs and about to exit from the queue. Generally, these are some of the processes that are used by the threat actors when they attack some system. Most of them use the dll injection process in order to obfuscate into another process. Now by using such techniques the tracks behind are limited and that’s where the memory comes in by using it, we can create its dumps and perform analysis and collect the traces which an attacker leaves in the system. Now the experts have the ability to examine such memory processes using the forensics tools like Volatility, FTK, and some other tools. Several studies show that the use of these tools plugins helps examiners to collect important artifacts [1] [3].

In Today’s world, the use of modern attack techniques to hide malware and to remove its footprints are widely used by attackers and sometimes they leave no traces. But the forensic examiners and the threat hunters also use modern tools and tactics, and techniques in order to increase the validation of artifacts so that they can easily be used in forensics [2]. The main contribution of this research study is as follows:

- Advanced Techniques used for memory forensics.
- Highlighting the Importance of Recovering Volatile Data
- Memory Artifacts importance in court Proceedings.

2. Literature Review

2.1. Overview of Memory Forensics

2.1.1. Definition and Importance

Digital analysis of RAM involves collection, examination, of a computer's volatile memory, which is where the operating system and currently running applications store their active data and code. This way provides investigators with the information using which they can determine which information is present or not on the system. These include the connection to specific systems the RSA keys, the file sharing services the jobs that are running and stopped.

Using the information an examiner gained he can make a series of events that show how a security breach occur or how the attacker uses the security hole to access to the system. This could also reveal if some attack vector uses the malware to gain access to the system or if he plugs some USB etc. [2].

2.1.2. Purpose and Scope

The primary and leading objective of this type of work is to get as much information as possible from the memory dump. So, that we can uncover the footprints of the attacker or APT. this knowledge also helps an examiner to determine the timeline of the events which is how an attacker exploit the security hole present in the system and the steps he gains gradually to breach the system.

We can tell whether he do some malicious activity or download any scripts or send some data to his server.

Imagine a crime scene where the only clues are the whispers of the wind and the faint echoes of footsteps. Memory forensics is the digital equivalent of a skilled detective, able to listen to the silent conversations of computer memory, revealing the secrets that lurk beneath the surface of a silent system [3].

2.1.3. Evolution and Significance

As cyber threats continue to grow in complexity, memory forensics has rapidly evolved to meet these challenges. Relying solely on traditional disk-based forensics often fails to provide a comprehensive understanding of an incident, especially given the modern threat actors use different services like Raas. DDOS, BAD USB etc.

The past complements methods by using which we are revealing critical information about the system's state when some events occur, such as files shared, smb connections, and other artifacts. This integration of the analysis of volatile memory plays a very important role in the fight against cybercrime, leading to the development of specialized tools and procedures designed to enhance the effectiveness of investigations. In a world where cyber threats are constantly changing, memory forensics serves as a key ally for investigators, helping to uncover hidden details that can make all the difference in understanding and responding to security incidents.

2.2. Memory Forensics Process

2.2.1. Acquisition process

There are many tools to get a memory image like Dumpit, FTKImager, Magnet RAM etc. but here we will be using Dumpit and FTKImager

Dumpit: It is a tool used for collection of Memory Images from a Windows Machine.

After downloading and extracting to a folder, we have to execute dumpit.exe it and it will ask for administrator permissions.

Once it is executed, it will show the memory size and path where it will dump the memory. You just have to type ‘y’ and it will start the process.

Once the process completes, the success message will appear seen in SS. Memory Image is saved and named as TESTING-PC-20221231-035522 (SS attached).

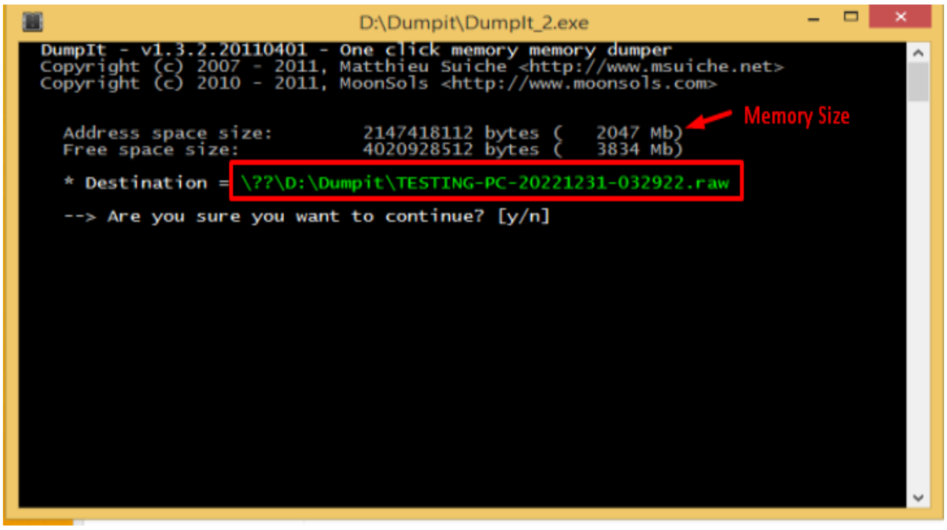
The same process with FTK Imager which is also a useful tool to get a memory image, although I found it much faster than others. Another benefit is it is quite simple to use!

Download and install using the below link.

https://accessdata.com/product-download/ftk-imager-version-4-7-1

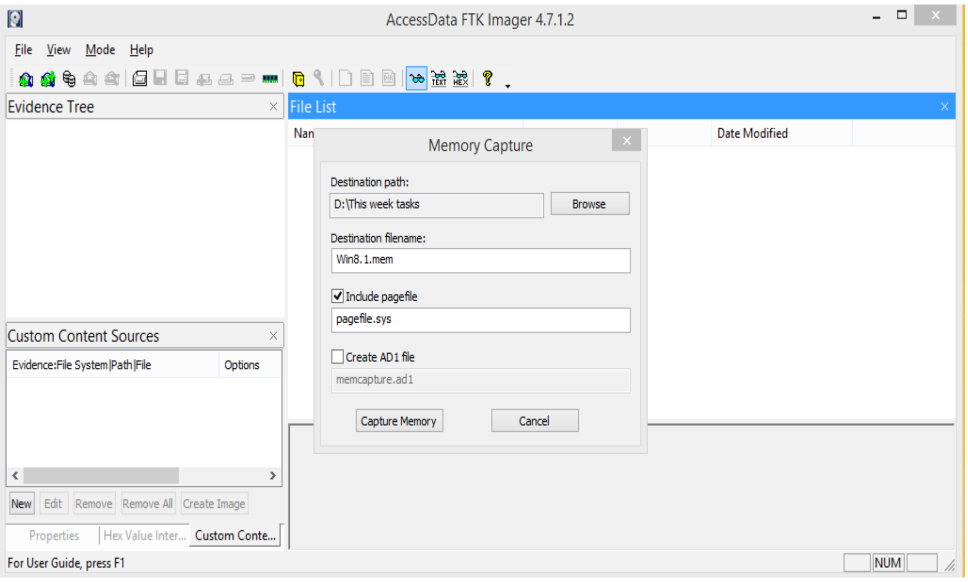
Once it is installed, then just go to File > Capture Memory Image

It will ask for destination where image file will save and file name for the memory image, after just hit capture.



```
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

   Address space size:          2147418112 bytes (  2047 Mb)
   Free space size:             4020928512 bytes (  3834 Mb)

   * Destination = \??\D:\Dumpit\TESTING-PC-20221231-032922.raw

   --> Are you sure you want to continue? [y/n]
```

Table 1. Memory Acquiring Process.



Memory Capture

Destination path: D:\This week tasks

Destination filename: Win8.1.mem

☑ Include pagefile

pagefile.sys

□ Create AD1 file

memcapture.ad1

Table 2. Memory Acquisition Using FTK Imager.

2.2.2. Investigation Process

It is the stage which tells us what the information present inside of a memory dump. As we acquired the dump using the above tool, we are now started to investigate it for the valuable information like the process obfuscation or the unwanted file sharing.

For this we have to perform in depth analysis of the image and check for the type of the processes like the parent PID, PID and other info. Also to get information on the user part we have to parse its hives its NTuser and see if there some type of suspicious activity occurs on the system [6].

2.3. Confidentiality and Ethical Practice:

2.3.1. In-Court Proceeding's:

Today the finding from the memory dump is admissible in the courts. The Modern tool like Volatility and FTK gives us important information when investigating memory dumps. By utilizing the evidence memory forensics plays a vital role in in criminal cases or in the corporate security breaches. As The Volatility framework is widely recognized for its ability to analyze memory dumps and retrieve significant data, such as running processes, network connections, and user credentials, which are often not preserved on disk.

2.4. Types of Memory

2.4.1. Physical Memory

Physical memory refers to the component in a computer system which is also called RAM that provides temporary, high-speed storage for actively running processes and controls the system processes, data. Unlike other permanent storage devices such as HDD or SSD drives, physical memory is volatile, meaning it loses all information stored inside of it when the power is turned off. This type of memory is essential for the efficient operation of a computer, as it allows (CPU) to quickly access data and execute every type of program, significantly enhancing overall system performance [4].

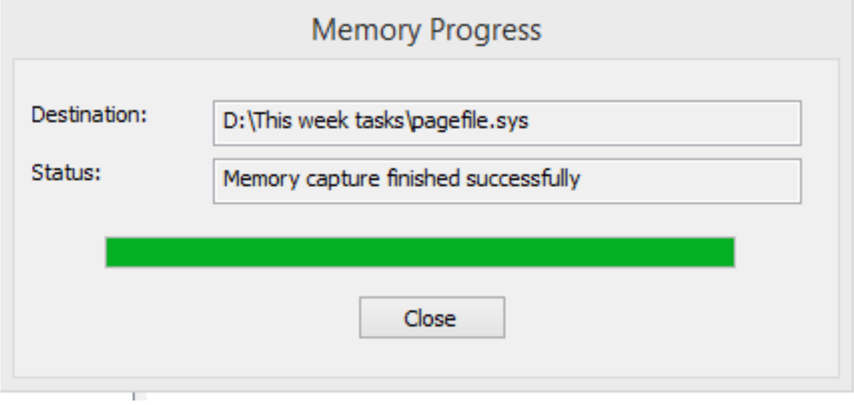
2.4.2. Virtual Memory

Virtual memory is a capability of the computer system using which it manages the memory management. It can use hard drive space as an extension of RAM. This enables systems to run larger applications or multiple applications, even when the physical memory is insufficient of the system all the memory was managed using the hard drive. However, relying too heavily on virtual memory can lead to performance degradation, as accessing data from a hard drive is slower because ram works faster, and some systems have hdd which work slow in the processing of the data [5].

2.5. Analysis of the Memory Image

2.5.1. In-Depth Analysis

So, For the Analysis part we are utilizing the images taken from the FTK we have different option of tools I am using volatility for in depth Analysis. Also, for the collection part we use FTK and other tools.



Memory Progress

Destination: D:\This week tasks\pagefile.sys

Status: Memory capture finished successfully

Table 3. Collection Successful Using FTK

3. Methodology

3.1. Mechanism for Analysis

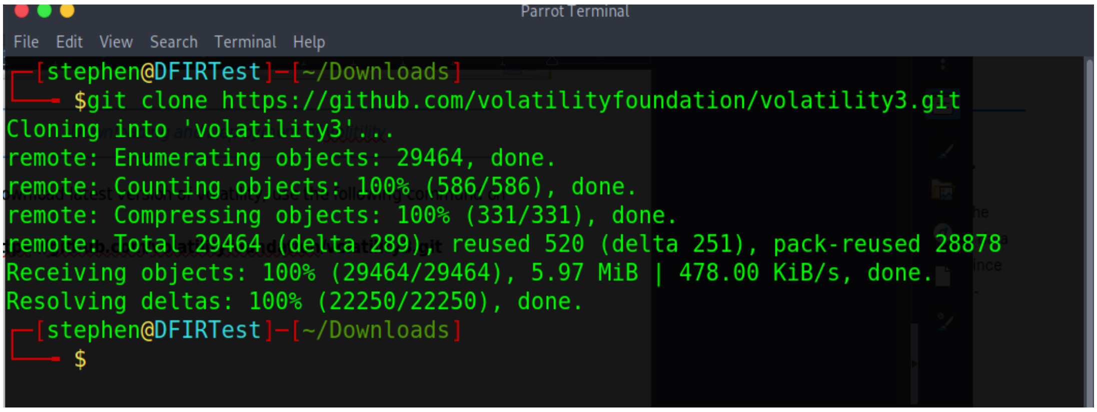
The Resources used in this scenario includes:

- The Volatility2.6
- Bulk extractor
- String
- Forensic Toolkit

3.1.1. The Volatility2.6

This tool is an open-source tool and widely used by many forensic examiners. It was written in python language and under the licensed authorities.

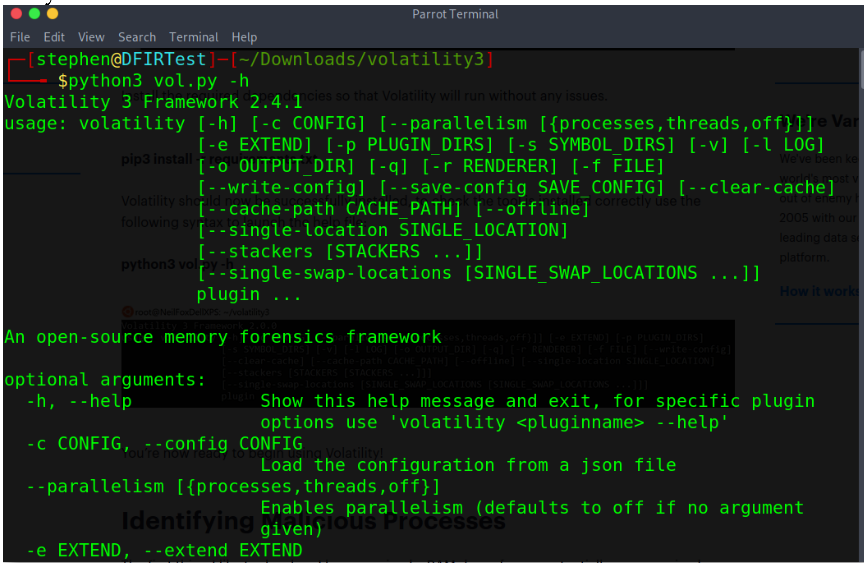
Download it from its GitHub page and clone it.



```
┌─[stephen@DFIRTest]─[~/Downloads]
└──╼ $git clone https://github.com/volatilityfoundation/volatility3.git
Cloning into 'volatility3'...
remote: Enumerating objects: 29464, done.
remote: Counting objects: 100% (586/586), done.
remote: Compressing objects: 100% (331/331), done.
remote: Total 29464 (delta 289), reused 520 (delta 251), pack-reused 28878
Receiving objects: 100% (29464/29464), 5.97 MiB | 478.00 KiB/s, done.
Resolving deltas: 100% (22250/22250), done.
┌─[stephen@DFIRTest]─[~/Downloads]
└──╼ $
```

Figure 4. Downloading Volatility

As the downloading is completed just type the command
Python3 vol.py -h
And the volatility will run from the command prompt. The -h plugin is used to show the list of plugins available in volatility.



```
┌─[stephen@DFIRTest]─[~/Downloads/volatility3]
└──╼ $python3 vol.py -h
Volatility 3 Framework 2.4.1
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]]
                  [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG]
                  [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE]
                  [--write-config] [--save-config SAVE_CONFIG] [--clear-cache]
                  [--cache-path CACHE_PATH] [--offline]
                  [--single-location SINGLE_LOCATION]
                  [--stackers [STACKERS ...]]
                  [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
                  plugin ...

An open-source memory forensics framework

optional arguments:
  -h, --help            Show this help message and exit, for specific plugin
                        options use 'volatility <pluginname> --help'
  -c CONFIG, --config CONFIG
                        Load the configuration from a json file
  --parallelism [{processes,threads,off}]
                        Enables parallelism (defaults to off if no argument
                        given)
  -e EXTEND, --extend EXTEND
```

Figure 5. Volatility Options

In the above Table No 5 we can see these are the options that are the options widely used during the analysis part.

Case: A company reported to their IT guy that their all-company system slow from the past two days and some unknown terminal appear on the screen. The IT team thought that it might be some update issue but gradually one of their computer files start encrypting and some files are transferring from their file server to an unknown destination. The team revoke the unauthorized access to the system and disconnect the system and start investigating it. During the investigation they take evidence from the hard drive and also captured the memory image of the system [7].

The company contact their forensic examiners and start investigating the collected artifacts. The artifacts contain the information from the system that was taken by the various forensic tools and contains the company critical systems data.

The examiners start the investigation from the disk images and after checking file, shimcache, appcompact, LNk, Jumplist. They move towards the memory dump and start investigating it alongside with page file and hibr file.

This memory image contains data related to user activities, system activities and the activities performed by the attacker on the system. The examiner uses volatility2.6 in order to determine how this attack happened.

3.2. Analysis

Several the analysis might reveal a malicious process masquerading as a legitimate application, along with unauthorized outbound connections to external servers. By conducting this memory forensic analysis.

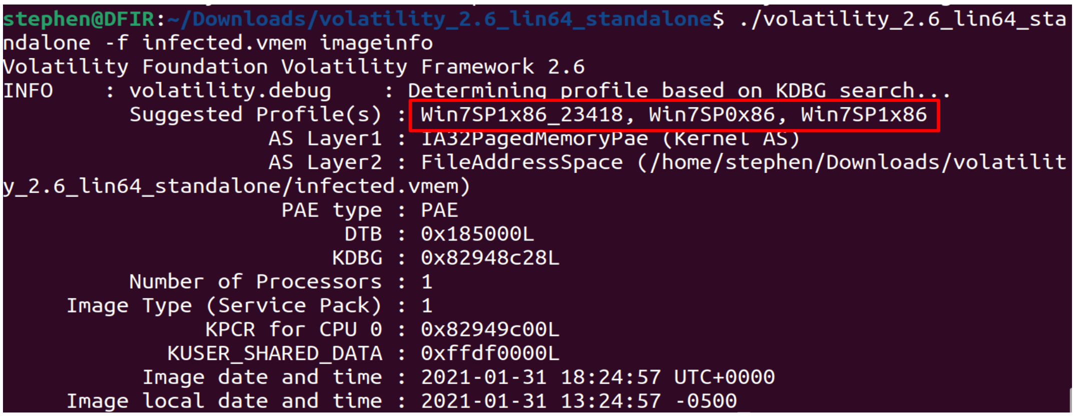
3.2.1. Basic Information from Memory

Command to retrieve version of the memory dump (It is to be noted that without opting version of a memory dump, plugins can't be run, so it is must to firstly acquire the OS version of the memory image [8].

- ./volatility_2.6_lin64_standalone -f <MemoryImage> imageinfo

3.2.2. Hidden processes.

Hidden processes are a common tactic used by malware to evade detection and maintain control over compromised systems. These processes are often designed to be invisible to standard operating system tools, making them a significant challenge for forensic investigators. Memory forensics, particularly using tools like the Volatility framework, plays a crucial role in uncovering these hidden processes by analyzing the volatile memory (RAM) of a system.

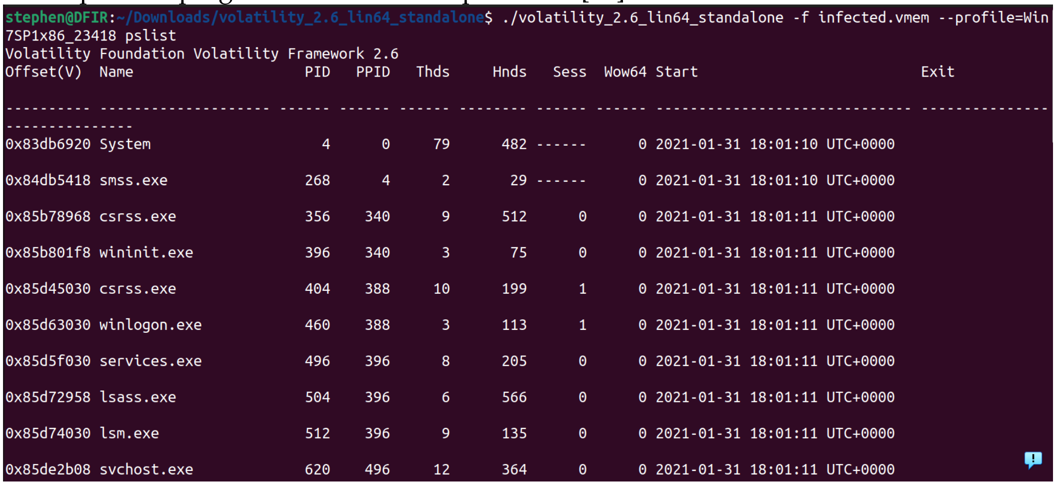


```
stephen@DFIR:~/Downloads/volatility_2.6_lin64_standalone$ ./volatility_2.6_lin64_sta
ndalone -f infected.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/stephen/Downloads/volatilit
y_2.6_lin64_standalone/infected.vmem)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82948c28L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82949c00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2021-01-31 18:24:57 UTC+0000
     Image local date and time : 2021-01-31 13:24:57 -0500
```

Figure 6. System information from Memory image using volatility.

- ./volatility_2.6_lin64_standalone -f <MemoryImage> --profile=<VersionofOS> pslist

  We use "psscan" plugin to list all hidden processes [10].



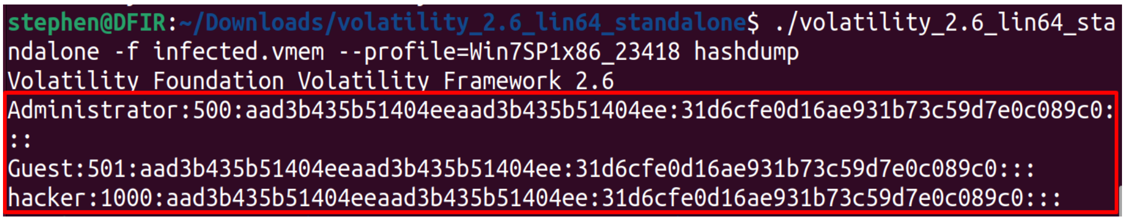
```
stephen@DFIR:~/Downloads/volatility_2.6_lin64_standalone$ ./volatility_2.6_lin64_standalone -f infected.vmem --profile=Win
7SP1x86_23418 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit

---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ --------------
--------------
0x83db6920 System                    4      0     79      482 ------      0 2021-01-31 18:01:10 UTC+0000

0x84db5418 smss.exe                268      4      2       29 ------      0 2021-01-31 18:01:10 UTC+0000

0x85b78968 csrss.exe               356    340      9      512      0      0 2021-01-31 18:01:11 UTC+0000

0x85b801f8 wininit.exe             396    340      3       75      0      0 2021-01-31 18:01:11 UTC+0000

0x85d45030 csrss.exe               404    388     10      199      1      0 2021-01-31 18:01:11 UTC+0000

0x85d63030 winlogon.exe            460    388      3      113      1      0 2021-01-31 18:01:11 UTC+0000

0x85d5f030 services.exe            496    396      8      205      0      0 2021-01-31 18:01:11 UTC+0000

0x85d72958 lsass.exe               504    396      6      566      0      0 2021-01-31 18:01:11 UTC+0000

0x85d74030 lsm.exe                 512    396      9      135      0      0 2021-01-31 18:01:11 UTC+0000

0x85de2b08 svchost.exe             620    496     12      364      0      0 2021-01-31 18:01:11 UTC+0000
```

Figure 7. Processes List Present In RAM.

3.2.3. Shimcache

When an application is executed, the shimcache logs the event, allowing investigators to build a timeline of application usage. This can be particularly useful in identifying potentially malicious activity, as hidden or suspicious executables may appear in the shimcache entries. The data stored in shimcache can provide insights into when an application was last executed, aiding forensic analysts in correlating this information with other artifacts, such as the Windows Event Log or the prefetch folder [11].

./volatility_2.6_lin64_standalone -f <MemoryImage> --profile=<VersionofOS) shimcache



```
stephen@DFIR:~/Downloads/volatility_2.6_lin64_standalone$ ./volatility_2.6_lin64_sta
ndalone -f infected.vmem --profile=Win7SP1x86_23418 hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:
::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
hacker:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Figure 8. shimcache information.

3.2.4. Switching to Volatility3 and Difference between Version 2 & 3

In order to analyze memory images of latest OS like Windows 10 (newer versions), Windows 11 Volatility3 will be used because Volatility2 doesn't support these versions.

Installing Volatility3: In order to get the latest version of Volatility3, visit this link here and click on "source-code.zip" the file will be downloaded. Once you unzip the file. Type the following command to install all requirements.

Sudo pip3 install -r requirements.txt (Note: Please install pip3 before executing the main command, by typing this command sudo apt install python3-pip)

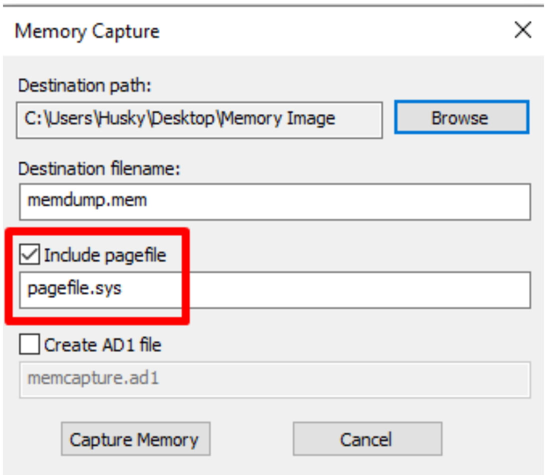
3.3. Advance Forensics Analysis

3.3.1. Pagefile Forensics:

The "pagefile.sys" was used by the Microsoft as a virtual memory extension. It acts as a "paging file" or "swap file," used to supplement physical RAM when it's running low. When the memory is completely used by the system processes and there is not more memory present in the system then the system instructs to write the reaming processes in the page file. This whole work is called "paging" or "swapping."

3.3.2. Obtaining the Page File

Pagefile can be obtained using FTK Imager with memory dump. Open FTK Imager > Capture Memory Dump (Select destination folder and mark "pagefile.sys". Once the process completes, both memory dump and pagefile will be available. (Velociraptor can also help in acquiring the Pagefile). As shown in the given figure 9.



Memory Capture

Destination path: C:\Users\Husky\Desktop\Memory Image

Destination filename: memdump.mem

☑ Include pagefile

pagefile.sys

☐ Create AD1 file

memcapture.ad1

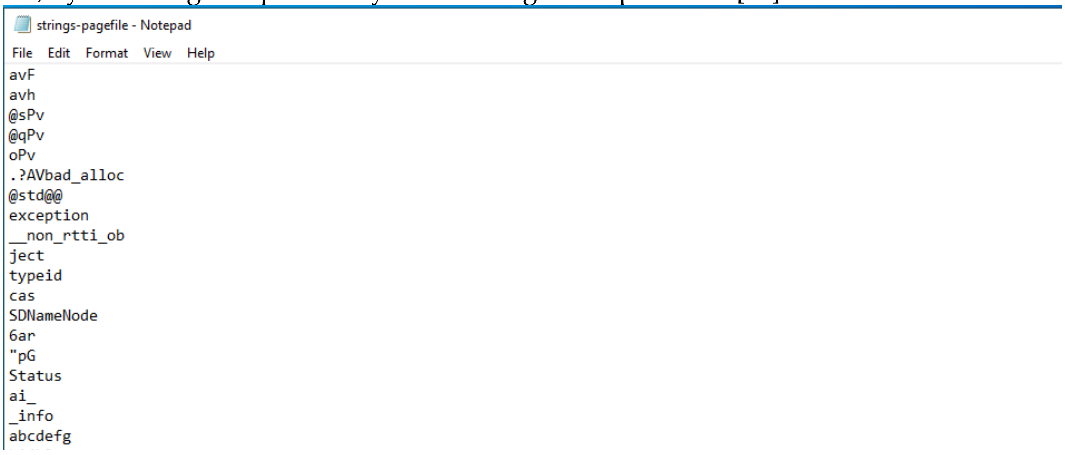
Figure 9. Acquiring Page File.

In order to extract information from pagefile, we will use some open-source tools available. We will use "Strings from SysInternals", Download and run using cmd.

Command to parse information from pagefile.sys

- Strings.exe /accepteula pagefile.sys > pagefile_output.txt

The strings command, forensic analysts can search through a disk image to locate specific text patterns. This method is effective for identifying sensitive information, such as credit card numbers or user credentials, by searching for specific keywords or regular expressions [12].



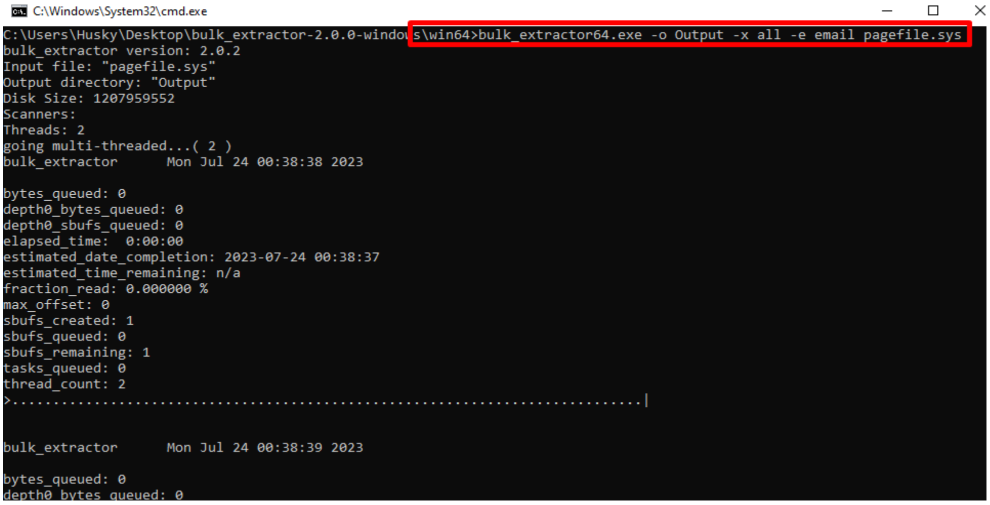
strings-pagefile - Notepad

```
avF
avh
@sPv
@qPv
oPv
.?AVbad_alloc
@std@@
exception
__non_rtti_ob
ject
typeid
cas
SDNameNode
6ar
"pG
Status
ai_
_info
abcdefg
```

Figure 10. Basic Strings from Memory Image

Now we will use another tool "BulkExtractor", Download and run using cmd.

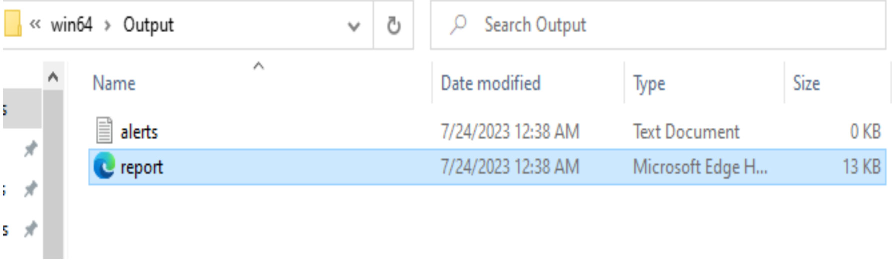
bulk_extractor64.exe -o Output -x all -e email pagefile.sys



```
C:\Users\Husky\Desktop\bulk_extractor-2.0.0-windows\win64>bulk_extractor64.exe -o Output -x all -e email pagefile.sys
bulk_extractor version: 2.0.2
Input file: "pagefile.sys"
Output directory: "Output"
Disk Size: 1207959552
Scanners:
Threads: 2
going multi-threaded...( 2 )
bulk_extractor      Mon Jul 24 00:38:38 2023

bytes_queued: 0
depth0_bytes_queued: 0
depth0_sbufs_queued: 0
elapsed_time:  0:00:00
estimated_date_completion: 2023-07-24 00:38:37
estimated_time_remaining: n/a
fraction_read: 0.000000 %
max_offset: 0
sbufs_created: 1
sbufs_queued: 0
sbufs_remaining: 1
tasks_queued: 0
thread_count: 2
>.............................................................................|


bulk_extractor      Mon Jul 24 00:38:39 2023

bytes_queued: 0
depth0_bytes_queued: 0
```

Figure 11. Result on Command line

Once the process is complete, the results will be displayed. It has found only 1 file named as alerts.



Name	Date modified	Type	Size
alerts	7/24/2023 12:38 AM	Text Document	0 KB
report	7/24/2023 12:38 AM	Microsoft Edge H...	13 KB

Figure 12. Report Generate in HTML format.

4. Conclusion

In order to avoid the security breaches and security incidents a complex infrastructure with good resources is required to overcome any type of mishap-pinning. Furthermore, the complete audit of the company is required to see the security holes present in the environment.

Lastly there is a need to utilize two factor security and least privilege so that the person who have the privileges can used the admin resource. Most of the time these security measures does not present and the attacker exploit these type of hole to access the system. So, it is a best way to avoid any future incident.

5. Recommendations

Some of the recommendations which enhance the security posture of the companies are given.

- The ISO 27001 provides a best way to assess the control assessment for the organizations for better security controls implementation it should be done according to company policies. [13]
- Two factor security is the best way to identify every user so it should be implemented.[14]
- Most of the cyber security incidents happened because of the employees so the company have to arrange this session for better awareness [14] [15].
- Make sure to use the no trust policy so that no one can access the network other than the company [14].
- Keep your windows up to date and patch the vulnerabilities present in your environment either you have to add firewall or deploy solutions [14].
- The best thing is to have your own incident response team so that if any misshapen occur the company can easily renew their work [14] [15]
- Deploy Security Solutions like SIEM and SOC services for continuous monitoring [16].

6. Limitations and Challenges

The use of memory forensic in today's world is increasing day by day. As the attacker are using advance method for the malware deployments the examiners are also using advance techniques like memory forensics to detect these types of attackers. The use of these techniques to find digital evidence and to uncover the attacker attacks plays an important role in court proceedings but it also comes with its limitations and challenges.

As we deep dive into forensic analysis we have to see some hurdles as sometimes the attacker uses tools that encrypt various parts of the memory so that they can remove their footprints. So, this is the main difficulty faced by the examiner as the encrypted memory takes a huge time to decrypt and during the decryption some time the artifact failure occurs.

Now the next limitation is the usage of anti-forensic tools used by the attack vector to completely erase or disrupt the systems and as the evidence is completely destroyed there is not any way to recover artifacts.

7. Documentation and Preservation

In order to maintain trust and ethical consideration during the progress the CIA model is used to main maintain the confidentiality, integrity, and availability of the case in the court. Furthermore the proper documentation is made step by step as the case progress so that the evidence is also admissible in the court proceedings. Also details about how the data is collected and how it is processed and how the forensic analysis is done is also noted.

In this way the integrity of the case is also verified also the chain of custody is properly maintained so that it can easily be traced from where the evidence originate and whose possession it was and how it was preserved.

Lastly the hashes of the forensic image was properly maintained so that it was reliable in the court.

Reference

1. Case, A., & Richard, G. (2018). Memory forensics: The path forward. Digital Investigation, 24, 1-9.
2. Ligh, M., Case, A., Levy, J., & Walters, A. (2014). The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory.
3. Sylve, J. T., Case, A., Marziale, L., & Richard, G. G. (2012). Acquisition and analysis of volatile memory from Android devices. Digital Investigation, 9(1), 1-15.
4. Khan, A. Q., Sun, G., Khalid, M., Imran, A., Bilal, A., Azam, M., & Sarwar, R. (2024). A novel fusion of genetic grey wolf optimization and kernel extreme learning machines for precise diabetic eye disease classification. PLOS ONE, 19(5), e0303094. Public Library of Science.
5. PCMag. (n.d.). Definition of physical memory. Retrieved from PCMag website: https://www.pcmag.com/encyclopedia/term/physical-memory
6. phoenixNAP. (2023, September 25). What Is Physical Memory? Retrieved from phoenixNAP IT Glossary: https://phoenixnap.com/glossary/physical-memory
7. ScienceDirect. (n.d.). Physical Memory - an overview. Retrieved from ScienceDirect Topics: https://www.sciencedirect.com/topics/computer-science/physical-memory
8. ADF Solutions. (n.d.). Memory Forensics: Effective Digital Forensics Investigations Basics. Retrieved from https://www.adfsolutions.com/adf-blog/memory-forensics-101-the-basics-you-need-to-know-for-effective-digital-forensics-investigations
9. SANS Institute. (n.d.). Memory Forensic Acquisition and Analysis 101. Retrieved from https://www.sans.org/blog/memory-forensic-acquisition-and-analysis-101
10. DTIC. (2014). Memory Forensics: Review of Acquisition and Analysis Techniques. Retrieved from https://apps.dtic.mil/sti/citations/ADA594490
11. Palutke, R., Block, F., Reichenberger, P., & Stripeika, D. (2020). Hiding Process Memory via Anti-Forensic Techniques. Digital Investigation, 30, 1-9. https://doi.org/10.1016/j.diin.2020.100798
12. Inception Security. (n.d.). Shimcache: A Crucial Tool for Digital Forensics and Incident Response. Retrieved from https://www.inceptionsecurity.com/post/shimcache-a-crucial-tool-for-digital-forensics-and-incident-response
13. Hacker Factor. (2021, September 14). With Strings Attached - The Hacker Factor Blog. Retrieved from https://www.hackerfactor.com/blog/index.php
14. Siraj, M. A., Rehman, A., Aziz, O., & Khan, M. F. (2021). Systematic Literature Review: Smart Drone for Early Smoke Detection in Forest Using IOT. Journal of Computing & Biomedical Informatics, 2(01), 80-88.
15. Splunk. (n.d.). Defining & Improving Your Security Posture. Retrieved from https://www.splunk.com/en_us/blog/learn/security-posture.html
16. TrueFort. (n.d.). Ten Ways Organizations Can Improve Security Posture. Retrieved from https://truefort.com/improve-security-posture/
17. Aqua Security. (n.d.). What Is a Cyber Security Posture and 5 Ways to Improve Yours. Retrieved from https://www.aquasec.com/cloud-native-academy/vulnerability-management/cyber-security-posture/
18. TechTarget. (2023). 16 common types of cyberattacks and how to prevent them. Retrieved from https://www.techtarget.com/searchsecurity/tip/6-common-types-of-cyber-attacks-and-how-to-prevent-them.
19. Ikram, A., Imran, A., Li, J., Alzubaidi, A., Fahim, S., Yasin, A. U., & Fathi, H. (2024). A systematic review on fundus image-based diabetic retinopathy detection and grading: Current status and future directions. IEEE Access.
20. Latif, S., Ilyas, M. S. B., Imran, A., Abosaq, H. A., Alzubaidi, A., & Karović Jr, V. (2024). Machine learning empowered security and privacy architecture for IoT networks with the integration of blockchain. Intelligent Automation & Soft Computing, 39(2), 353-379. Tech Science Press.