|  |  |
| --- | --- |
| Course | Computer Forensics |
| Lab | Lab 07 |
| Name of the Student | Maisha Khatoon |
| Student ID | 100899259 |

# **LAB: 07**

This lab focuses on memory analysis.

**Objective:**

* **Learn digital artifacts through Memory analysis with Volatility.**

**Learning Activities:**

At the end of these activities, you should understand:

* Engage in standard processes of identifying, collecting, and analyzing relevant digital artifacts while keeping in mind the principles of sound forensic investigation, such as evidence preservation, documentation, evidence-based conclusions, and artifacts.

**Tools to use:**

- Volatility (volatility\_2.6\_win64\_standalone.zip -> https://www.volatilityfoundation.org/26)

- Magnet Forensics RAM Capture (<https://www.magnetforensics.com/resources/magnet-ram-capture/>)

-Python (https://github.com/volatilityfoundation/volatility/blob/master/README.txt)

**Note: Please include a screenshot of each step. Corp your screenshot to show relevant information only. Uncropped screenshots will result in a 10% deduction from your marks.**

As you know, attackers often target servers or exploit employee workstations or end-user devices through phishing, and these systems and devices are on practically all the time, or at least most of the day. As such, acquiring images and/or potential evidence from a live machine is likely in many digital forensic investigations. However, when you encounter a victim system it may not be feasible to shut it down, or an intruder may still be poking around the system/network and you may not want to alert him or her to your presence. Besides, there is a plethora of potential evidence to be had from a victim system left running in its current state. The volatile contents of RAM should be captured as a snapshot of what is running on the system at that precise time, not to mention that it contains information that is not necessarily kept on the system's physical drive. Let's start here and capture the

memory from the victim system.

There are many tools that can capture the memory from a live system, but we will be using FTK Imager Lite from AccessData. It is a GUI tool and compared to some other similarly purposed command-line tools, it leaves a larger footprint on the machine; however, all considering, its impact on the system is still rather minimal and it tends to collect more reliable images. As an investigator, you will have to decide if it is more acceptable to lose the volatile information contained in RAM or, alternatively, to interact with the system and alter some information on the physical drive.

**Task 1:**

**Memory Capture**

* 1. Insert your USB stick. If necessary, connect it to the VM. Navigate to it in Windows Explorer and execute FTK Imager Lite. Click Yes in the User Account Control window.

1.2. Find the little memory stick icon in the FTK Imager Lite toolbar. If you hold the mouse over it, it should say 'Capture Memory'. Click it to view the Memory Capture window.

1.3. Select Browse and set your Destination Path to somewhere on your removable USB drive. Then, you may change the name of the captured memory file to whatever you like. Note, FTK Imager will create a raw memory capture, just be aware of different formats used in different tools. Leave the boxes unchecked and click the Capture Memory button. This will take a little while as it is capturing XXGB of memory.

1.4 When the capture has completed, the Status line should read 'Memory capture finished successfully'. Now, you have captured the memory from a live system. Click Close, but keep FTK Imager Lite running. We will analyze the memory capture later.

What is the size of the file (captured mem file)? \_\_\_\_\_\_\_512 MB\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Take a screenshot of this result)

A screenshot of a computer

Description automatically generated

***Note: You may use Magnet RAM Capture utility to capture memory.***

**Task-2:**

**Memory Analysis**

For this part of the lab, you can disconnect your USB drive from the VM and make it accessible to your main operating system. We will be using Volatility Framework to analyze the raw memory dump that you saved to your USB drive. Volatility uses plugins, which makes it rather extensible, and the framework provides a powerful and dynamic memory analysis tool used by many investigators throughout the digital forensics community. I encourage you to explore this tool as much as possible. To start, you might check out the basic usage instructions at the following link: <https://www.forwarddefense.com/pdfs/Memory-Analysis-with-Volatility.pdf>.

2.1 Start a command shell and navigate to where your standalone Volatility executable is. Note, it may be helpful to have your memory image and the standalone Volatility exe in the same directory, whether on your USB drive or copied onto your main hard drive.

2.2 Typically, you would run the 'imageinfo' plugin to determine the proper profile to use with any particular memory image you may be analyzing, but since that can take some time. In the shell, enter the following command:

(Take a screenshot of this result)

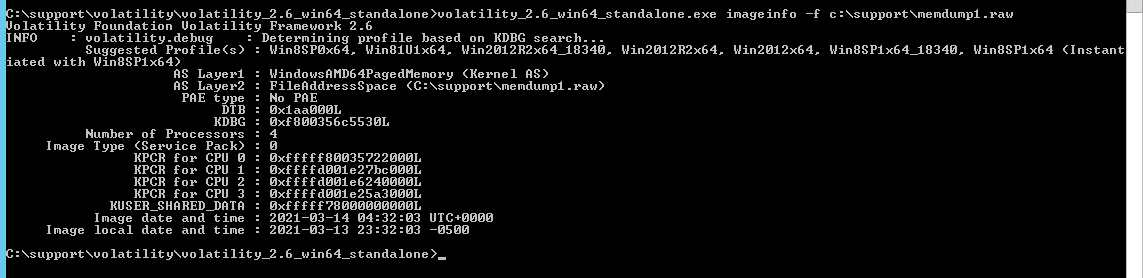
*C:\support\volatility\volatility\_2.6\_win64\_standalone>volatility\_2.6\_win64\_standalone.exe imageinfo -f c:\support\memdump1.raw*

*Note: The above command may take up to 15 minutes to display the output.*

Ex:

“C:\support\volatility\volatility\_2.6\_win64\_standalone” is the volatility utility directory

“C:\support\memdump1.raw “ is the captured mem file



My screenshot:

A screenshot of a computer program

Description automatically generated with medium confidence

2.3 Next, enter the following command:

(Take a screenshot of this result)

*C:\support\volatility\volatility\_2.6\_win64\_standalone>volatility\_2.6\_win64\_standalone.exe --profile=Win2012R2x64\_18340 -f c:\support\memdump1.raw netscan*

Note, it is often helpful to send the output to a text file, especially if you are using a Windows command shell, it's just easier to read. The above command, which uses the 'netscan' plugin, lists all network connections, protocols, IP addresses, ports, and associated processes.

A black screen with white text

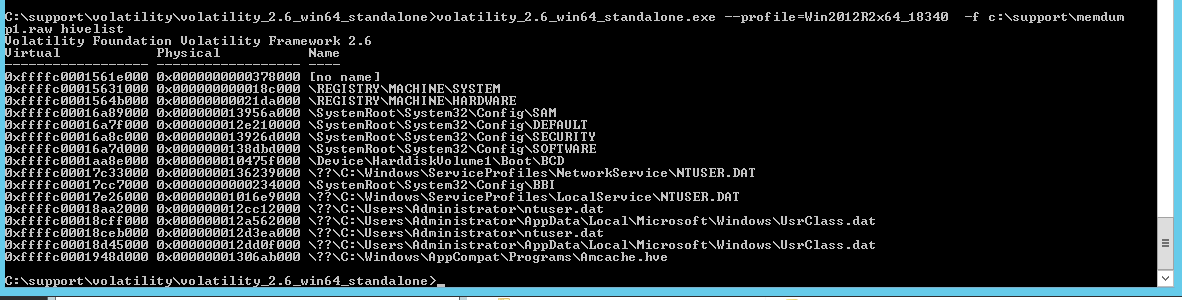
Description automatically generated with low confidence

What is the command to send the output of the above command to a text file for later analysis? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_output.txt\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2.4 To locate the virtual addresses of registry hives in memory, and the full paths to the corresponding hive on disk, use the hivelist command. If you want to print values from a certain hive, run this command first so you can see the address of the hives.

(Take a screenshot of this result)

*C:\support\volatility\volatility\_2.6\_win64\_standalone>volatility\_2.6\_win64\_standalone.exe --profile=Win2012R2x64\_18340 -f c:\support\memdump1.raw hivelist*



My screenshot:

A screenshot of a computer screen

Description automatically generated with medium confidence

2.5 The next command would output list multiple hives (DEFAULT and ntuser.dat) contain the same key “Software\Microsoft\Windows NT\CurrentVersion”. (Take a screenshot of this result)

*C:\support\volatility\volatility\_2.6\_win64\_standalone>volatility\_2.6\_win64\_standalone.exe --profile=Win2012R2x64\_18340 -f c:\support\memdump1.raw printkey v-K "Software\Microsoft\Windows NT\CurrentVersion"*

A screenshot of a computer program

Description automatically generated with medium confidence

2.6 Next, the following command would display a list of running process:

*C:\support\volatility\volatility\_2.6\_win64\_standalone>volatility\_2.6\_win64\_standalone.exe --profile=Win2012R2x64\_18340 -f c:\support\memdump1.raw pslist*

(Take a screenshot of this result)

A screenshot of a computer

Description automatically generated

2.7 Next command would display the process tree:

*C:\support\volatility\volatility\_2.6\_win64\_standalone>volatility\_2.6\_win64\_standalone.exe --profile=Win2012R2x64\_18340 -f c:\support\memdump1.raw pstree*

(Take a screenshot of this result)

A screenshot of a computer

Description automatically generated

2.8 To view the SIDs associated with a process, use the getsids command:

*C:\support\volatility\volatility\_2.6\_win64\_standalone>volatility\_2.6\_win64\_standalone.exe --profile=Win2012R2x64\_18340 -f c:\support\memdump1.raw getsids*

(Take a screenshot of this result)

A screenshot of a computer

Description automatically generated

2.9 What is the command to display the loaded DLLs? \_\_\_\_\_\_\_\_\_\_\_dlllist\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3.0 What is the command to display process privileges detail? \_\_\_\_\_\_\_\_\_\_\_\_privs\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Reflective statements (end-of-exercise):**

You should reflect on these questions:

1. How can the Forensics Investigators preserve volatile evidence at the crime scene?

To protect the integrity and admissibility of volatile evidence in court, forensic investigators must preserve it at the site of the crime. The following broad actions may be done to safeguard volatile evidence:

Safety First: Investigators must first protect their personal safety and the safety of those present at the crime scene before trying to gather any explosive evidence. Wearing personal protection equipment (PPE) including gloves, masks, and goggles as well as adopting safety measures to avoid fires or explosions may be necessary in order to accomplish this.

Identify and Record: Any possible sources of flammable evidence at the crime scene should be noted by investigators and recorded. This could include things like explosives, solvents, or accelerators. The context and location of the evidence may be established with the use of thorough documentation including notes, photos, and drawings.

Control the Environment: Preserving volatile evidence requires strict environmental control. It is important to take precautions to reduce any elements that can hasten the evaporation or deterioration of the volatile compounds. This may include preventing others from entering the crime scene, locking windows and doors, and regulating the temperature and humidity.

|  |  |
| --- | --- |
|  |  |

1. How can the Forensics Investigators make use of Artificial Intelligence (AI) and Machine Learning (ML) in digital forensics?

To improve their investigation powers and speed up the study of digital evidence, forensic investigators might use artificial intelligence (AI) and machine learning (ML) methods in digital forensics. The following are some applications of AI and ML in digital forensics:

Automated data processing: The first processing of substantial amounts of digital data may be carried out automatically using AI and ML algorithms. This comprises activities like data indexing, data classification, and data extraction. Investigators may concentrate on more involved analysis while saving time by automating these operations.

AI and machine learning systems are excellent at pattern identification and anomaly detection. These methods may be used in digital forensics to locate suspicious or possibly important patterns in data, such as hidden files, encrypted data, or irregularities in network traffic. This aids detectives in finding possible evidence that could otherwise escape their attention.

AI and ML may be used to evaluate multimedia material, including pictures, videos, and audio files. While audio analysis algorithms may assist with voice recognition and the identification of certain audio patterns, picture recognition algorithms can help in the identification of objects, people, or places represented in photos or films. These tools may help investigators locate pertinent evidence in multimedia files.

1. What is the difference between artifacts and evidence?

Any proof is given to a court to help establish the truth of anything else, including evidence that something exists or is true. a piece of evidence that is offered to back up an answer that is given in response to a query, such as text or a reference to a resource. If an artifact is digital, it is also the record of user action that has been stored in a device or file. Similar to the idea of digital fingerprints, this. When conducting their examination, digital forensic investigators will look in certain places for signs of user activity.

**References**

1. https://www.volatilityfoundation.org/26
2. https://en.wikipedia.org/wiki/Memory\_forensics
3. https://www.sans.org/reading-room/whitepapers/forensics/techniques-tools-recovering-analyzing-data-volatile-memory-33049
4. https://www.sciencedirect.com/topics/computer-science/memory-forensics