CA-3

On

(Volatility Framework)

Submitted by

Name of Student: Venkata Kireeti Savarala

Registration No: 11905507

Roll No: B53

Program Name: Open Source Technologies

Under the Guidance of

Dr. Manjot Kaur

School of Computer Science & Engineering

Lovely Professional University, Phagwara

(March, 2023)

Q) Investigate the system run time state of a device (RAM), extract the information present in RAM with the help of volatility Framework.

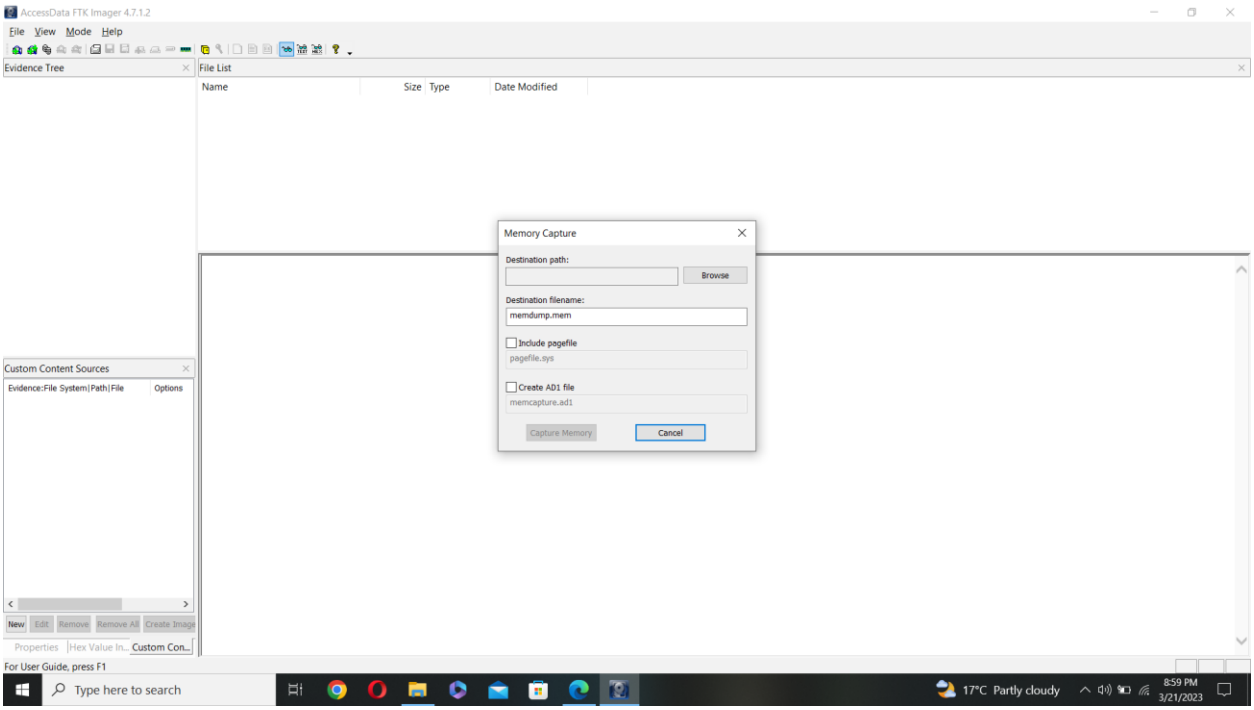
GITHUB link: kireeeti2612002/INT-301_CA-3 (github.com)

Step – 1:

Install Access Data FTK Imager by using below link and this FTK imager helps for getting memory dump into our PC. After installing open it and go to file and click on capture memory. It will look like below image.

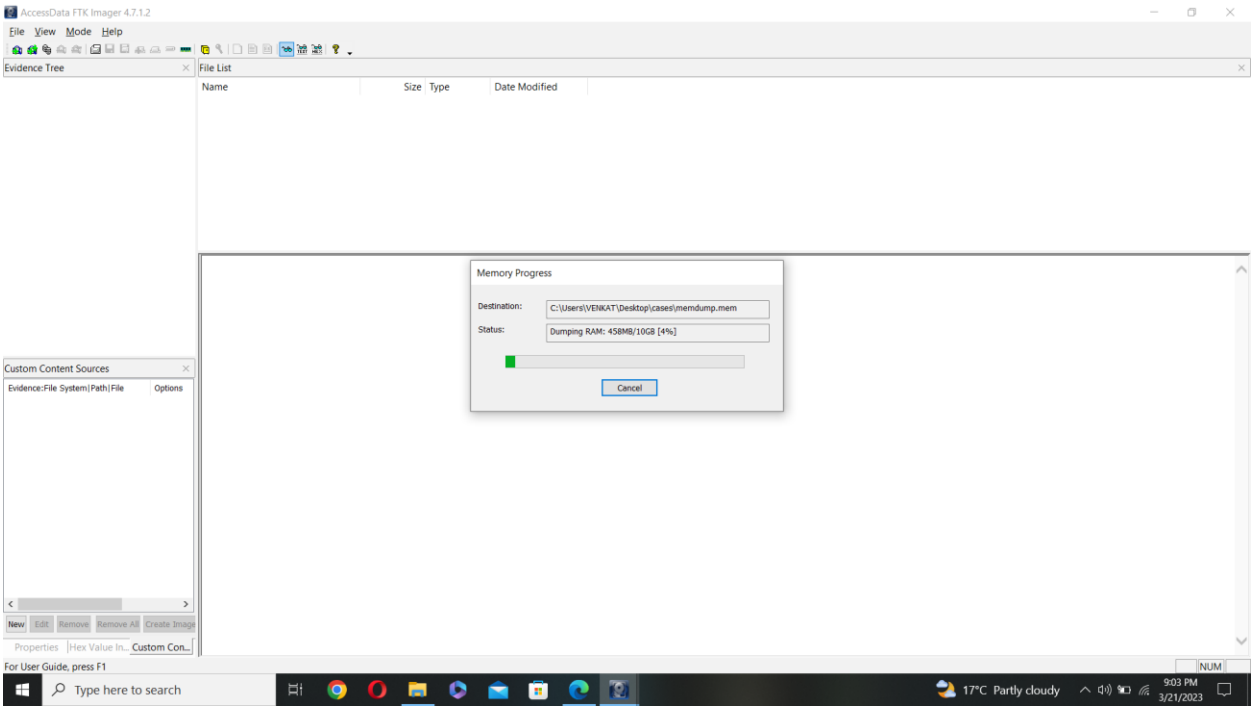
This memory dump of the device will help to investigate the RAM.

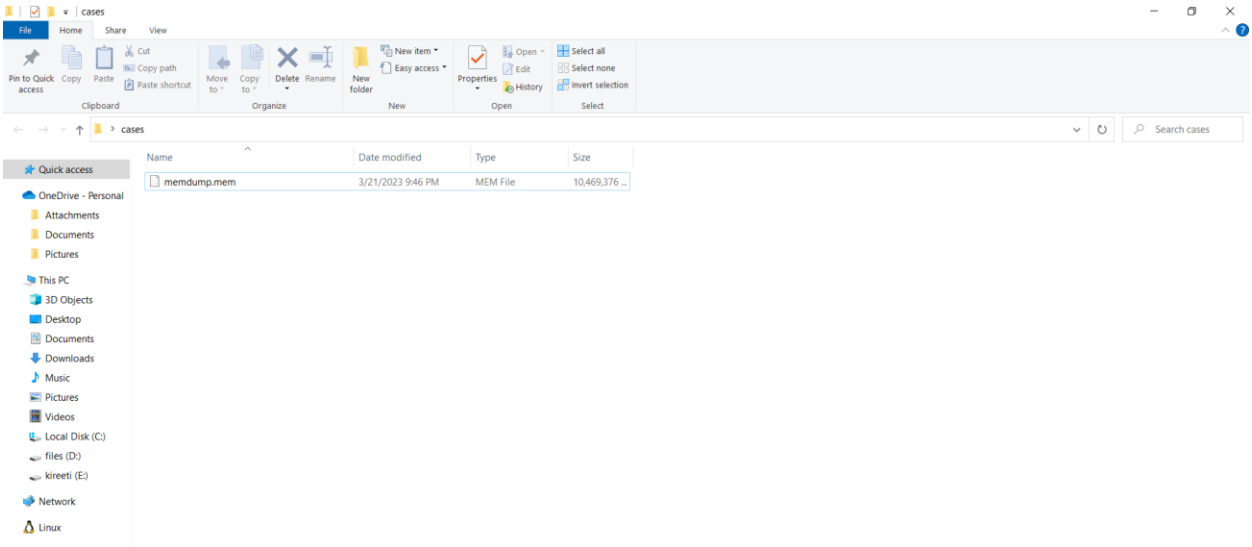
Link: https://www.exterro.com/ftk-imager



Step – 2:

After completing step-1, give the path where to acquire the memory dump. I have given it in a folder called “cases” on Desktop. So after giving path click on capture memory and it will start acquiring memory (mine was 10 GB). It should look like below image and also the memory dump file looks like given image.

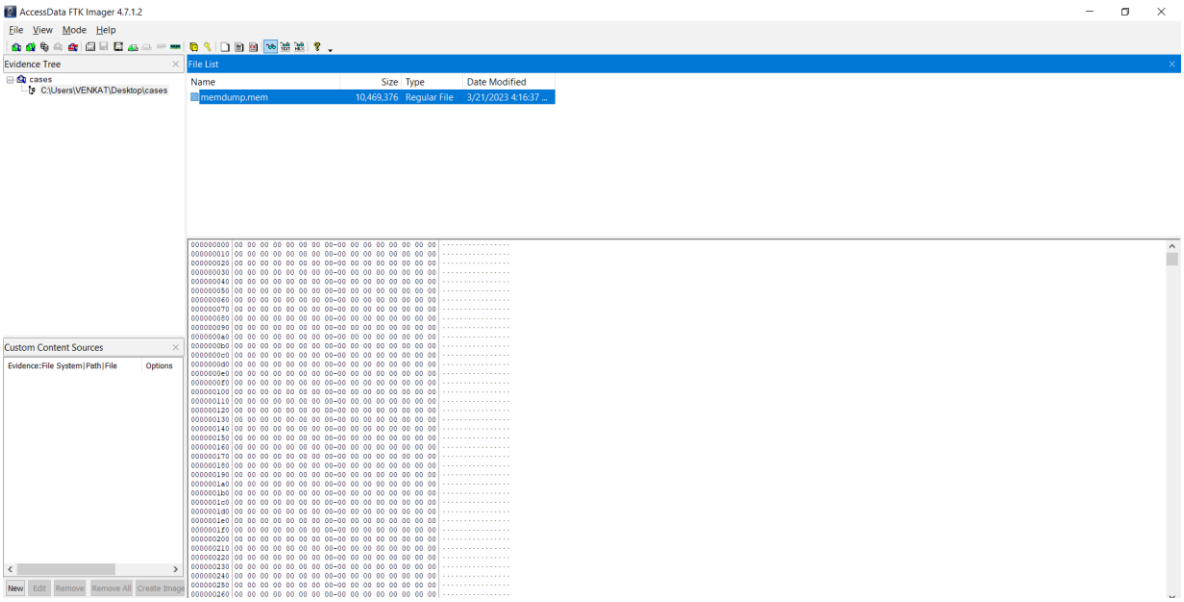


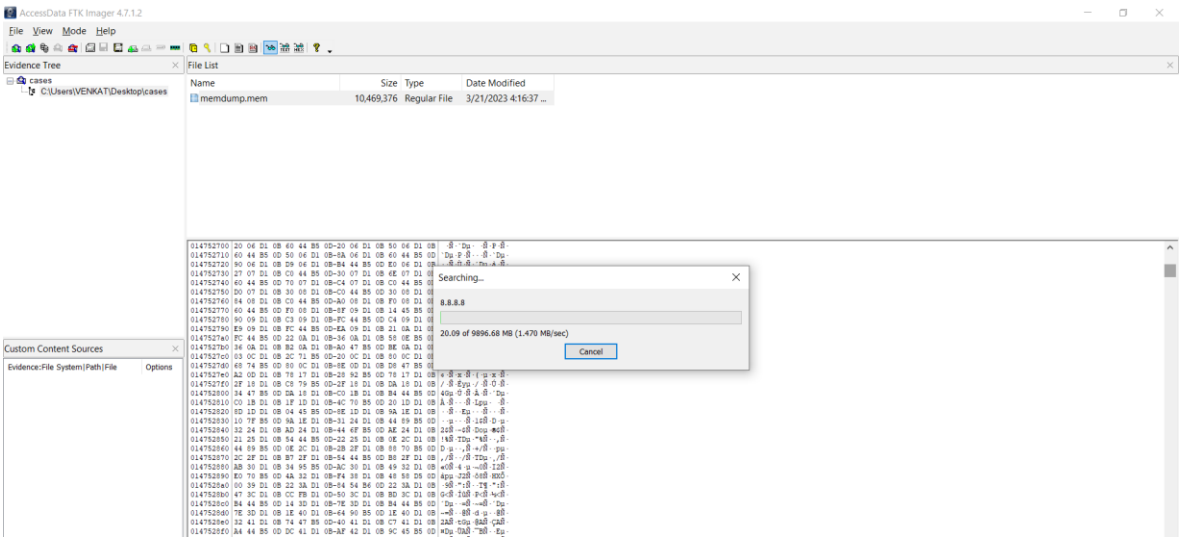


Step – 3:

After completing the process of acquiring memory dump, go Access Data FTK imager, go to file and click on “Add evidence item”, then select “contents of a folder” and give the path of the memory dump file location.

You can see the file on the FTK imager. By clicking on the left side file path, you can view all the information present in it (usernames, network information, etc.). You can also search by using find option like below given image.





Step – 4:

To extract information from RAM we use Volatility Framework, install it by link given below and also to use volatility framework we require Python, so install python by given link below. Also download symbols file to analyze the memory dump.

Volatility Framework link: https://www.volatilityfoundation.org/

Install Python link: https://www.python.org/downloads/

Symbols file link: https://tinyurl.com/4xff653v

Step – 5:

After downloading both Volatility framework and python, put the volatility extracted file in disk (C or D disk) by giving a new folder. Check whether all the files are there in the folder.

The downloaded symbols zip file move it to the symbols folder of volatility3 folder inside volatility folder we created.

Also move the memory dump file into the "D:\volatility3-1.0.0".

Step – 6:

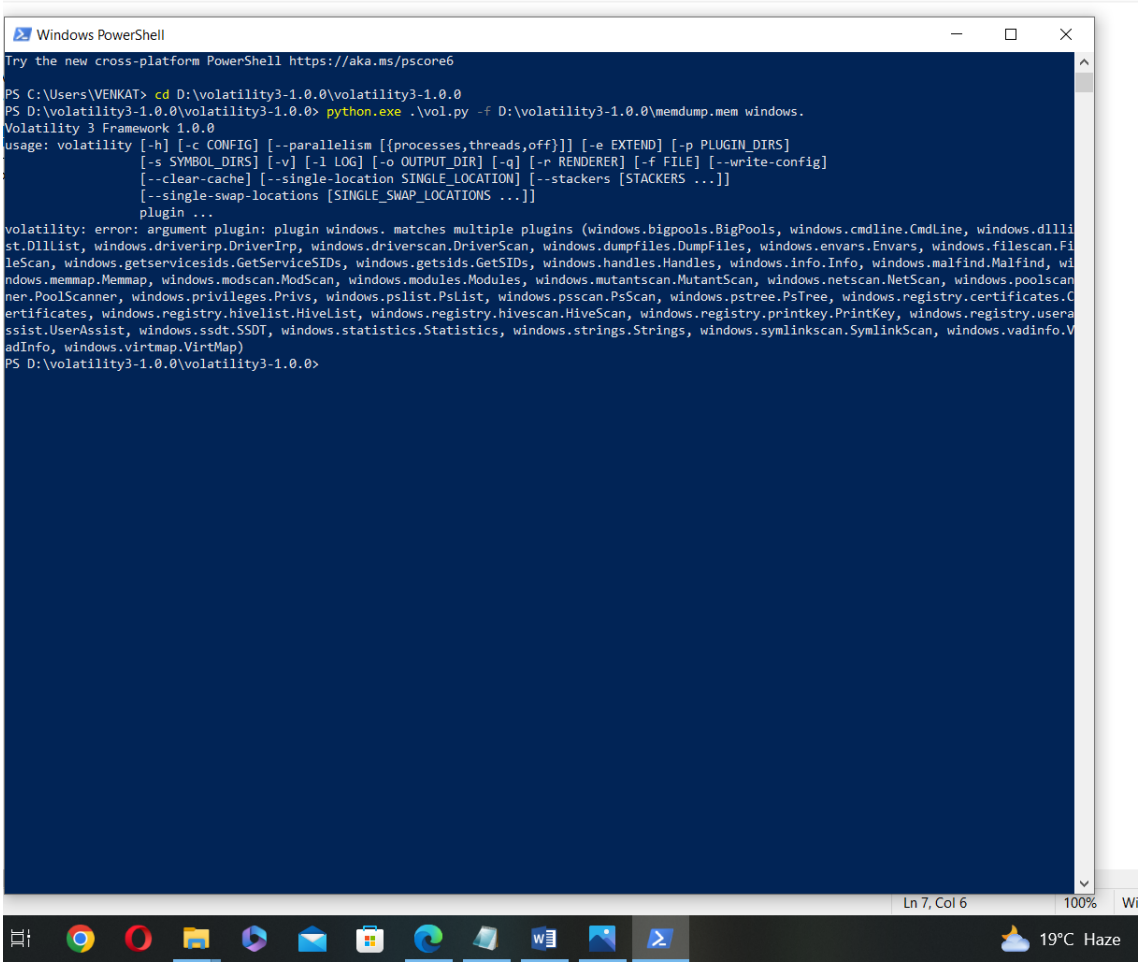
Open PowerShell in PC, first change the directory by using "cd" command. "cd D:\volatility3-1.0.0\volatility3-1.0.0" use this command so that you will be moved to the directory.

After this use "ls" command to list the files present inside the directory and check whether the "vol.py" file is present.

If all ok, then proceed by executing the below commands to extract information from RAM.

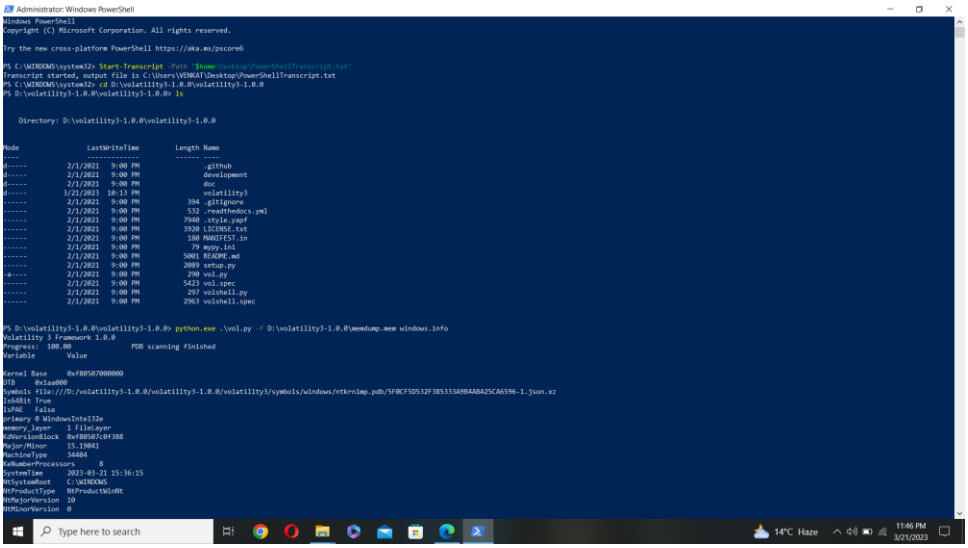
Step – 7:

Use “python.exe .\vol.py -f D:\volatility3-1.0.0\memdump.mem windows.” command to get the plugins which we can use to extract information from memory dump, here you should give the path of volatility folder.



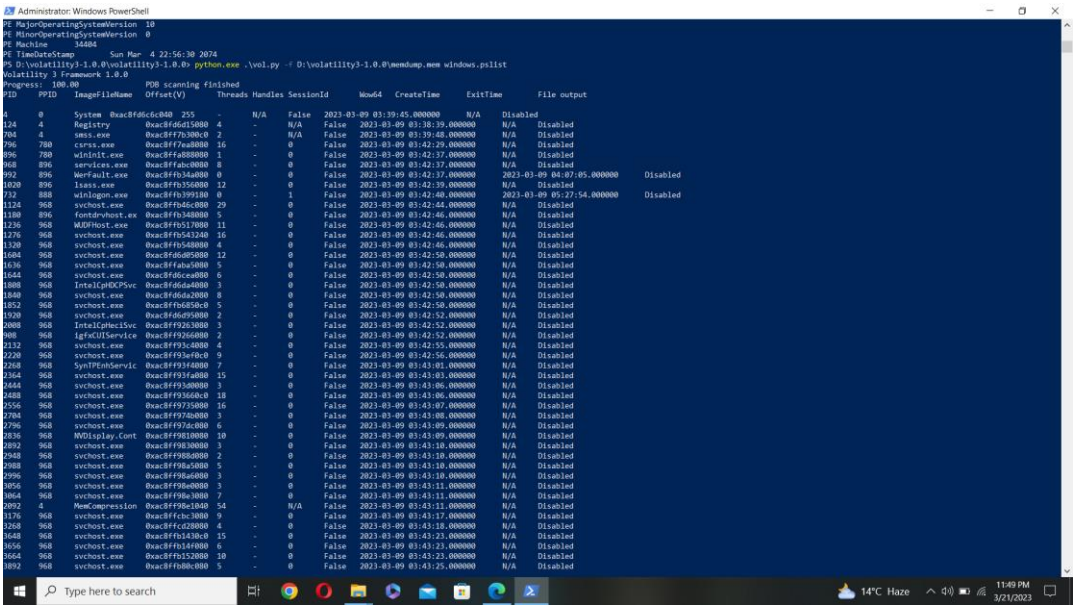
Step – 8:

Use “python.exe .\vol.py -f D:\volatility3-1.0.0\memdump.mem windows.info” plugin and command to get the full information about the windows of our PC from memory dump.



Step -9:

Use “python.exe .\vol.py -f D:\volatility3-1.0.0\memdump.mem windows.pslist” plugin and command to get the list all running processes on the system.



We can use various plugins and commands available in the Volatility framework.

pstree: This command displays the running processes in a hierarchical tree view.

psscan: This command used to scan the memory for processes and provides us the detailed information about the each process.

filescan: This command scans the memory for open files and provides detailed information of each file.

netscan: This command lists all the network connections that currently active on the system.

dumpfiles: This command is used to extract files from memory to disk.

malfind: This command is used to scan the memory for suspicious code or malware.

These are some examples of plugins and commands available in the Volatility framework. To use any of these commands, simply specify the name of the plugin or command when running the Volatility framework.