**Lab – 6**

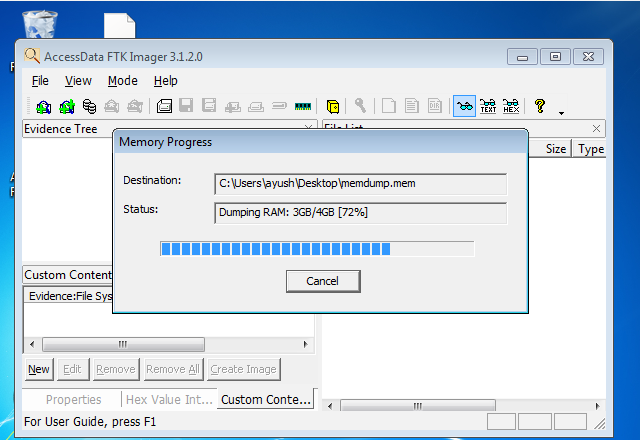
**AIM**: - To collect memory dump and perform different operations using Volatility.

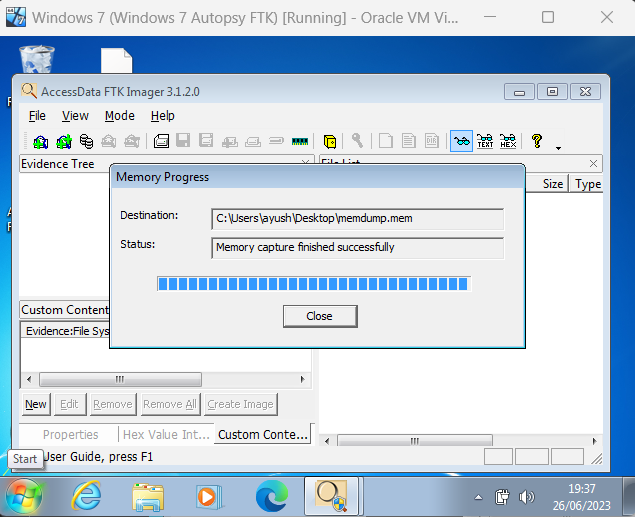
**Software Used**: -

* FTK Imager
* Volatility

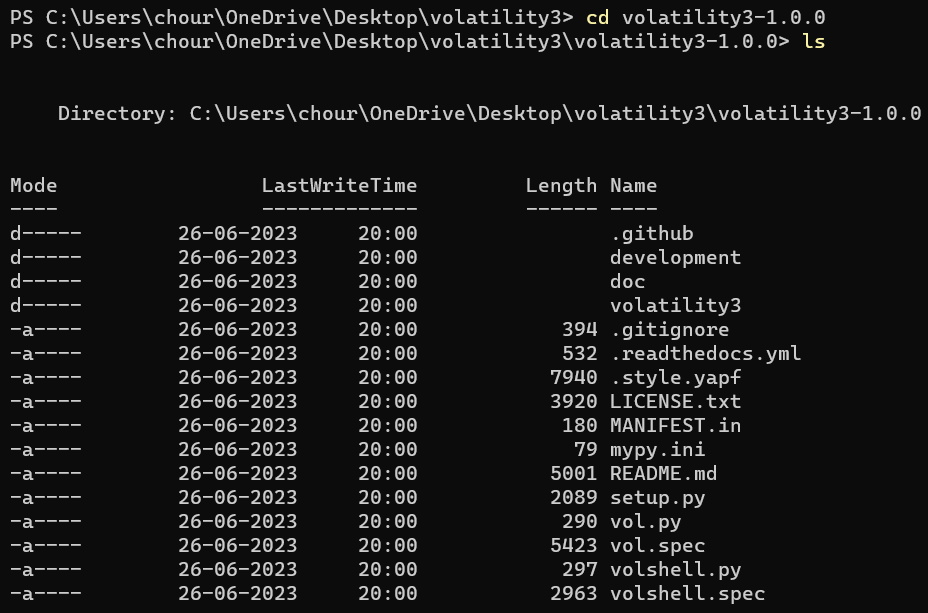
**Steps for performing operations on Volatility**: -

1. Create a memory dump of the RAM of your system through FTK Imager.Once the dump is created the status will be flashed with the message “Memory capture finished successfully. ”

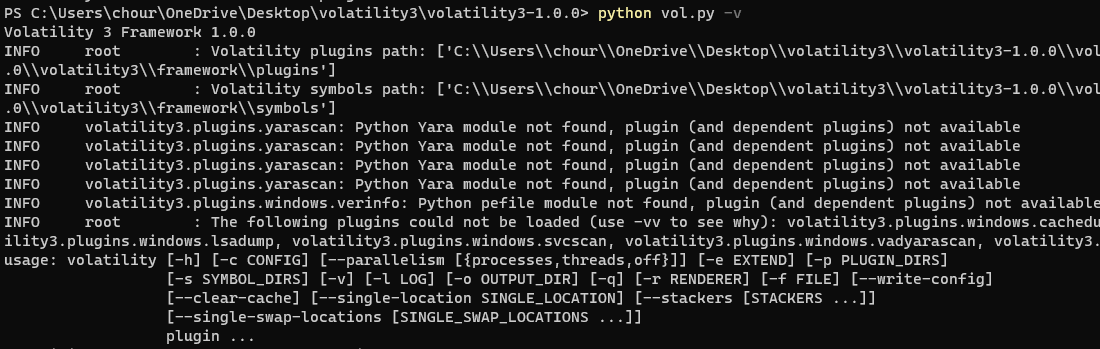




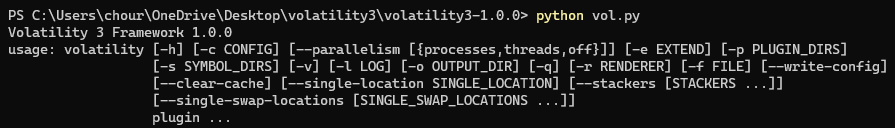
1. Download Volatility from the office volatility website and extract the file to the destination where you want to store volatility.
2. Open Powershell in windows and Traverse to place where the file has been extracted.



1. Check the framework of the volatility tool by running the command with the suffix **-v**.



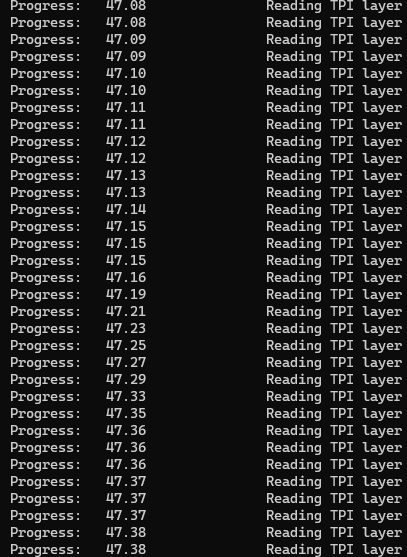
1. When you run the command for the framework you will get a list of suffixes that you can use for different other functions in volatility.



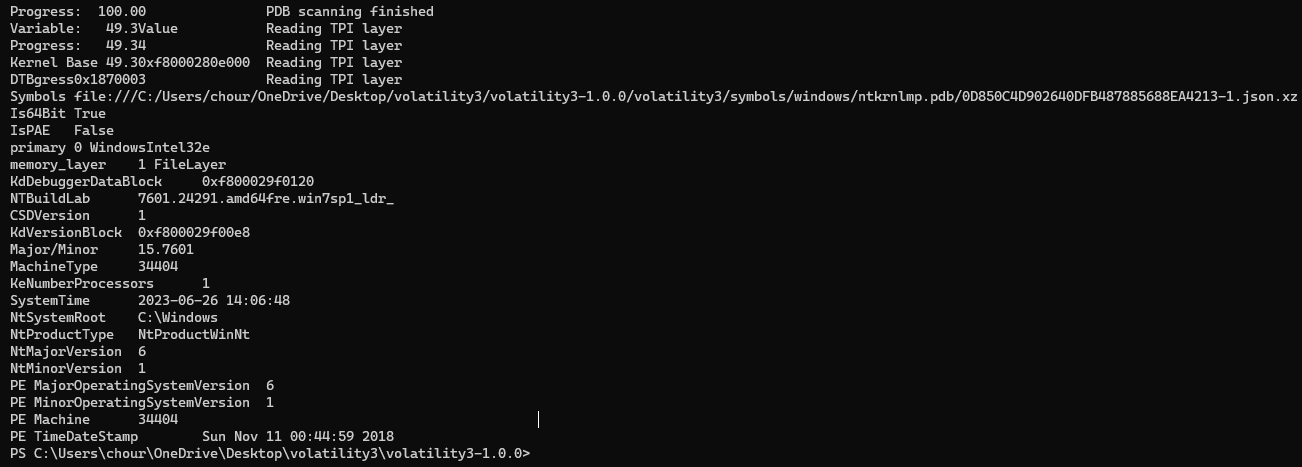
1. Run the command to perform operation on the memory dump file using the suffix **-f**.



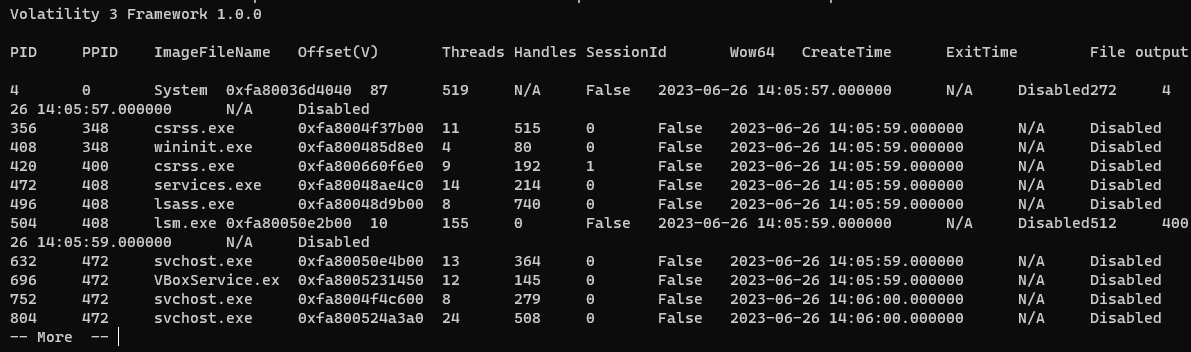
1. It would take some time to analyze the memory dump file and then show the progress.



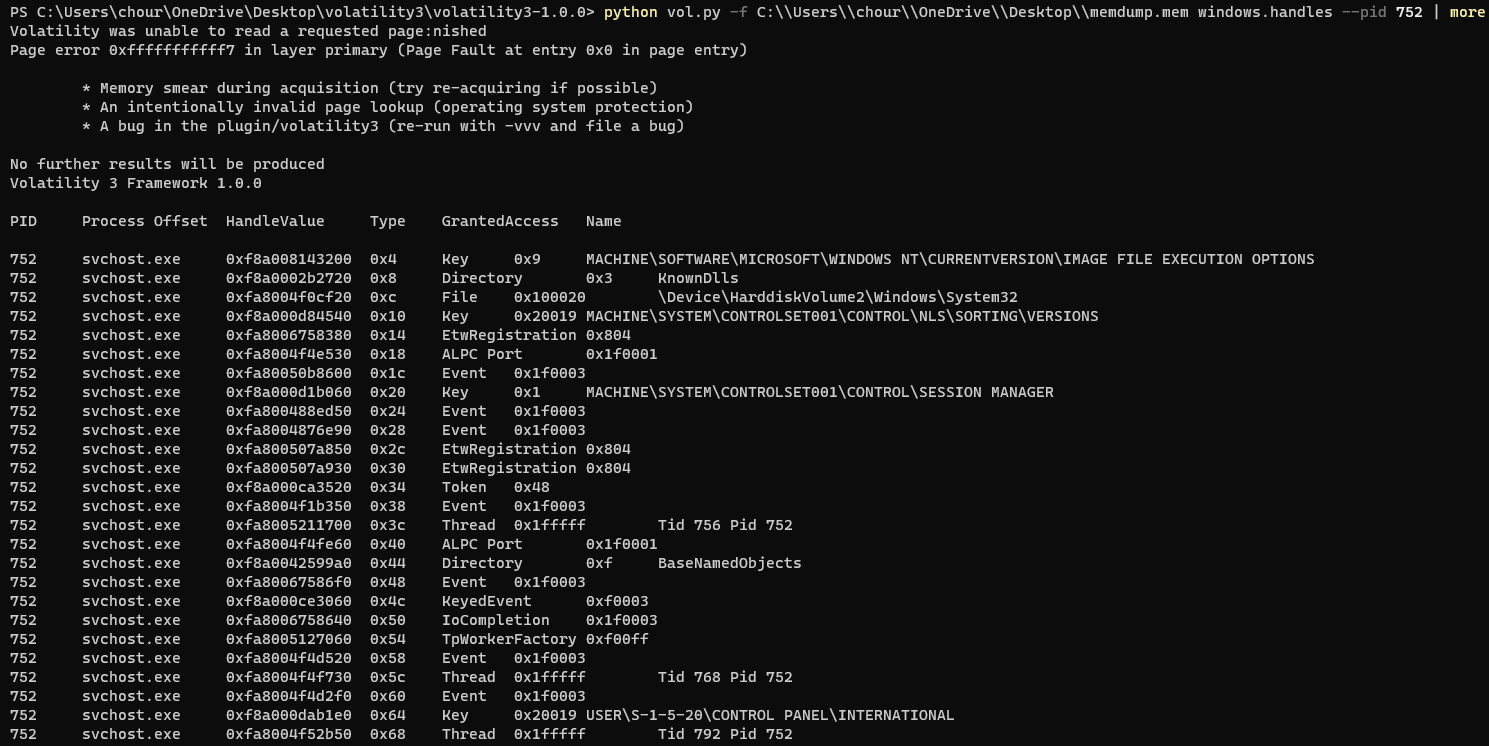
1. When the file is read completely by volatility it would show you the attributes of the file and progress completed in reading the file.



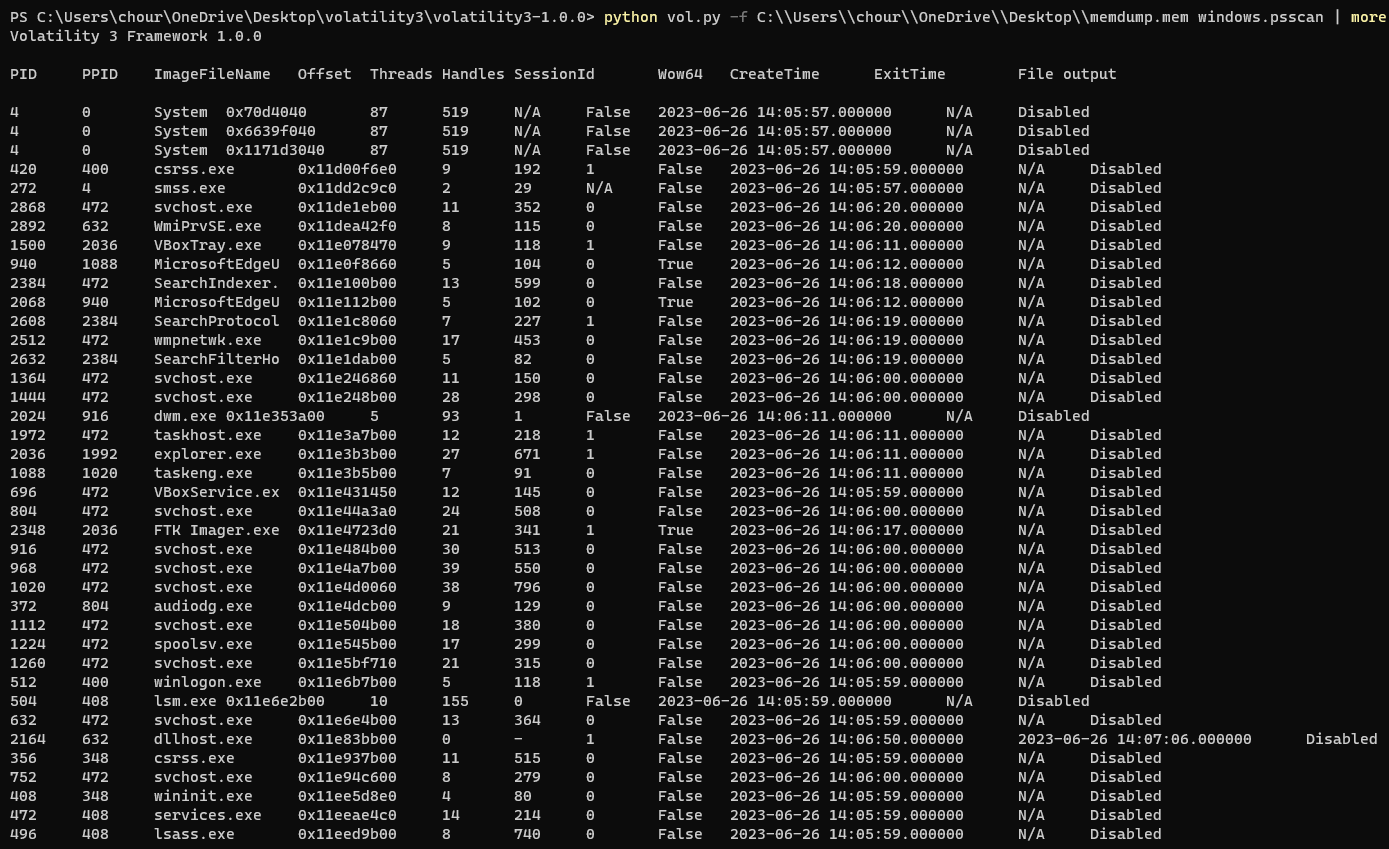
1. On running the command with “**.pslist | more” ,** the process id’s along with the information of other processes is shown on the screen.



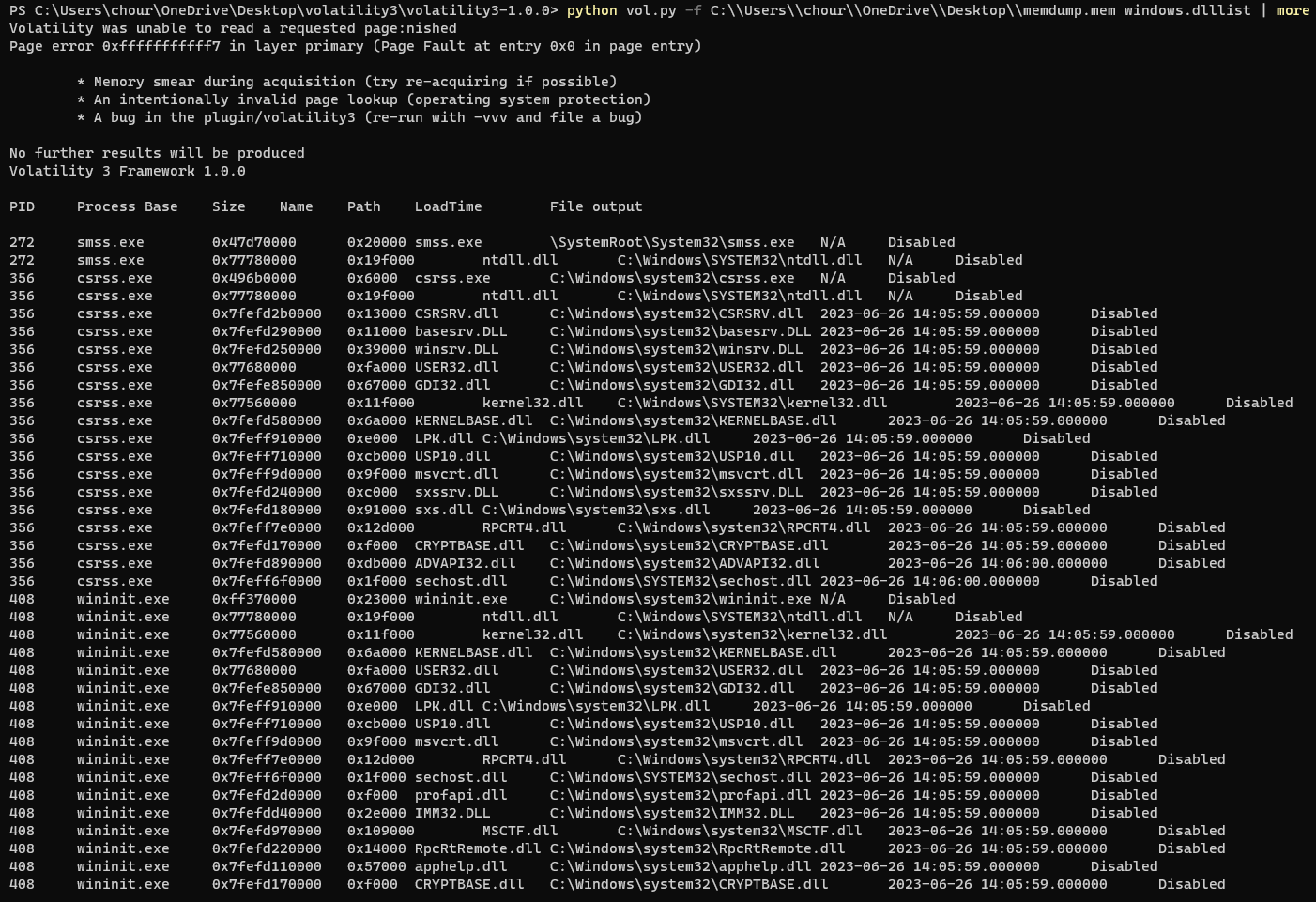
1. On running the command with “**.handles --pid | more” ,** details about that particular process is showed in elaborate format.



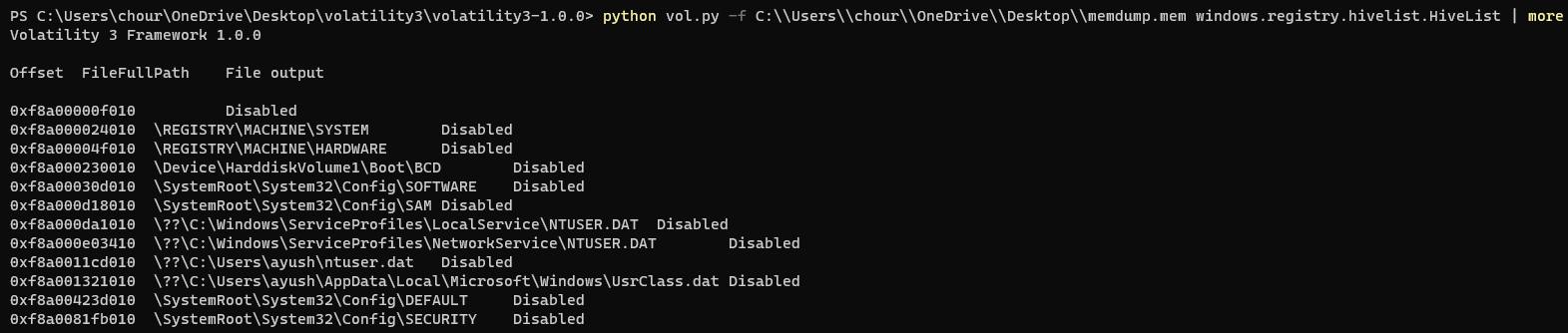
1. On running the command with “**.psscan | more” ,** details about all the hidden processes is shown along with the process id, threads, handles, session id, etc.



1. On running the command with “**.dlllist | more” ,** details about all the dll’s in the image file is presented.



1. On running the command with “**.registry.hivelist.HiveList | more” ,** details about all the registry files including the system and the hardware in the image file are presented.



1. On running the command with “**.registry.hivescan.HiveScan | more” ,** details about the addresses of the registry files and the offset they are located in.

