Forensic Image Analysis

Seneca | SCHOOL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

TERM	NAME – Student ID	COURSE CODE	WEIGHT
Winter 2025	LEANDRO DELGADO-114416241	CYT215	

Lab Objectives

Upon completion of this lab, you will be able to perform the following:

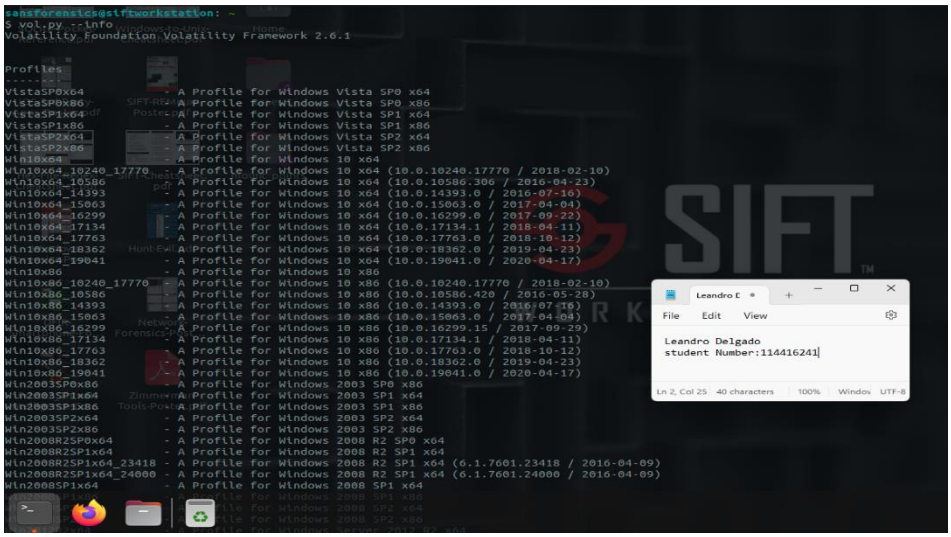
- Analyze memory dump with Volatility forensics framework.
  - Find Operating System information from the memory dump.
  - List all running process.
  - List all open DLLs.
  - Recover DDLs.
  - List network connections that were established at the time of the image acquisition.
  - Find websites that web browsers were connected to at the time of the image acquisition.
- Use different Volatility plugins to find various artifacts.

Lab Instructions

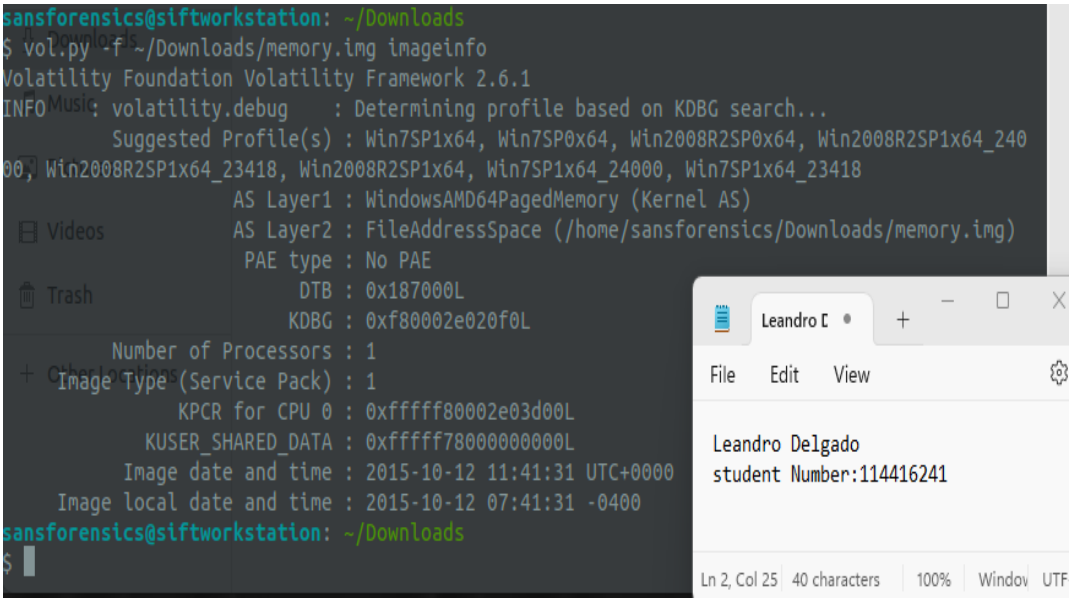
Part 2: Choosing a profile. *Imageinfo* Plugin

All OSs store information in RAM, however, they may use different locations within the memory. We must choose a profile that best identifies the type of OS that helps Volatility in identifying locations that store artifacts and useful information.

1. You may see all supported profiles with the following command:



2. The **imageinfo** plugin gives information about the images used, including the suggested operating system and Image Type (Service Pack), the Number of Processors used, and the date and time of the image.
3. Go to *Desktop* directory where you placed *memory.img* file. At the prompt type the following command and press the "Enter" key to display the operating system information of the computer from which the memory acquisition was performed:



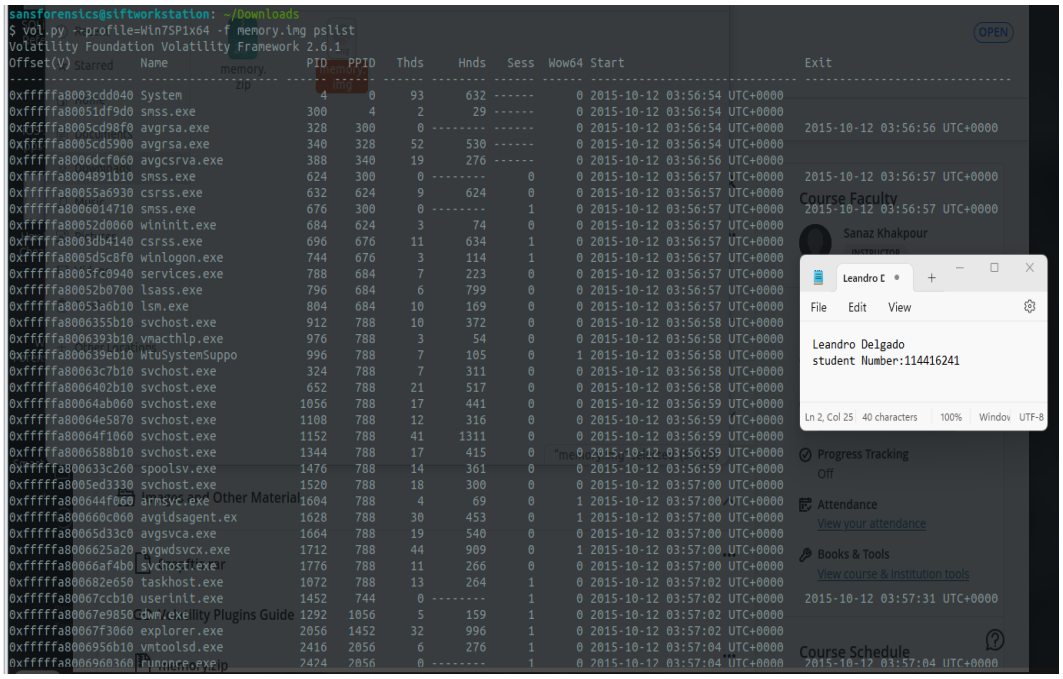
4. Observe, that based on the output, the following information is available:
   a. Operating system was Windows. It was either Win7SP1x64] or Win7SP0x64];
   b. The suggested profiles are: [Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418]
   c. The processor was [64] -----bit processor.
5. This information will be used to run other Volatility commands.

Part 3: Processes running in memory

1. Volatility allows to list of all running processes, but also gives useful information such as the Process ID (PID) and the Parent PID (PPID), and also shows the time the processes were started.

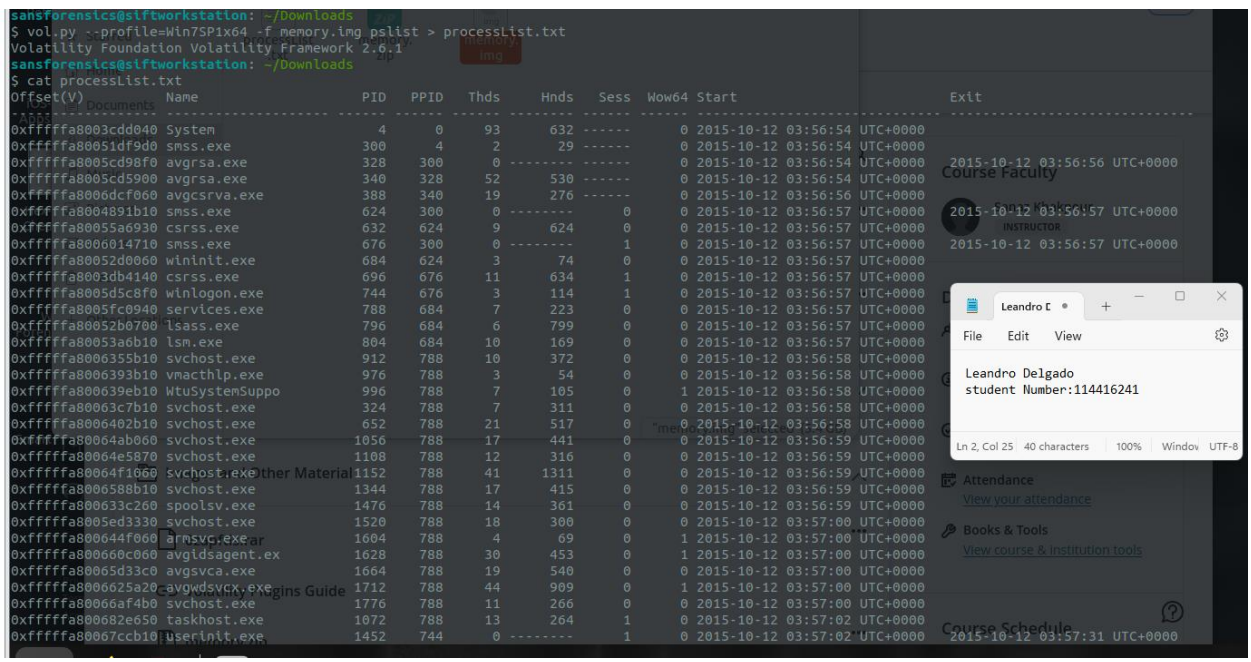
2. At the prompt, type the right plugin and press the "Enter" key to display the list of processes, which were running at the time of the acquisition (It is possible to use the various suggested profiles in a trial-and-error technique. This particular computer was running Win7SP1x64.):

$ volatility –-profile=Win7SP1x64 -f memory.img [Type Plugin] [Screenshot showing the command and the output]



3. Redirect the output to *processList.txt* file using the right command:

$ volatility –-profile=Win7SP1x64 -f memory.img [Command] [Screenshot showing the command and the output]



4. Open your *processlist.txt* file and answer the following question:

Based on the results, which browser(s) were running at the time of the acquisition?

```
0xfffffa8006939b10 chrome.exe          3564   2056     31      765      1      1 2015-10-1
2 11:34:25 UTC+0000
0xfffffa8004639060 chrome.exe          4316   3564      5      166      1      1 2015-10-1
2 11:34:26 UTC+0000
0xfffffa80067e2060 chrome.exe          3120   3564      8      167      1      1 2015-10-1
2 11:34:38 UTC+0000
0xfffffa8006b26b10 iexplore.exe         768   2056     16      542      1      0 2015-10-1
2 11:34:42 UTC+0000
0xfffffa80068cb060 iexplore.exe        4352    768     53      879      1      1 2015-10-1
2 11:34:43 UTC+0000
0xfffffa8006c6e060 iexplore.exe        3684    768     31      711      1      1 2015-10-1
2 11:35:03 UTC+0000
```

What application was using Process ID 3780?

```
0xfffffa80042a1b10 AcroRd32.exe        3780   4368      7      318      1      1 2015-10-1
2 11:05:26 UTC+0000
```

What application was used to acquire the contents of memory?

```
0xfffffa8006fb5270 FTK Imager.exe      3460   2056     14      375      1      1 2015-10-1
2 11:41:01 UTC+0000
sansforensics@siftworkstation: ~/Downloads
$
```

Part 4: Use *the* Plugin to List Dynamic Link Libraries (DLLs)

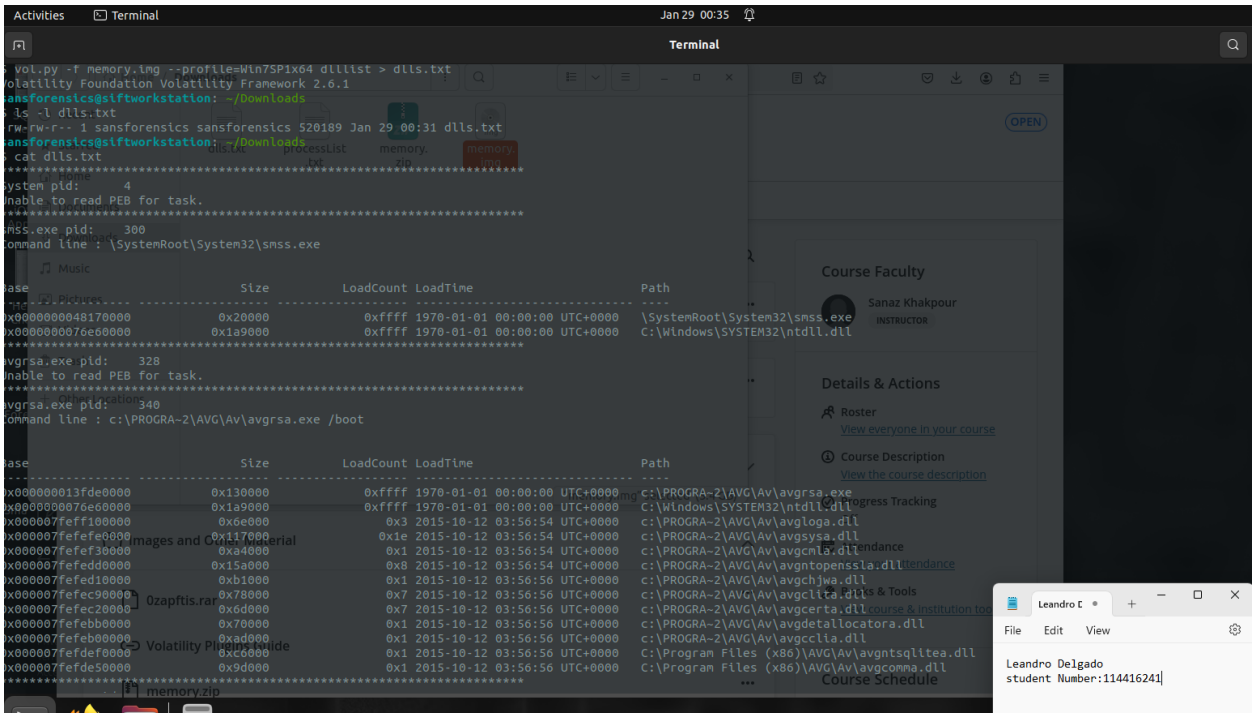
1. At the prompt, type the right command and press the "Enter" key to display the list of DLLs, which were running at the time of the acquisition:
   $ volatility -f memory.img --profile=Win7SP1x64 **[Command]** [Screenshot showing the command and the output]

```
sansforensics@siftworkstation: ~/Downloads
$ vol.py -f memory.img --profile=Win7SP1x64 dlllist
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
System pid:      4
Unable to read PEB for task.
************************************************************************
smss.exe pid:    300
Command line : \SystemRoot\System32\smss.exe

Base                             Size          LoadCount LoadTime                       Path
---------------- ---------- ---------- ------------------------------ ----
0x0000000048170000           0x20000            0xffff 1970-01-01 00:00:00 UTC+0000   \SystemRoot\
System32\smss.exe
0x0000000076e60000           0x1a9000           0xffff 1970-01-01 00:00:00 UTC+0000   C:\Windows\S
YSTEM32\ntdll.dll
************************************************************************
avgrsa.exe pid:    328
Unable to read PEB for task.
************************************************************************
avgrsa.exe pid:    340
Command line : c:\PROGRA~2\AVG\Av\avgrsa.exe /boot

Base                             Size          LoadCount LoadTime
---------------- ---------- ---------- ------------------------------
0x000000013fde0000           0x130000           0xffff 1970-01-01 00:00:00 UTC+0000   c:\PROGRA~2\
```

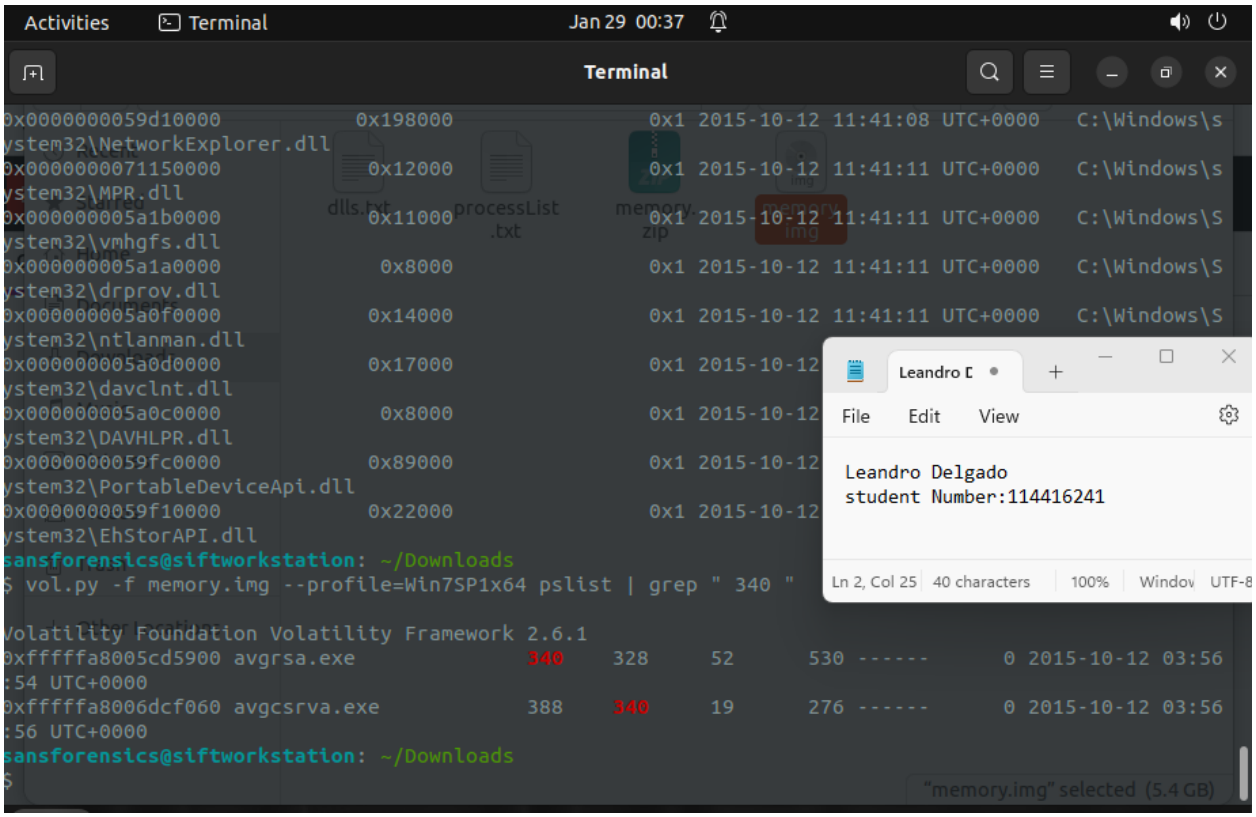
```
Leandro D
File   Edit   View

Leandro Delgado
student Number:114416241

Ln 2, Col 25   40 characters   100%   Win
```

Redirect the list of DDLs to a file called dlls.txt

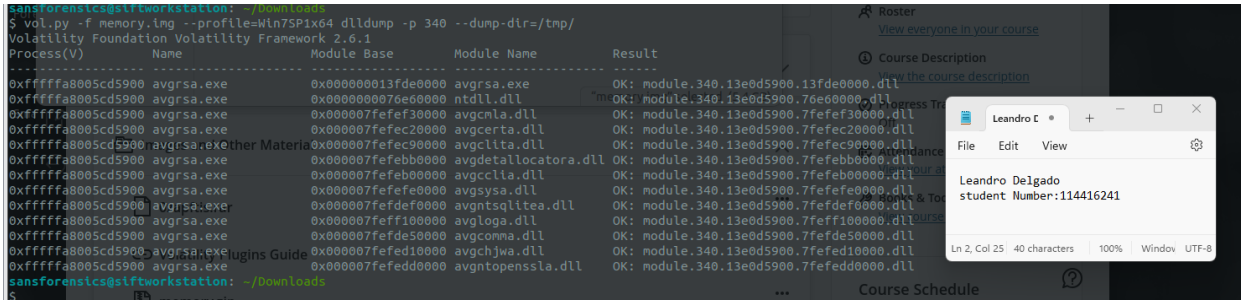
2. Open the text file named dlls.txt to see the results. [Screenshot showing the command and the output]



3. Recover the DLLs from memory for *Process ID 340*, i.e., *smss.exe*, and store them in the temporary directory, type the right command at the prompt and press the “Enter” key:



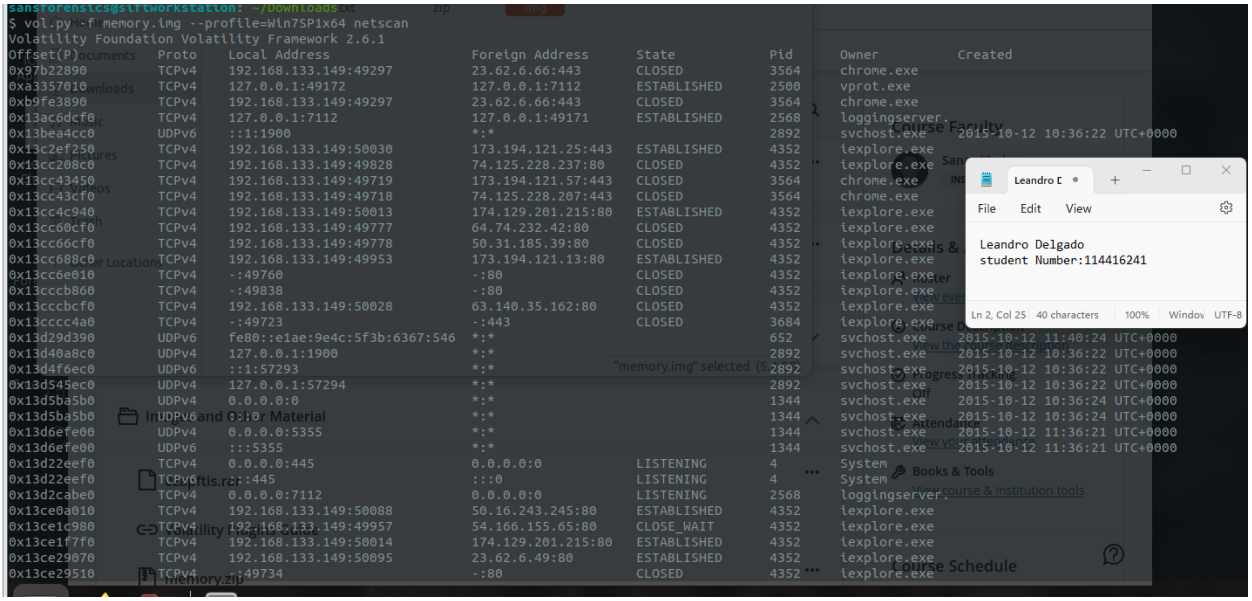
4. List all recovered DLLs:



5. Malware scans and reverse engineering can be performed on the recovered DLL files.

Part 5: Network Connections Analysis

1. At the prompt, type the right command and press the “Enter” key to display the list of the network connections, which were established at the time of the acquisition. Output the connections to a file names netscan.txt and screenshot the results.



2. Find out what internet website Windows Internet Explorer was connected to (IP address: 173.194.121.25) using IP lookup tool at http://whatismyipaddress.com/ip-lookup [Answer]