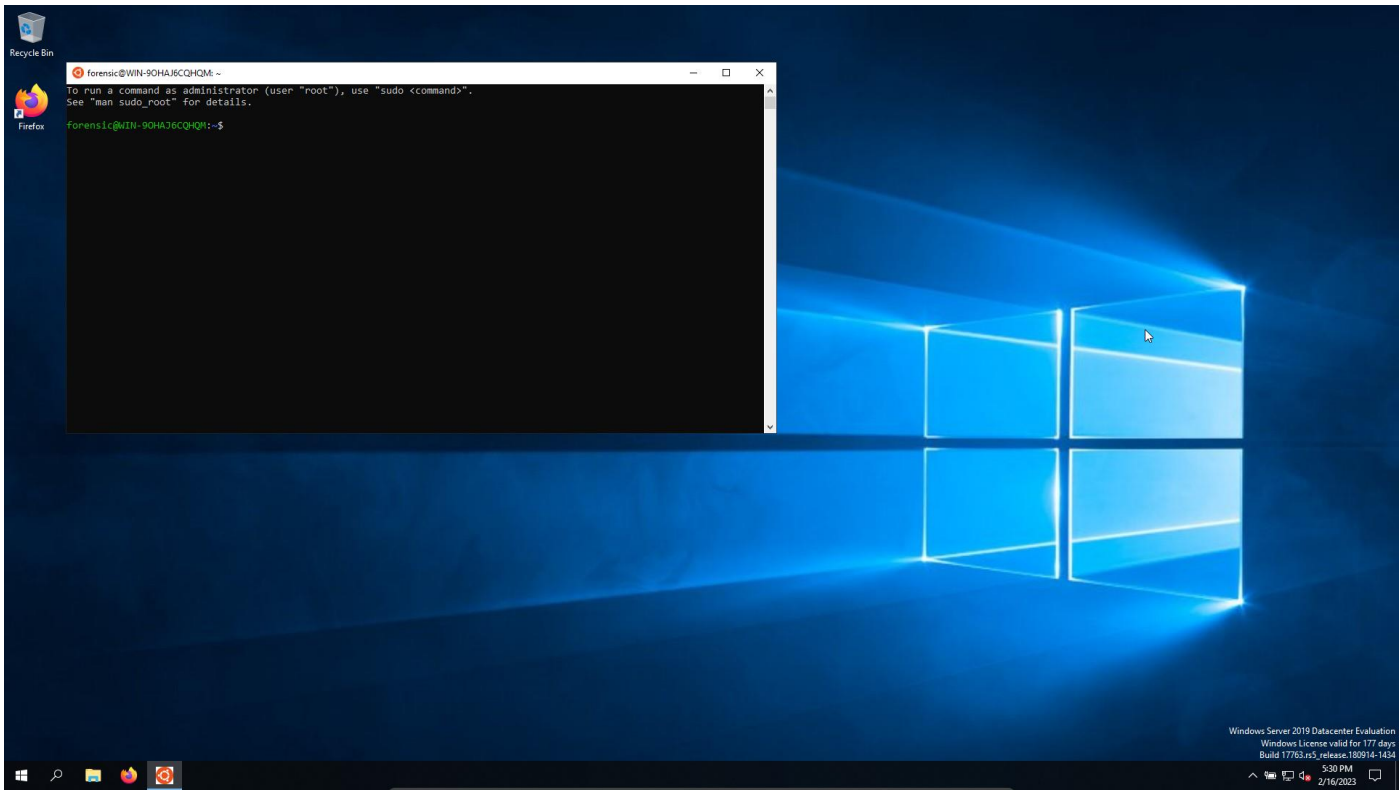
Forensic analysis of Random Access Memory:

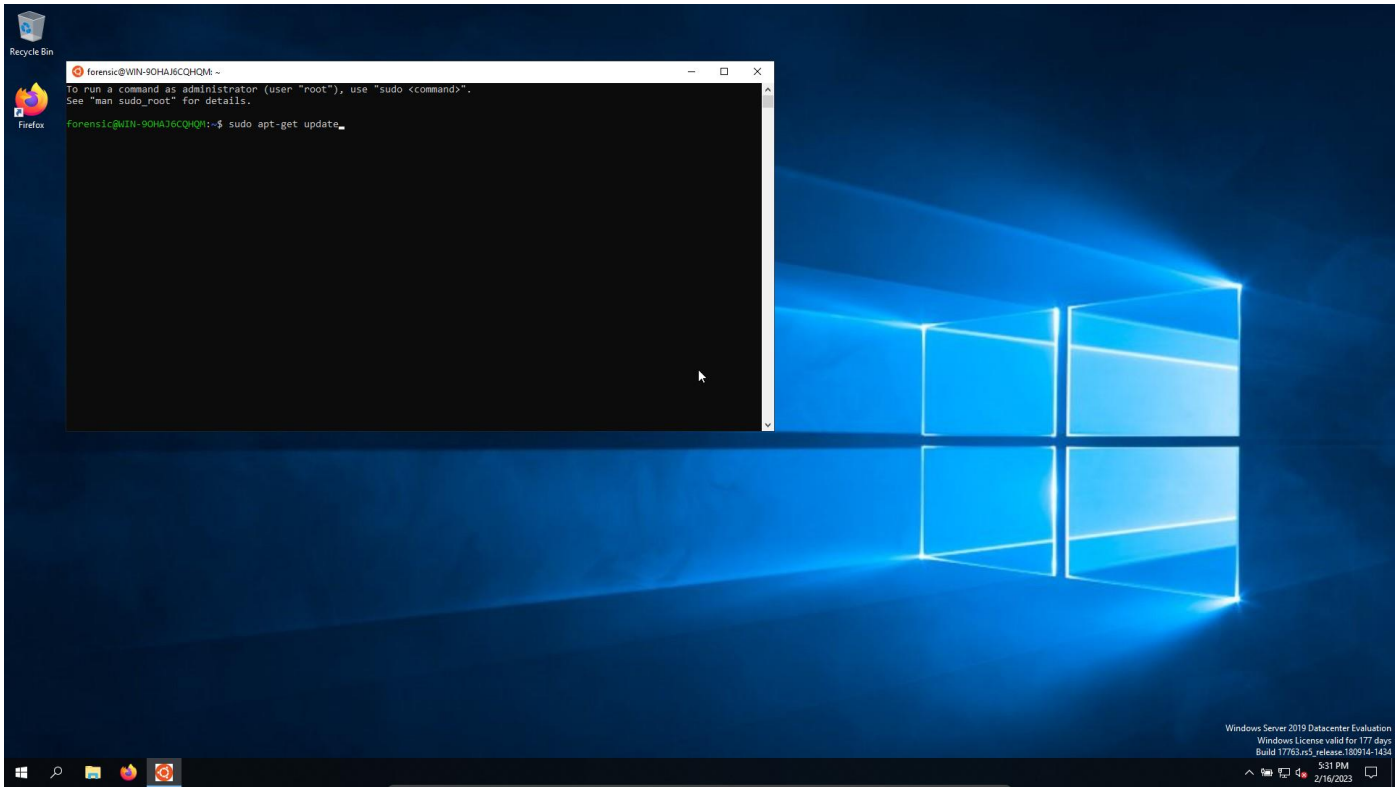
- Installing Volatility3
- Important files for memory analysis
- Windows system information
- Suspicious processes
- Dumping processes
- Injected DLLs
- Process owners
- Malicious registry key entries

Installing Volatility3

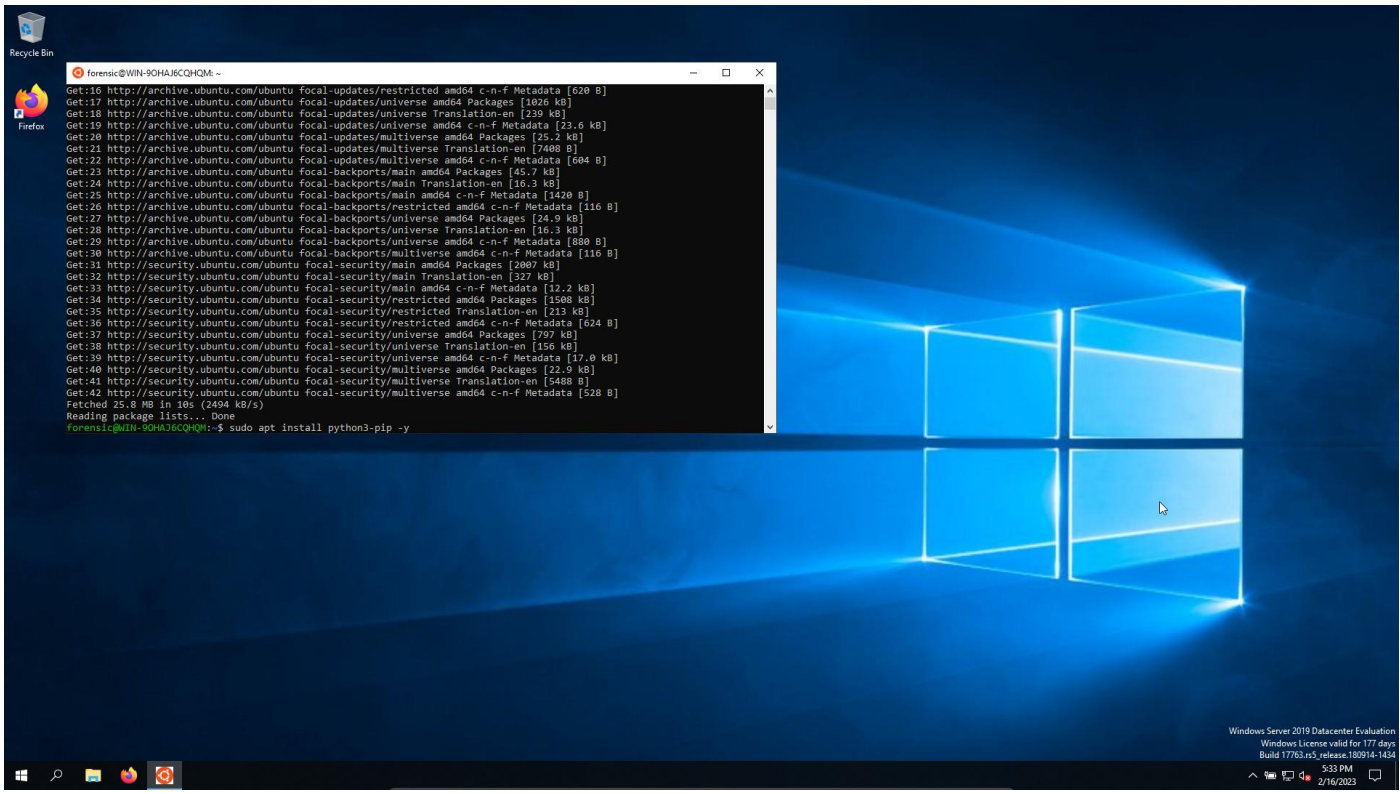
- Installing volatility3 on ubuntu distribution subsystem:



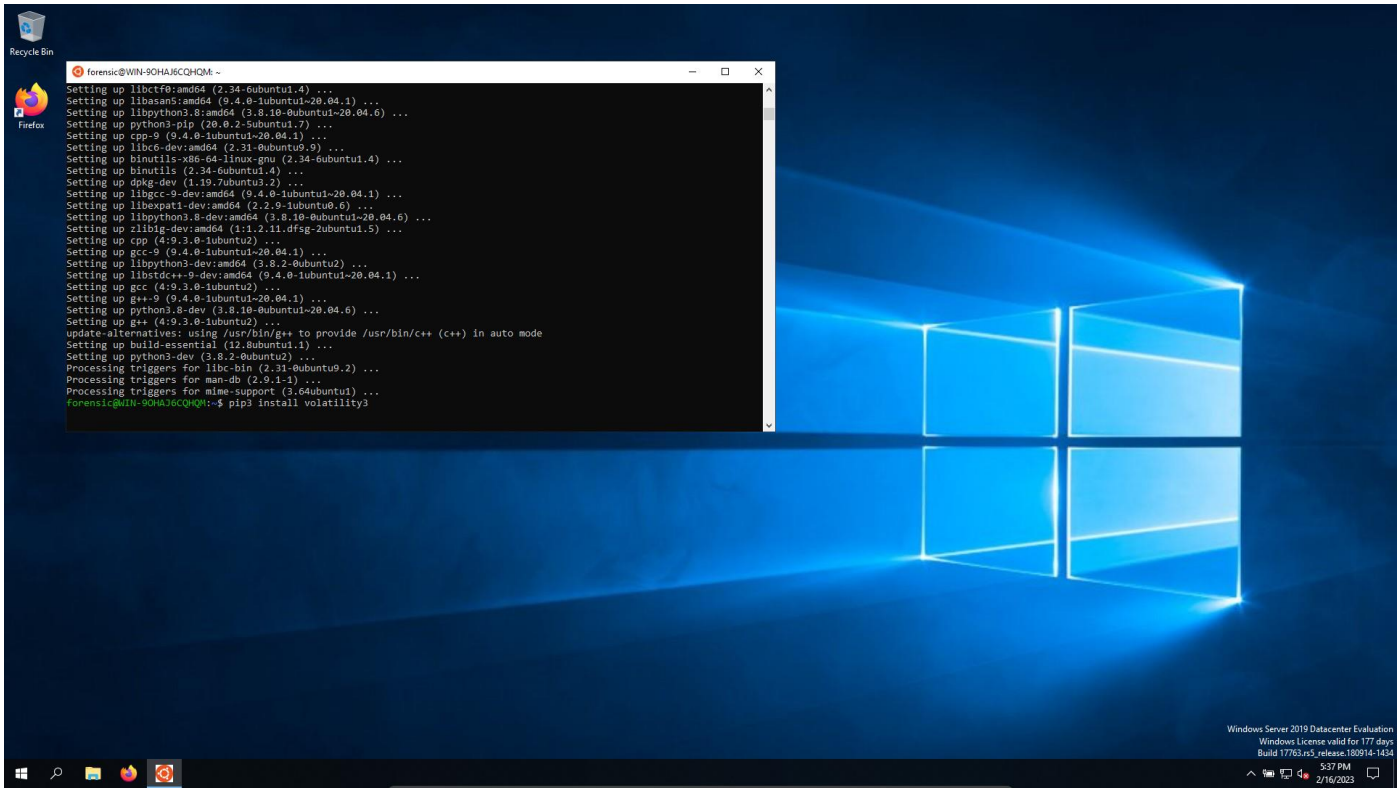
- Update the packets



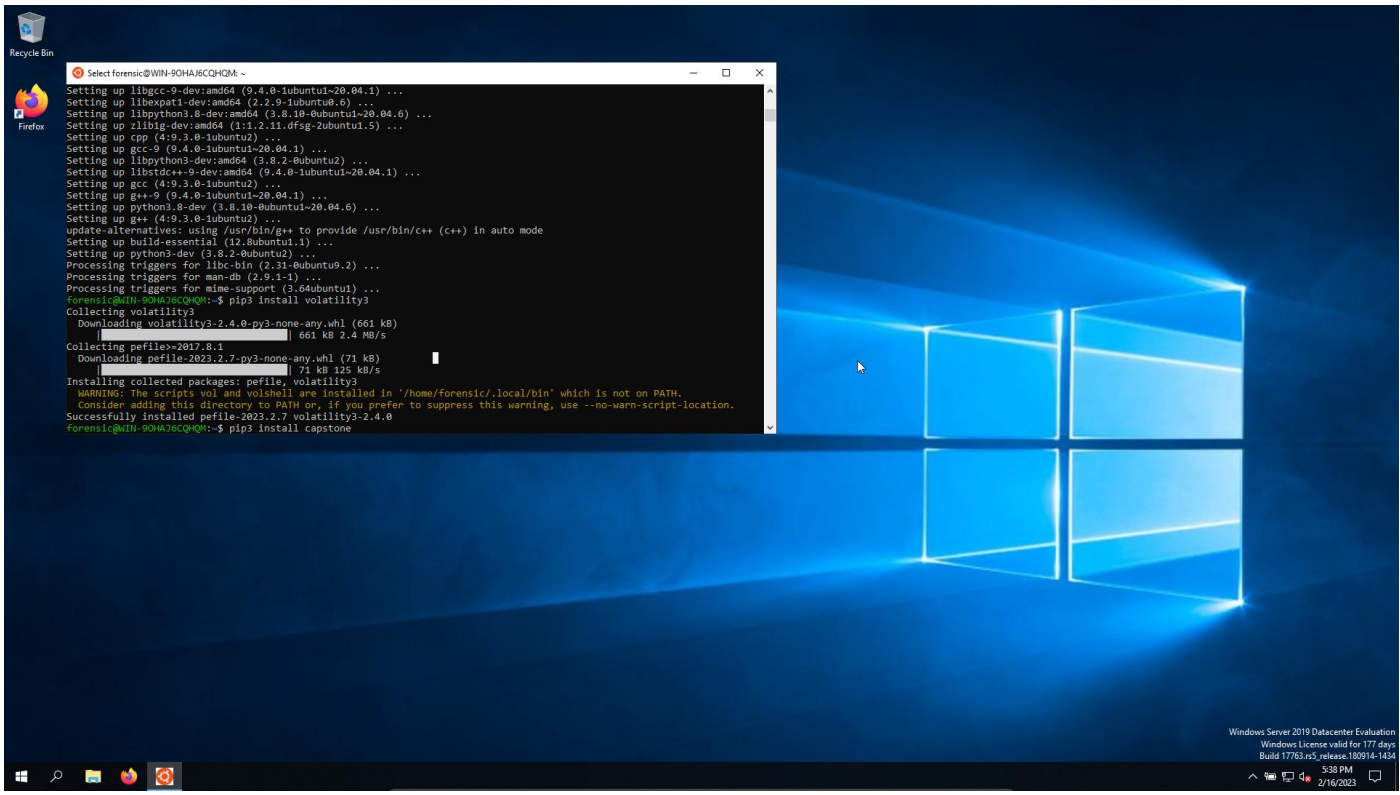
- Pip3



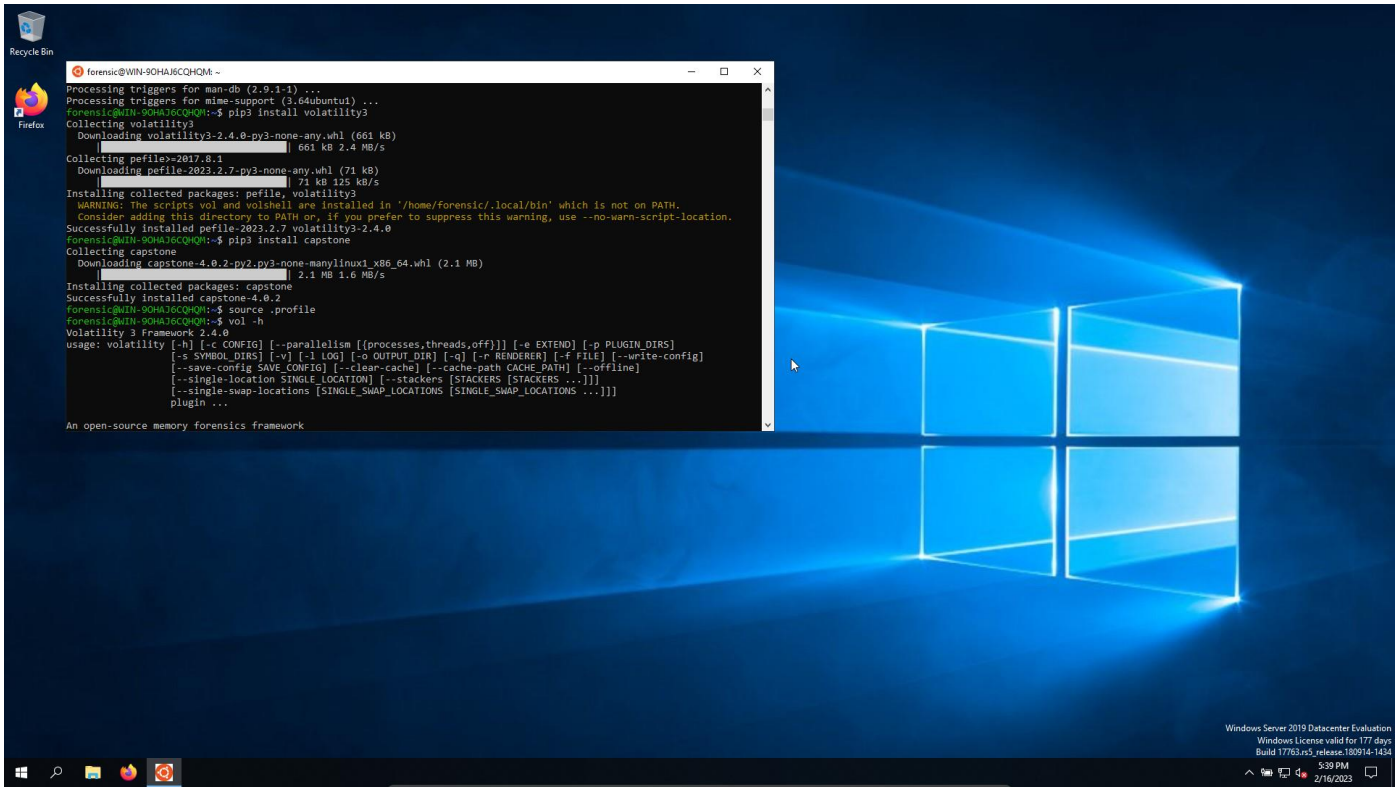
- Volatility3



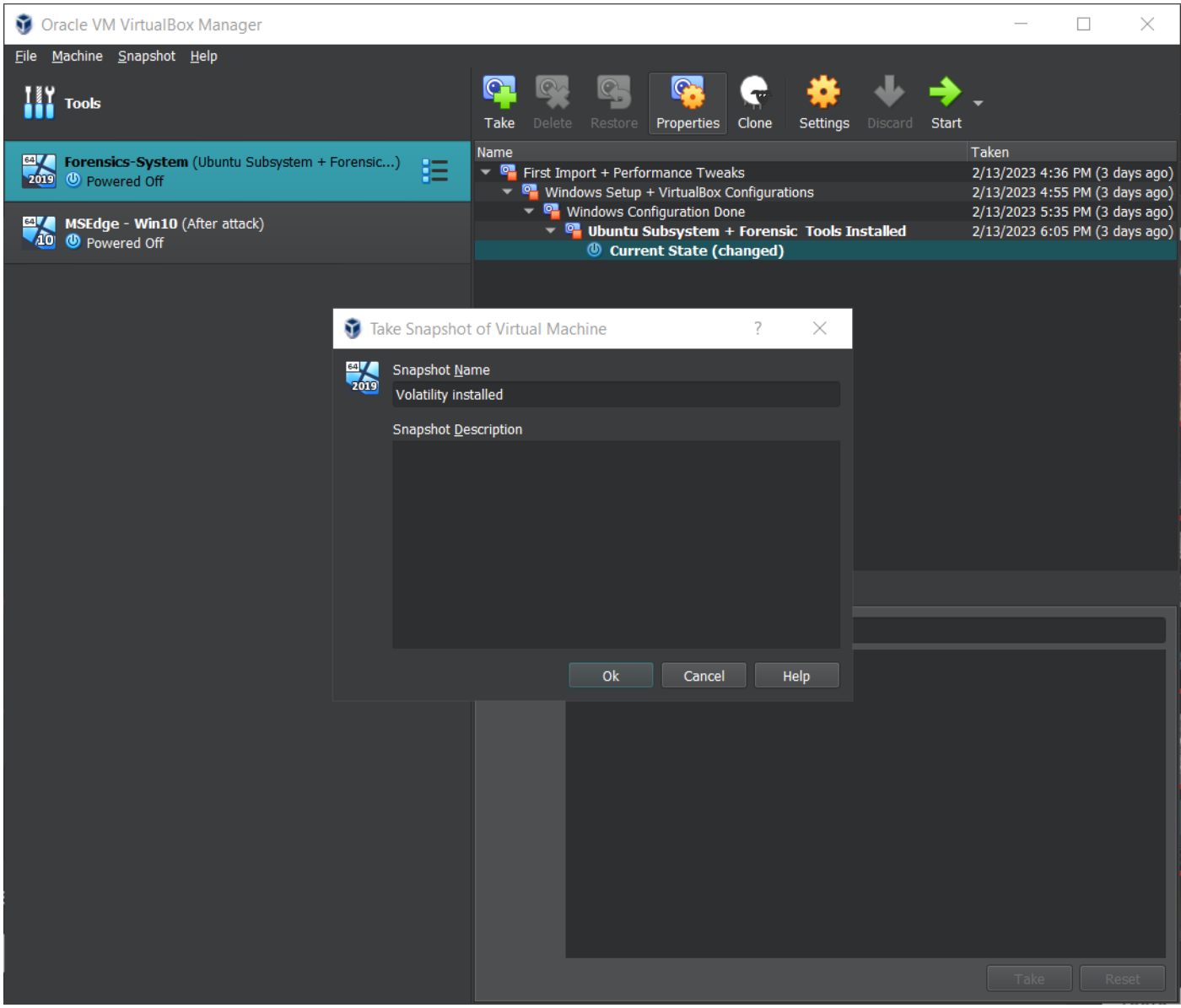
- Plugins for volatility



- Reload the bash profile and check the volatility3.



- Snapshot of the forensic virtual machine:

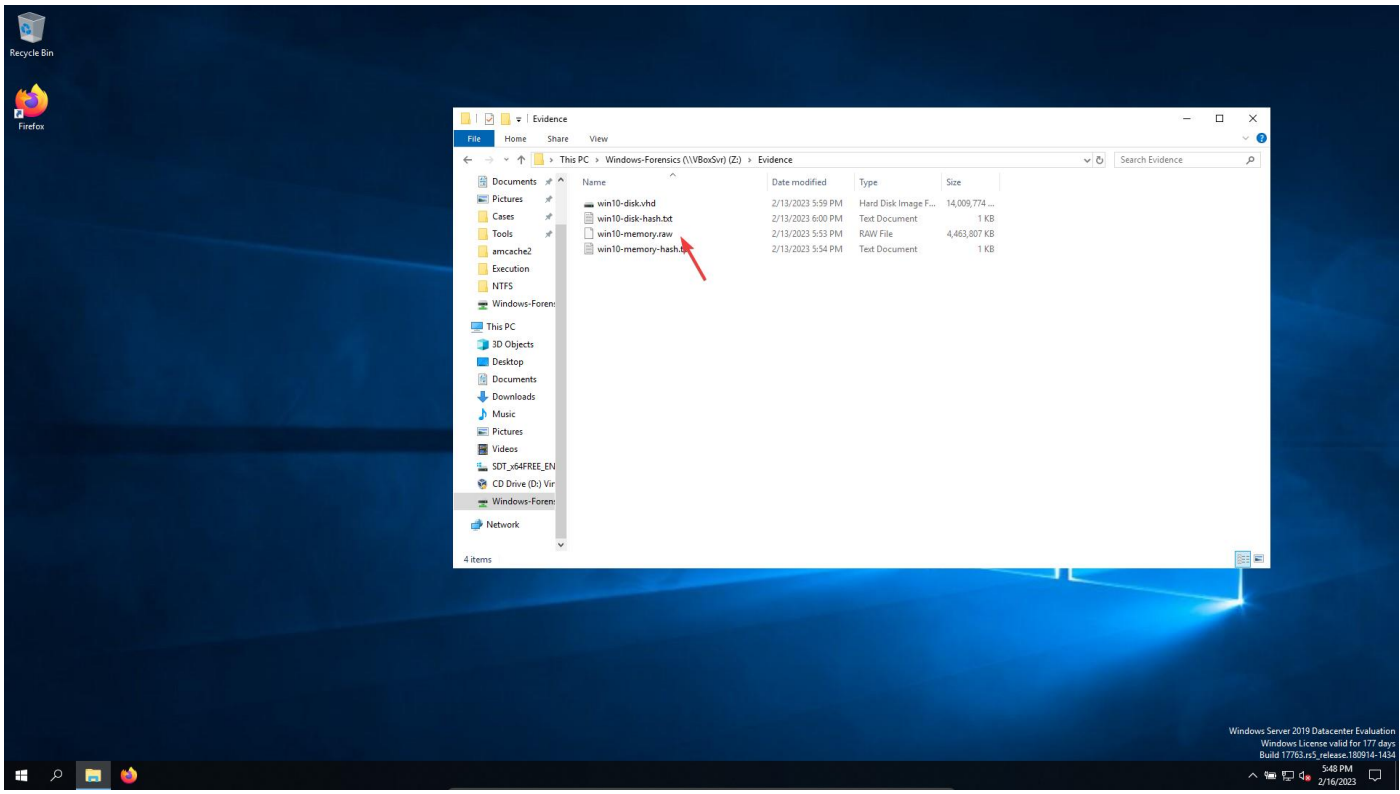


Important files for memory analysis

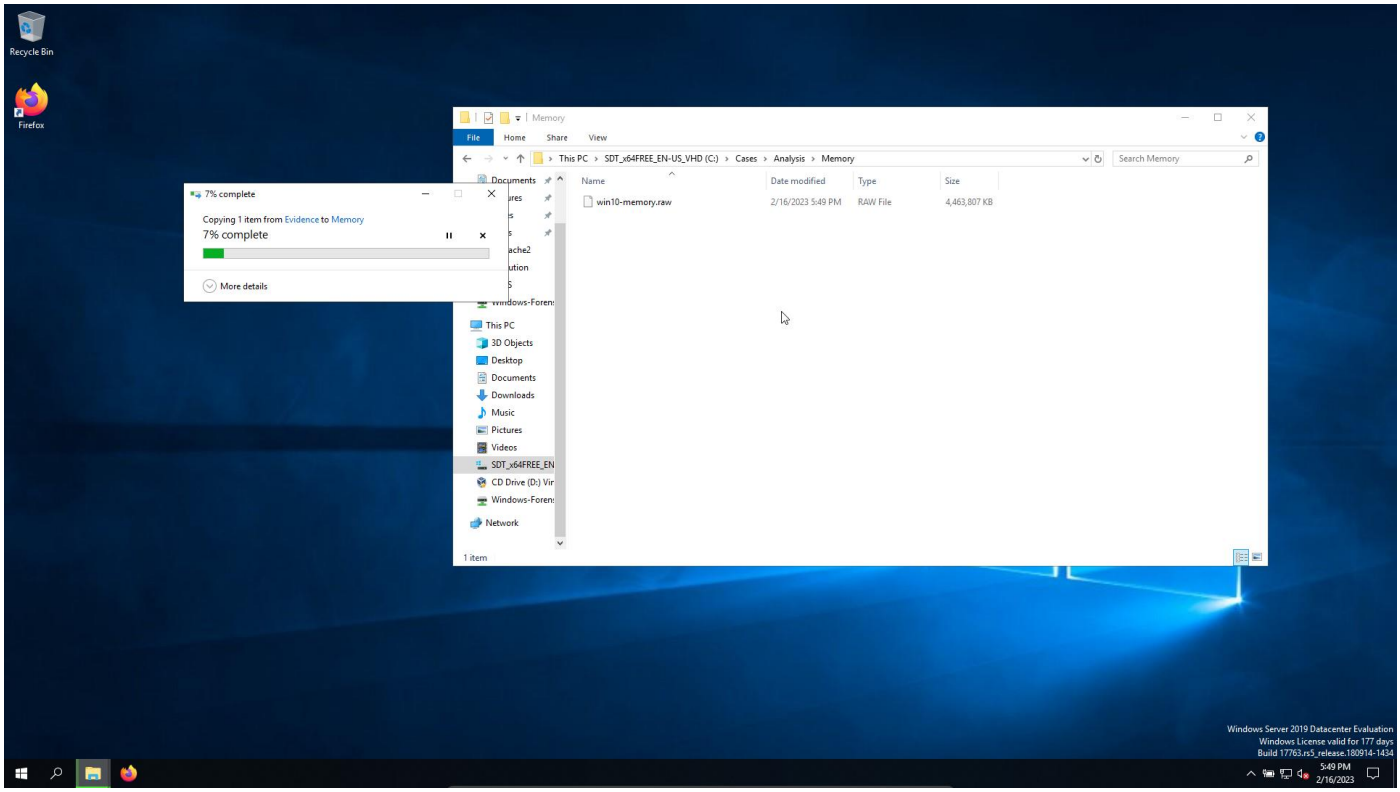
- The memory is volatile data
- Files important for memory analysis:
    - Hiberfil.sys - Hibernation file, Windows creates this file when you put your computer to sleep , it will write the memory to the disk , so it can load the memory faster. Volatility can read this kind of file, memory analysis can be done without the RAM image of a computer system.

- Pagefile.sys and Swapfile.sys , exists for saving some space .

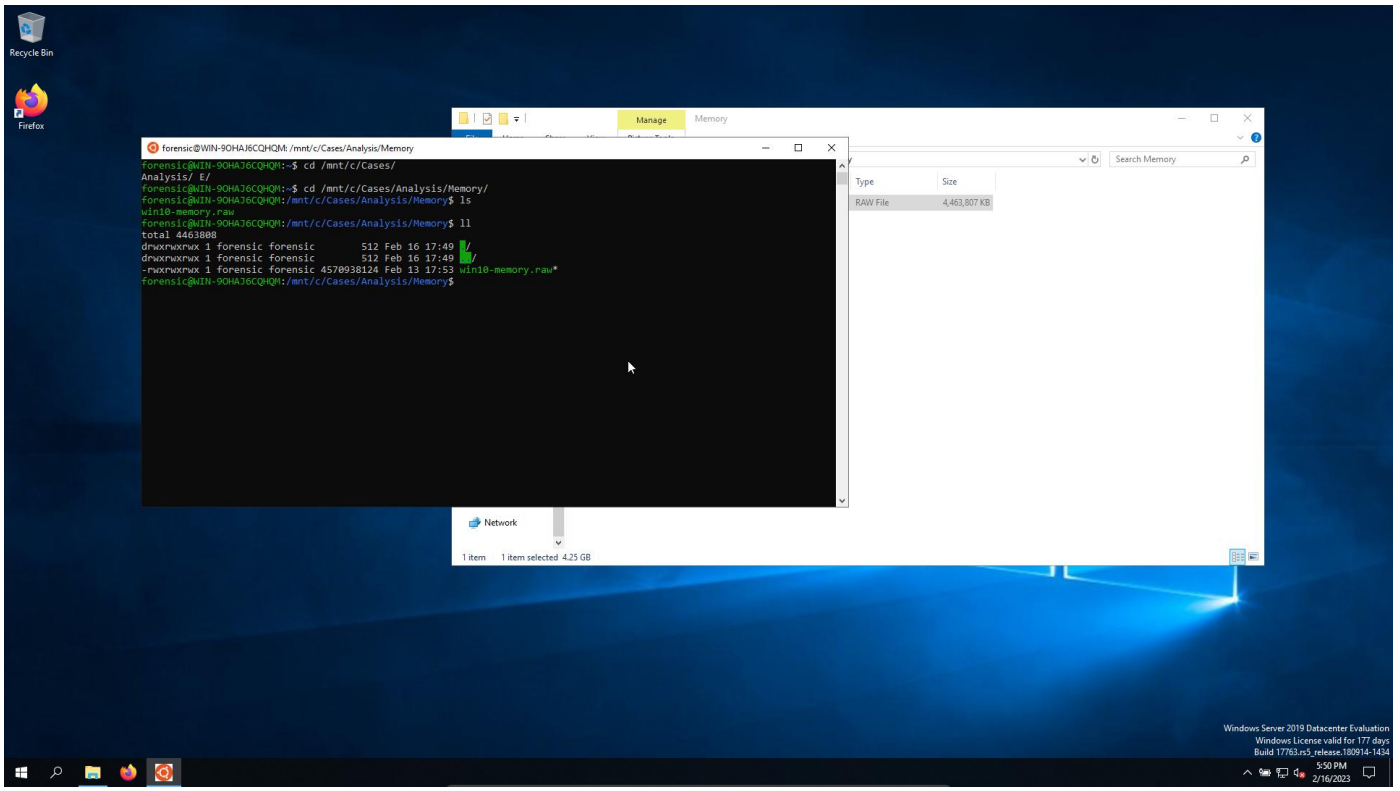
- Acquired memory iamge evidence:



- Copy image to the Case\Analysis\Memory\ to have it on the system.

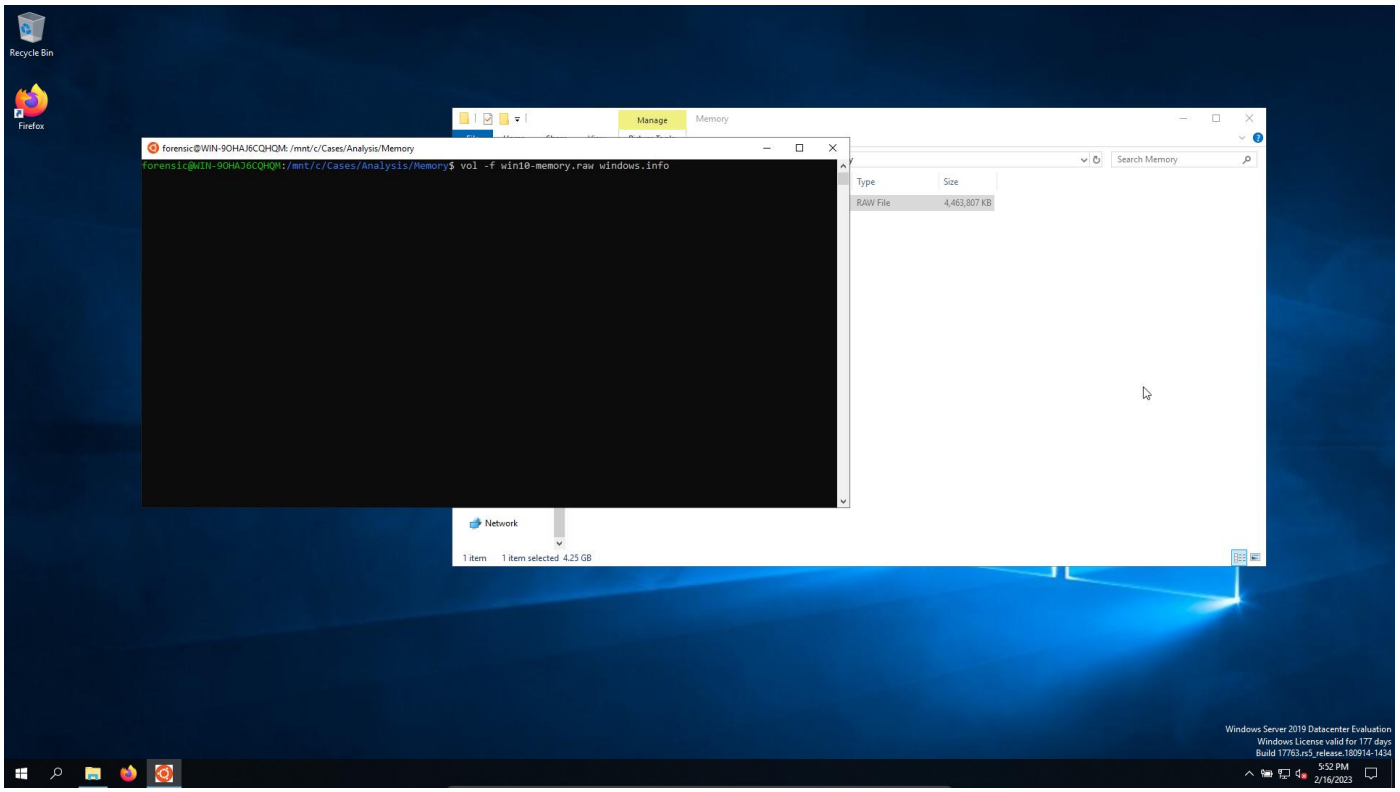


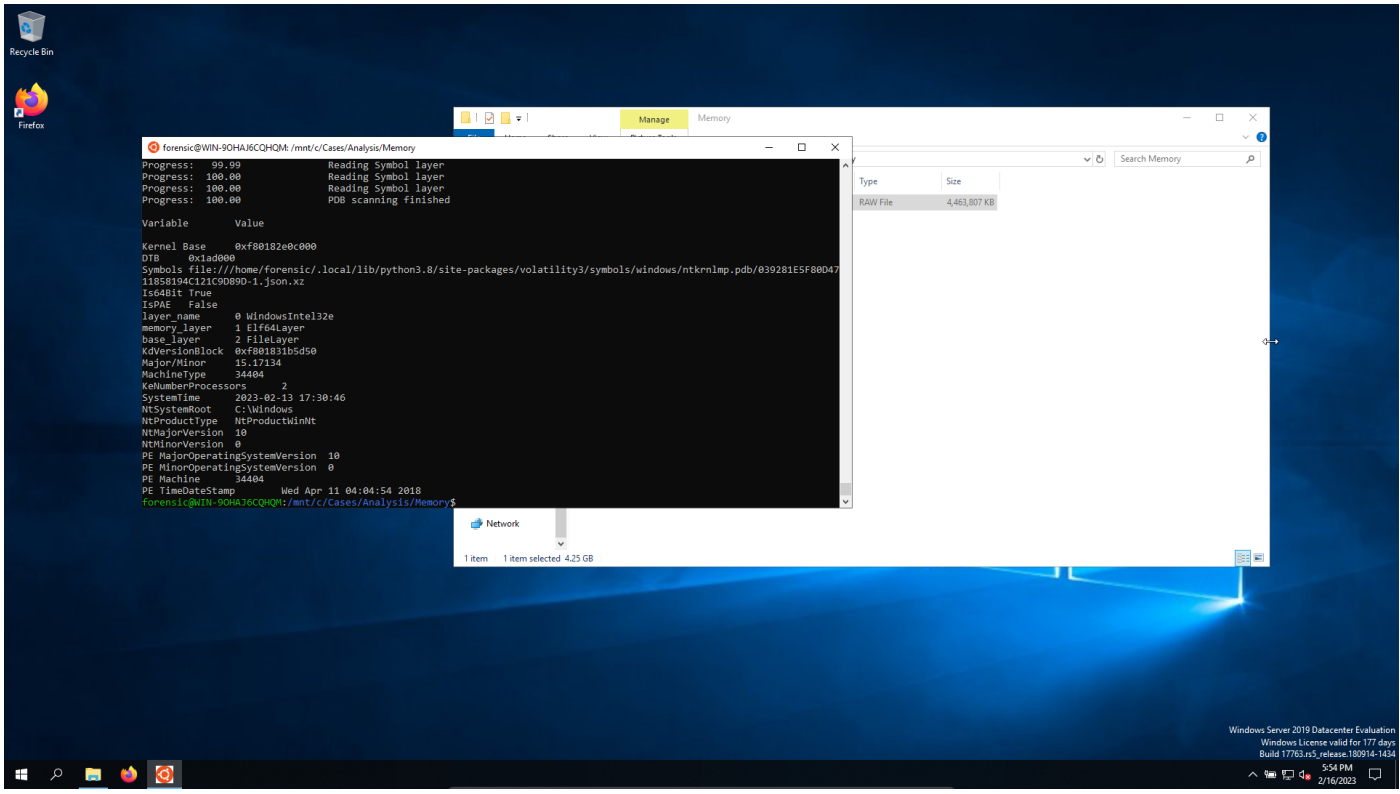
- Go to the location of the memory file, in ubuntu subsystem:



Windows system information

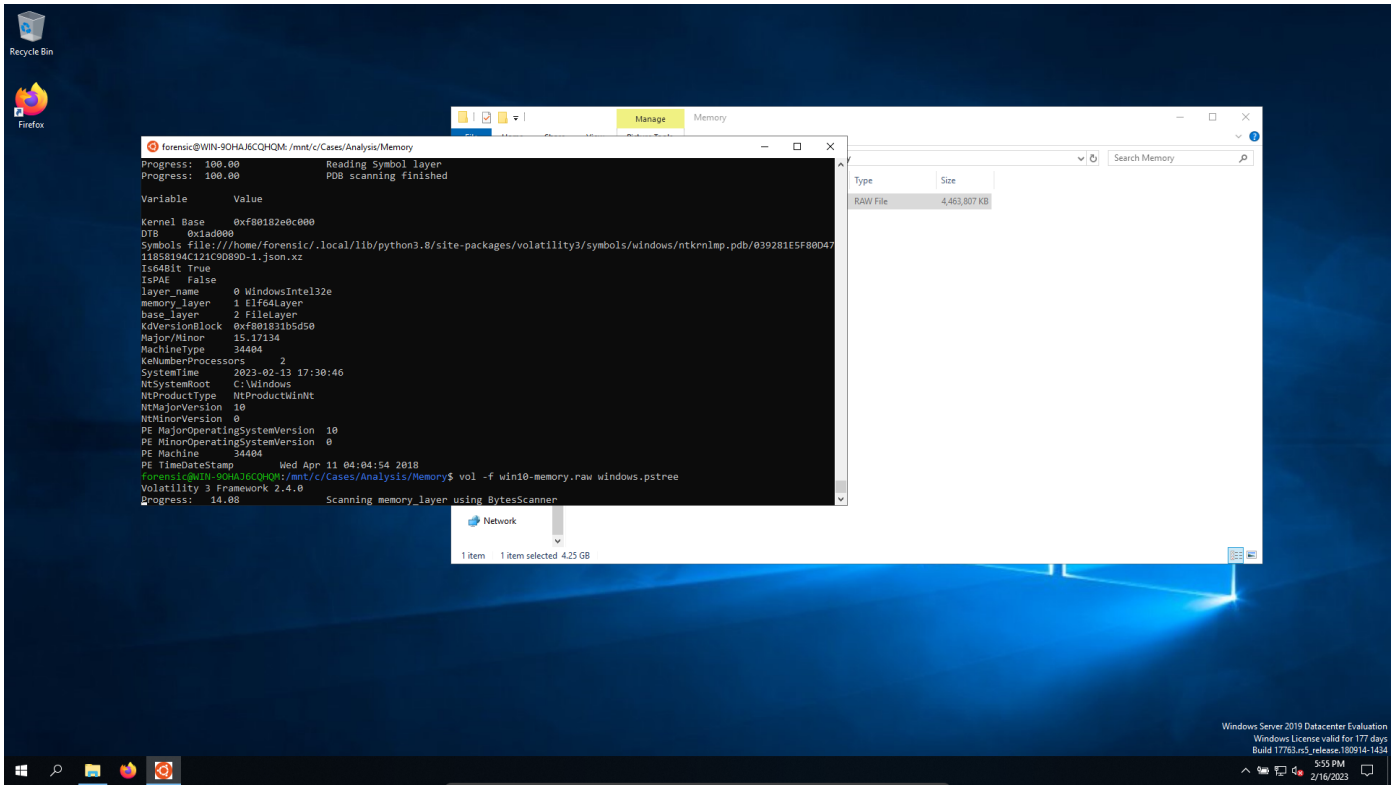
- With volatility3 , the profile is no longer needed to give as a command argument, it searches and downloads the specific symbol table needed and profile.
- Volatility3 plugin for windows system information:

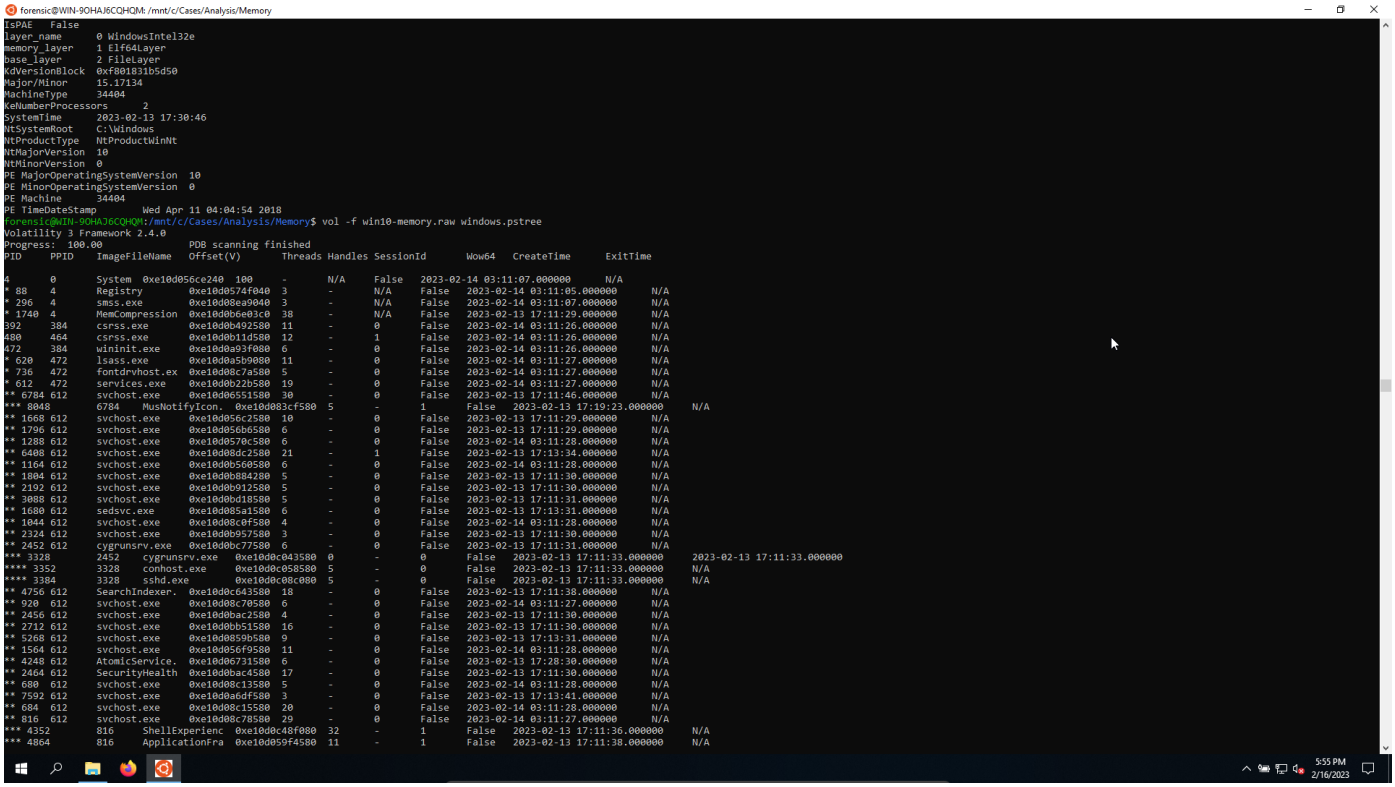




Suspicious processes

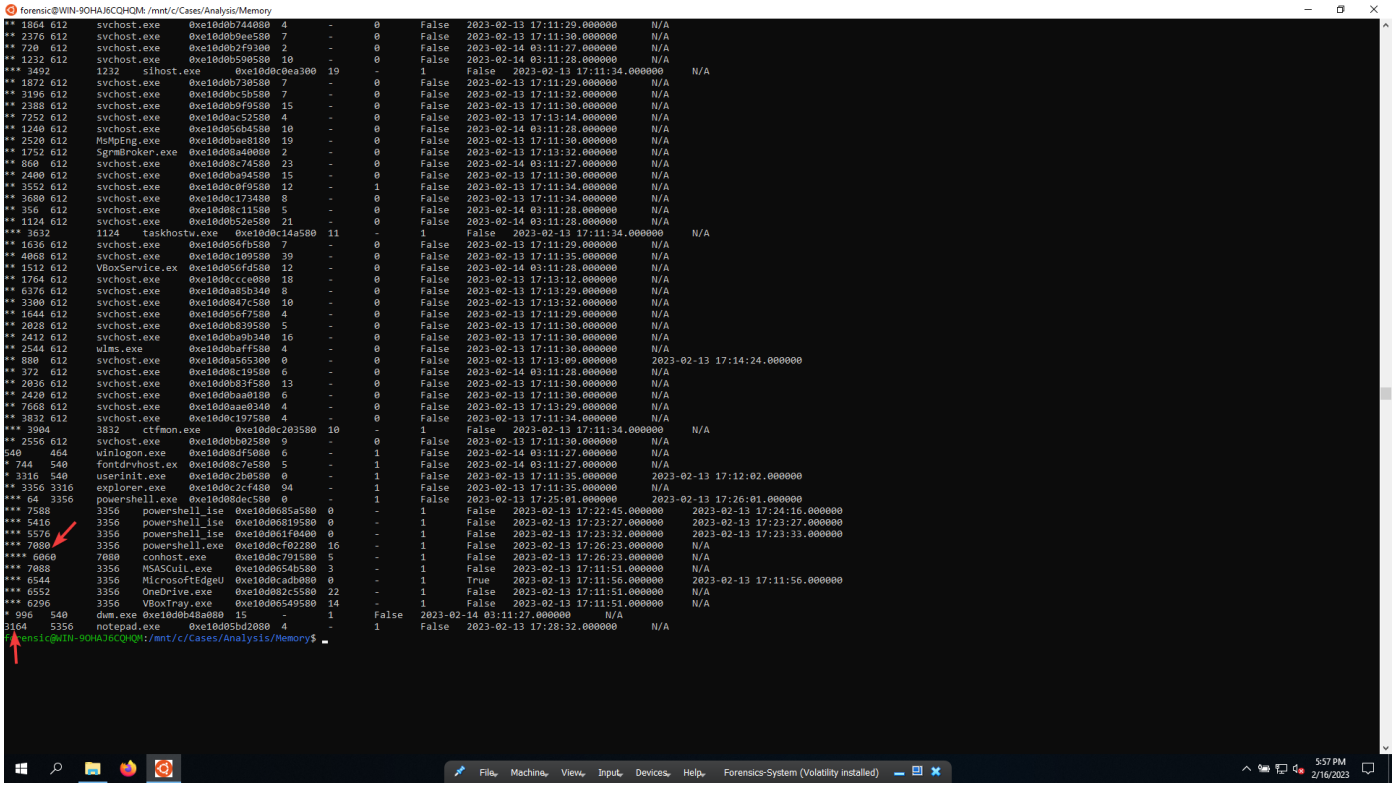
- See the process tree :





- Put output into a text file for easier search:

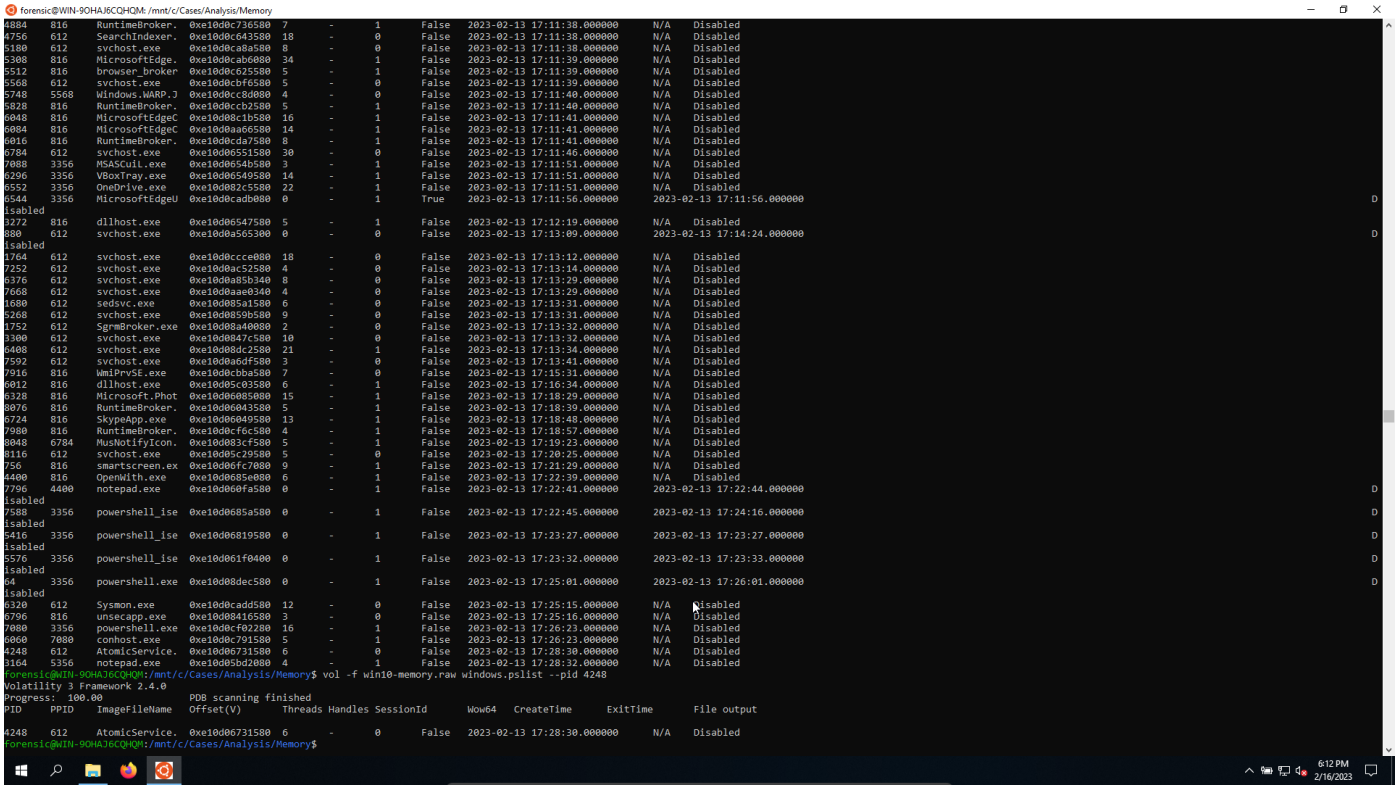
- Search for notepad.exe,AtomicService.exe and powershell.exe pid:



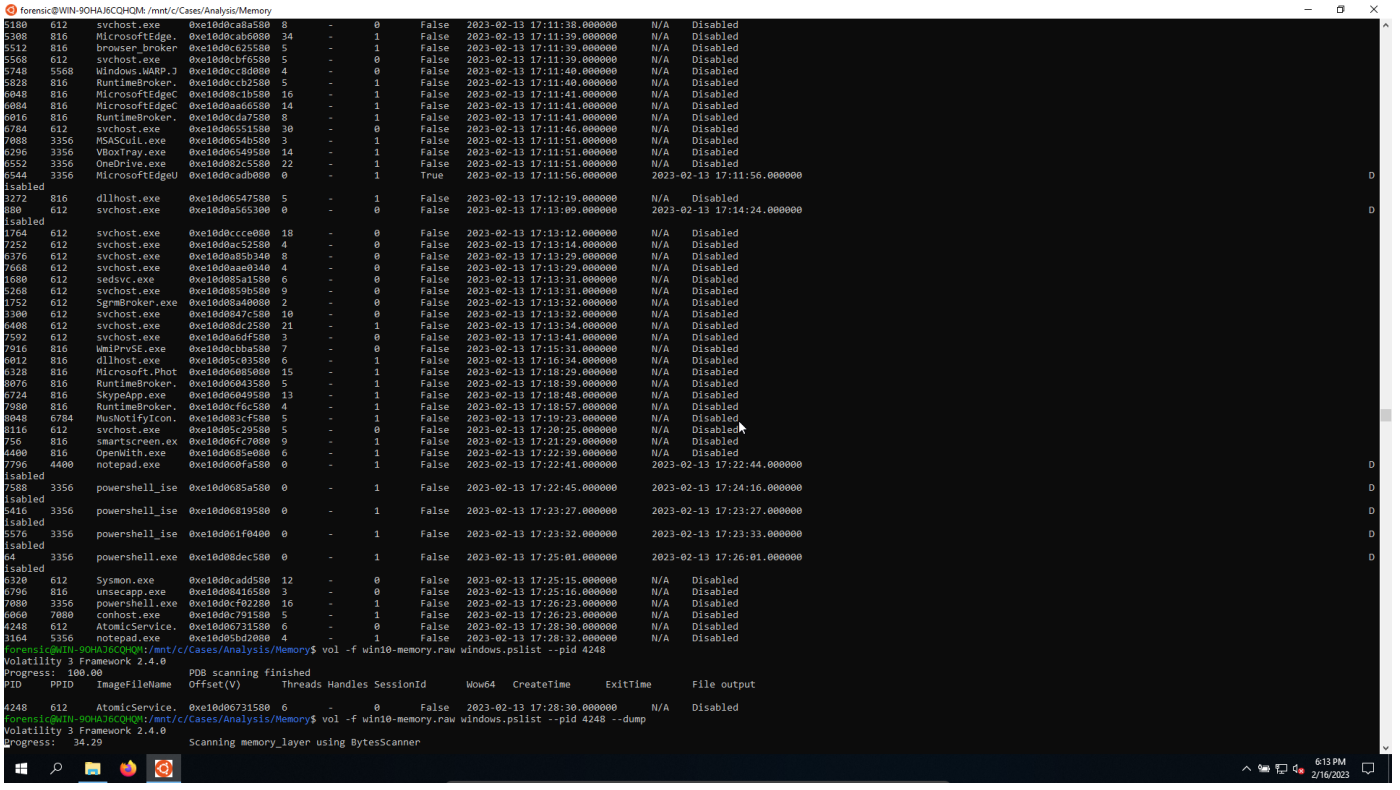
- Pids:
  - Notepad: 3164
  - Powershell:7080
  - AtomicService: 4248

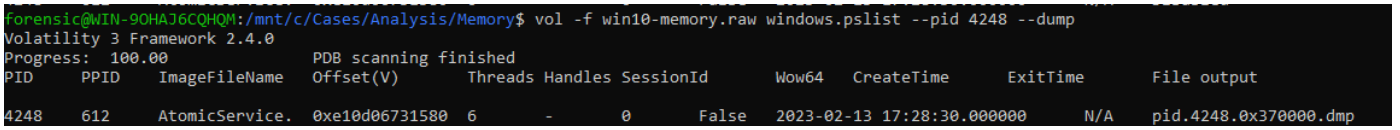
Dumping processes

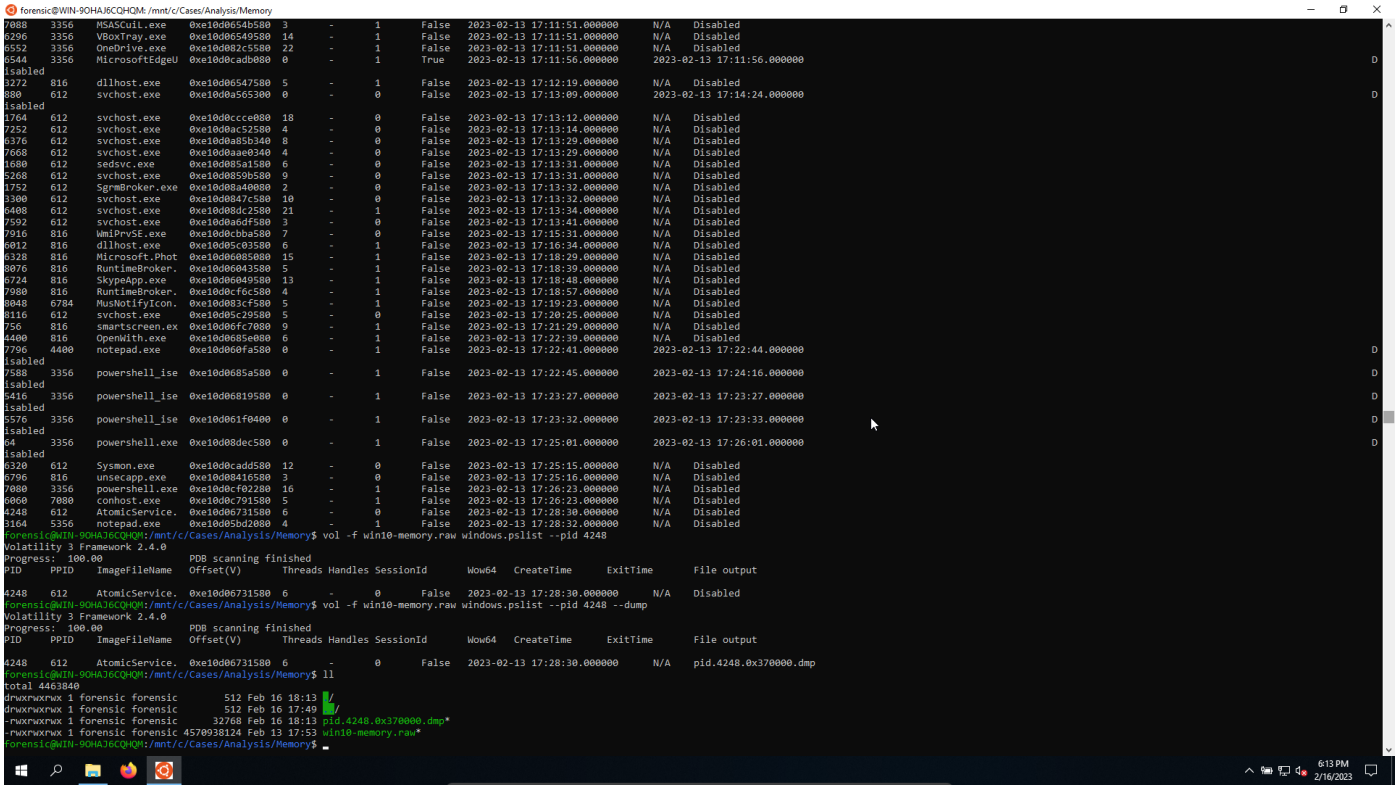
- Printing of a particular processe:



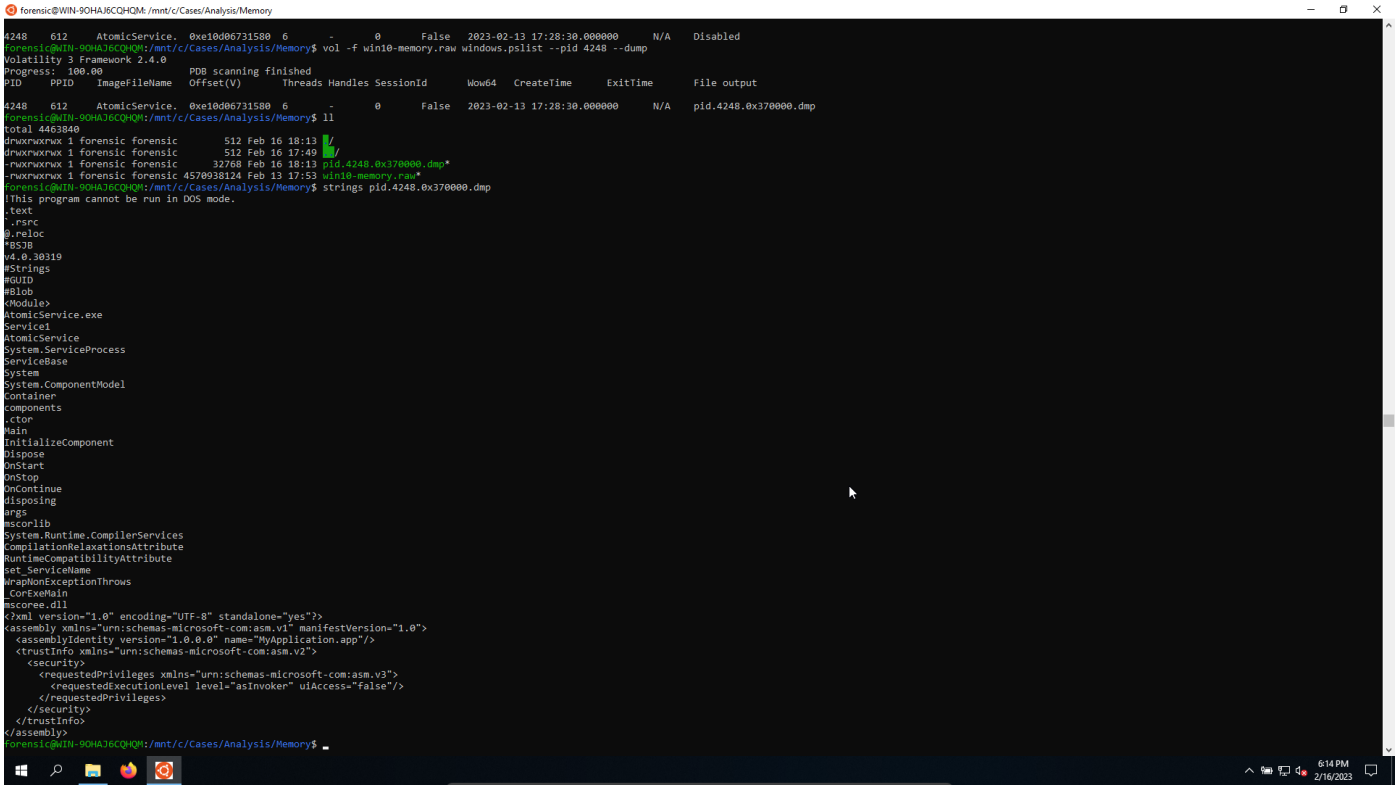
- Dumping a particular process:



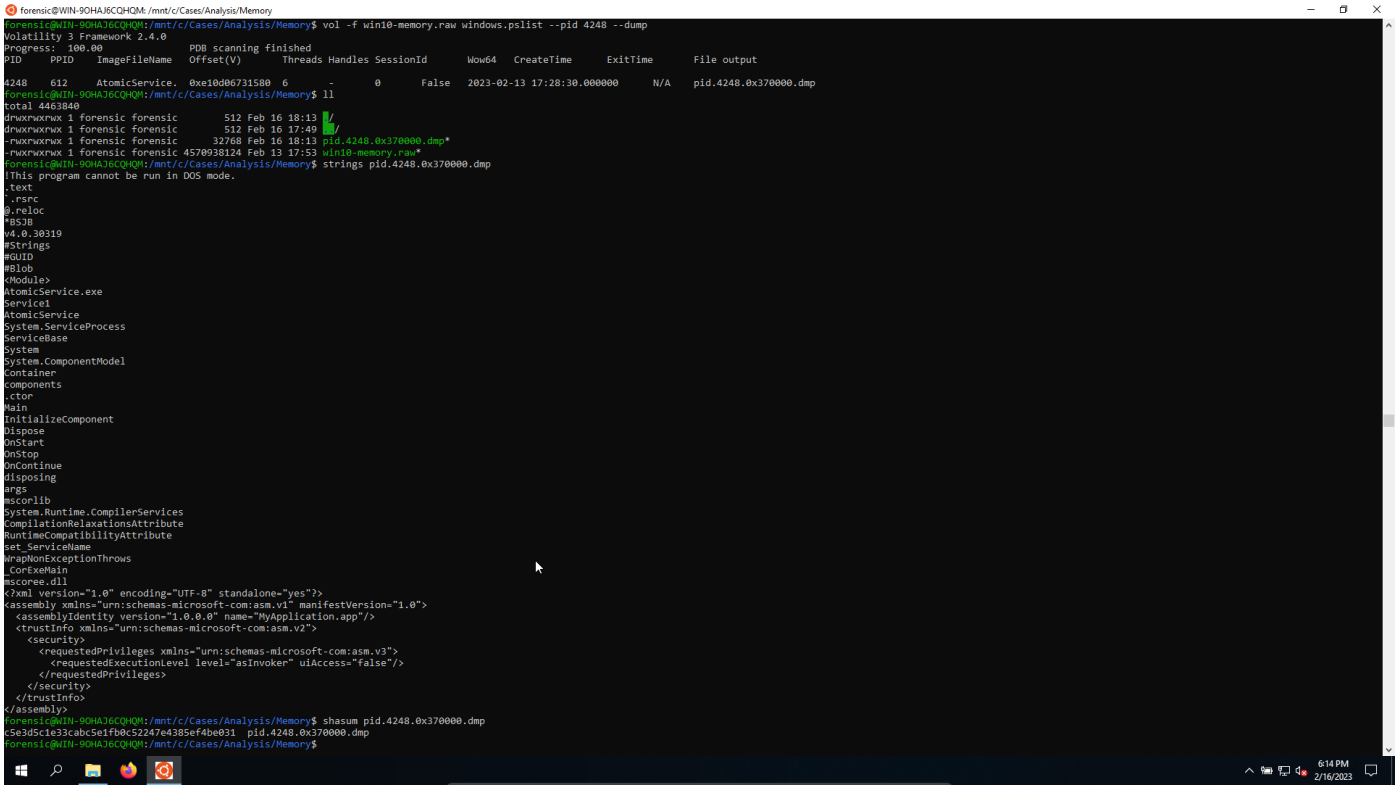




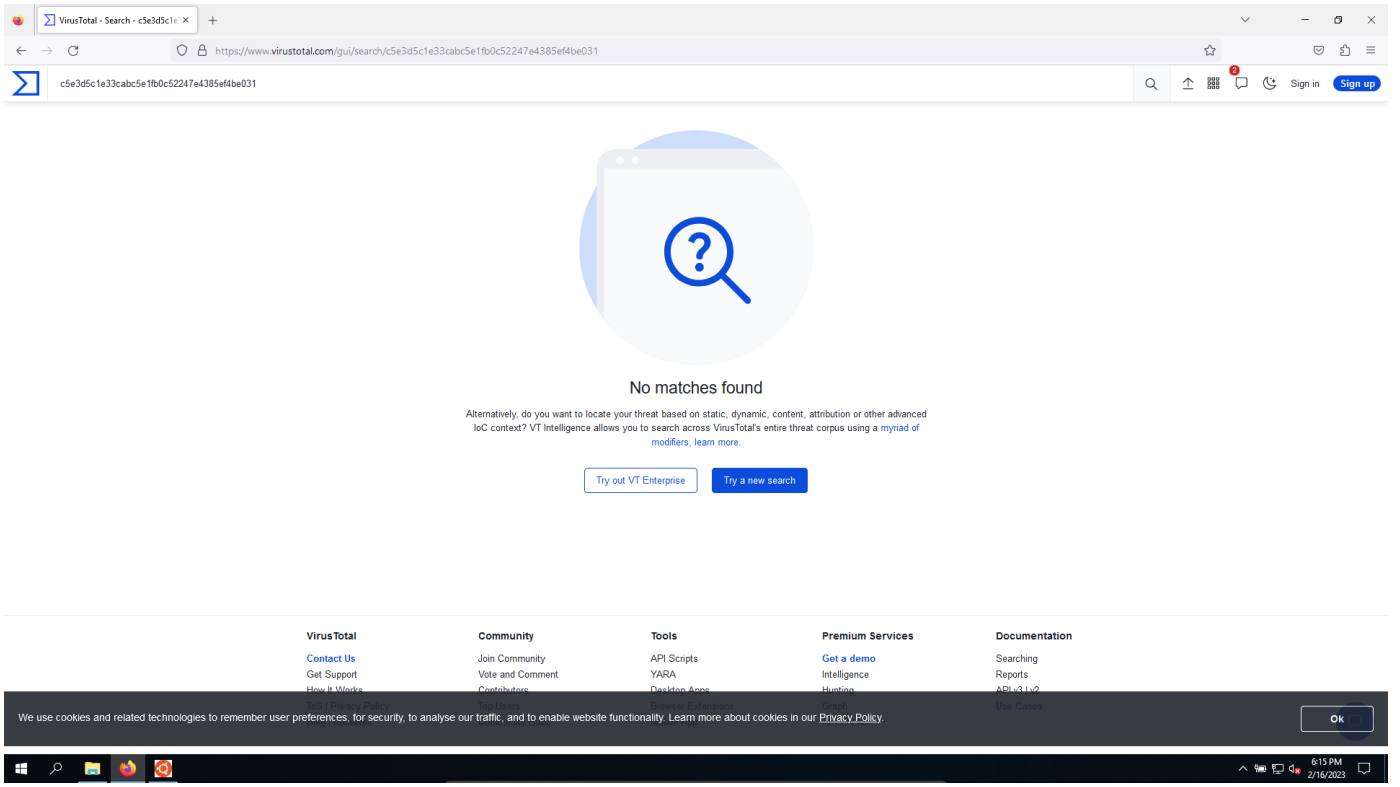
- Analysis of the dump process:



- We could hash the dump and search it on VirusTotal:

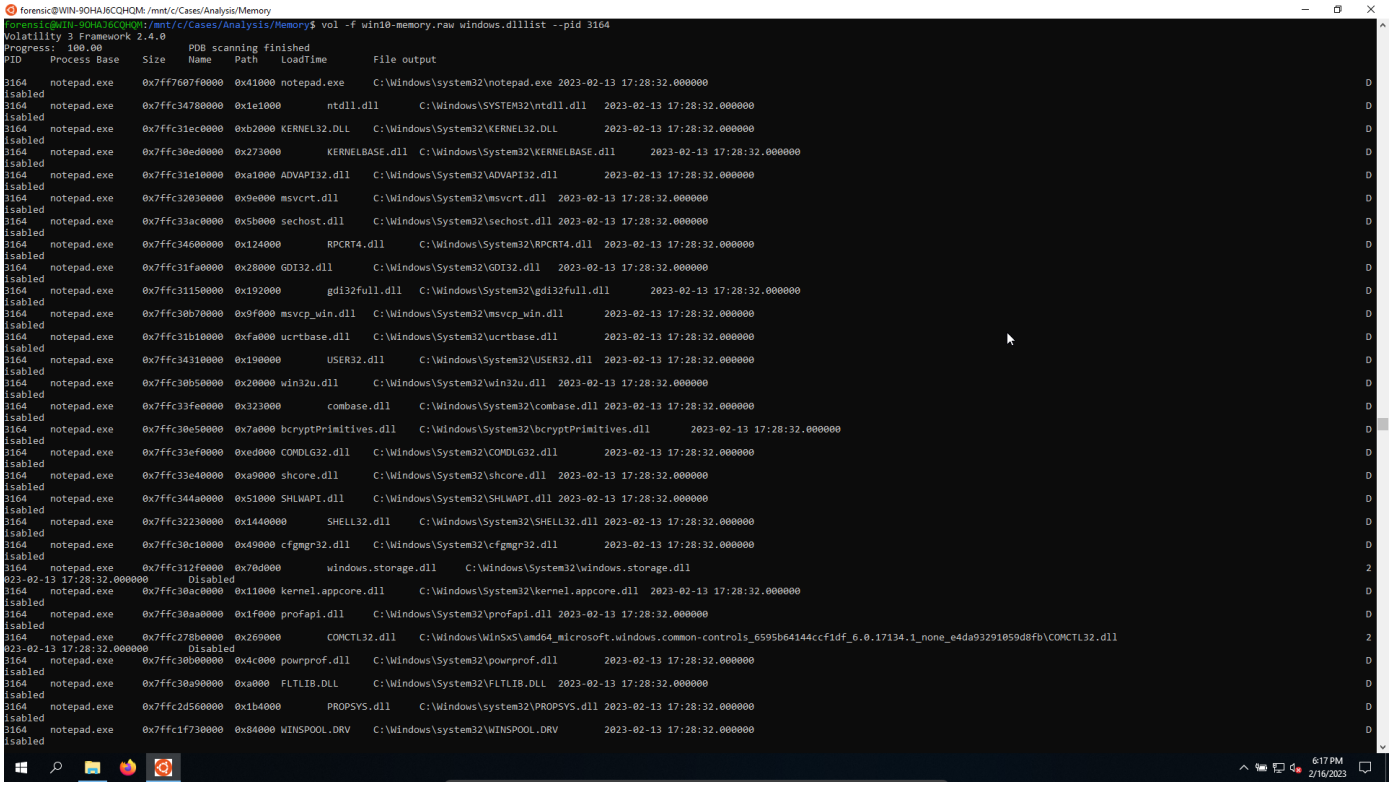


- c5e3d5c1e33cabc5e1fb0c52247e4385ef4be031

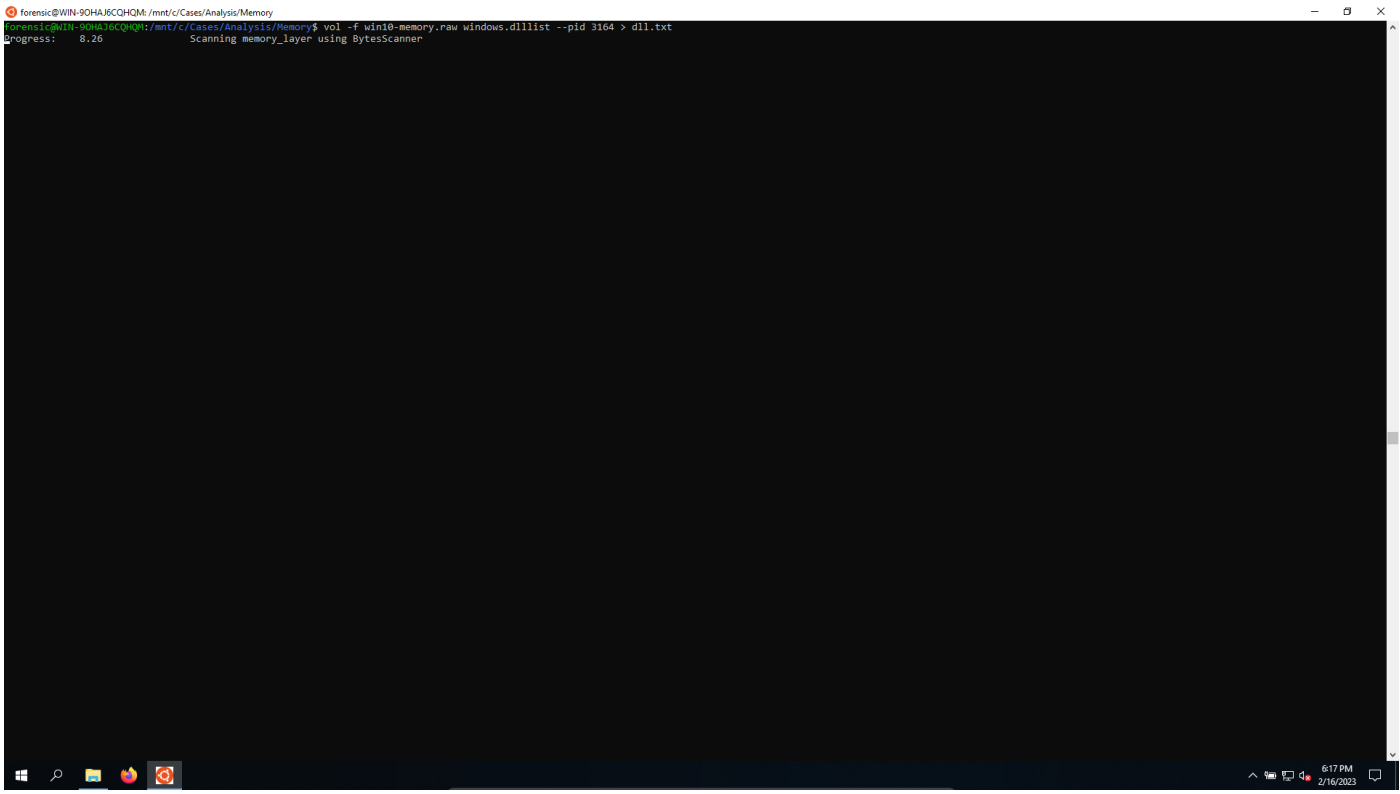


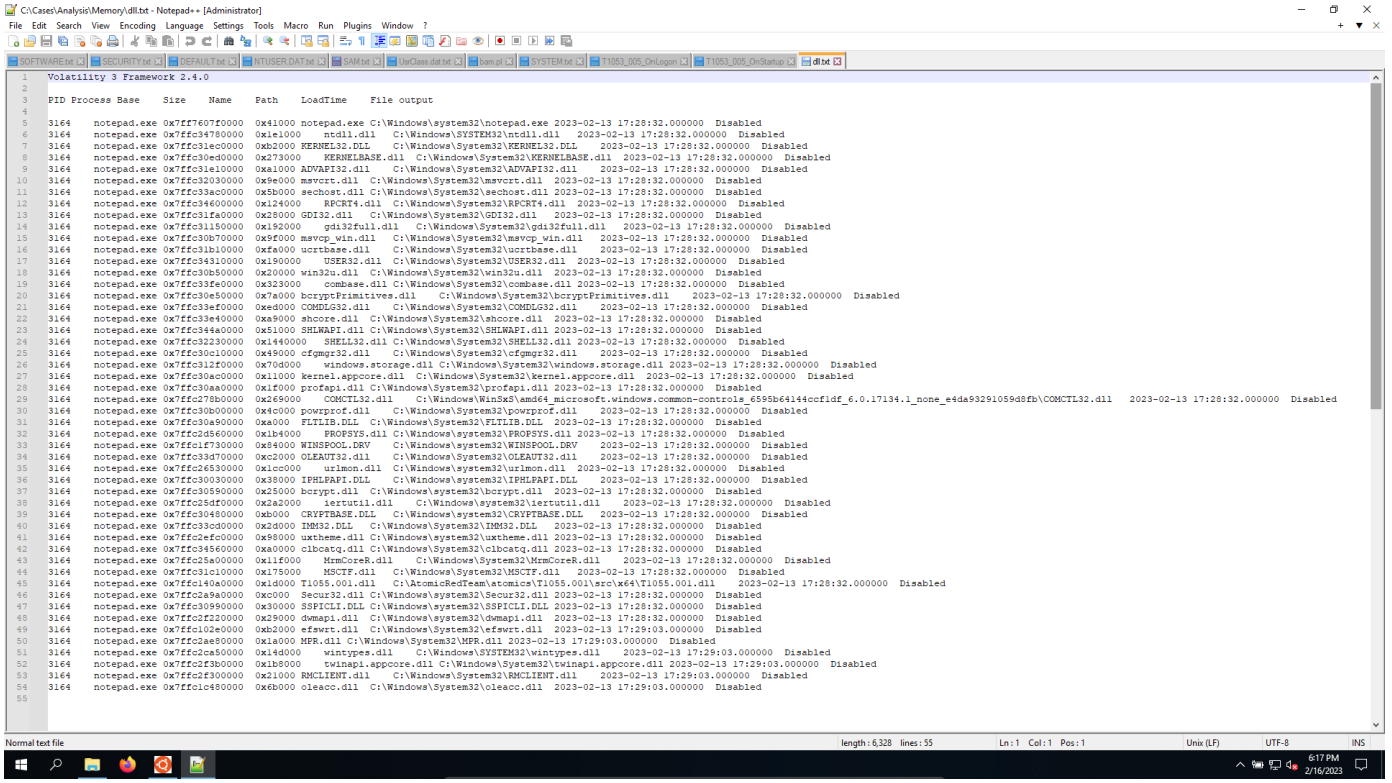
Injected DLLs

- Print dll used by a process:

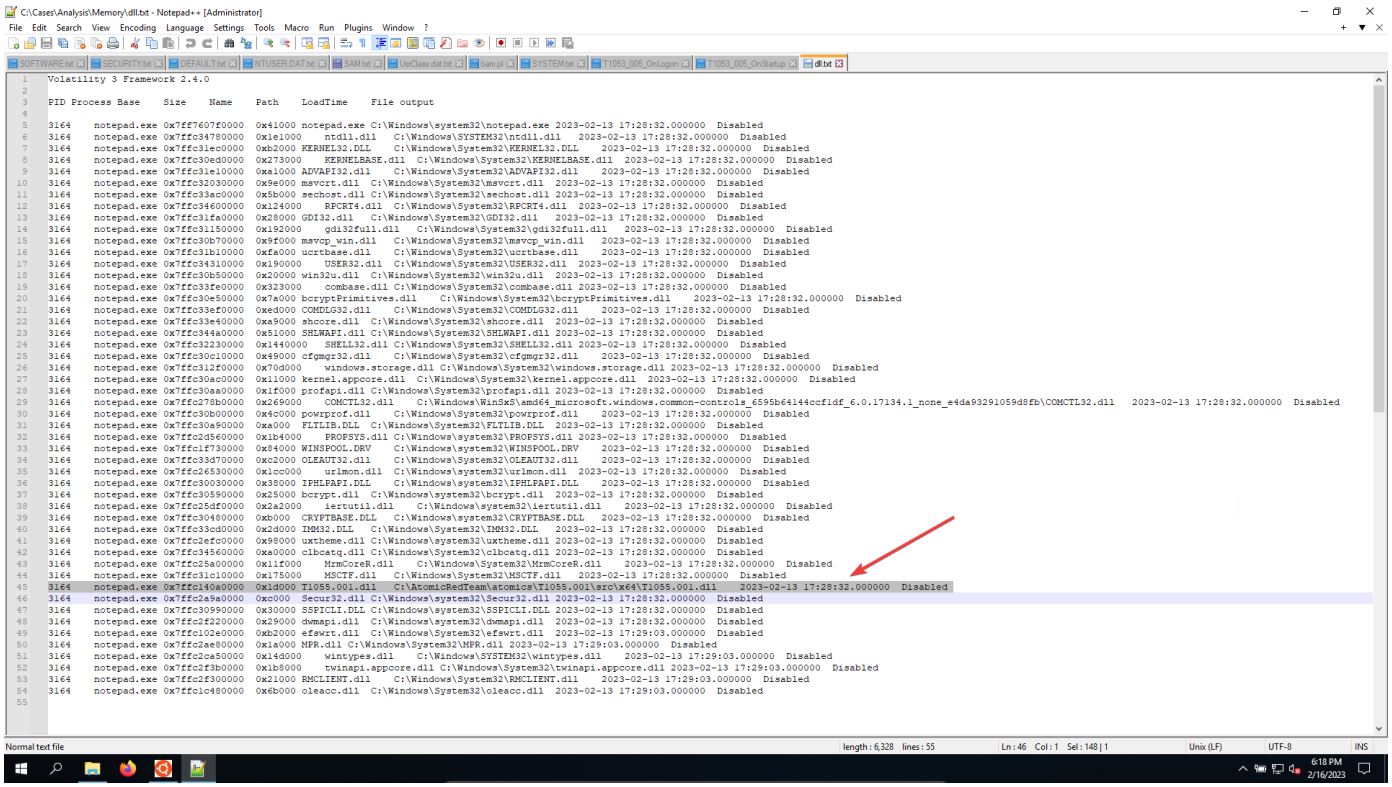


- Print the output to a text file:

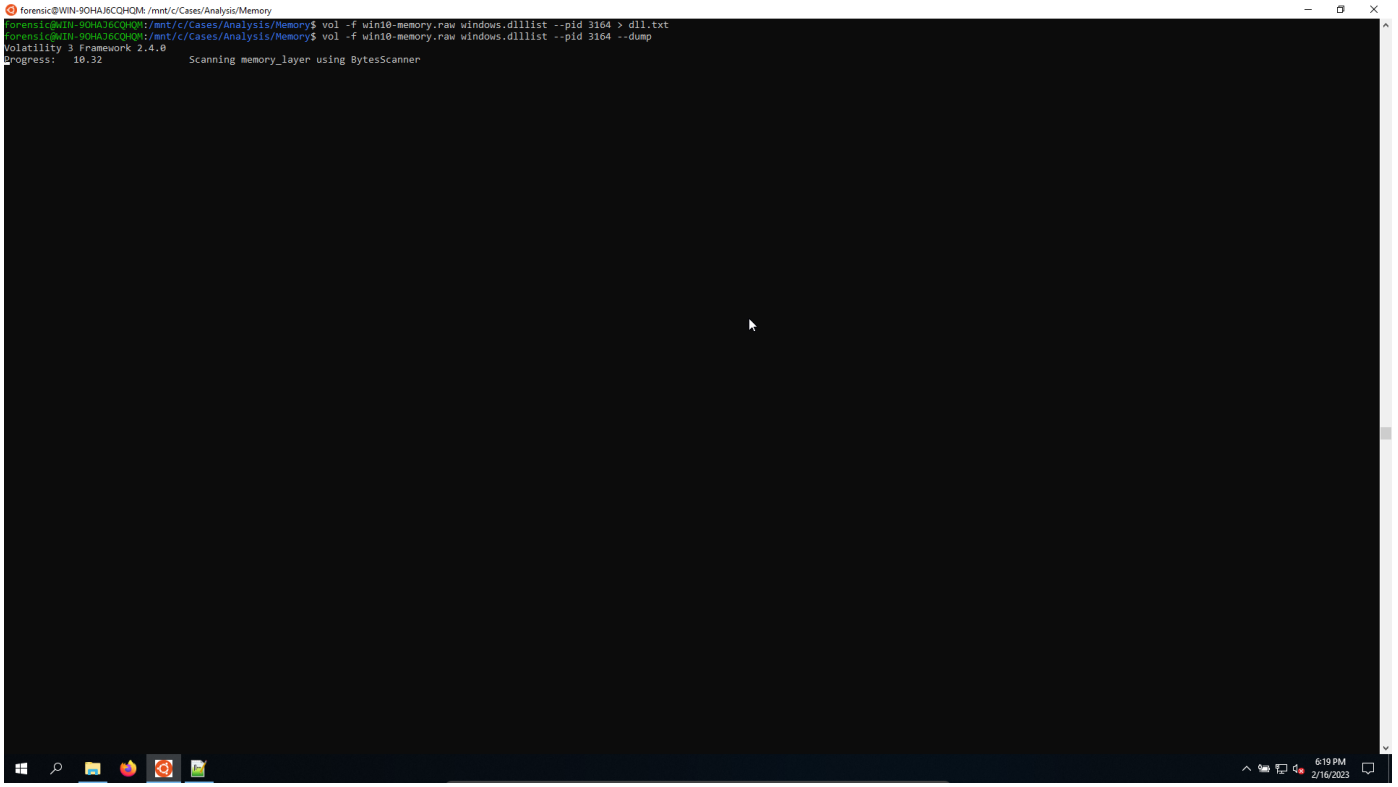


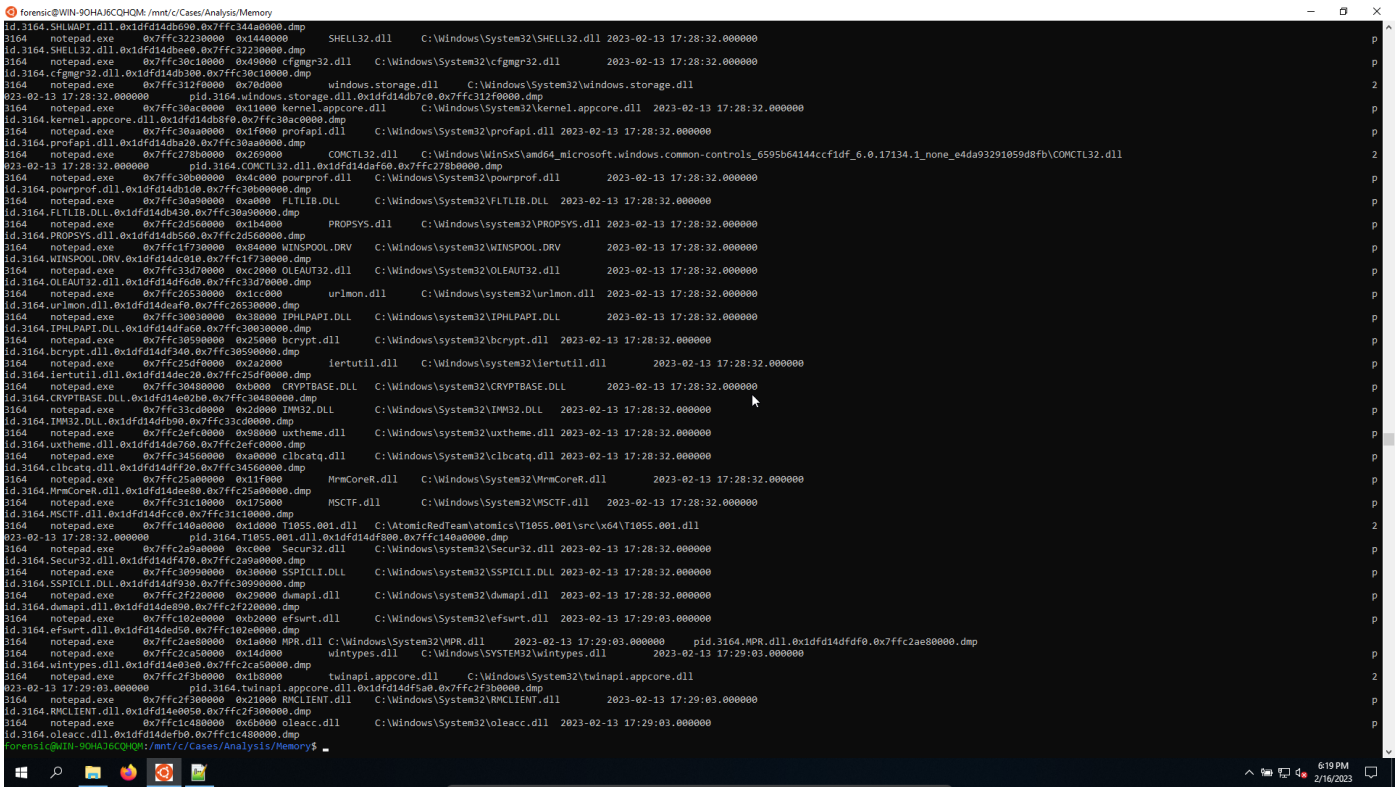


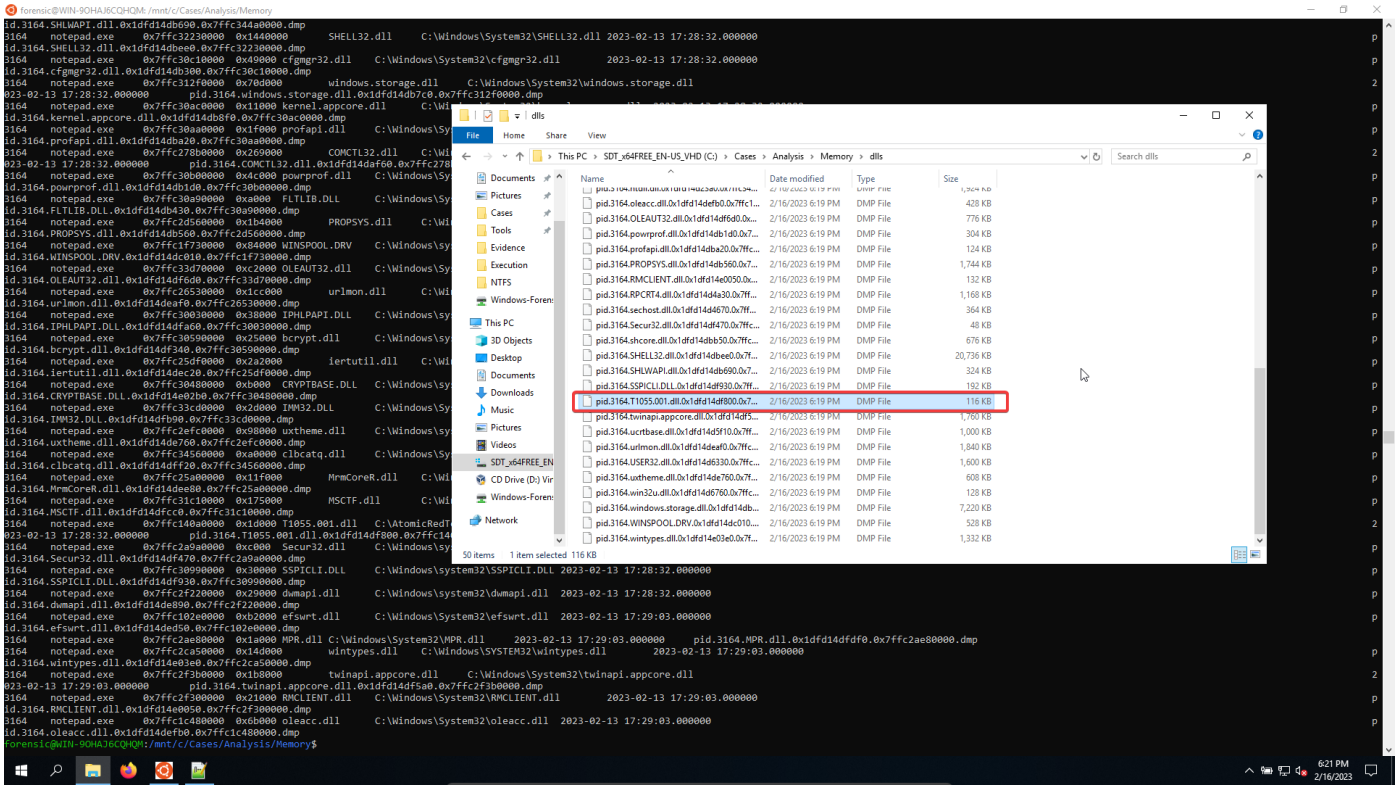
- Observe the injected dll.



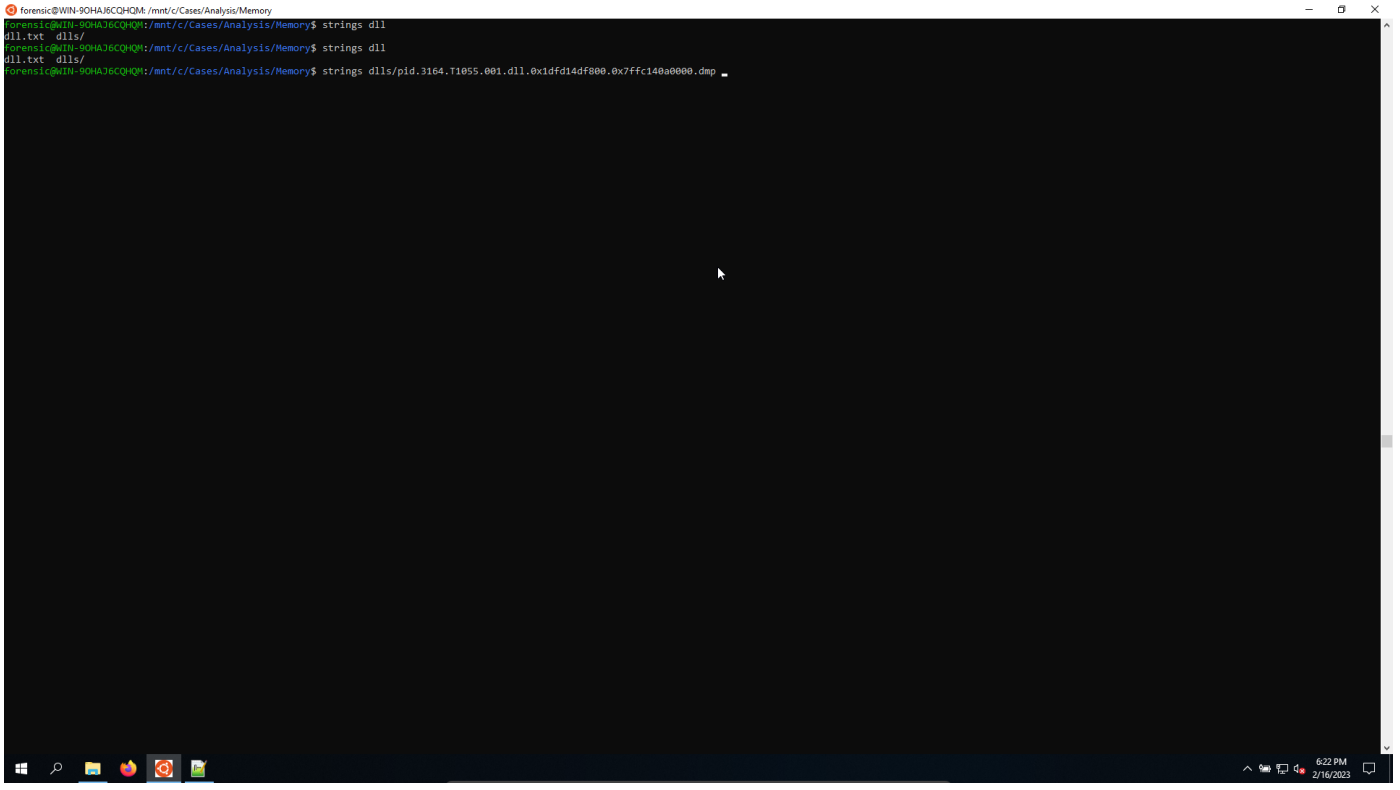
- Dump the dlls:

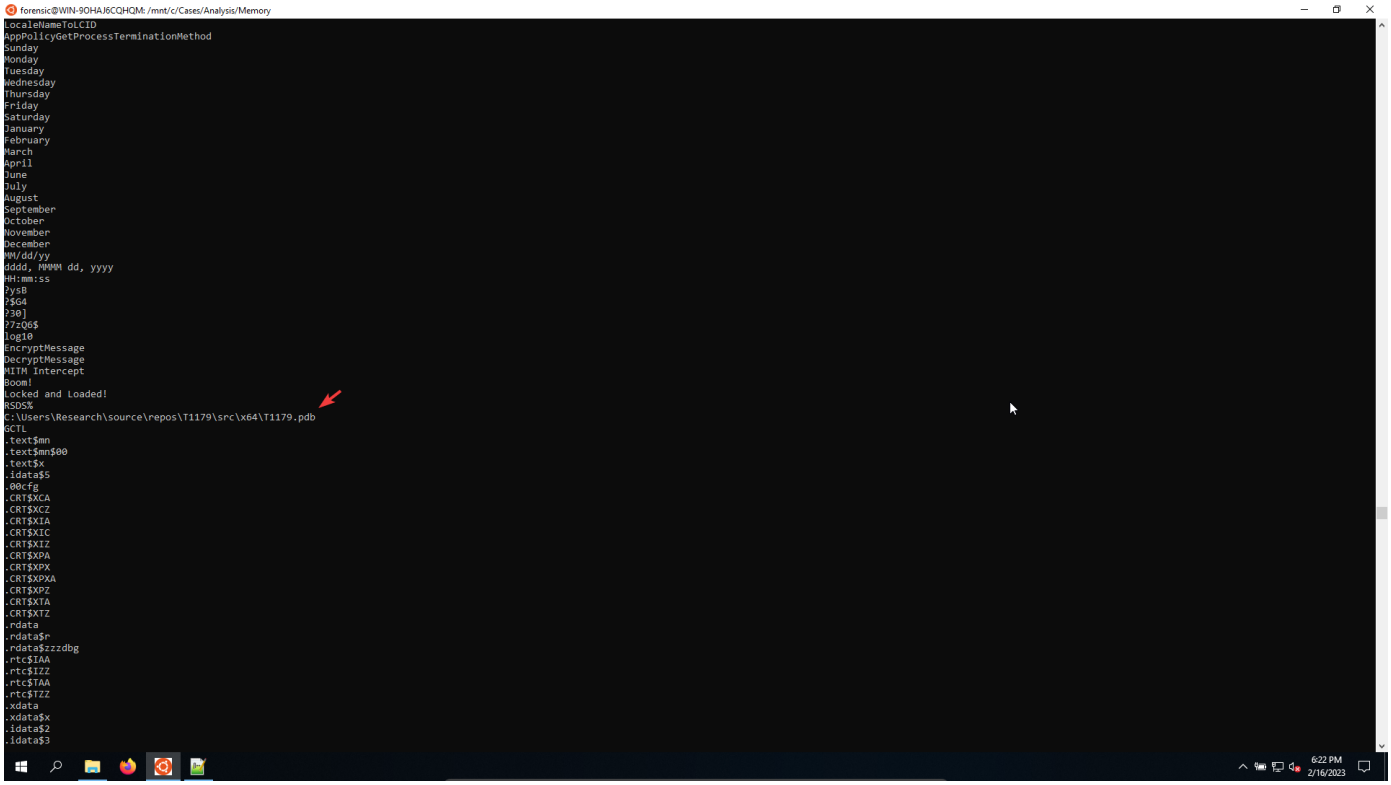

forensic@WIN-9OHAJ6CQHQM: /mnt/c/Cases/Analysis/Memory
forensic@WIN-9OHAJ6CQHQM:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.dlllist --pid 3164 > dll.txt
forensic@WIN-9OHAJ6CQHQM:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.dlllist --pid 3164 --dump
Volatility 3 Framework 2.4.0
Progress: 10.32 Scanning memory_layer using BytesScanner
6:19 PM
2/16/2023

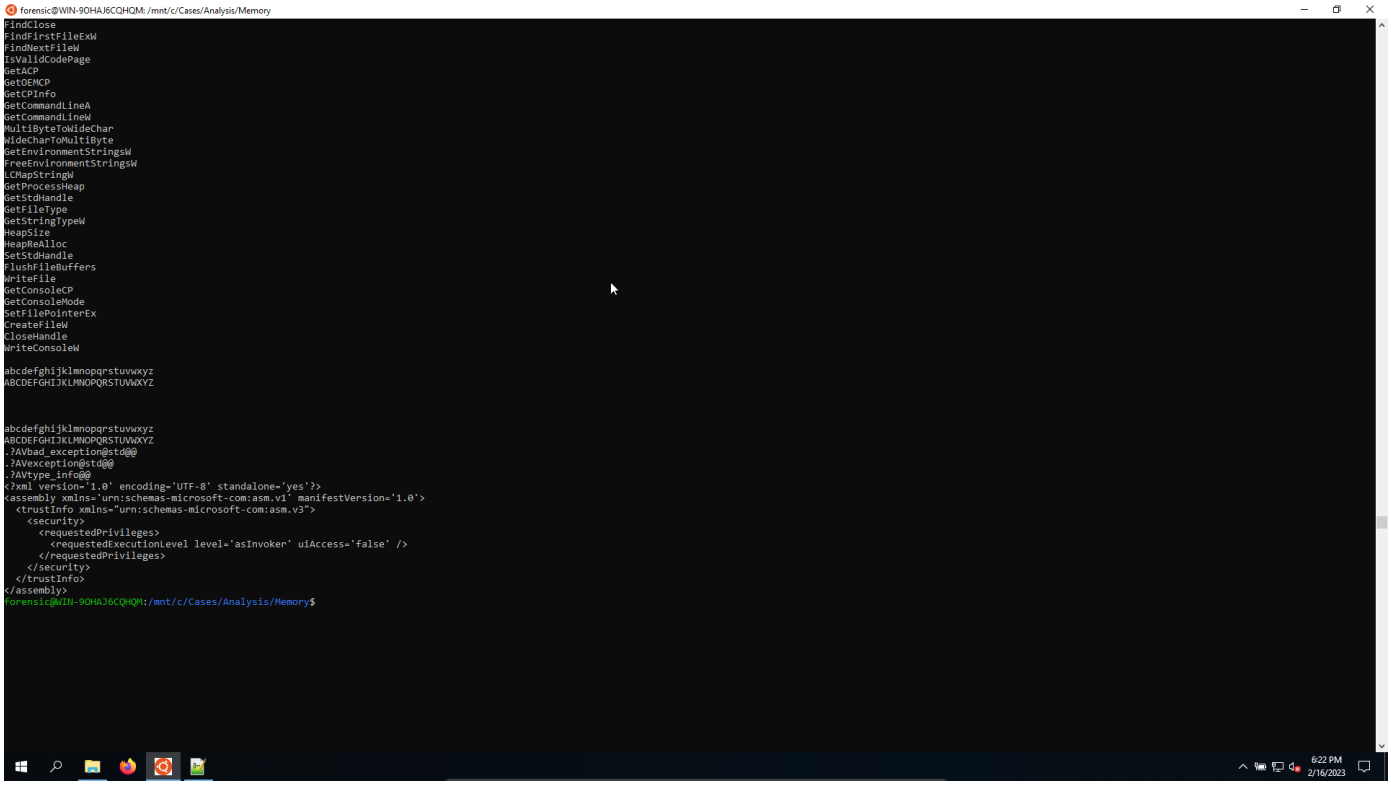

forensic@WIN-9OHAJ6CQHQM: /mnt/c/Cases/Analysis/Memory
id.3164.SHLWAPI.dll.0x1dfd14db690.0x7ffc344a0000.dmp
3164 notepad.exe 0x7ffc32230000 0x1440000 SHELL32.dll C:\Windows\System32\SHELL32.dll 2023-02-13 17:28:32.000000
id.3164.SHELL32.dll.0x1dfd14dbee0.0x7ffc32230000.dmp
3164 notepad.exe 0x7ffc30c10000 0x49000 cfgmgr32.dll C:\Windows\System32\cfgmgr32.dll 2023-02-13 17:28:32.000000
id.3164.cfgmgr32.dll.0x1dfd14db300.0x7ffc30c10000.dmp
3164 notepad.exe 0x7ffc312f0000 0x70d000 windows.storage.dll C:\Windows\System32\windows.storage.dll
023-02-13 17:28:32.000000 pid.3164.windows.storage.dll.0x1dfd14db7c0.0x7ffc312f0000.dmp
3164 notepad.exe 0x7ffc30ac0000 0x11000 kernel.appcore.dll C:\Windows\System32\kernel.appcore.dll 2023-02-13 17:28:32.000000
id.3164.kernel.appcore.dll.0x1dfd14db8f0.0x7ffc30ac0000.dmp
3164 notepad.exe 0x7ffc30aa0000 0x1f000 profapi.dll C:\Windows\System32\profapi.dll 2023-02-13 17:28:32.000000
id.3164.profapi.dll.0x1dfd14dba20.0x7ffc30aa0000.dmp
3164 notepad.exe 0x7ffc278b0000 0x269000 COMCTL32.dll C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17134.1_none_e4da93291059d8fb\COMCTL32.dll
023-02-13 17:28:32.000000 pid.3164.COMCTL32.dll.0x1dfd14daf60.0x7ffc278b0000.dmp
3164 notepad.exe 0x7ffc30b00000 0x4c000 powrprof.dll C:\Windows\System32\powrprof.dll 2023-02-13 17:28:32.000000
id.3164.powrprof.dll.0x1dfd14db1d0.0x7ffc30b00000.dmp
3164 notepad.exe 0x7ffc30a90000 0xa000 FLTLIB.DLL C:\Windows\System32\FLTLIB.DLL 2023-02-13 17:28:32.000000
id.3164.FLTLIB.DLL.0x1dfd14db430.0x7ffc30a90000.dmp
3164 notepad.exe 0x7ffc2d560000 0x1b4000 PROPSYS.dll C:\Windows\system32\PROPSYS.dll 2023-02-13 17:28:32.000000
id.3164.PROPSYS.dll.0x1dfd14db560.0x7ffc2d560000.dmp
3164 notepad.exe 0x7ffc1f730000 0x84000 WINSPOOL.DRV C:\Windows\system32\WINSPOOL.DRV 2023-02-13 17:28:32.000000
id.3164.WINSPOOL.DRV.0x1dfd14dc010.0x7ffc1f730000.dmp
3164 notepad.exe 0x7ffc33d70000 0xc2000 OLEAUT32.dll C:\Windows\System32\OLEAUT32.dll 2023-02-13 17:28:32.000000
id.3164.OLEAUT32.dll.0x1dfd14df6d0.0x7ffc33d70000.dmp
3164 notepad.exe 0x7ffc26530000 0x1cc000 urlmon.dll C:\Windows\system32\urlmon.dll 2023-02-13 17:28:32.000000
id.3164.urlmon.dll.0x1dfd14deaf0.0x7ffc26530000.dmp
3164 notepad.exe 0x7ffc30030000 0x38000 IPHLPAPI.DLL C:\Windows\system32\IPHLPAPI.DLL 2023-02-13 17:28:32.000000
id.3164.IPHLPAPI.DLL.0x1dfd14dfa60.0x7ffc30030000.dmp
3164 notepad.exe 0x7ffc30590000 0x25000 bcrypt.dll C:\Windows\system32\bcrypt.dll 2023-02-13 17:28:32.000000
id.3164.bcrypt.dll.0x1dfd14df340.0x7ffc30590000.dmp
3164 notepad.exe 0x7ffc25df0000 0x2a2000 iertutil.dll C:\Windows\system32\iertutil.dll 2023-02-13 17:28:32.000000
id.3164.iertutil.dll.0x1dfd14dec20.0x7ffc25df0000.dmp
3164 notepad.exe 0x7ffc30480000 0xb000 CRYPTBASE.DLL C:\Windows\system32\CRYPTBASE.DLL 2023-02-13 17:28:32.000000
id.3164.CRYPTBASE.DLL.0x1dfd14e02b0.0x7ffc30480000.dmp
3164 notepad.exe 0x7ffc33cd0000 0x2d000 IMM32.DLL C:\Windows\System32\IMM32.DLL 2023-02-13 17:28:32.000000
id.3164.IMM32.DLL.0x1dfd14dfb90.0x7ffc33cd0000.dmp
3164 notepad.exe 0x7ffc2efc0000 0x98000 uxtheme.dll C:\Windows\system32\uxtheme.dll 2023-02-13 17:28:32.000000
id.3164.uxtheme.dll.0x1dfd14de760.0x7ffc2efc0000.dmp
3164 notepad.exe 0x7ffc34560000 0xa0000 clbcatq.dll C:\Windows\System32\clbcatq.dll 2023-02-13 17:28:32.000000
id.3164.clbcatq.dll.0x1dfd14dff20.0x7ffc34560000.dmp
3164 notepad.exe 0x7ffc25a00000 0x11f000 MrmCoreR.dll C:\Windows\System32\MrmCoreR.dll 2023-02-13 17:28:32.000000
id.3164.MrmCoreR.dll.0x1dfd14dee80.0x7ffc25a00000.dmp
3164 notepad.exe 0x7ffc31c10000 0x175000 MSCTF.dll C:\Windows\System32\MSCTF.dll 2023-02-13 17:28:32.000000
id.3164.MSCTF.dll.0x1dfd14dfcc0.0x7ffc31c10000.dmp
3164 notepad.exe 0x7ffc140a0000 0x1d000 T1055.001.dll C:\AtomicRedTeam\atomics\T1055.001\src\x64\T1055.001.dll
023-02-13 17:28:32.000000 pid.3164.T1055.001.dll.0x1dfd14df800.0x7ffc140a0000.dmp
3164 notepad.exe 0x7ffc2a9a0000 0xc000 Secur32.dll C:\Windows\system32\Secur32.dll 2023-02-13 17:28:32.000000
id.3164.Secur32.dll.0x1dfd14df470.0x7ffc2a9a0000.dmp
3164 notepad.exe 0x7ffc30990000 0x30000 SSPICLI.DLL C:\Windows\system32\SSPICLI.DLL 2023-02-13 17:28:32.000000
id.3164.SSPICLI.DLL.0x1dfd14df930.0x7ffc30990000.dmp
3164 notepad.exe 0x7ffc2f220000 0x29000 dwmapi.dll C:\Windows\system32\dwmapi.dll 2023-02-13 17:28:32.000000
id.3164.dwmapi.dll.0x1dfd14de890.0x7ffc2f220000.dmp
3164 notepad.exe 0x7ffc102e0000 0xb2000 efswrt.dll C:\Windows\System32\efswrt.dll 2023-02-13 17:29:03.000000
id.3164.efswrt.dll.0x1dfd14ded50.0x7ffc102e0000.dmp
3164 notepad.exe 0x7ffc2ae80000 0x1a000 MPR.dll C:\Windows\System32\MPR.dll 2023-02-13 17:29:03.000000 pid.3164.MPR.dll.0x1dfd14dfdf0.0x7ffc2ae80000.dmp
3164 notepad.exe 0x7ffc2ca50000 0x14d000 wintypes.dll C:\Windows\SYSTEM32\wintypes.dll 2023-02-13 17:29:03.000000
id.3164.wintypes.dll.0x1dfd14e03e0.0x7ffc2ca50000.dmp
3164 notepad.exe 0x7ffc2f3b0000 0x1b8000 twinapi.appcore.dll C:\Windows\System32\twinapi.appcore.dll
023-02-13 17:29:03.000000 pid.3164.twinapi.appcore.dll.0x1dfd14df5a0.0x7ffc2f3b0000.dmp
3164 notepad.exe 0x7ffc2f300000 0x21000 RMCLIENT.dll C:\Windows\System32\RMCLIENT.dll 2023-02-13 17:29:03.000000
id.3164.RMCLIENT.dll.0x1dfd14e0050.0x7ffc2f300000.dmp
3164 notepad.exe 0x7ffc1c480000 0x6b000 oleacc.dll C:\Windows\System32\oleacc.dll 2023-02-13 17:29:03.000000
id.3164.oleacc.dll.0x1dfd14defb0.0x7ffc1c480000.dmp
forensic@WIN-9OHAJ6CQHQM:/mnt/c/Cases/Analysis/Memory$
6:19 PM
2/16/2023



- Analysis of the suspicious DLL:

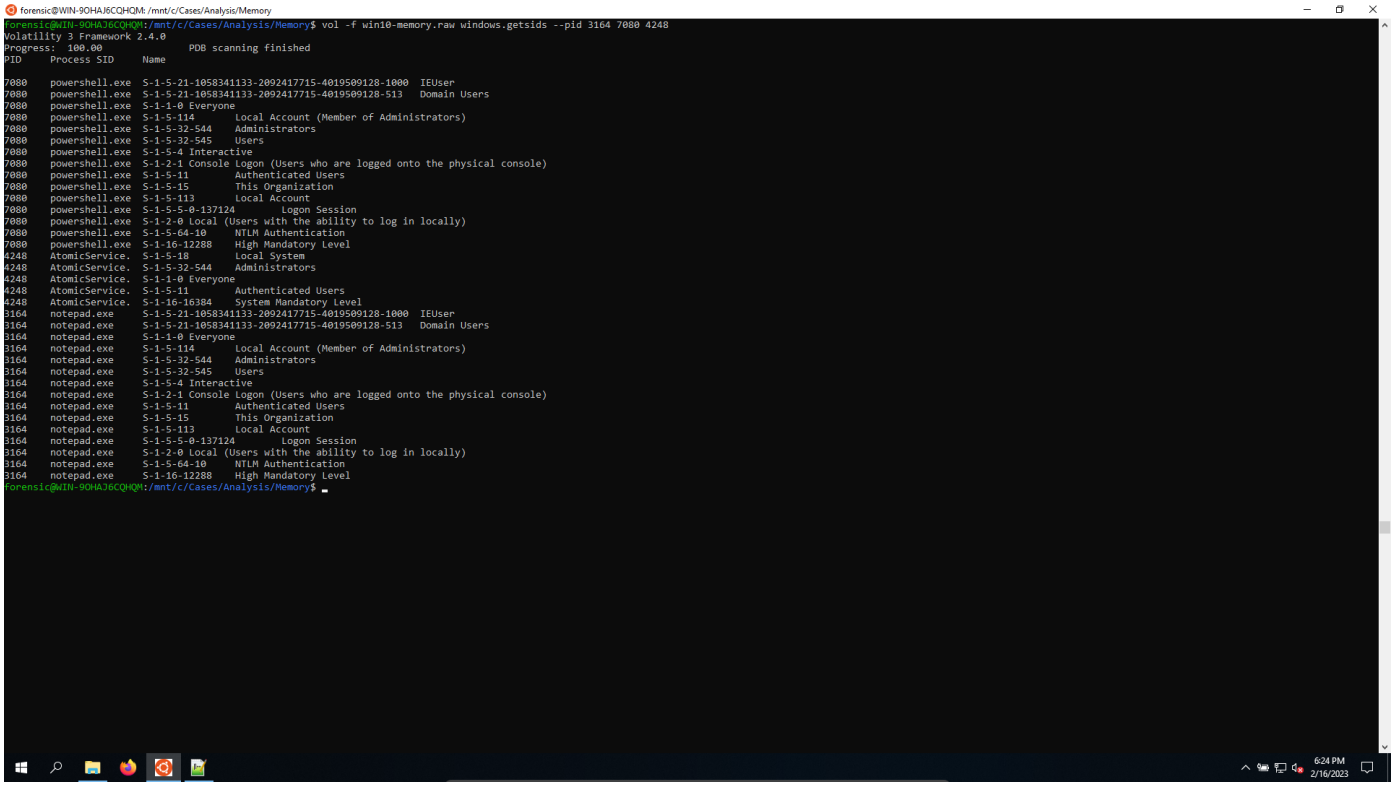






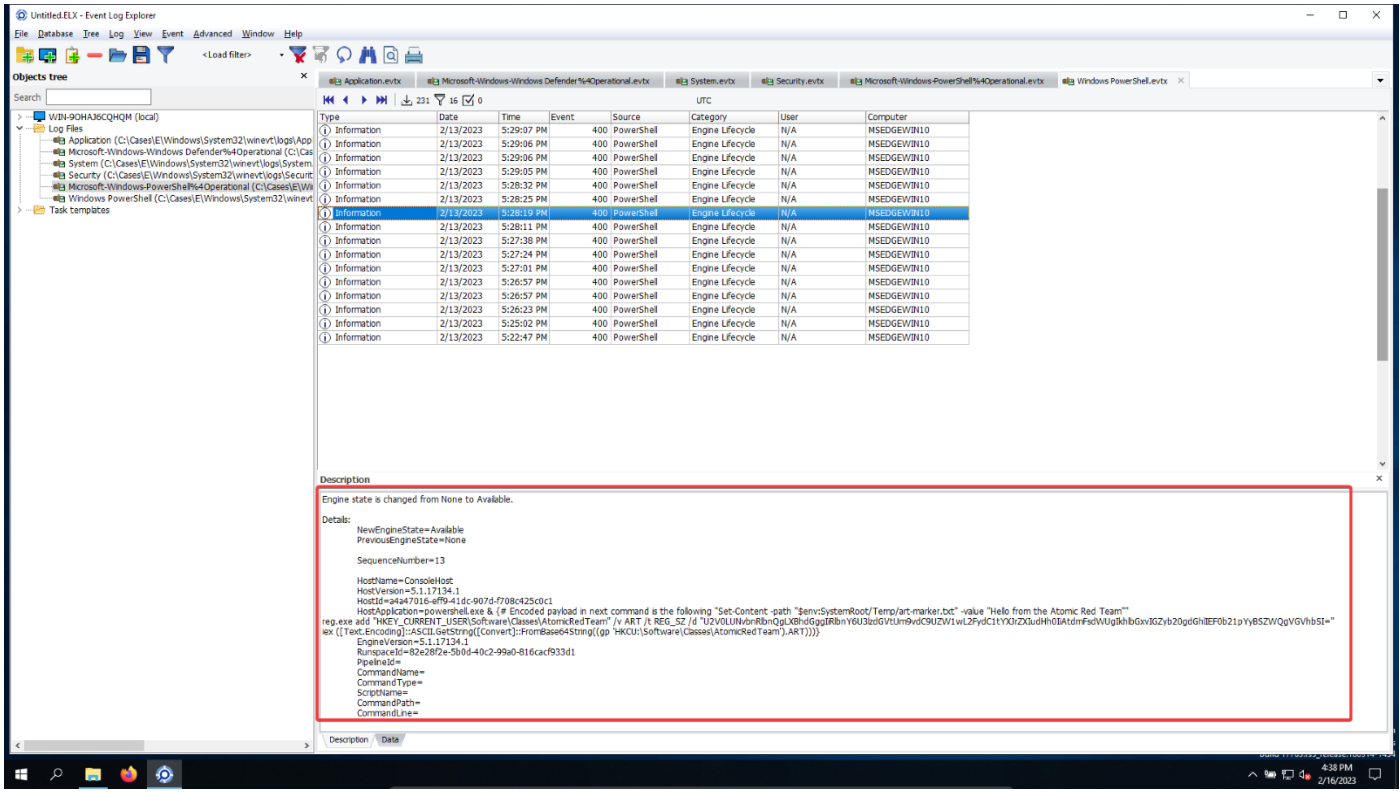
Process owners

- Get the SID for the processes:

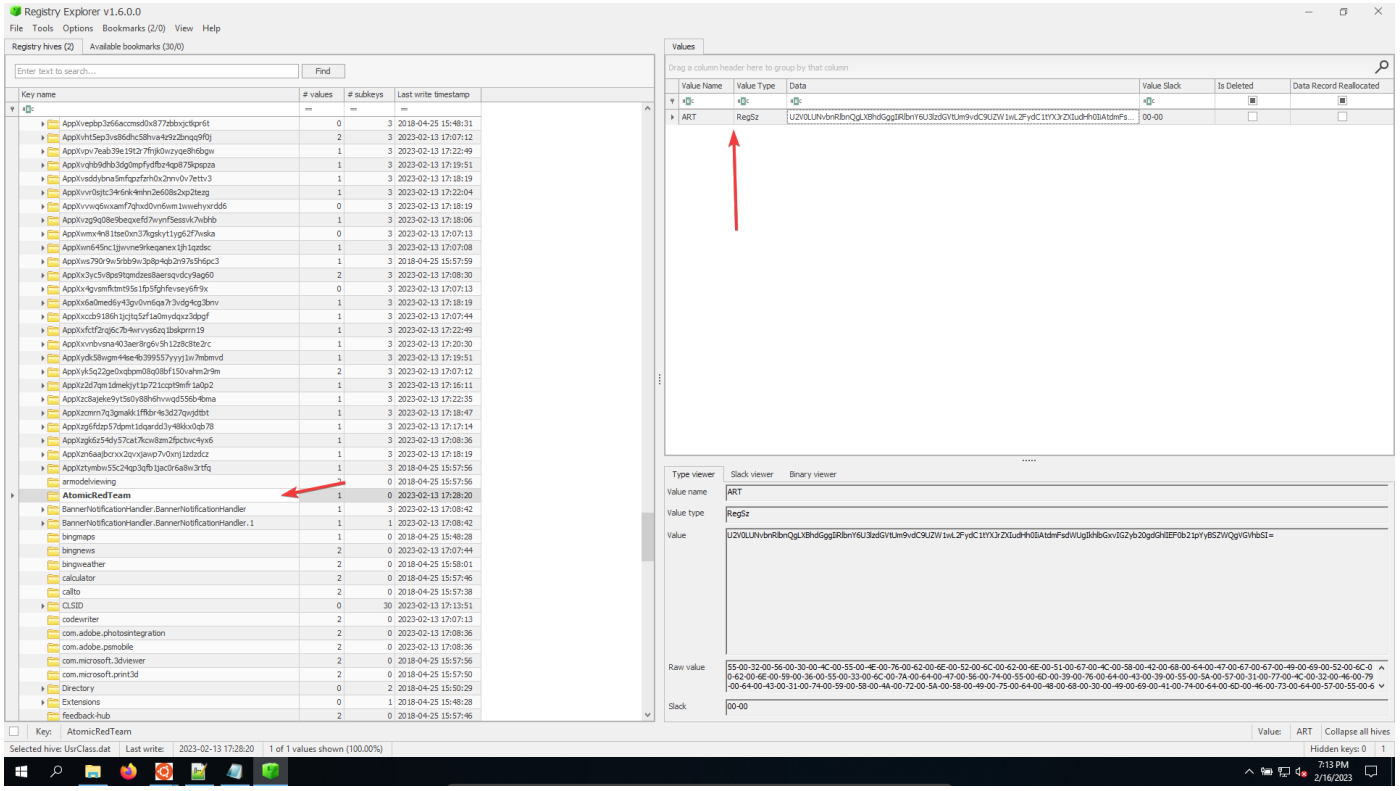


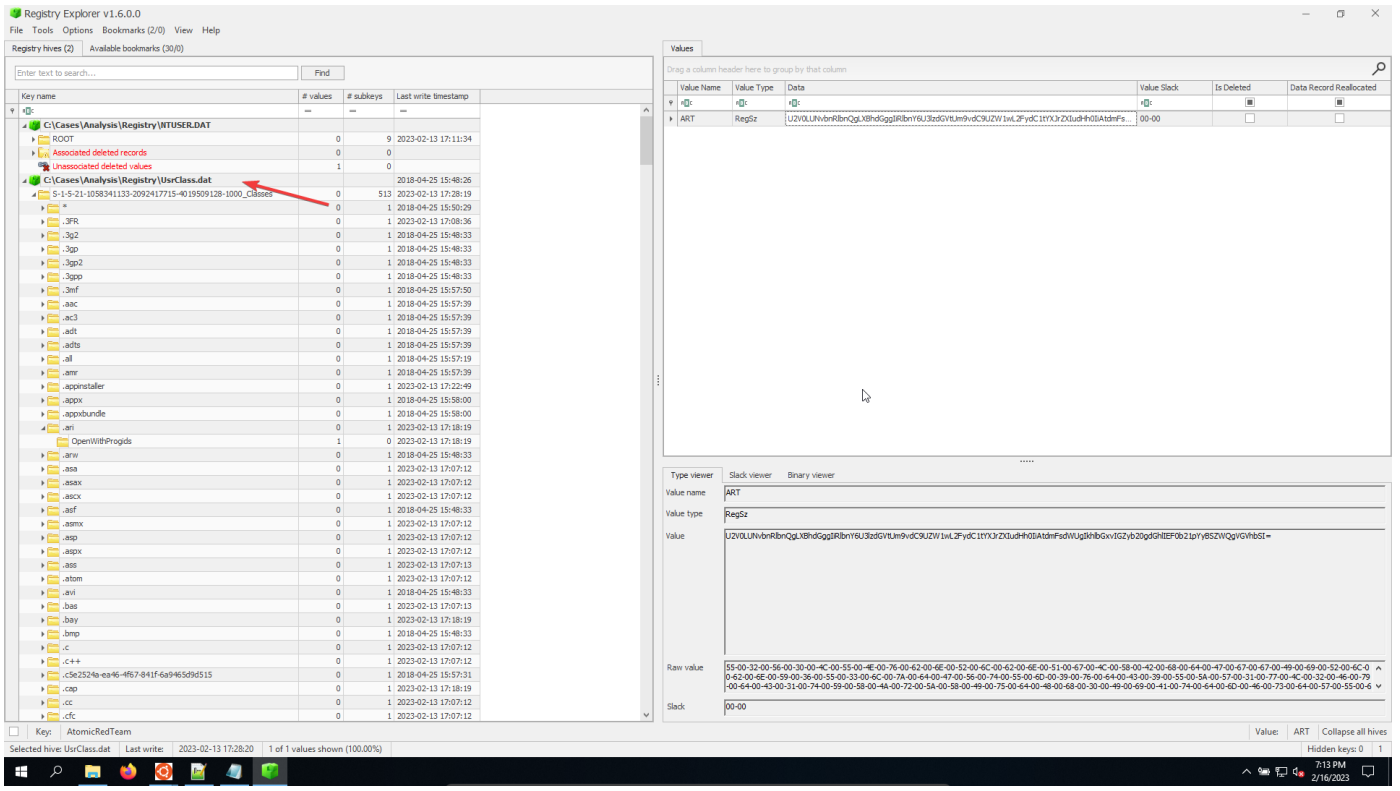
Malicious registry key entries

- Suspicious Registry Key:

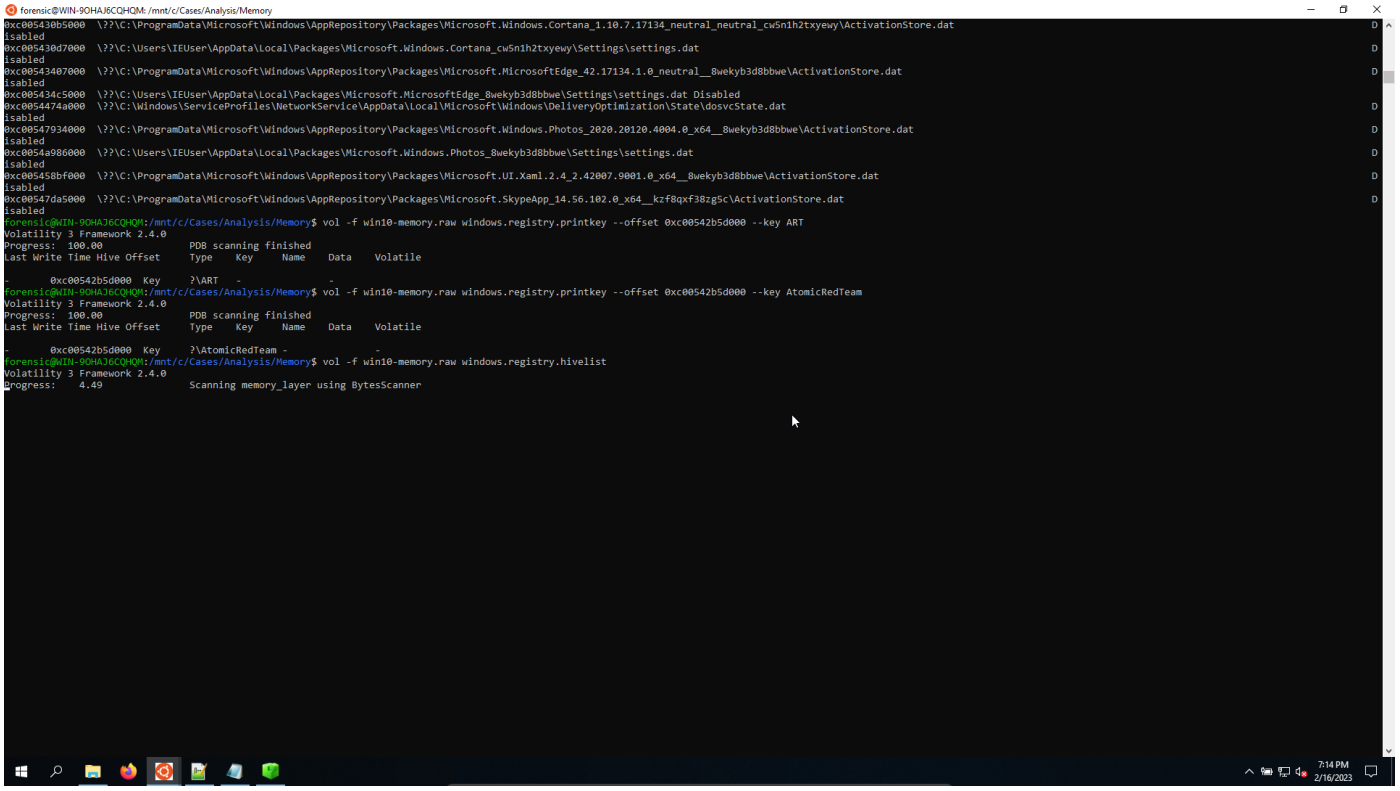


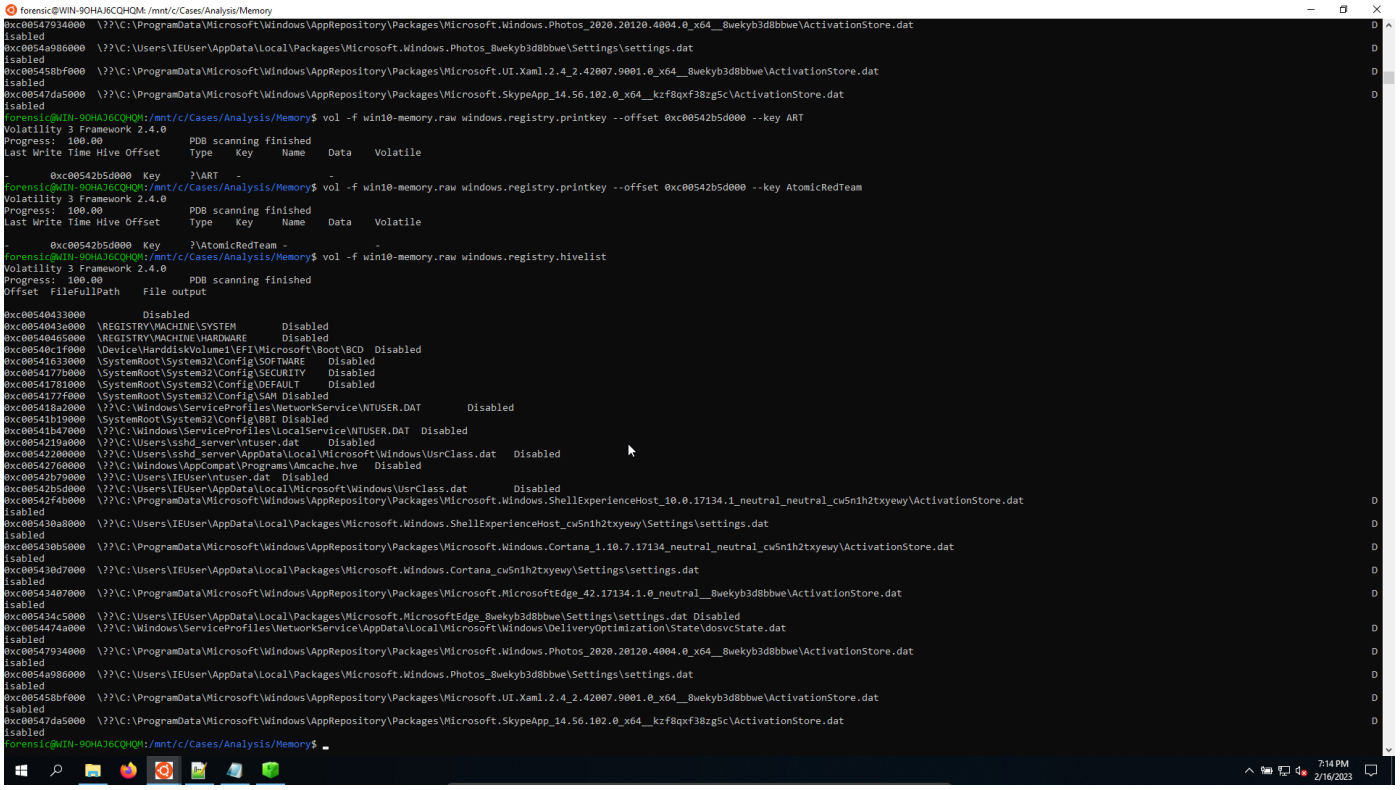
- Unfortunately, I could not find the registry key in the volatile memory , i have searched for it in the registry hive with registry explorer and found it .

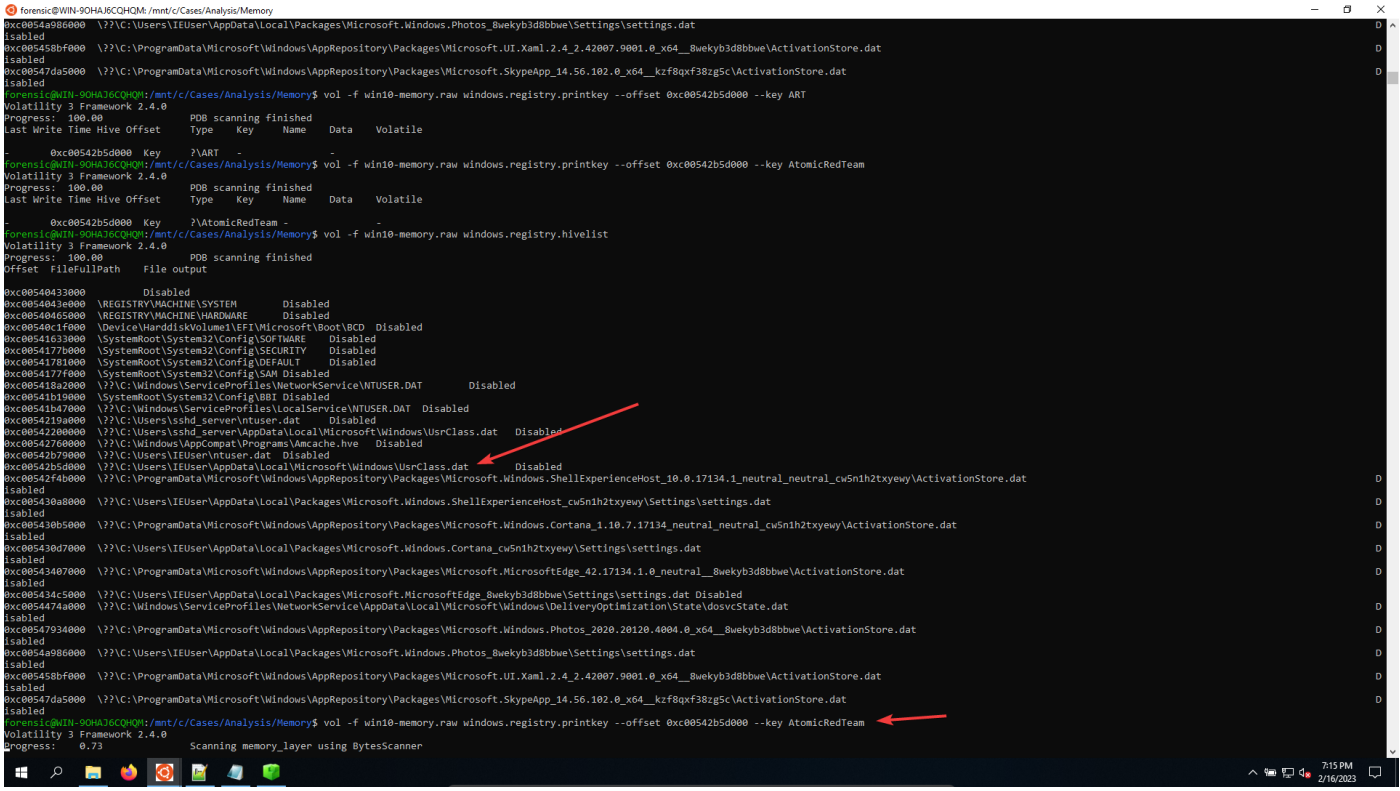




- You can search the offset of the hive and search for the key with this command:






forensic@WIN-9OHAJ6CQHQM: /mnt/c/Cases/Analysis/Memory
0xc0054a986000 \??\C:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settings\settings.dat
isabled
0xc005458bf000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.UI.Xaml.2.4_2.42007.9001.0_x64__8wekyb3d8bbwe\ActivationStore.dat
isabled
0xc00547da5000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.SkypeApp_14.56.102.0_x64__kzf8qxf38zg5c\ActivationStore.dat
isabled
forensic@WIN-9OHAJ6CQHQM:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.registry.printkey --offset 0xc00542b5d000 --key ART
Volatility 3 Framework 2.4.0
Progress: 100.00 PDB scanning finished
Last Write Time Hive Offset Type Key Name Data Volatile
- 0xc00542b5d000 Key ?\ART - -
forensic@WIN-9OHAJ6CQHQM:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.registry.printkey --offset 0xc00542b5d000 --key AtomicRedTeam
Volatility 3 Framework 2.4.0
Progress: 100.00 PDB scanning finished
Last Write Time Hive Offset Type Key Name Data Volatile
- 0xc00542b5d000 Key ?\AtomicRedTeam - -
forensic@WIN-9OHAJ6CQHQM:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.registry.hivelist
Volatility 3 Framework 2.4.0
Progress: 100.00 PDB scanning finished
Offset FileFullPath File output
0xc00540433000 Disabled
0xc0054043e000 \REGISTRY\MACHINE\SYSTEM Disabled
0xc00540465000 \REGISTRY\MACHINE\HARDWARE Disabled
0xc00540c1f000 \Device\HarddiskVolume1\EFI\Microsoft\Boot\BCD Disabled
0xc00541633000 \SystemRoot\System32\Config\SOFTWARE Disabled
0xc005417b000 \SystemRoot\System32\Config\SECURITY Disabled
0xc00541781000 \SystemRoot\System32\Config\DEFAULT Disabled
0xc0054177f000 \SystemRoot\System32\Config\SAM Disabled
0xc005418a2000 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT Disabled
0xc00541b19000 \SystemRoot\System32\Config\BBI Disabled
0xc00541b47000 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT Disabled
0xc0054219a000 \??\C:\Users\sshd_server\ntuser.dat Disabled
0xc00542200000 \??\C:\Users\sshd_server\AppData\Local\Microsoft\Windows\UsrClass.dat Disabled
0xc00542760000 \??\C:\Windows\AppCompat\Programs\Amcache.hve Disabled
0xc00542b79000 \??\C:\Users\IEUser\ntuser.dat Disabled
0xc00542b5d000 \??\C:\Users\IEUser\AppData\Local\Microsoft\Windows\UsrClass.dat Disabled
0xc00542f4b000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.ShellExperienceHost_10.0.17134.1_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat
isabled
0xc005430a8000 \??\C:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\Settings\settings.dat
isabled
0xc005430b5000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Cortana_1.10.7.17134_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat
isabled
0xc005430d7000 \??\C:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\Settings\settings.dat
isabled
0xc00543407000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.MicrosoftEdge_42.17134.1.0_neutral__8wekyb3d8bbwe\ActivationStore.dat
isabled
0xc005434c5000 \??\C:\Users\IEUser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat Disabled
0xc0054474a000 \??\C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\State\dosvcState.dat
isabled
0xc00547934000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Photos_2020.20120.4004.0_x64__8wekyb3d8bbwe\ActivationStore.dat
isabled
0xc0054a986000 \??\C:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settings\settings.dat
isabled
0xc005458bf000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.UI.Xaml.2.4_2.42007.9001.0_x64__8wekyb3d8bbwe\ActivationStore.dat
isabled
0xc00547da5000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.SkypeApp_14.56.102.0_x64__kzf8qxf38zg5c\ActivationStore.dat
isabled
forensic@WIN-9OHAJ6CQHQM:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.registry.printkey --offset 0xc00542b5d000 --key AtomicRedTeam
Volatility 3 Framework 2.4.0
Progress: 0.73 Scanning memory_layer using BytesScanner
7:15 PM
2/16/2023