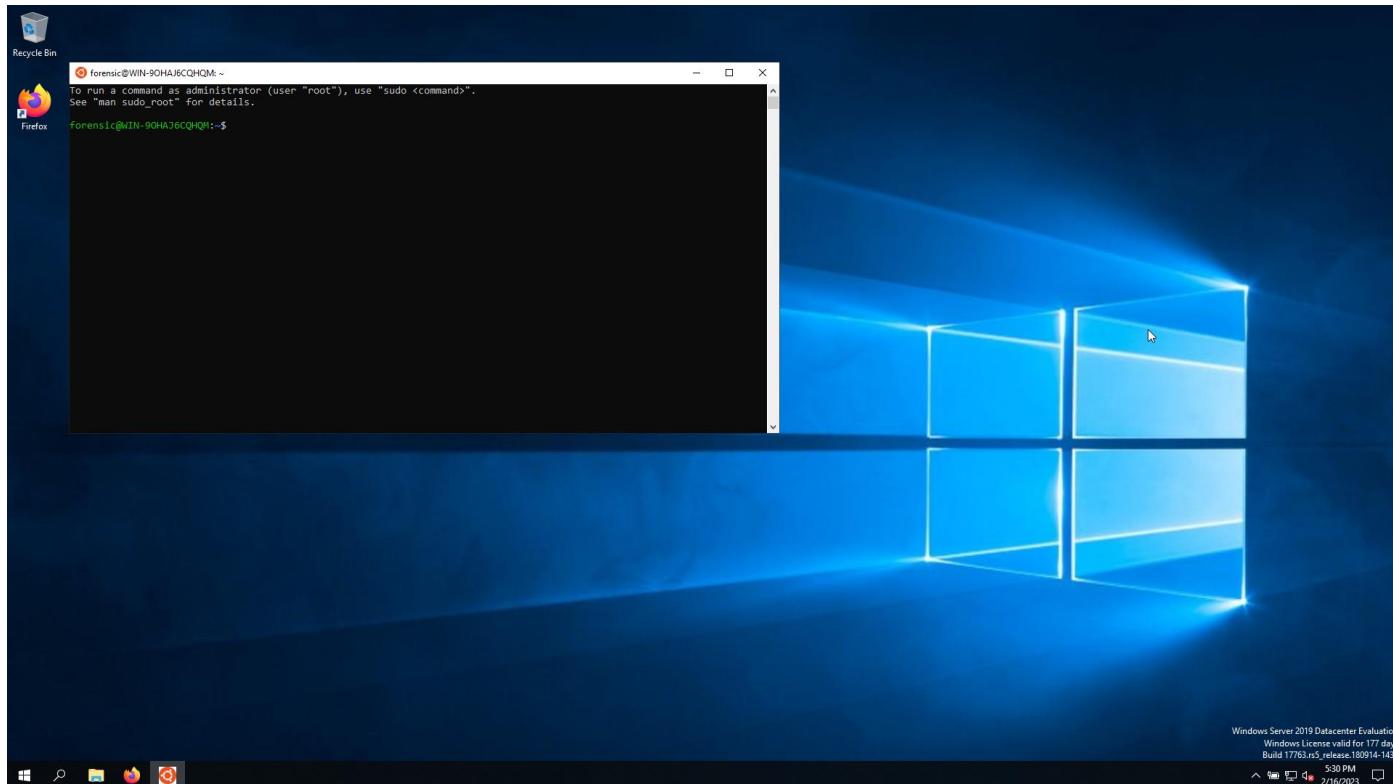


# Forensic analysis of Random Access Memory:

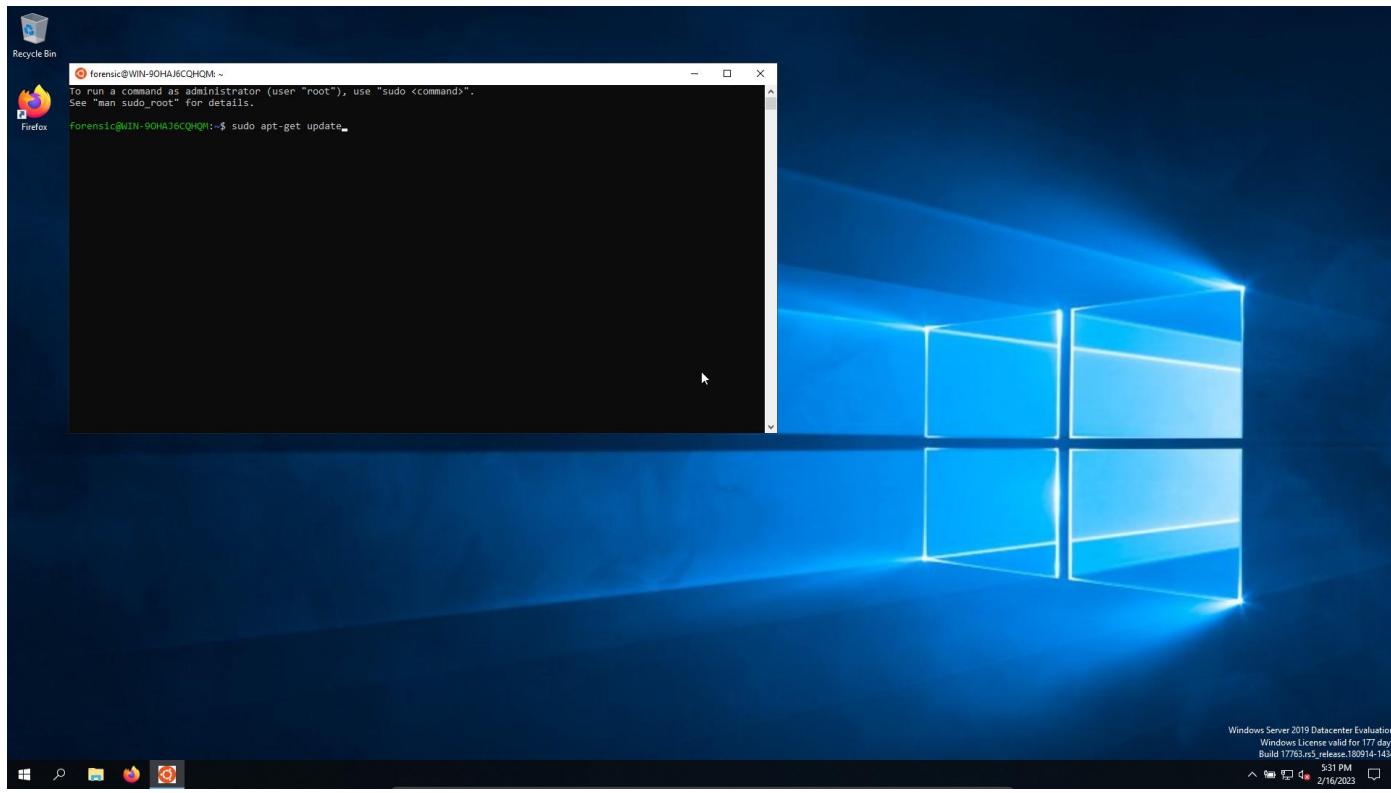
- Installing Volatility3
- Important files for memory analysis
- Windows system information
- Suspicious processes
- Dumping processes
- Injected DLLs
- Process owners
- Malicious registry key entries

## Installing Volatility3

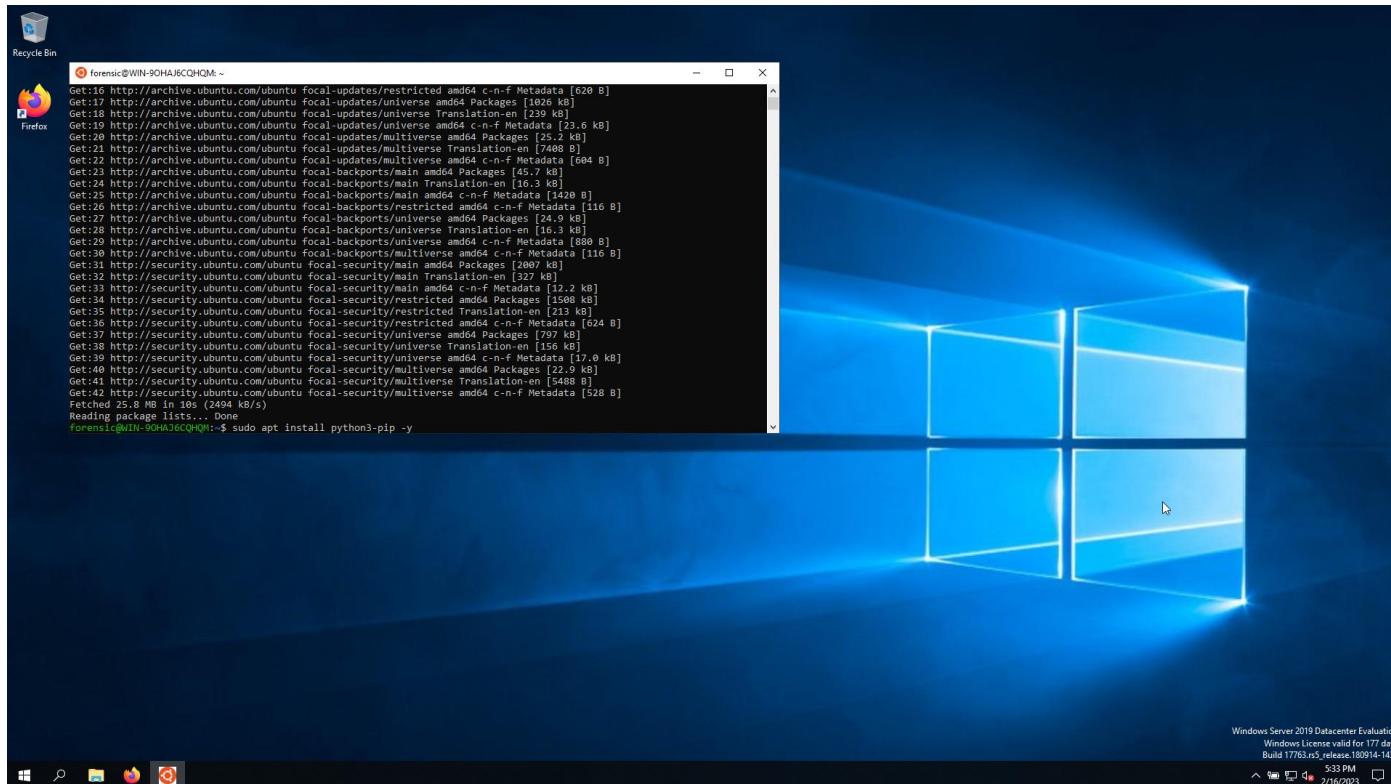
- Installing volatility3 on ubuntu distribution subsystem:



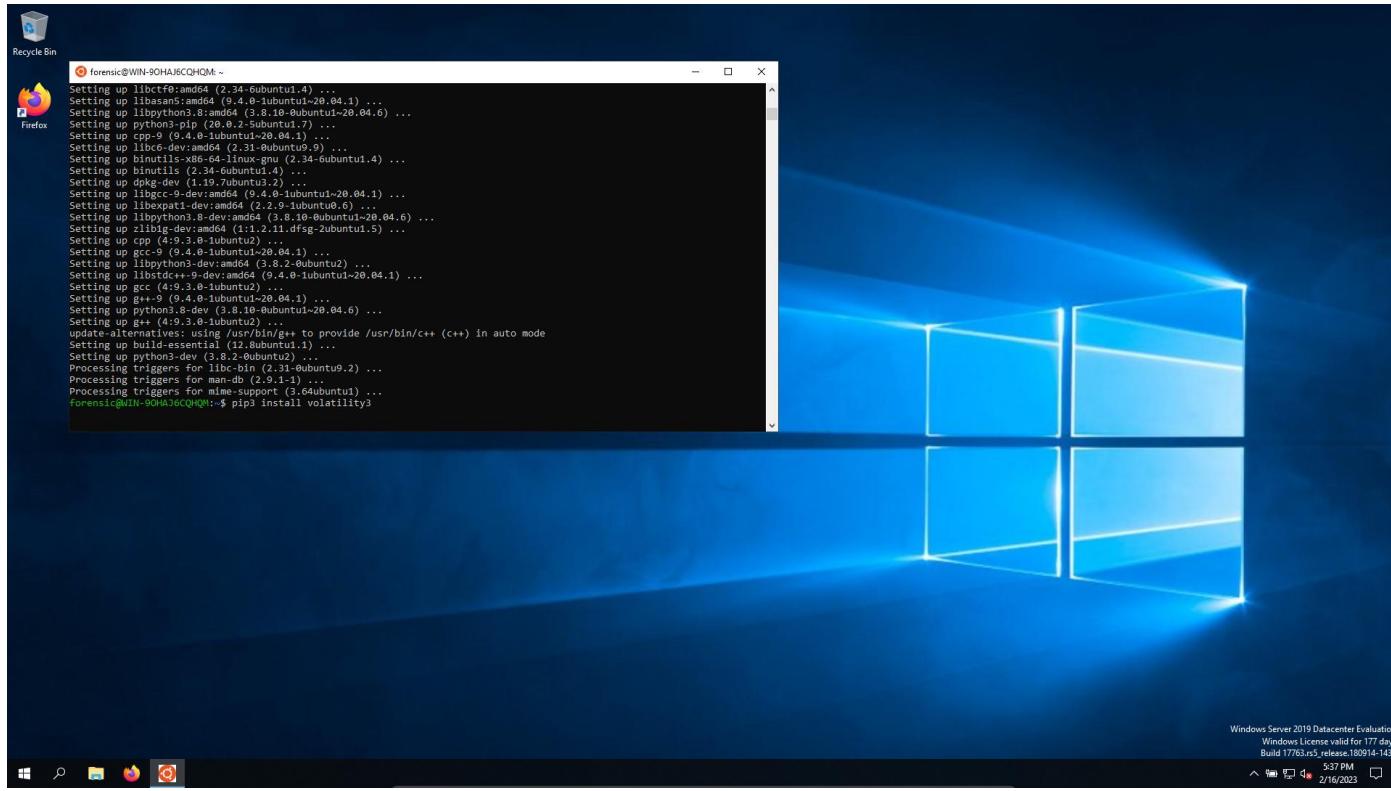
- Update the packets



## - Pip3



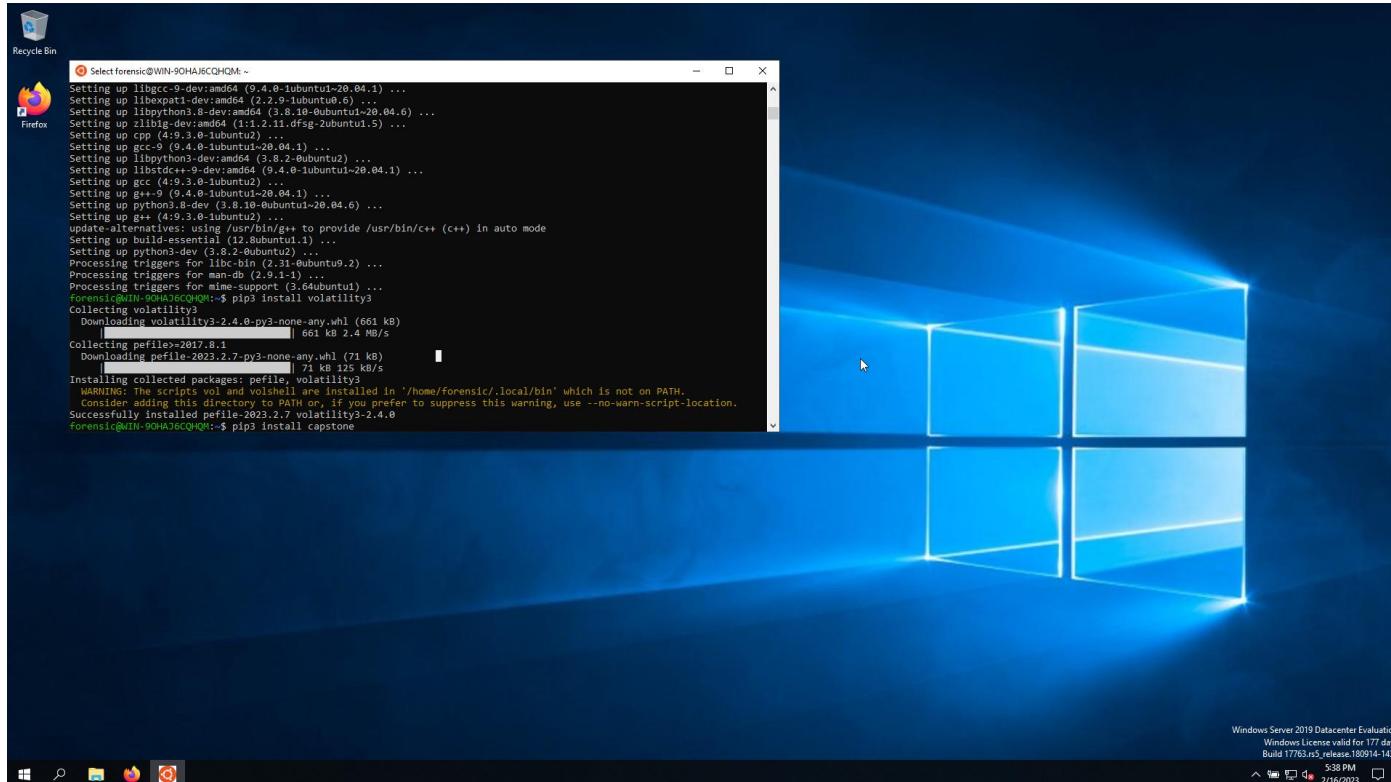
## - Volatility3



```
forensic@WIN-90HAJRCQHQ: ~
Setting up liblctf0:amd64 (2.34~ubuntu1.4) ...
Setting up libasans:amd64 (9.4.0~ubuntul~20.04.1) ...
Setting up libpython3.8:amd64 (3.8.10~ubuntul~20.04.6) ...
Setting up python3-pip (20.0.2~ubuntul.7) ...
Setting up liblctf1:amd64 (2.31~ubuntul~20.04.1) ...
Setting up libc-dev:amd64 (2.31~ubuntul~20.04.9) ...
Setting up binutils-x86_64-linux-gnu (2.34~ubuntul.4) ...
Setting up binutils (2.34~ubuntul.4) ...
Setting up dpkg-dev (1.19.7ubuntul.3) ...
Setting up libgc-9-dev:amd64 (2.2.9~ubuntul~20.04.1) ...
Setting up liblctf1:amd64 (2.31~ubuntul~20.04.1) ...
Setting up libpython3.8-dev:amd64 (3.8.10~ubuntul~20.04.6) ...
Setting up zlib1g-dev:amd64 (1:1.2.11.dfsg-2ubuntul.5) ...
Setting up cpp (4:9.3.0~ubuntul2) ...
Setting up gcc-9 (9.4.0~ubuntul~20.04.1) ...
Setting up libpython3.8-dev:amd64 (3.8.2~ubuntul2) ...
Setting up libstdc++-9-dev:amd64 (9.4.0~ubuntul~20.04.1) ...
Setting up gcc (4:9.3.0~ubuntul2) ...
Setting up g++-9 (9.4.0~ubuntul~20.04.1) ...
Setting up python3.8-dev (3.8.10~ubuntul~20.04.6) ...
Setting up g++ (4:9.3.0~ubuntul2) ...
update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto mode
Setting up build-essential (12.8ubuntul.1) ...
Setting up python3-dev (3.8.2~ubuntul2) ...
Processing triggers for libc-bin (2.31~ubuntul~2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for mime-support (3.64ubuntul) ...
forensic@WIN-90HAJRCQHQ: ~$ pip3 install volatility
```

Windows Server 2019 Datacenter Evaluation  
Windows License valid for 177 days  
Build 17763.555 release.180914-1434  
5:37 PM 2/16/2023

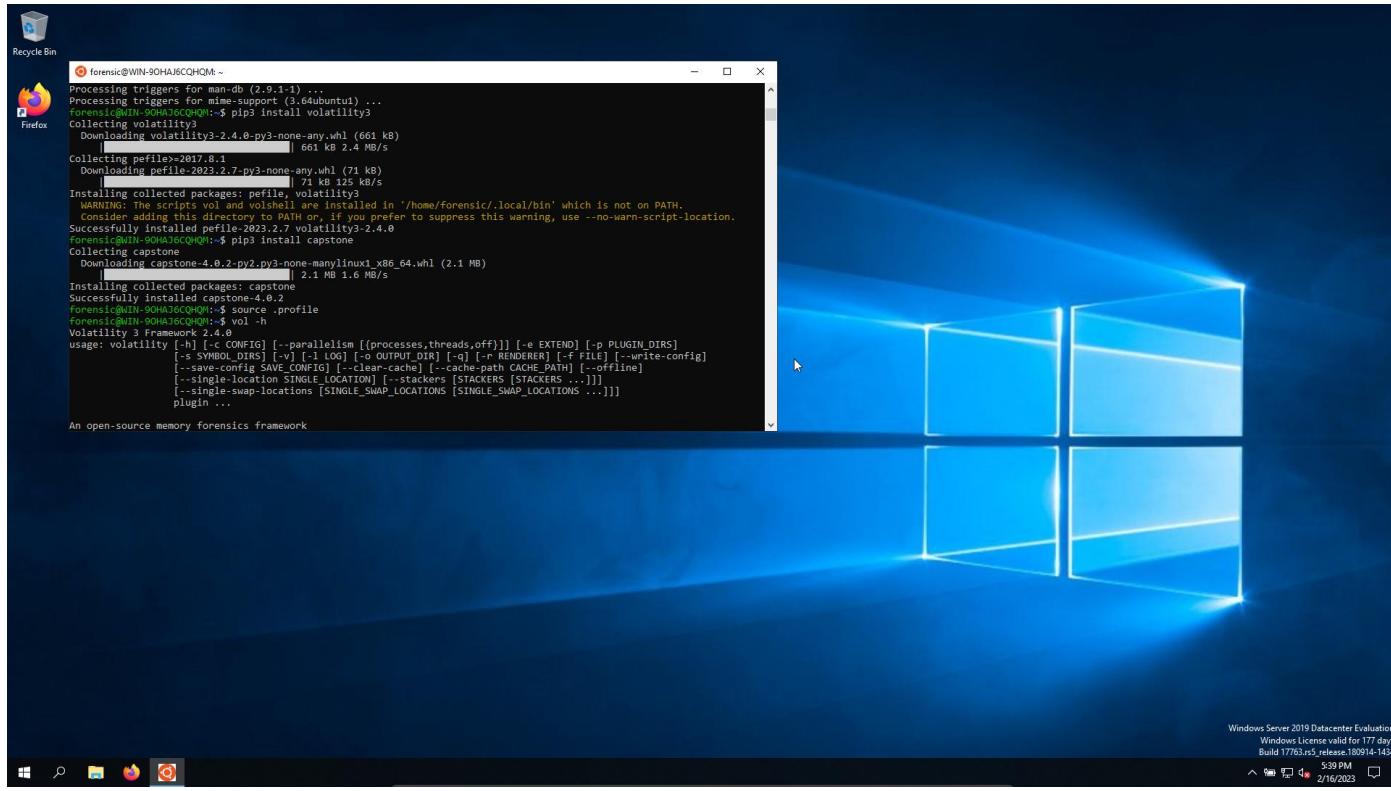
- Plugins for volatility



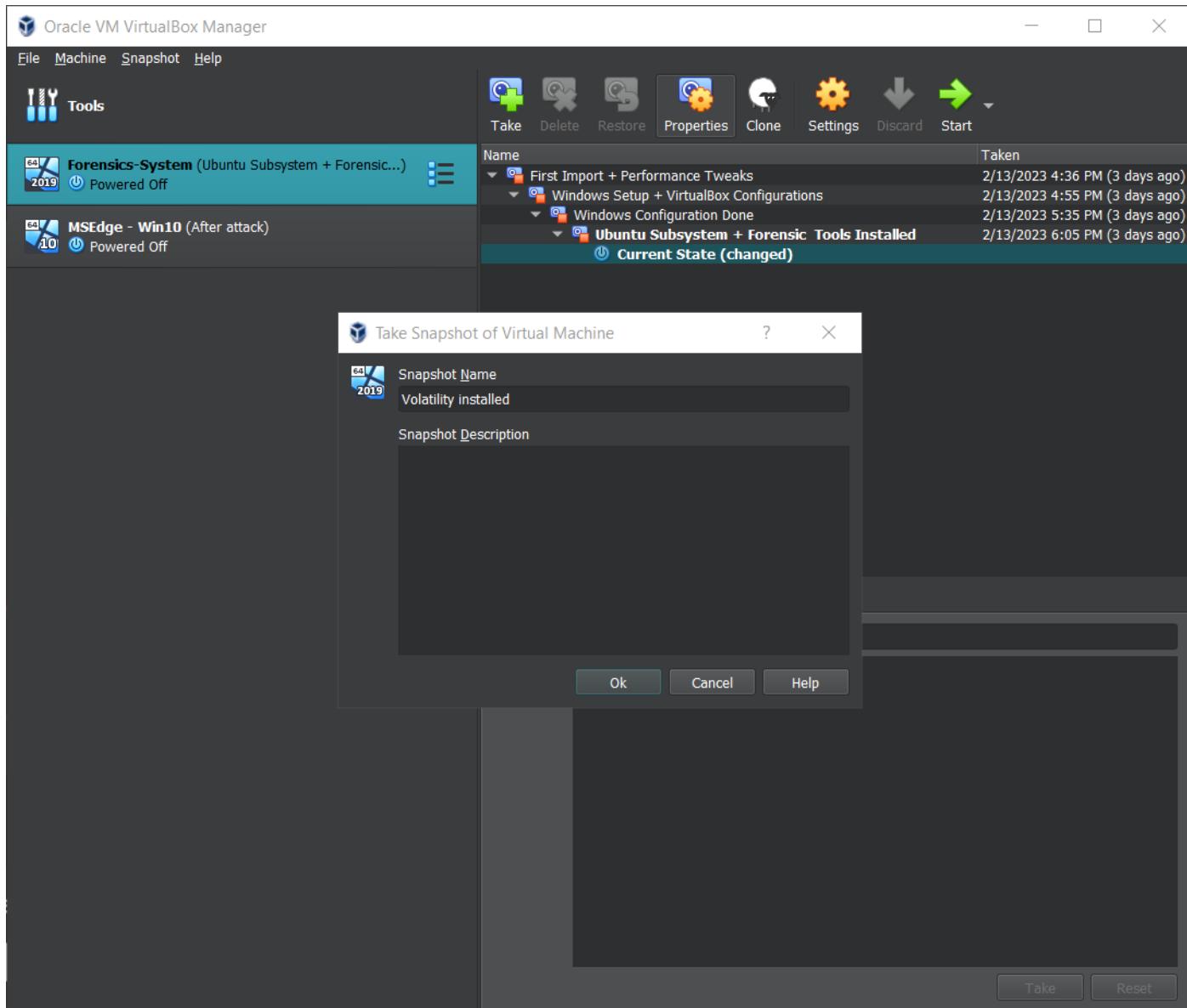
```
forensic@WIN-90HAJRCQHQ: ~
Select forensic@WIN-90HAJRCQHQ: ~
Setting up liblctf0:amd64 (9.4.0~ubuntul~20.04.1) ...
Setting up libxpat1-dev:amd64 (2.2.9~ubuntul0.6) ...
Setting up libpython3.8-dev:amd64 (3.8.10~ubuntul~20.04.6) ...
Setting up zlib1g-dev:amd64 (1:1.2.11.dfsg-2ubuntul.5) ...
Setting up liblctf1:amd64 (2.31~ubuntul~20.04.1) ...
Setting up gcc-9 (9.4.0~ubuntul~20.04.1) ...
Setting up libpython3.8-dev:amd64 (3.8.2~ubuntul2) ...
Setting up libstdc++-9-dev:amd64 (9.4.0~ubuntul~20.04.1) ...
Setting up gcc (4:9.3.0~ubuntul2) ...
Setting up g++-9 (9.4.0~ubuntul~20.04.1) ...
Setting up python3.8-dev (3.8.10~ubuntul~20.04.6) ...
Setting up g++ (4:9.3.0~ubuntul2) ...
update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto mode
Setting up build-essential (12.8ubuntul.1) ...
Setting up python3-dev (3.8.2~ubuntul2) ...
Processing triggers for libc-bin (2.31~ubuntul~2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for mime-support (3.64ubuntul) ...
forensic@WIN-90HAJRCQHQ: ~$ pip3 install volatility3
Collecting volatility3
  Downloading volatility3-2.4.0-py3-none-any.whl (661 kB)
    661 kB 2.4 MB/s
Collecting pefile>=2017.8.1
  Downloading pefile-2023.2.7-py3-none-any.whl (73 kB)
    73 kB 125 kB/s
Installing collected packages: pefile, volatility3
  WARNING: The scripts vol and volshell are installed in '/home/forensic/.local/bin' which is not on PATH.
  Consider adding this directory to PATH or --no-warn-script-location.
Successfully installed pefile-2023.2.7 volatility3-2.4.0
forensic@WIN-90HAJRCQHQ: ~$ pip3 install capstone
```

Windows Server 2019 Datacenter Evaluation  
Windows License valid for 177 days  
Build 17763.555 release.180914-1434  
5:38 PM 2/16/2023

- Reload the bash profile and check the volatility3.



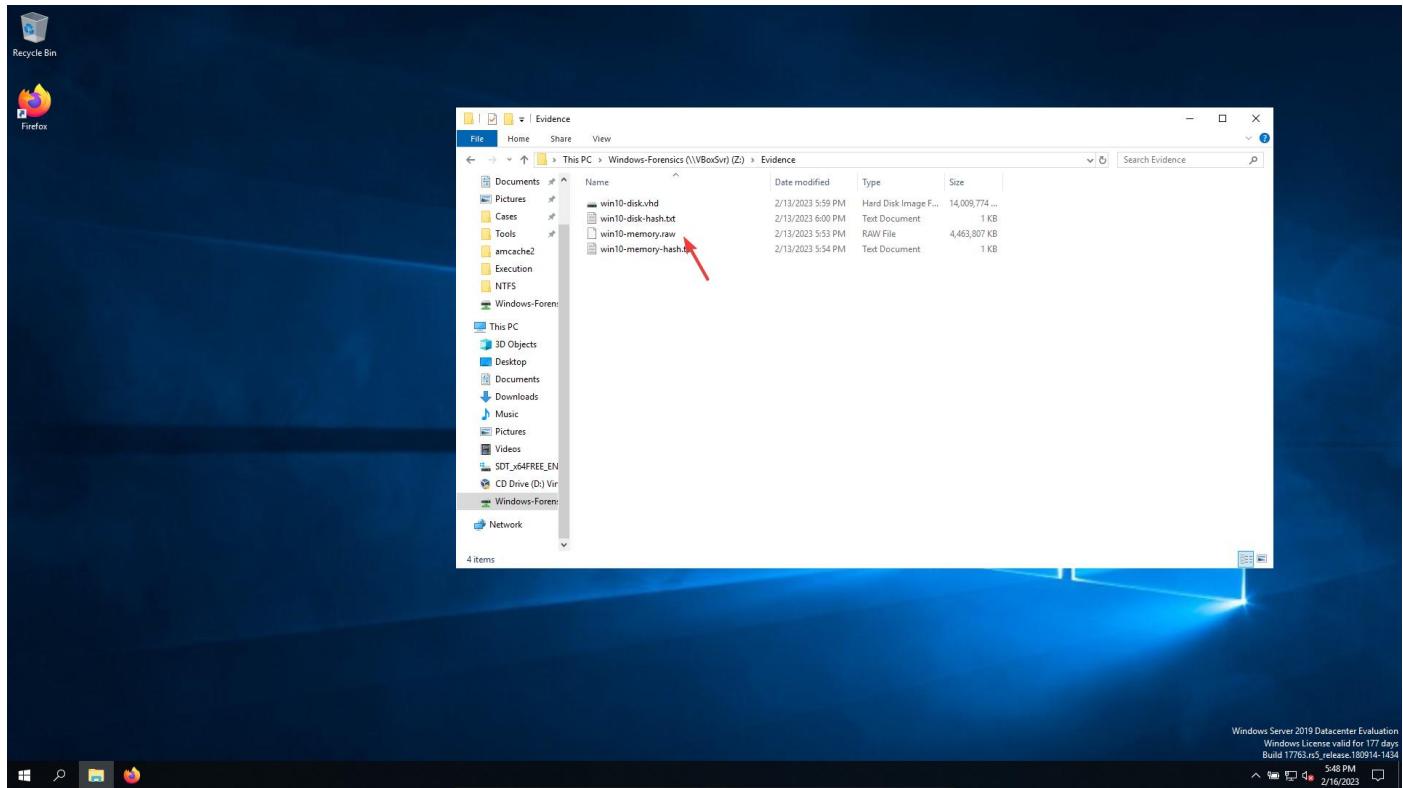
- Snapshot of the forensic virtual machine:



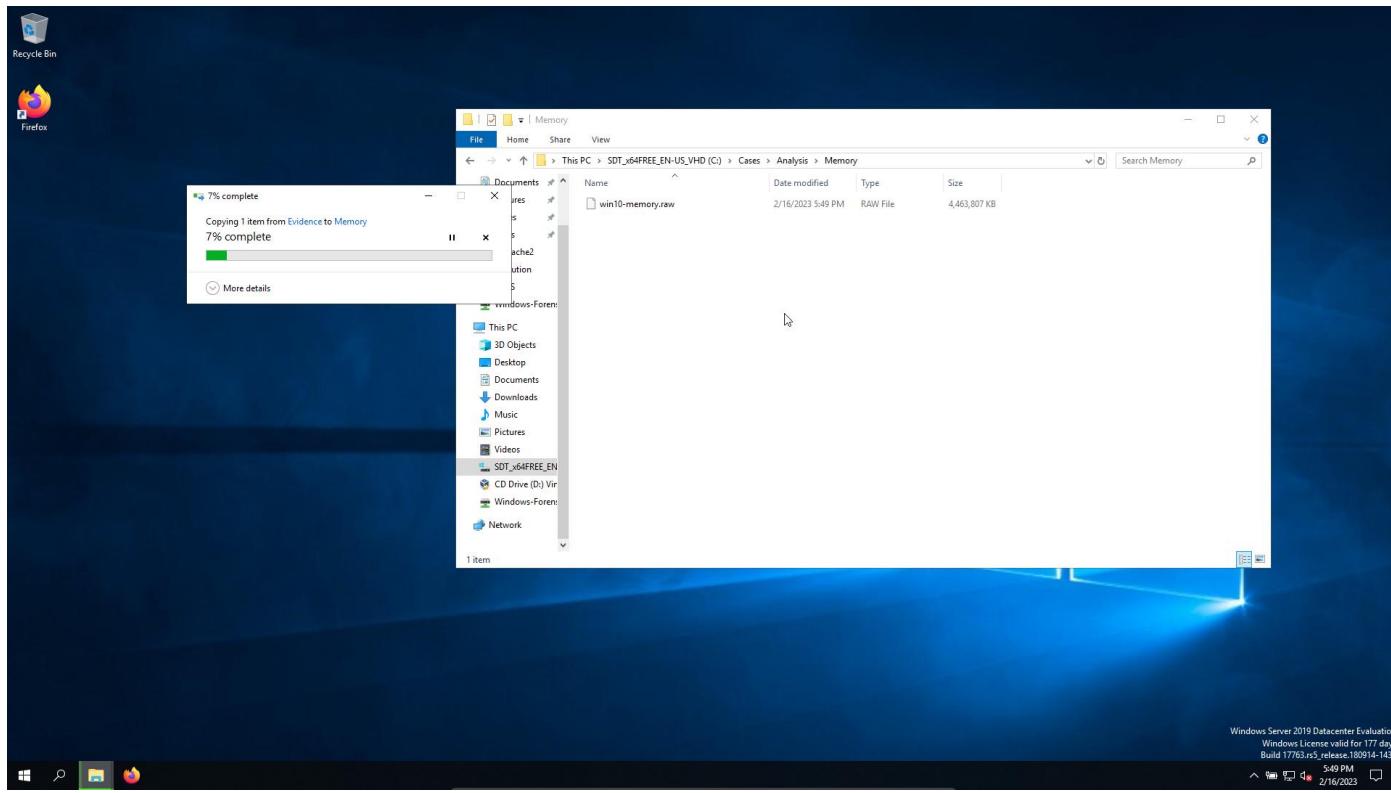
## Important files for memory analysis

- The memory is volatile data
- Files important for memory analysis:
  - o 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.

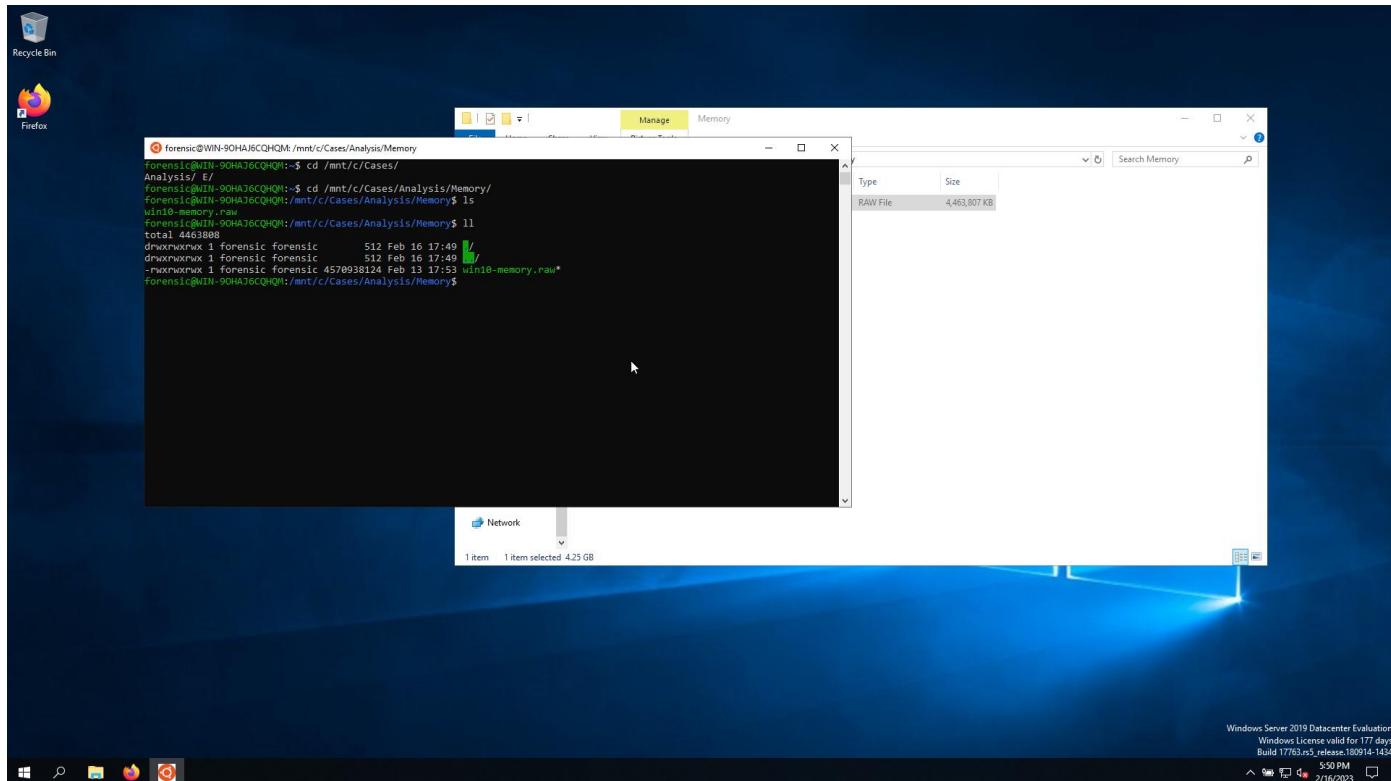
- Pagefile.sys and Swapfile.sys , exists for saving some space .
- Acquired memory iamge evidence:



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

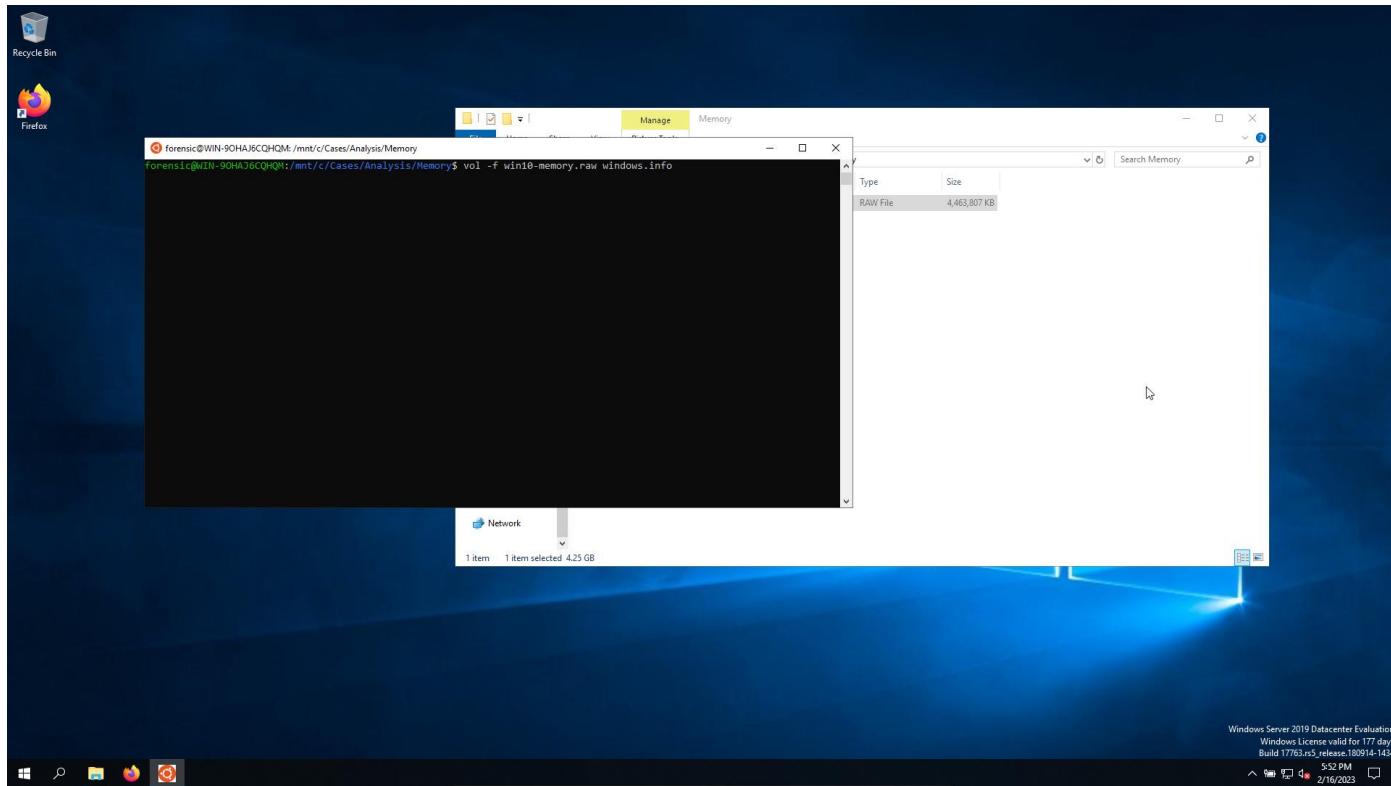


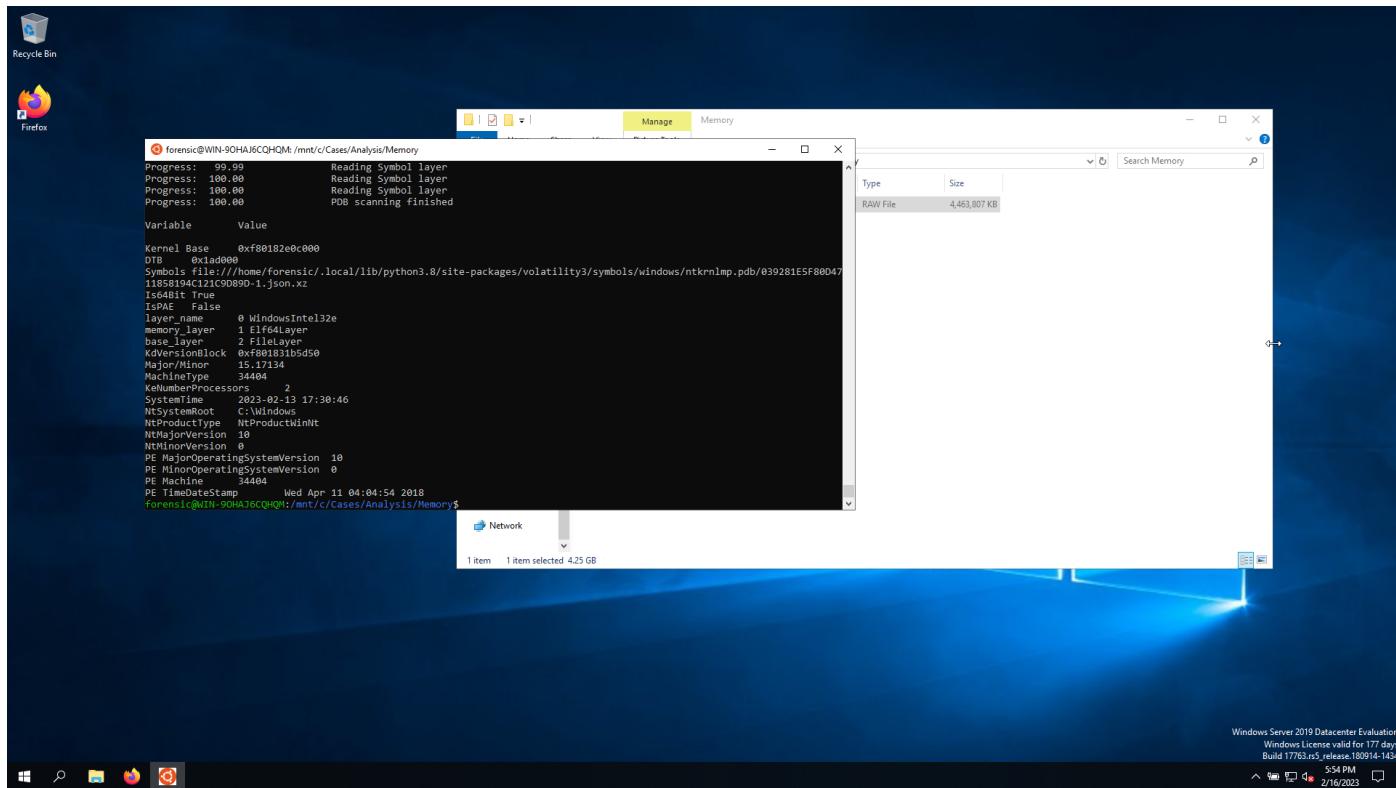
- Go to the location of the memory file, in ubuntu subsystem:



## Windows system information

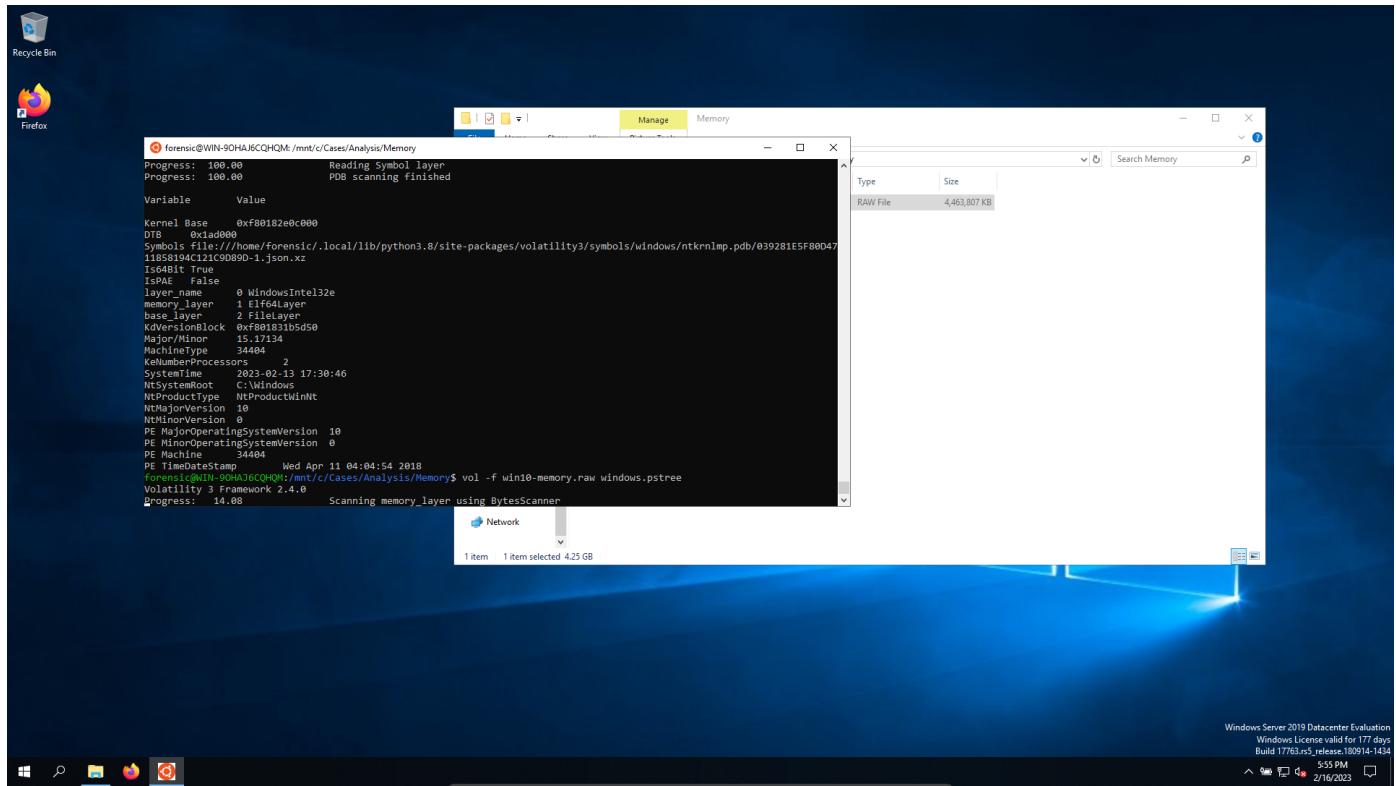
- With volatility3 , the profile is no longer needed to give as a command argument, it searches and downloads the specific symbol table needed and profile.
- Volatility3 plugin for windows system information:





## Suspicious processes

- See the process tree :



```

forensic@WIN-90HAJ6CQHQM:/mnt/c/Cases/Analysis/Memory
IsPAE False
LayeredMemory 0 WindowsIntel32e
memory_layer 1 Elf64Loser
base_layer 2 FileLayer
KdVersionBlock 0xf801831b5d50
MajorVersion 15.1734
MachineType 34404
MemoryCompression 2
SystemTime 2023-02-13 17:30:46
NtSystemRoot C:\Windows
NtProductType NTProductWinNt
NtMajorVersion 10
NtMinorVersion 0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine 34404
PE TimeStamp Wed Apr 11 04:04:54 2018
Forensic@WIN-90HAJ6CQHQM:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.psTree
Volatility Framework 2.4.0
Progress: 100.00 PDB scanning finished
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime
4 0 System 0xe10d056cc240 100 - N/A False 2023-02-14 03:11:07.000000 N/A
4 4 Registry 0xe10d0574f0d0 3 - N/A False 2023-02-14 03:11:07.000000 N/A
296 4 smss.exe 0xe10d0574f0d0 3 - N/A False 2023-02-13 17:11:27.000000 N/A
* 1740 4 Memcompression 0xe10d06ee9c0 38 - N/A False 2023-02-13 17:11:27.000000 N/A
392 384 csrss.exe 0xe10d0b0402580 11 - 0 False 2023-02-14 03:11:26.000000 N/A
480 464 csrss.exe 0xe10d0b11d580 12 - 1 False 2023-02-14 03:11:26.000000 N/A
472 384 wininit.exe 0xe10d0a93f080 6 - 0 False 2023-02-14 03:11:26.000000 N/A
* 620 472 lsass.exe 0xe10d0a599080 11 - 0 False 2023-02-14 03:11:27.000000 N/A
* 736 472 faketcpport.exe 0xe10d0b22b580 5 - 0 False 2023-02-13 17:11:27.000000 N/A
* 612 472 services.exe 0xe10d0b22b580 19 - 0 False 2023-02-14 03:11:27.000000 N/A
** 6784 612 svchost.exe 0xe10d06515180 30 - 0 False 2023-02-13 17:11:46.000000 N/A
*** 8048 6784 MusNotifyIcon_ 0xe10d083cf580 5 - 1 False 2023-02-13 17:19:23.000000 N/A
* 1668 612 svchost.exe 0xe10d056c2580 10 - 0 False 2023-02-13 17:11:29.000000 N/A
* 1740 612 svchost.exe 0xe10d0574f0d0 6 - 0 False 2023-02-13 17:11:29.000000 N/A
* 1288 612 svchost.exe 0xe10d0578c580 6 - 0 False 2023-02-14 03:11:26.000000 N/A
* 6408 612 svchost.exe 0xe10d08dc2580 21 - 1 False 2023-02-13 17:13:34.000000 N/A
** 1154 612 svchost.exe 0xe10d0b05080 6 - 0 False 2023-02-14 03:11:28.000000 N/A
* 1804 612 svchost.exe 0xe10d0b084230 5 - 0 False 2023-02-13 17:11:30.000000 N/A
* 2192 612 svchost.exe 0xe10d0b091380 5 - 0 False 2023-02-13 17:11:30.000000 N/A
* 3064 612 svchost.exe 0xe10d0b091380 5 - 0 False 2023-02-13 17:11:30.000000 N/A
* 1638 612 svchost.exe 0xe10d08515180 6 - 0 False 2023-02-13 17:13:31.000000 N/A
** 1844 612 svchost.exe 0xe10d08c0cf580 4 - 0 False 2023-02-14 03:11:28.000000 N/A
* 2324 612 svchost.exe 0xe10d0b0957580 3 - 0 False 2023-02-13 17:11:30.000000 N/A
** 2452 612 cygrunsrv.exe 0xe10d0bc77580 6 - 0 False 2023-02-13 17:11:31.000000 N/A
* 3328 2452 cygrunsrv.exe 0xe10d0c4d3580 0 - 0 False 2023-02-13 17:11:33.000000 2023-02-13 17:11:33.000000
*** 3328 3328 svchost.exe 0xe10d0b0c05580 5 - 0 False 2023-02-13 17:11:33.000000 N/A
*** 3328 3328 sshd.exe 0xe10d0c080800 5 - 0 False 2023-02-13 17:11:33.000000 N/A
** 4756 612 SearchIndexer_ 0xe10d0c4d3580 18 - 0 False 2023-02-13 17:11:38.000000 N/A
** 926 612 svchost.exe 0xe10d08c70580 6 - 0 False 2023-02-14 03:11:27.000000 N/A
** 2456 612 svchost.exe 0xe10d0bab2c080 4 - 0 False 2023-02-13 17:11:30.000000 N/A
* 77 612 svchost.exe 0xe10d0bb50580 16 - 0 False 2023-02-13 17:11:30.000000 N/A
* 5268 612 svchost.exe 0xe10d0bb50580 9 - 0 False 2023-02-13 17:11:31.000000 N/A
** 1554 612 svchost.exe 0xe10d056f9580 11 - 0 False 2023-02-14 03:11:28.000000 N/A
** 4248 612 AtomicService. 0xe10d0b6731580 6 - 0 False 2023-02-13 17:28:30.000000 N/A
** 2464 612 SecurityHealth 0xe10d0bab4580 17 - 0 False 2023-02-13 17:11:30.000000 N/A
* 680 612 svchost.exe 0xe10d0b0c1380 5 - 0 False 2023-02-14 03:11:28.000000 N/A
* 751 612 svchost.exe 0xe10d0b0c1380 3 - 0 False 2023-02-14 03:11:28.000000 N/A
* 604 612 svchost.exe 0xe10d0b0c15580 39 - 0 False 2023-02-14 03:11:28.000000 N/A
** 816 612 svchost.exe 0xe10d0b0c78580 29 - 0 False 2023-02-14 03:11:27.000000 N/A
** 4352 816 ShellExperience 0xe10d0c48f080 32 - 1 False 2023-02-13 17:11:36.000000 N/A
** 4864 816 ApplicationFra 0xe10d059f4580 11 - 1 False 2023-02-13 17:11:38.000000 N/A

```

- Put output into a text file for easier search:

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

```

forensic@WIN-90HAJ6CQHOM:/mnt/c/Cases/Analysis/Memory
*** 1864 612 svchost.exe 0xe10dd0b744000 4 - 0 False 2023-02-13 17:11:29.000000 N/A
*** 1872 612 svchost.exe 0xe10dd0c595000 7 - 0 False 2023-02-13 17:11:32.000000 N/A
*** 730 612 svchost.exe 0xe10dd0c7f9100 2 - 0 False 2023-02-14 03:11:27.000000 N/A
*** 1232 612 svchost.exe 0xe10dd0509500 10 - 0 False 2023-02-14 03:11:28.000000 N/A
*** 3492 1232 svhost.exe 0xe10dd0c0cea300 19 - 1 False 2023-02-13 17:11:34.000000 N/A
*** 1872 612 svchost.exe 0xe10dd0730500 7 - 0 False 2023-02-13 17:11:29.000000 N/A
*** 3195 612 svchost.exe 0xe10dd0c595000 7 - 0 False 2023-02-13 17:11:32.000000 N/A
*** 2302 612 svchost.exe 0xe10dd0c595100 15 - 0 False 2023-02-13 17:11:32.000000 N/A
*** 7252 612 svchost.exe 0xe10ddac52500 4 - 0 False 2023-02-13 17:13:14.000000 N/A
*** 1240 612 svchost.exe 0xe10dd05604500 10 - 0 False 2023-02-14 03:11:28.000000 N/A
*** 2520 612 MsMpEng.exe 0xe10dd0bae8100 19 - 0 False 2023-02-13 17:11:30.000000 N/A
*** 1752 612 SgrmBroker.exe 0xe10dd08a40000 2 - 0 False 2023-02-13 17:13:32.000000 N/A
*** 868 612 svchost.exe 0xe10dd08c745000 23 - 0 False 2023-02-13 17:11:32.000000 N/A
*** 2400 612 svchost.exe 0xe10dd08c745100 15 - 0 False 2023-02-13 17:11:32.000000 N/A
*** 3552 612 svchost.exe 0xe10dd0c0f9500 12 - 1 False 2023-02-13 17:11:34.000000 N/A
*** 3688 612 svchost.exe 0xe10dd0c173400 8 - 0 False 2023-02-13 17:11:34.000000 N/A
*** 354 612 svchost.exe 0xe10dd08c11500 5 - 0 False 2023-02-14 03:11:28.000000 N/A
*** 1124 612 svchost.exe 0xe10dd052e300 21 - 0 False 2023-02-14 03:11:28.000000 N/A
*** 1124 612 svchost.exe 0xe10dd052e300 11 - 1 False 2023-02-13 17:11:34.000000 N/A
*** 1636 612 svchost.exe 0xe10dd056fd500 0 - 0 False 2023-02-13 17:11:29.000000 N/A
*** 4688 612 svchost.exe 0xe10dd0199500 39 - 0 False 2023-02-13 17:11:35.000000 N/A
*** 1512 612 VBoxService.exe 0xe10dd056fd500 12 - 0 False 2023-02-14 03:11:28.000000 N/A
*** 1764 612 svchost.exe 0xe10dd0ccc0000 18 - 0 False 2023-02-13 17:13:12.000000 N/A
*** 6376 612 svchost.exe 0xe10dd0a85b3400 8 - 0 False 2023-02-13 17:13:29.000000 N/A
*** 3932 612 svchost.exe 0xe10dd0a85b3400 10 - 0 False 2023-02-13 17:13:29.000000 N/A
*** 1644 612 svchost.exe 0xe10dd056cf7500 4 - 0 False 2023-02-13 17:11:29.000000 N/A
*** 2028 612 svchost.exe 0xe10dd0a039500 5 - 0 False 2023-02-13 17:11:30.000000 N/A
*** 2412 612 svchost.exe 0xe10dd0ba0b3400 16 - 0 False 2023-02-13 17:11:30.000000 N/A
*** 2544 612 wlms.exe 0xe10dd0ba0f500 4 - 0 False 2023-02-13 17:11:30.000000 N/A
*** 880 612 svchost.exe 0xe10dd0a565000 0 - 0 False 2023-02-13 17:13:09.000000 2023-02-13 17:14:24.000000
*** 3752 612 svchost.exe 0xe10dd0a565000 6 - 0 False 2023-02-13 17:13:09.000000 N/A
*** 2036 612 svchost.exe 0xe10dd0b03f500 13 - 0 False 2023-02-13 17:11:30.000000 N/A
*** 2420 612 svchost.exe 0xe10dd0baa0100 6 - 0 False 2023-02-13 17:11:30.000000 N/A
*** 7668 612 svchost.exe 0xe10dd0aae0340 4 - 0 False 2023-02-13 17:13:29.000000 N/A
*** 3832 612 svchost.exe 0xe10dd0c197500 4 - 0 False 2023-02-13 17:11:34.000000 N/A
*** 3984 612 3932 612 ctmon.exe 0xe10dd0c203500 10 - 1 False 2023-02-13 17:11:34.000000 N/A
*** 2556 612 svchost.exe 0xe10dd0bb01200 9 - 0 False 2023-02-13 17:11:30.000000 N/A
*** 548 464 winlogon.exe 0xe10dd08dff5000 6 - 1 False 2023-02-14 03:11:27.000000 N/A
*** 744 540 fontdrvhost.exe 0xe10dd08c7e500 5 - 1 False 2023-02-14 03:11:27.000000 N/A
*** 3116 540 userinit.exe 0xe10dd0c200500 0 - 1 False 2023-02-13 17:11:35.000000 2023-02-13 17:12:02.000000
*** 3356 3316 explorer.exe 0xe10dd02c2f400 94 - 1 False 2023-02-13 17:11:35.000000 N/A
*** 65 3356 powershell.exe 0xe10dd02c2f400 0 - 1 False 2023-02-13 17:11:35.000000 2023-02-13 17:26:91.000000
*** 5582 612 powershell_ise.exe 0xe10dd065a5500 0 - 1 False 2023-02-13 17:22:45.000000 2023-02-13 17:24:16.000000
*** 5416 3356 powershell_ise.exe 0xe10dd06819580 0 - 1 False 2023-02-13 17:23:27.000000 2023-02-13 17:23:27.000000
*** 5576 3356 powershell_ise.exe 0xe10dd061f0400 0 - 1 False 2023-02-13 17:23:32.000000 2023-02-13 17:23:33.000000
*** 7080 3356 powershell.exe 0xe10dd0c0f02280 16 - 1 False 2023-02-13 17:26:23.000000 N/A
*** 6600 7080 powershell.exe 0xe10dd0c0f74000 5 - 1 False 2023-02-13 17:26:23.000000 N/A
*** 7080 3356 powershell_ise.exe 0xe10dd0c0f4000 3 - 1 False 2023-02-13 17:26:23.000000 N/A
*** 6544 3356 MicrosofttfdGpu.exe 0xe10dd0cad0800 0 - 1 True 2023-02-13 17:11:56.000000 2023-02-13 17:11:56.000000
*** 6552 3356 OneDrive.exe 0xe10dd082c5580 22 - 1 False 2023-02-13 17:11:51.000000 N/A
*** 6296 3356 VBoxTray.exe 0xe10dd06549580 14 - 1 False 2023-02-13 17:11:51.000000 N/A
*** 996 540 dvm.exe 0xe10dd0b48a00 15 - 1 False 2023-02-14 03:11:27.000000 N/A
*** 3164 5356 notepad.exe 0xe10dd05b2080 4 - 1 False 2023-02-13 17:28:32.000000 N/A
3164 5356 notepad.exe 0xe10dd05b2080 4 - 1 False 2023-02-13 17:28:32.000000 N/A
forensic@WIN-90HAJ6CQHOM:/mnt/c/Cases/Analysis/Memory$ -

```

## - Pids:

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

## Dumping processes

### - Printing of a particular process:

- Dumping a particular process:

```
forensic@NIN-90HAJ6CQHQM:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pslist --pid 4248 --dump
Volatility 3 Framework 2.4.0
Progress: 100.00          PDB scanning finished
PID      PPID      ImageFileName  Offset(V)      Threads Handles SessionId      Wow64   CreateTime           ExitTime      File output
4248      612      AtomicService.  0xe10d06731580  6      -      0      False  2023-02-13 17:28:30.0000000  N/A      pid.4248.0x370000.dmp
```

```

forensic@WIN-9OHAJ6CQHOM:/mnt/c/Cases/Analysis/Memory$ 
7088 3356 MSACUil.exe 0xe10dd064b580 3 - 1 False 2023-02-13 17:11:51.000000 N/A Disabled
0392 3356 VBoxTray.exe 0xe10dd064b580 14 - 1 False 2023-02-13 17:11:51.000000 N/A Disabled
0552 3356 OneDrive.exe 0xe10dd062c580 22 - 1 False 2023-02-13 17:11:51.000000 N/A Disabled
0544 3356 MicrosoftEdgeU 0xe10dd0cadb880 0 - 1 True 2023-02-13 17:11:56.000000 2023-02-13 17:11:56.000000
isabled
3272 816 dllhost.exe 0xe10dd0647580 5 - 1 False 2023-02-13 17:12:19.000000 N/A Disabled
888 612 svchost.exe 0xe10dd0a5d5300 0 - 0 False 2023-02-13 17:13:09.000000 2023-02-13 17:14:24.000000
isabled
1586 612 svchost.exe 0xe10dd0cce088 18 - 0 False 2023-02-13 17:13:12.000000 N/A Disabled
7252 612 svchost.exe 0xe10dd0ac52580 4 - 0 False 2023-02-13 17:13:14.000000 N/A Disabled
6376 612 svchost.exe 0xe10dd0a85b340 8 - 0 False 2023-02-13 17:13:29.000000 N/A Disabled
7668 612 svchost.exe 0xe10dd0aae0340 4 - 0 False 2023-02-13 17:13:29.000000 N/A Disabled
1688 612 sedisvc.exe 0xe10dd085a1880 6 - 0 False 2023-02-13 17:13:31.000000 N/A Disabled
5262 612 svchost.exe 0xe10dd0a85b340 9 - 0 False 2023-02-13 17:13:33.000000 N/A Disabled
1752 612 SgvBroker.exe 0xe10dd08a40080 2 - 0 False 2023-02-13 17:13:32.000000 N/A Disabled
1300 612 svchost.exe 0xe10dd0847c7580 10 - 0 False 2023-02-13 17:13:32.000000 N/A Disabled
6408 612 svchost.exe 0xe10dd08d7c580 21 - 1 False 2023-02-13 17:13:34.000000 N/A Disabled
7592 612 svchost.exe 0xe10dd0a6df580 3 - 0 False 2023-02-13 17:13:41.000000 N/A Disabled
7912 816 Win32-Driver 0xe10dd0a65c9388 7 - 0 False 2023-02-13 17:13:44.000000 N/A Disabled
8012 816 dllhost.exe 0xe10dd0a65c9388 6 - 0 False 2023-02-13 17:16:34.000000 N/A Disabled
6328 816 Microsoft.Photo 0xe10dd0a605808 15 - 1 False 2023-02-13 17:18:29.000000 N/A Disabled
8076 816 RuntimeBroker 0xe10dd0a6043580 5 - 1 False 2023-02-13 17:18:39.000000 N/A Disabled
6724 816 SkypeApp.exe 0xe10dd0a49580 13 - 1 False 2023-02-13 17:18:48.000000 N/A Disabled
7980 816 RuntimeBroker 0xe10dd0fcfc580 4 - 1 False 2023-02-13 17:18:57.000000 N/A Disabled
6098 6708 MusNotifyIcon 0xe10dd0a65c9388 5 - 1 False 2023-02-13 17:19:06.000000 N/A Disabled
6116 612 svchost.exe 0xe10dd0c52988 5 - 0 False 2023-02-13 17:19:26.000000 N/A Disabled
756 816 smartscreen.exe 0xe10dd06f7c7880 9 - 1 False 2023-02-13 17:21:29.000000 N/A Disabled
4400 816 OpenWith.exe 0xe10dd0685e088 6 - 1 False 2023-02-13 17:22:39.000000 N/A Disabled
7796 4400 notepad.exe 0xe10dd00fa580 0 - 1 False 2023-02-13 17:22:41.000000 2023-02-13 17:22:44.000000
isabled
5896 3356 powershell_ise 0xe10dd0685a580 0 - 1 False 2023-02-13 17:22:45.000000 2023-02-13 17:24:16.000000
isabled
5416 3356 powershell_ise 0xe10dd06819580 0 - 1 False 2023-02-13 17:23:27.000000 2023-02-13 17:23:27.000000
isabled
5576 3356 powershell_ise 0xe10dd061f0400 0 - 1 False 2023-02-13 17:23:32.000000 2023-02-13 17:23:33.000000
isabled
54 3356 powershell.exe 0xe10dd08dec580 0 - 1 False 2023-02-13 17:25:01.000000 2023-02-13 17:26:01.000000
isabled
6320 612 Sysmon.exe 0xe10dd0cad580 12 - 0 False 2023-02-13 17:25:15.000000 N/A Disabled
6796 816 unscapp.exe 0xe10dd08416580 3 - 0 False 2023-02-13 17:25:16.000000 N/A Disabled
7080 3356 powershell.exe 0xe10dd0f62280 16 - 1 False 2023-02-13 17:26:23.000000 N/A Disabled
6068 7088 conhost.exe 0xe10dd0c79388 5 - 1 False 2023-02-13 17:26:23.000000 N/A Disabled
3242 612 AppContainer.exe 0xe10dd0c31880 6 - 0 False 2023-02-13 17:28:31.000000 N/A Disabled
3164 5356 notepad.exe 0xe10dd05bd2880 4 - 1 False 2023-02-13 17:28:32.000000 N/A Disabled
Forensic@WIN-9OHAJ6CQHOM:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pslist --pid 4248
Volatility 3 Framework 2.4.0
Progress: 100.00 PDB scanning finished PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime File output
4248 612 AtomicService. 0xe10dd0671580 6 - 0 False 2023-02-13 17:28:30.000000 2023-02-13 17:24:16.000000
Forensic@WIN-9OHAJ6CQHOM:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pslist --pid 4248 --dump
Volatility 3 Framework 2.4.0
Progress: 100.00 PDB scanning finished PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime File output
4248 612 AtomicService. 0xe10dd0671580 6 - 0 False 2023-02-13 17:28:30.000000 N/A pid.4248.0x370000.dmp
Forensic@WIN-9OHAJ6CQHOM:/mnt/c/Cases/Analysis/Memory$ ll
total 4463840
drwxrwxrwx 1 forensic forensic 512 Feb 16 18:13 /forensic
drwxrwxrwx 1 forensic forensic 512 Feb 16 17:59 /forensic/forensic
-rw-rwxrwx 1 forensic forensic 32768 Feb 16 18:13 pid.4248.0x370000.dmp*
-rw-rwxrwx 1 forensic forensic 4579938124 Feb 13 17:53 win10-memory.raw*
Forensic@WIN-9OHAJ6CQHOM:/mnt/c/Cases/Analysis/Memory$ 

```

## - Analysis of the dump process:

```

forensic@WIN-9OHAJ6CQHOM:/mnt/c/Cases/Analysis/Memory$ 
4248 612 AtomicService. 0xe10dd0671580 6 - 0 False 2023-02-13 17:28:30.000000 N/A Disabled
Forensic@WIN-9OHAJ6CQHOM:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.pslist --pid 4248 -dump
Volatility 3 Framework 2.4.0
Progress: 100.00 PDB scanning finished PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime File output
4248 612 AtomicService. 0xe10dd0671580 6 - 0 False 2023-02-13 17:28:30.000000 N/A pid.4248.0x370000.dmp
Forensic@WIN-9OHAJ6CQHOM:/mnt/c/Cases/Analysis/Memory$ ll
total 4463840
drwxrwxrwx 1 forensic forensic 512 Feb 16 18:13 /forensic
drwxrwxrwx 1 forensic forensic 512 Feb 16 17:49 /forensic/forensic
-rw-rwxrwx 1 forensic forensic 32768 Feb 16 18:13 pid.4248.0x370000.dmp*
-rw-rwxrwx 1 forensic forensic 4579938124 Feb 13 17:53 win10-memory.raw*
Forensic@WIN-9OHAJ6CQHOM:/mnt/c/Cases/Analysis/Memory$ strings pid.4248.0x370000.dmp
!This program cannot be run in DOS mode.
.text
._rsrc
._reloc
._res
v4.0.30319
#Strings
#GUID
#Blob
#WOW64
AtomicService.exe
Service1
AtomicService
System.ServiceProcess
ServiceBase
System
System.ComponentModel
Container
Components
._ctor
Main
InitializeComponent
Dispose
OnStart
OnStop
OnContinue
disposing
EventArgs
mscorlib
System.Runtime.CompilerServices
CompilationRelaxationsAttribute
RuntimeCompatibilityAttribute
get_ServiceName
get_WrapExceptionThrows
_CorExhail
Mscoree.dll
<xml version="1.0" encoding="UTF-8" standalone="yes">
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0" >
<assemblyIdentity version="1.0.0.0" name="MyApplication.app" />
<trustInfo xmlns="urn:schemas-microsoft-com:asms.v2" >
<requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3" >
<requestedExecutionLevel level="asInvoker" uiAccess="false"/>
</requestedPrivileges>
</security>
</trustInfo>
</assembly>
Forensic@WIN-9OHAJ6CQHOM:/mnt/c/Cases/Analysis/Memory$ 

```

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

```

forensic@WIN-90HAJ6CQHOM:/mnt/c/Cases/Analysis/Memory
[forensic@WIN-90HAJ6CQHOM:/mnt/c/Cases/Analysis/Memory]$ vol -f win10-memory.raw windows.pslist -pid 4248 --dump
Volatility Framework 2.4.0
Progress: 100.00% PDB scanning finished
PID    PPID   ImageFileName  Offset(V)  Threads Handles SessionId  Wow64  CreateTime      ExitTime      File output
4248   612    AtomicService.  0xe10dd6731580  6      0     False  2023-02-13 17:28:30.000000  N/A   pid.4248.0x370000.dmp
forensic@WIN-90HAJ6CQHOM:/mnt/c/Cases/Analysis/Memory$ ll
total 448
drwxrwxrwx 1 forensic forensic 512 Feb 16 18:13 .
drwxrwxrwx 1 forensic forensic 512 Feb 16 17:49 .
-rw-rwxrwx 1 forensic forensic 32768 Feb 16 18:13 pid.4248.0x370000.dmp*
-rw-rwxrwx 1 forensic forensic 4570938124 Feb 13 17:53 win10-memory.raw*
forensic@WIN-90HAJ6CQHOM:/mnt/c/Cases/Analysis/Memory$ strings pid.4248.0x370000.dmp
This program cannot be run in DOS mode.
.text
.rsrc
@.reloc
*BSJB
.WEBP.B3B19
.MSFTLangs
#GUID
#Blob
<Module>
AtomicService.exe
Service
AtomicService
System.ServiceProcess
ServiceBase
System
System.ComponentModel
Container
Components
.Lctor
Main
InitializeComponent
Dispose
OnStart
OnStop
OnContinue
OnDispose
OnPosing
.Args
argscorlib
System.Runtime.CompilerServices
CompilationRelaxationsAttribute
RuntimeCompatibilityAttribute
Set_ServiceName
WrapNonExceptionThrows
CorExImpl
MergeManifest
MergeManifest.dll
<?xml version="1.0" encoding="UTF-8" standalone="yes">
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
<security>
<requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
<requestedExecutionLevel level="asInvoker" uiAccess="false"/>
</requestedPrivileges>
</security>
</trustInfo>
</assembly>
[forensic@WIN-90HAJ6CQHOM:/mnt/c/Cases/Analysis/Memory]$ shasum pid.4248.0x370000.dmp
c5e3d5c1e33cabcb5e1fb0c52247e4385ef4be031
[forensic@WIN-90HAJ6CQHOM:/mnt/c/Cases/Analysis/Memory$]

```

- c5e3d5c1e33cabcb5e1fb0c52247e4385ef4be031

No matches found

Alternatively, do you want to locate your threat based on static, dynamic, content, attribution or other advanced IoC context? VT Intelligence allows you to search across VirusTotal's entire threat corpus using a myriad of modifiers, learn more.

[Try out VT Enterprise](#) [Try a new search](#)

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our [Privacy Policy](#).

## Injected DLLs

- Print dll used by a process:

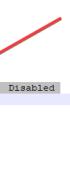
Process	Base Address	Size	Name	LoadTime	File output
notepad.exe	0x7ff7f607f0000	0x41000	notepad.exe	C:\Windows\System32\notepad.exe	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc34780000	0x1e1000	ntdll.dll	C:\Windows\SYSTEM32\ntdll.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc31ec0000	0xb2000	KERNEL32.DLL	C:\Windows\System32\KERNEL32.DLL	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc30ed0000	0x273000	KERNELBASE.dll	C:\Windows\System32\KERNELBASE.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc31e10000	0xa1000	ADVAPI32.dll	C:\Windows\System32\ADVAPI32.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc32030000	0x9e000	msvcrt.dll	C:\Windows\System32\msvcrt.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc33ac0000	0x5b0000	sehost.dll	C:\Windows\System32\sehost.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc34600000	0x124000	RPCRT4.dll	C:\Windows\System32\RPCRT4.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc31fa0000	0x28000	GDI32.dll	C:\Windows\System32\GDI32.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc31150000	0x192000	gdip32full.dll	C:\Windows\System32\gdip32full.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc30b70000	0x9f000	msvcp_win.dll	C:\Windows\System32\msvcp_win.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc31b10000	0xa0000	ucrtbase.dll	C:\Windows\System32\ucrtbase.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc34310000	0x10000	USER32.dll	C:\Windows\System32\USER32.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc30b50000	0x20000	win32u.dll	C:\Windows\System32\win32u.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc33fe0000	0x323000	combase.dll	C:\Windows\System32\combase.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc30e50000	0x7a000	bcryptPrimitives.dll	C:\Windows\System32\bcryptPrimitives.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc33e0f0000	0xed000	COMDLG32.dll	C:\Windows\System32\COMDLG32.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc33e40000	0xa9000	shcore.dll	C:\Windows\System32\shcore.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc344a0000	0x51000	SHLWAPI.dll	C:\Windows\System32\SHLWAPI.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc32320000	0x1440000	SHELL32.dll	C:\Windows\System32\SHELL32.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc30c10000	0x49000	cfgmgr32.dll	C:\Windows\System32\cfgmgr32.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc312f0000	0x7d000	windows.storage.dll	C:\Windows\System32\windows.storage.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc30ac0000	0x11000	kernel.appcore.dll	C:\Windows\System32\kernel.appcore.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc30aa0000	0x1f000	profapi.dll	C:\Windows\System32\profapi.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc278b0000	0x269000	COMCTL32.dll	C:\Windows\WinSxS\am64_microsoft.windows.common-controls_6595b64144cc1df_6.0.17134.1_none_e4da93291059d8fb\COMCTL32.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc30b00000	0x4c000	powrprof.dll	C:\Windows\System32\powrprof.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc30a90000	0xa000	FLTLIB.DLL	C:\Windows\System32\FLTLIB.DLL	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc2d560000	0x1b4000	PROPSYS.dll	C:\Windows\System32\PROPSYS.dll	2023-02-13 17:28:32.000000
notepad.exe	0x7ffc1f730000	0x84000	WINSPOOL.DRV	C:\Windows\System32\WINSPOOL.DRV	2023-02-13 17:28:32.000000

- Print the output to a text file:

```
forensic@WIN-90HAJ6COHOM: /mnt/c/Cases/Analysis/Memory
[forensic@WIN-90HAJ6COHOM: /mnt/c/Cases/Analysis/Memory]$ Vol -f win10-memory.raw windows.dlllist --pid 3164 > dll.txt
Progress: 8.26
Scanning memory_layer using BytesScanner
```

- Observe the injected dll.

```
C:\Case\Analysis\Memory\ddltxt - Notepad++ (Administrator)
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
SOFTWARE [ SECURITY [ DEFAULT [ ] ] ] HKEY_CURRENT_USER DAT MFT SAM BCD FileClass.dat MFT Logon SYSTEM MFT T1093_005_OnLogon [ ] T1093_005_OnStartup [ ] ddltxt [ ]
1 Volatility 3 Framework 2.4.0
2
3 PID Process Base Size Name Path LoadTime File output
4
5 3164 notepad.exe 0x7ff7e07f6000 0x41000 notepad.exe C:\Windows\system32\notepad.exe 2023-02-13 17:28:32.000000 Disabled
6 3164 notepad.exe 0x7ff3c375000 0x10000 ntdll.dll C:\Windows\System32\ntdll.dll 2023-02-13 17:28:32.000000 Disabled
7 3164 notepad.exe 0x7ff3c31c000 0x10000 KERNEL32.DLL C:\Windows\System32\KERNEL32.DLL 2023-02-13 17:28:32.000000 Disabled
8 3164 notepad.exe 0x7ff3c30e000 0x273000 KERNELBASE.dll C:\Windows\System32\KERNELBASE.dll 2023-02-13 17:28:32.000000 Disabled
9 3164 notepad.exe 0x7ff3c31e000 0x10000 ADVAPI32.dll C:\Windows\System32\ADVAPI32.dll 2023-02-13 17:28:32.000000 Disabled
10 3164 notepad.exe 0x7ff3d320000 0x9e0000 msasn1.dll C:\Windows\System32\msasn1.dll 2023-02-13 17:28:32.000000 Disabled
11 3164 notepad.exe 0x7ff3d340000 0x10000 cryptbase.dll C:\Windows\System32\cryptbase.dll 2023-02-13 17:28:32.000000 Disabled
12 3164 notepad.exe 0x7ff3d3460000 0x14000 RPCRT4.dll C:\Windows\System32\rpcrt4.dll 2023-02-13 17:28:32.000000 Disabled
13 3164 notepad.exe 0x7ff3c31fa000 0x280000 GDIM32.dll C:\Windows\System32\GDIM32.dll 2023-02-13 17:28:32.000000 Disabled
14 3164 notepad.exe 0x7ff3c315000 0x192000 gdi32full.dll C:\Windows\System32\gdi32full.dll 2023-02-13 17:28:32.000000 Disabled
15 3164 notepad.exe 0x7ff3c30b7000 0x89000 msasn1.dll C:\Windows\System32\msasn1.dll 2023-02-13 17:28:32.000000 Disabled
16 3164 notepad.exe 0x7ff3c31b1000 0x10000 userbase.dll C:\Windows\System32\userbase.dll 2023-02-13 17:28:32.000000 Disabled
17 3164 notepad.exe 0x7ff3c31b2000 0x10000 cryptui.dll C:\Windows\System32\cryptui.dll 2023-02-13 17:28:32.000000 Disabled
18 3164 notepad.exe 0x7ff3c31c5000 0x200000 win32k.dll C:\Windows\System32\win32k.dll 2023-02-13 17:28:32.000000 Disabled
19 3164 notepad.exe 0x7ff3c33f5000 0x323000 combase.dll C:\Windows\System32\combase.dll 2023-02-13 17:28:32.000000 Disabled
20 3164 notepad.exe 0x7ff3c30e5000 0x74000 bcryptPrimitives.dll C:\Windows\System32\bcryptPrimitives.dll 2023-02-13 17:28:32.000000 Disabled
21 3164 notepad.exe 0x7ff3c33e7000 0x400000 COMDLG32.dll C:\Windows\System32\COMDLG32.dll 2023-02-13 17:28:32.000000 Disabled
22 3164 notepad.exe 0x7ff3c33e4000 0xa9000 share.dll C:\Windows\System32\share.dll 2023-02-13 17:28:32.000000 Disabled
23 3164 notepad.exe 0x7ff3c344000 0x10000 cryptui.dll C:\Windows\System32\cryptui.dll 2023-02-13 17:28:32.000000 Disabled
24 3164 notepad.exe 0x7ff3c3441000 0x14000 SHLWAPI.dll C:\Windows\System32\SHLWAPI.dll 2023-02-13 17:28:32.000000 Disabled
25 3164 notepad.exe 0x7ff3c30c1000 0x490000 cfgmgr32.dll C:\Windows\System32\cfgmgr32.dll 2023-02-13 17:28:32.000000 Disabled
26 3164 notepad.exe 0x7ff3c3120000 0x704000 windows.storage.dll C:\Windows\System32\windows.storage.dll 2023-02-13 17:28:32.000000 Disabled
27 3164 notepad.exe 0x7ff3c30a0000 0x110000 kernel.apcprox.dll C:\Windows\System32\kernel.apcprox.dll 2023-02-13 17:28:32.000000 Disabled
28 3164 notepad.exe 0x7ff3c30a0000 0x101000 profapi.dll C:\Windows\System32\profapi.dll 2023-02-13 17:28:32.000000 Disabled
29 3164 notepad.exe 0x7ff3c3070000 0x10000 cryptui.dll C:\Windows\System32\cryptui.dll 2023-02-13 17:28:32.000000 Disabled
30 3164 notepad.exe 0x7ff3c3030000 0x10000 provider.dll C:\Windows\System32\provider.dll 2023-02-13 17:28:32.000000 Disabled
31 3164 notepad.exe 0x7ff3c3030000 0x10000 FTLLIB.dll C:\Windows\System32\FTLLIB.dll 2023-02-13 17:28:32.000000 Disabled
32 3164 notepad.exe 0x7ff3c2d50000 0x101000 PROFSYS.dll C:\Windows\System32\PROFSYS.dll 2023-02-13 17:28:32.000000 Disabled
33 3164 notepad.exe 0x7ff3c1730000 0x10000 WINPOOL.DRV C:\Windows\System32\WINPOOL.DRV 2023-02-13 17:28:32.000000 Disabled
34 3164 notepad.exe 0x7ff3c33d7000 0x200000 OLEAUT32.dll C:\Windows\System32\OLEAUT32.dll 2023-02-13 17:28:32.000000 Disabled
35 3164 notepad.exe 0x7ff3c3153000 0x10000 urlmon.dll C:\Windows\System32?urlmon.dll 2023-02-13 17:28:32.000000 Disabled
36 3164 notepad.exe 0x7ff3c3050000 0x380000 IMAGEHLP.DLL C:\Windows\System32\IMAGEHLP.DLL 2023-02-13 17:28:32.000000 Disabled
37 3164 notepad.exe 0x7ff3c3050000 0x250000 bcrypt.dll C:\Windows\System32\bcrypt.dll 2023-02-13 17:28:32.000000 Disabled
38 3164 notepad.exe 0x7ff3c32d0000 0xa2000 iesutil.dll C:\Windows\System32\iesutil.dll 2023-02-13 17:28:32.000000 Disabled
39 3164 notepad.exe 0x7ff3c3040000 0x90000 CRYPTBASE.DLL C:\Windows\System32\CRYPTBASE.DLL 2023-02-13 17:28:32.000000 Disabled
40 3164 notepad.exe 0x7ff3c33d30000 0x200000 TMM32.DLL C:\Windows\System32\TMM32.DLL 2023-02-13 17:28:32.000000 Disabled
41 3164 notepad.exe 0x7ff3c2fe00000 0x99000 uxtheme.dll C:\Windows\System32\uxtheme.dll 2023-02-13 17:28:32.000000 Disabled
42 3164 notepad.exe 0x7ff3c33d20000 0x10000 cryptui.dll C:\Windows\System32\cryptui.dll 2023-02-13 17:28:32.000000 Disabled
43 3164 notepad.exe 0x7ff3c31c0000 0x101000 Msasn1.dll C:\Windows\System32\Msasn1.dll 2023-02-13 17:28:32.000000 Disabled
44 3164 notepad.exe 0x7ff3c1750000 0x55000 MSCFT.DLL C:\Windows\System32\MSCFT.dll 2023-02-13 17:28:32.000000 Disabled
45 3164 notepad.exe 0x7ff3c1040000 0x10000 T055_001.dll C:\AtomicReTeam\atomica\T1055_001\arc\x64\T1055_001.dll 2023-02-13 17:28:32.000000 Disabled
46 3164 notepad.exe 0x7ff3c2a90000 0x80000 Secur32.dll C:\Windows\System32\Secur32.dll 2023-02-13 17:28:32.000000 Disabled
47 3164 notepad.exe 0x7ff3c3095000 0x300000 SFICL1.DLL C:\Windows\System32\SFICL1.DLL 2023-02-13 17:28:32.000000 Disabled
48 3164 notepad.exe 0x7ff3c3095000 0x10000 cryptui.dll C:\Windows\System32\cryptui.dll 2023-02-13 17:28:32.000000 Disabled
49 3164 notepad.exe 0x7ff3c3104000 0x200000 cryptui.dll C:\Windows\System32\cryptui.dll 2023-02-13 17:28:32.000000 Disabled
50 3164 notepad.exe 0x7ff3c2a00000 0x101000 MPR.dll C:\Windows\System32\MPR.dll 2023-02-13 17:29:03.000000 Disabled
51 3164 notepad.exe 0x7ff3c2a00000 0x104000 wintypes.dll C:\Windows\SYSTEM32\wintypes.dll 2023-02-13 17:29:03.000000 Disabled
52 3164 notepad.exe 0x7ff3c23b0000 0x1b1000 twinapi.appcore.dll C:\Windows\System32\twinapi.appcore.dll 2023-02-13 17:29:03.000000 Disabled
53 3164 notepad.exe 0x7ff3c2300000 0x21000 RMCLIENT.dll C:\Windows\System32\RMCLIENT.dll 2023-02-13 17:29:03.000000 Disabled
54 3164 notepad.exe 0x7ff3c1c480000 0x6b000 oleacc.dll C:\Windows\System32\oleacc.dll 2023-02-13 17:29:03.000000 Disabled
55


```

#### - Dump the dlls:



#### - Analysis of the suspicious DLL:

```
forensic@WIN-90HA47C0HQM:/mnt/c/Cases/Analysis/Memory$ strings dll  
Forensic@WIN-90HA47C0HQM:/mnt/c/Cases/Analysis/Memory$ strings dll  
Forensic@WIN-90HA47C0HQM:/mnt/c/Cases/Analysis/Memory$ strings dll  
Forensic@WIN-90HA47C0HQM:/mnt/c/Cases/Analysis/Memory$ strings pid/3164.T1055.001.dll  
Forensic@WIN-90HA47C0HQM:/mnt/c/Cases/Analysis/Memory$ strings pid/3164.T1055.001.dll
```

```
forensic@WIN-90HAJ6CQHQH: /mnt/c/Cases/Analysis/Memory
LocaleNameToLCID
ProcessGetProcessTerminationMethod
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
January
February
March
April
May
June
July
August
September
October
November
December
MM/dd/yy
dd/MM/yyyy
HH:mm:ss
/ysB
%30%
?z:06$  
log10
EncryptMessage
DecryptMessage
TLS Intercept
Boomi Intercept
Locked and Loaded!
RS05%
c:/Users/Research/source/repos/T1179/src/x64/T1179.pdb
.DOT
.text$mn
.text$mn$00
.text$xx
.idata$5
.00CTF
.CRT$KA
.CRT$XC2
.CRT$XIA
.CRT$XIC
.CRT$XIZ
.CRT$XPW
.CRT$XPY
.CRT$XPXA
.CRT$XPZ
.CRT$XTA
.CRT$XTZ
.rdata$0
.rdata$0r
.rdata$zzzdbg
 rtc$IAA
 rtc$IZZ
 rtc$TAA
 rtc$TZZ
.xdata
.xdata$x
.idata$2
.idata$3
Windows Task Manager
```

```
forensic@WIN-90HAJ6CQHQH: /mnt/c/Cases/Analysis/Memory
FindClose
FindFirstFileExW
FindFirstFileW
IsValidCodePage
GetACP
GetOEMCP
GetCPInfo
GetCommandLineA
GetCommandLineW
MultiByteToWideChar
WideCharToMultiByte
GetEnvironmentStringsW
FreeEnvironmentStringsW
LChaps$W
GetAccessMap
GetStdHandle
GetFileType
GetStringTypeW
HeapSize
HeapAlloc
SetStdHandle
FlushFileBuffers
WriteFile
GetConsoleCP
GetConsoleMode
CreateFileForEx
CreateFileW
CloseHandle
WriteConsoleW
abcdefhijklmnopqrstuvwxyz
ABCDEFGHIJKLMNPQRSTUVWXYZ

abcdeghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNPQRSTUVWXYZ
?Vbad_exception@std@@
.?VException@std@@
.?Vtype_info@@
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<assembly ns="urn:schemas-microsoft-com:asm.v1" manifestVersion='1.0'>
  <trustInfo ns="urn:schemas-microsoft-com:asm.v3">
    <security>
      <requestedPrivileges>
        <requestedExecutionLevel level='asInvoker' uiAccess='false' />
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
Forensic@WIN-90HAJ6CQHQH: /mnt/c/Cases/Analysis/Memory$
```

## Process owners

- Get the SID for the processes:

```

forensic@WIN-90HAJ6CQHQ:~/.mmt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.getsids --pid 3164 7080 4248
Volatility Framework 2.4.0
progress: 100.00    PDB scanning finished
PID   Process SID     Name
7080  powershell.exe S-1-5-21-1058341133-2092417715-4019589128-1000  IUSER
7080  powershell.exe S-1-5-21-1058341133-2092417715-4019589128-513  Domain Users
7080  powershell.exe S-1-5-0-Everyone
7080  powershell.exe S-1-5-114  Local Account (Member of Administrators)
7080  powershell.exe S-1-5-32-544  Administrators
7080  powershell.exe S-1-5-32-545  Users
7080  powershell.exe S-1-5-4 Interactive
7080  powershell.exe S-1-2-0 Local Logon (Users who are logged onto the physical console)
7080  powershell.exe S-1-5-11  Authenticated Users
7080  powershell.exe S-1-5-15  This Organization
7080  powershell.exe S-1-5-113  local Account
7080  powershell.exe S-1-5-5-0-137124  Logon Session
7080  powershell.exe S-1-2-0 Local (Users with the ability to log in locally)
7080  powershell.exe S-1-5-64-10  NTLM Authentication
7080  powershell.exe S-1-16-12288  High Mandatory Level
4248  AtomicService. S-1-5-18  Local System
4248  AtomicService. S-1-5-32-544  Administrators
4248  AtomicService. S-1-1-0 Everyone
4248  AtomicService. S-1-5-11  Authenticated Users
4248  AtomicService. S-1-5-64-10  NTLM Authentication
3164  notepad.exe  S-1-5-21-1058341133-2092417715-4019589128-1000  IUSER
3164  notepad.exe  S-1-5-21-1058341133-2092417715-4019589128-513  Domain Users
3164  notepad.exe  S-1-1-0 Everyone
3164  notepad.exe  S-1-5-114  Local Account (Member of Administrators)
3164  notepad.exe  S-1-5-32-544  Administrators
3164  notepad.exe  S-1-5-32-545  Users
3164  notepad.exe  S-1-5-4 Interactive
3164  notepad.exe  S-1-2-0 Local Logon (Users who are logged onto the physical console)
3164  notepad.exe  S-1-5-11  Authenticated Users
3164  notepad.exe  S-1-5-15  This Organization
3164  notepad.exe  S-1-5-113  local Account
3164  notepad.exe  S-1-5-5-0-137124  Logon Session
3164  notepad.exe  S-1-2-0 Local (Users with the ability to log in locally)
3164  notepad.exe  S-1-5-64-10  NTLM Authentication
3164  notepad.exe  S-1-16-12288  High Mandatory Level
forensic@WIN-90HAJ6CQHQ:~/.mmt/c/Cases/Analysis/Memory$ -

```

## Malicious registry key entries

- Suspicious Registry Key:

The screenshot shows the Event Log Explorer interface with the following details:

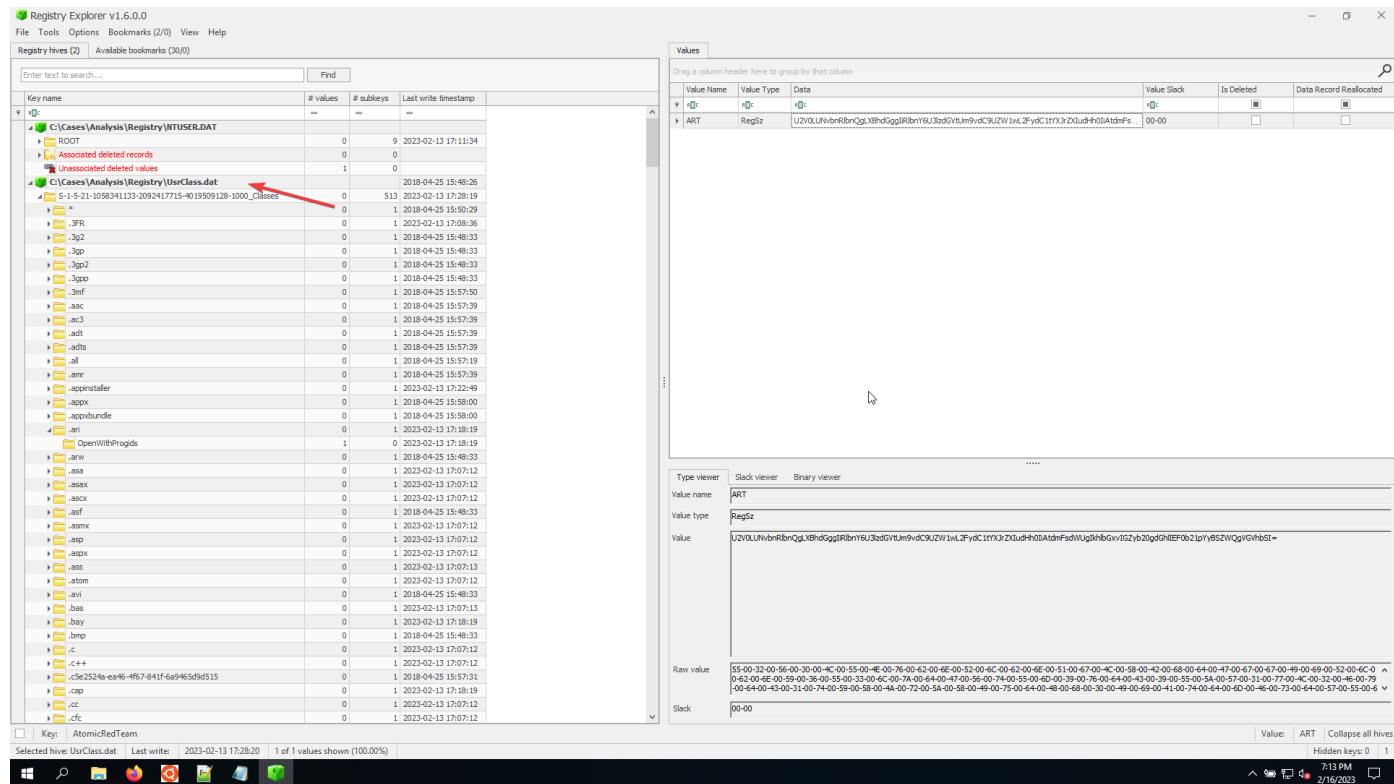
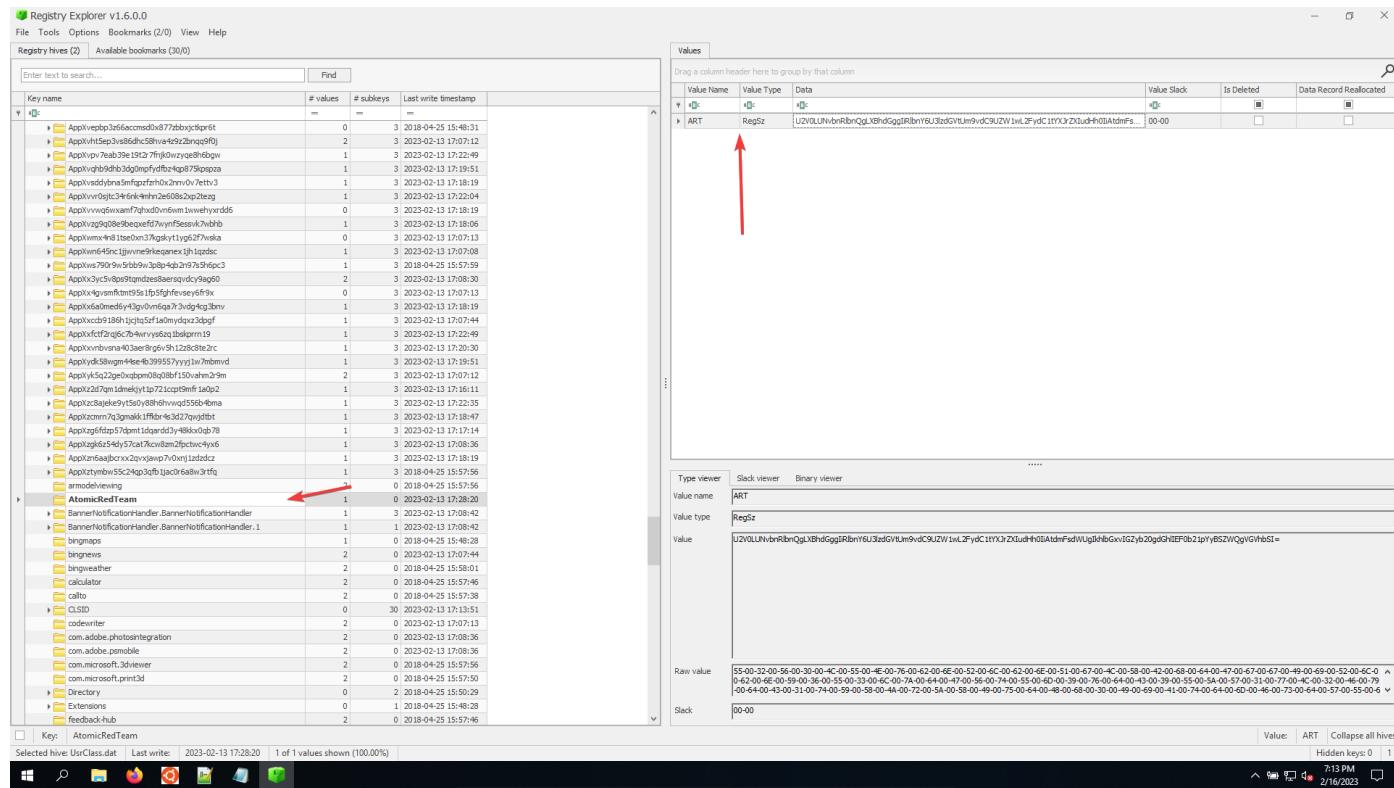
- Log:** Microsoft-Windows-PowerShell%4Operational.evtx
- Event Type:** Information
- Date:** 2/13/2023
- Time:** 5:28:19 PM
- Source:** PowerShell
- User:** N/A
- Computer:** MSEDGEWIN0
- Description:** Engine state is changed from None to Available.
- Details:**

```

NewEngineState=Available
PreviousEngineState=None
SequenceNumber=13
Hostname=ConsoleHost
HostId=a4x7016-ef9-41d-907d-7f08c425c01
HostApplication=powershell.exe & (# Encoded payload in next command is the following "Set-Content -path "$env:SystemRoot\Temp\art-marker.txt" -value "Hello from the Atomic Red Team"
reg.exe add "HKEY_CURRENT_USER\Software\Classes\{AtomicRedTeam}\ART" /REG_SZ /d "U2VUUmVnbnQuXbndgqRbnY6U3cgVGtUm9vdC02W1wL2FyC1tY0i2XjdHn0IAtdmFsdWUgkhbGxVbz20gdGhIEF0b21pYyB5ZVQgVGvhbSI="
hex ({[Text]}) | ConvertFrom-String((gp $Software\{AtomicRedTeam}\ART)))"
EngineVersion=5.1.17134.1
RunspaceId=b2e282e-3b0d-40c-2-99a0-816cacf933d1
PowerShellVersion=5.1.17134.1
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=

```

- 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-9OHAJGCOHOM:/mnt/c/Cases/Analysis/Memory
0xc00542b5000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\ Packages\Microsoft.Windows.Cortana_1.10.7.17134_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat
isEnabled
0xc00543d7000 \??\C:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\Settings\settings.dat
isEnabled
0xc00543d7000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\ Packages\Microsoft.MicrosoftEdge_42.17134.1.0_neutral__8wekyb3d8bbwe\ActivationStore.dat
isEnabled
0xc005434c5000 \??\C:\Users\IEUser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat Disabled
0xc005447a000 \??\C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\State\docsvcState.dat
isEnabled
0xc00547934000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\ Packages\Microsoft.Windows.Photos_2020.20120.4004.0_x64__8wekyb3d8bbwe\ActivationStore.dat
isEnabled
0xc0054986000 \??\C:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settings\settings.dat
isEnabled
0xc005458bf000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\ Packages\Microsoft.UI.Xaml.2.4_2.42007.9001.0_x64__8wekyb3d8bbwe\ActivationStore.dat
isEnabled
0xc00547da5000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\ Packages\Microsoft.SkypeApp_14.56.102.0_x64_kzf8qxf3bzg5c\ActivationStore.dat
isEnabled
Forensic@WIN-9OHAJGCOHOM:/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-9OHAJGCOHOM:/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-9OHAJGCOHOM:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.registry.hivelist
Volatility 3 Framework 2.4.0
Progress: 4.49 Scanning memory_layer using Bytescanner

```

```
forensic@WIN-9OHAJGCOHOM:/mnt/c/Cases/Analysis/Memory
0xc00547934000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\ Packages\Microsoft.Windows.Photos_2020.20120.4004.0_x64__8wekyb3d8bbwe\ActivationStore.dat
isEnabled
0xc00544986000 \??\C:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settings\settings.dat
isEnabled
0xc005458bf000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\ Packages\Microsoft.UI.Xaml.2.4_2.42007.9001.0_x64__8wekyb3d8bbwe\ActivationStore.dat
isEnabled
0xc00547da5000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\ Packages\Microsoft.SkypeApp_14.56.102.0_x64_kzf8qxf3bzg5c\ActivationStore.dat
isEnabled
Forensic@WIN-9OHAJGCOHOM:/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-9OHAJGCOHOM:/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-9OHAJGCOHOM:/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
0xc005404c1f000 \Device\Harddisk\Volume1\EFI\Microsoft\Boot\BCD Disabled
0xc00541633000 \SystemRoot\System32\Config\FTWARM Disabled
0xc00541781000 \SystemRoot\System32\Config\SECURITY Disabled
0xc00541781000 \SystemRoot\System32\Config\DEFAULT Disabled
0xc0054177f000 \SystemRoot\System32\Config\SAM Disabled
0xc005418a2000 \??\C:\Windows\ServiceProfiles\NetworkService\WUSER.DAT Disabled
0xc00541b1000 \SystemRoot\System32\Config\BII Disabled
0xc00541b470000 \??\C:\Windows\ServiceProfiles\localservice\WUSER.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
0xc00542b4f000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\ Packages\Microsoft.Windows.ShellExperienceHost_10.0.17134.1_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat
isEnabled
0xc005430a8000 \??\C:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy\Settings\settings.dat
isEnabled
0xc00543b05000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\ Packages\Microsoft.Windows.Cortana_1.10.7.17134_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat
isEnabled
0xc00543b0d7000 \??\C:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\Settings\settings.dat
isEnabled
0xc00543407000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\ Packages\Microsoft.MicrosoftEdge_42.17134.1.0_neutral__8wekyb3d8bbwe\ActivationStore.dat
isEnabled
0xc005434c5000 \??\C:\Users\IEUser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat Disabled
0xc005447a000 \??\C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\State\docsvcState.dat
isEnabled
0xc00547934000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\ Packages\Microsoft.Windows.Photos_2020.20120.4004.0_x64__8wekyb3d8bbwe\ActivationStore.dat
isEnabled
0xc0054986000 \??\C:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settings\settings.dat
isEnabled
0xc005458bf000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\ Packages\Microsoft.UI.Xaml.2.4_2.42007.9001.0_x64__8wekyb3d8bbwe\ActivationStore.dat
isEnabled
0xc00547da5000 \??\C:\ProgramData\Microsoft\Windows\AppRepository\ Packages\Microsoft.SkypeApp_14.56.102.0_x64_kzf8qxf3bzg5c\ActivationStore.dat
isEnabled
Forensic@WIN-9OHAJGCOHOM:/mnt/c/Cases/Analysis/Memory$
```

```

forensic@WIN-90HAJ6CQHOM:/mnt/c/Cases/Analysis/Memory
0xc0054a986000 \??C:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Photos_8wekyb3d8bbwe\Settings\settings.dat
0x0005458bf000 \??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_kzfbqxf3bzg5c\ActivationStore.dat
isabled
forensic@WIN-90HAJ6CQHOM:/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
Last Write Time Hive Offset Type Key Name Data Volatile
0xc00542b5d000 Key ?ART -
forensic@WIN-90HAJ6CQHOM:/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
Last Write Time Hive Offset Type Key Name Data Volatile
0xc00542b5d000 Key ?AtomicRedTeam -
forensic@WIN-90HAJ6CQHOM:/mnt/c/Cases/Analysis/Memory$ vol -f win10-memory.raw windows.registry.hivelist
Volatility 3 Framework 2.4.0
Progress: 100.00
Last Write Time Hive Offset FileFullpath File output
0xc00540433000 Disabled
0xc00540434000 \REGISTRY\HARDWARE\SYSTEM Disabled
0xc00540435000 \REGISTRY\MACHINE\HARDWARE Disabled
0xc0054041cf000 \Device\Harddisk\Volume1\EFI\Microsoft\Boot\BCD Disabled
0xc00541633000 \SystemRoot\System32\Config\SOFTWARE Disabled
0xc00541770000 \SystemRoot\System32\Config\SECURITY Disabled
0xc00541781000 \SystemRoot\System32\Config\DEFAULT Disabled
0xc00541782000 \SystemRoot\System32\Config\SYSTEM Disabled
0xc005418a2000 \??C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT Disabled
0xc00541b19000 \SystemRoot\System32\Config\LBII Disabled
0xc00541b47000 \??C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT Disabled
0xc0054219a000 \??C:\Users\ssh\server\ntuser.dat Disabled
0xc0054220000 \??C:\Users\ssh\server\appdata\local\Microsoft\Windows\UsrClass.dat Disabled
0xc0054230000 \??C:\Windows\SoftwareDistribution\catalog\hve Disabled
0xc0054257000 \??C:\Users\ItUser\ntuser.dat Disabled
0xc005425b5d000 \??C:\Users\IEUser\appdata\local\Microsoft\Windows\UsrClass.dat Disabled
0xc00542f4fb000 \??C:\ProgramData\Microsoft\Windows\AppBarRepository\ Packages\Microsoft.ShellExperienceHost_10.0.17134.1_neutral_neutral_cw5nh2txyewy\ActivationStore.dat
isabled
0xc005430a8000 \??C:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.ShellExperienceHost_cw5nh2txyewy\Settings\settings.dat
isabled
0xc005430b5000 \??C:\ProgramData\Microsoft\Windows\AppRepository\ Packages\Microsoft.Windows.Cortana_1.10.7.17134_neutral_neutral_cw5nh2txyewy\ActivationStore.dat
isabled
0xc005430d7000 \??C:\Users\IEUser\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5nh2txyewy\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\AppBarRepository\ Packages\Microsoft.Windows.Photos_2020.20120.4004.0_x64_8wekyb3d8bbwe\ActivationStore.dat
isabled
0xc00544996000 \??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_kzfbqxf3bzg5c\ActivationStore.dat
isabled
forensic@WIN-90HAJ6CQHOM:/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

```