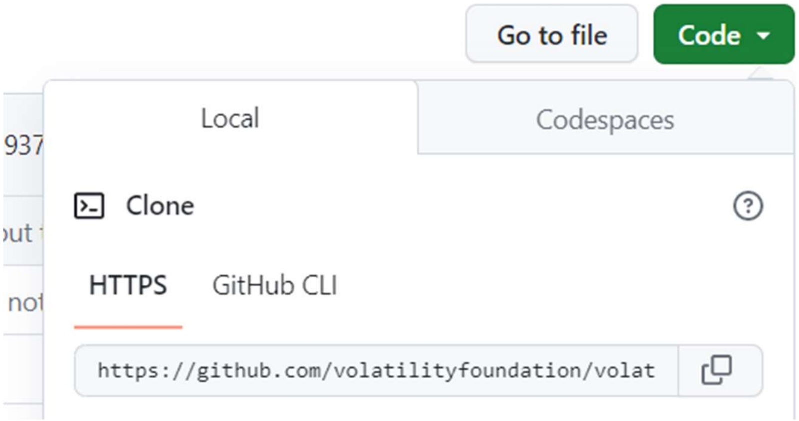
Memory Analysis on Stuxnet Malware Infected Machine

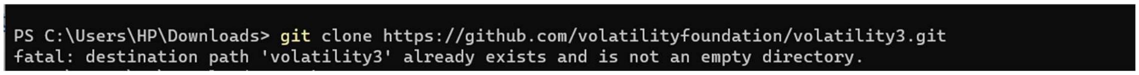
Go to volatility GitHub Link :

https://github.com/volatilityfoundation/volatility3



```
https://github.com/volatilityfoundation/volat
```

Using git clone can download that all file in yours pc

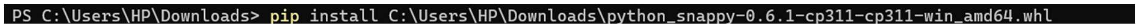


```
PS C:\Users\HP\Downloads> git clone https://github.com/volatilityfoundation/volatility3.git
fatal: destination path 'volatility3' already exists and is not an empty directory.
```

Install snappy tool – it's a package of python used to compress entire ram space for faster processing and faster Querying and it is a compression algorithm supported by google

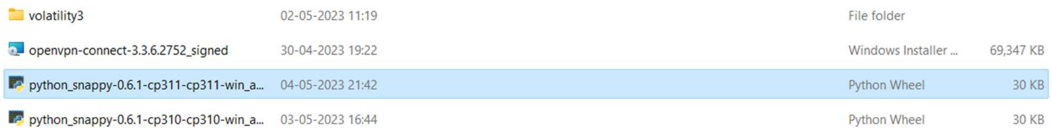
Install snappy where volatility existed

https://www.lfd.uci.edu/~gohlke/pythonlibs/#python-snappy



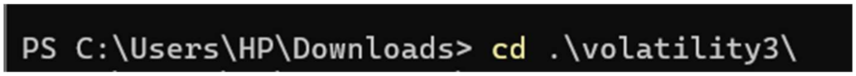
```
PS C:\Users\HP\Downloads> pip install C:\Users\HP\Downloads\python_snappy-0.6.1-cp311-cp311-win_amd64.whl
```

It installs python_snappy tool



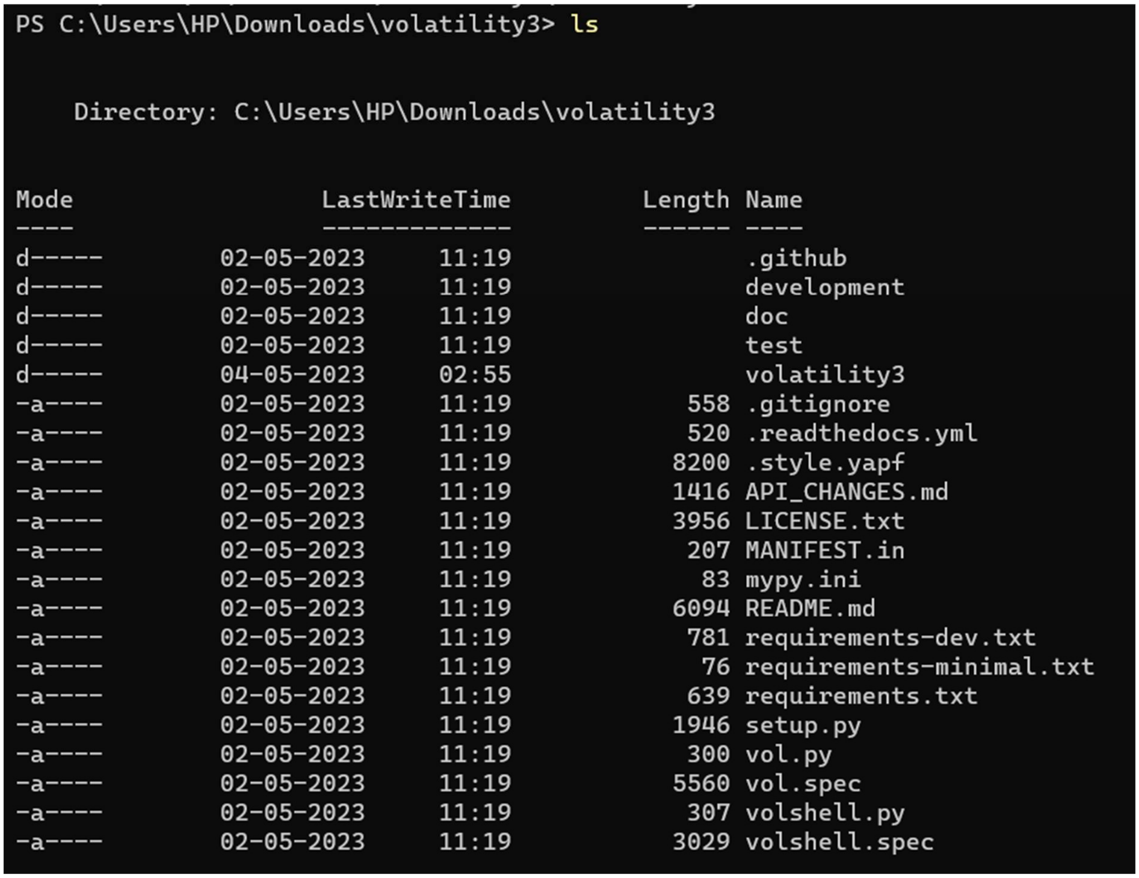
volatility3	02-05-2023 11:19	File folder	
openvpn-connect-3.3.6.2752_signed	30-04-2023 19:22	Windows Installer ...	69,347 KB
python_snappy-0.6.1-cp311-cp311-win_a...	04-05-2023 21:42	Python Wheel	30 KB
python_snappy-0.6.1-cp310-cp310-win_a...	03-05-2023 16:44	Python Wheel	30 KB

Go to volatility directory



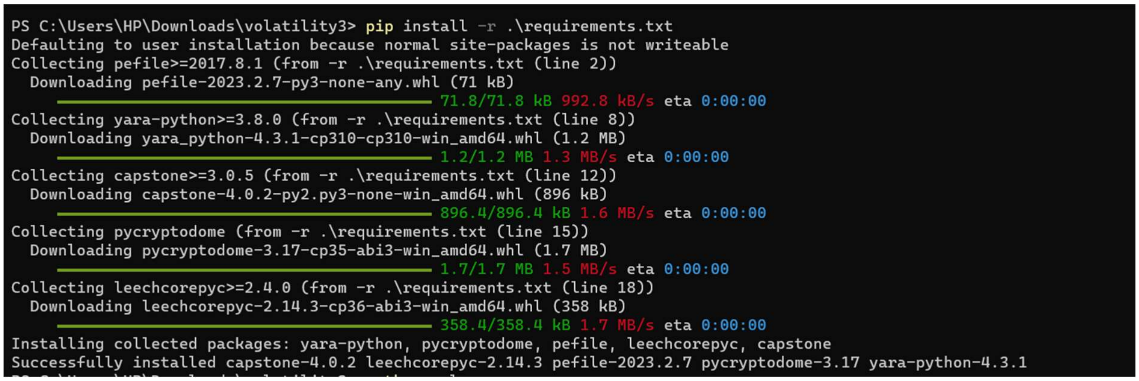
```
PS C:\Users\HP\Downloads> cd .\volatility3\
```

list all the files in volatility directory :



```
PS C:\Users\HP\Downloads\volatility3> ls


    Directory: C:\Users\HP\Downloads\volatility3


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        02-05-2023     11:19                .github
d-----        02-05-2023     11:19                development
d-----        02-05-2023     11:19                doc
d-----        02-05-2023     11:19                test
d-----        04-05-2023     02:55                volatility3
-a----        02-05-2023     11:19            558 .gitignore
-a----        02-05-2023     11:19            520 .readthedocs.yml
-a----        02-05-2023     11:19           8200 .style.yapf
-a----        02-05-2023     11:19           1416 API_CHANGES.md
-a----        02-05-2023     11:19           3956 LICENSE.txt
-a----        02-05-2023     11:19            207 MANIFEST.in
-a----        02-05-2023     11:19             83 mypy.ini
-a----        02-05-2023     11:19           6094 README.md
-a----        02-05-2023     11:19            781 requirements-dev.txt
-a----        02-05-2023     11:19             76 requirements-minimal.txt
-a----        02-05-2023     11:19            639 requirements.txt
-a----        02-05-2023     11:19           1946 setup.py
-a----        02-05-2023     11:19            300 vol.py
-a----        02-05-2023     11:19           5560 vol.spec
-a----        02-05-2023     11:19            307 volshell.py
-a----        02-05-2023     11:19           3029 volshell.spec
```

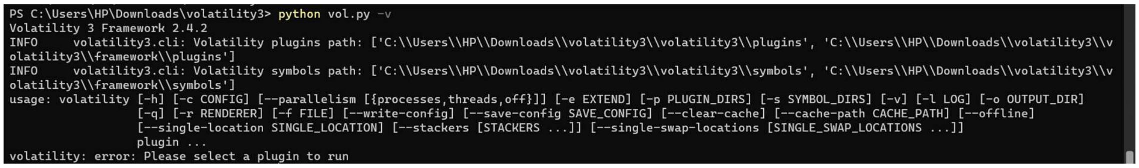
First install all the requirements



```
PS C:\Users\HP\Downloads\volatility3> pip install -r .\requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Collecting pefile>=2017.8.1 (from -r .\requirements.txt (line 2))
  Downloading pefile-2023.2.7-py3-none-any.whl (71 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 71.8/71.8 kB 992.8 kB/s eta 0:00:00
Collecting yara-python>=3.8.0 (from -r .\requirements.txt (line 8))
  Downloading yara_python-4.3.1-cp310-cp310-win_amd64.whl (1.2 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.2/1.2 MB 1.3 MB/s eta 0:00:00
Collecting capstone>=3.0.5 (from -r .\requirements.txt (line 12))
  Downloading capstone-4.0.2-py2.py3-none-win_amd64.whl (896 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 896.4/896.4 kB 1.6 MB/s eta 0:00:00
Collecting pycryptodome (from -r .\requirements.txt (line 15))
  Downloading pycryptodome-3.17-cp35-abi3-win_amd64.whl (1.7 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.7/1.7 MB 1.5 MB/s eta 0:00:00
Collecting leechcorepyc>=2.4.0 (from -r .\requirements.txt (line 18))
  Downloading leechcorepyc-2.14.3-cp36-abi3-win_amd64.whl (358 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 358.4/358.4 kB 1.7 MB/s eta 0:00:00
Installing collected packages: yara-python, pycryptodome, pefile, leechcorepyc, capstone
Successfully installed capstone-4.0.2 leechcorepyc-2.14.3 pefile-2023.2.7 pycryptodome-3.17 yara-python-4.3.1
```

```
PS C:\Users\HP\Downloads\volatility3> |
```

To check version of volatility3



```
PS C:\Users\HP\Downloads\volatility3> python vol.py -v
Volatility 3 Framework 2.4.2
INFO     volatility3.cli: Volatility plugins path: ['C:\\Users\\HP\\Downloads\\volatility3\\volatility3\\plugins', 'C:\\Users\\HP\\Downloads\\volatility3\\v
olatility3\\framework\\plugins']
INFO     volatility3.cli: Volatility symbols path: ['C:\\Users\\HP\\Downloads\\volatility3\\volatility3\\symbols', 'C:\\Users\\HP\\Downloads\\volatility3\\v
olatility3\\framework\\symbols']
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR]
                  [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [--offline]
                  [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]] [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
                  plugin ...
volatility: error: Please select a plugin to run
```

Take Stuxnet infected machine’s memory dump file and take its path

In this command :

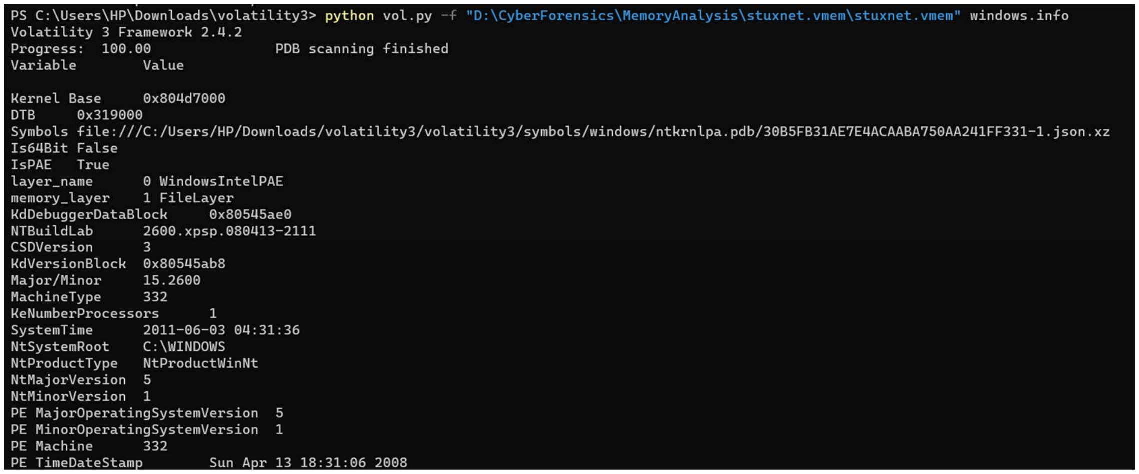
python vol.py -f "D:\CyberForensics\MemoryAnalysis\stuxnet.vmem\stuxnet.vmem" windows.info

python vol.py → to Check Volatility

-f → to get file path

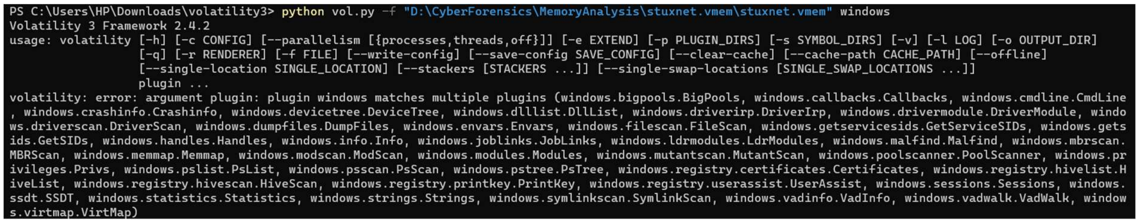
D:\CyberForensics\MemoryAnalysis\stuxnet.vmem\stuxnet.vmem → Path where dump file is there

windows.info → name of plugin



```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\stuxnet.vmem\stuxnet.vmem" windows.info
Volatility 3 Framework 2.4.2
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0x804d7000
DTB     0x319000
Symbols file:///C:/Users/HP/Downloads/volatility3/volatility3/symbols/windows/ntkrnlpa.pdb/30B5FB31AE7E4ACAABA750AA241FF331-1.json.xz
Is64Bit False
IsPAE   True
layer_name      0 WindowsIntelPAE
memory_layer    1 FileLayer
KdDebuggerDataBlock     0x80545ae0
NTBuildLab      2600.xpsp.080413-2111
CSDVersion      3
KdVersionBlock  0x80545ab8
Major/Minor     15.2600
MachineType     332
KeNumberProcessors      1
SystemTime      2011-06-03 04:31:36
NtSystemRoot    C:\WINDOWS
NtProductType   NtProductWinNt
NtMajorVersion  5
NtMinorVersion  1
PE MajorOperatingSystemVersion  5
PE MinorOperatingSystemVersion  1
PE Machine      332
PE TimeDateStamp        Sun Apr 13 18:31:06 2008
```

To check what are available plugins :



```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\stuxnet.vmem\stuxnet.vmem" windows
Volatility 3 Framework 2.4.2
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR]
                  [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [--offline]
                  [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]] [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
                  plugin ...
volatility: error: argument plugin: plugin windows matches multiple plugins (windows.bigpools.BigPools, windows.callbacks.Callbacks, windows.cmdline.CmdLine
, windows.crashinfo.Crashinfo, windows.devicetree.DeviceTree, windows.dlllist.DllList, windows.driverirp.DriverIrp, windows.drivermodule.DriverModule, windo
ws.driverscan.DriverScan, windows.dumpfiles.DumpFiles, windows.envars.Envars, windows.filescan.FileScan, windows.getservicesids.GetServiceSIDs, windows.gets
ids.GetSIDs, windows.handles.Handles, windows.info.Info, windows.joblinks.JobLinks, windows.ldrmodules.LdrModules, windows.malfind.Malfind, windows.mbrscan.
MBRScan, windows.memmap.Memmap, windows.modscan.ModScan, windows.modules.Modules, windows.mutantscan.MutantScan, windows.poolscanner.PoolScanner, windows.pr
ivileges.Privs, windows.pslist.PsList, windows.psscan.PsScan, windows.pstree.PsTree, windows.registry.certificates.Certificates, windows.registry.hivelist.H
iveList, windows.registry.hivescan.HiveScan, windows.registry.printkey.PrintKey, windows.registry.userassist.UserAssist, windows.sessions.Sessions, windows.
ssdt.SSDT, windows.statistics.Statistics, windows.strings.Strings, windows.symlinkscan.SymlinkScan, windows.vadinfo.VadInfo, windows.vadwalk.VadWalk, window
s.virtmap.VirtMap)
```

You can explore all plugins giving at the end plugin name

Exploring a few important plugins :

Windows.pslist plugin :

pslist – Process list

pslist is a plugin that gives information like

PID – Process ID

PPID – Parent Process ID

Image File Name – all those exe's

Threads – It shows how many threads are executed

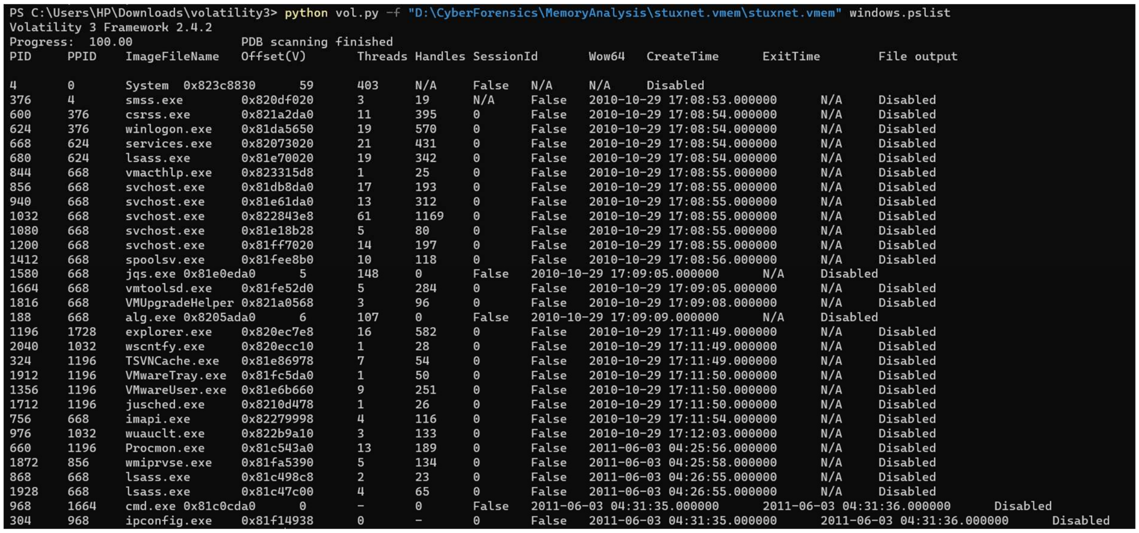
Handles - typically refers to an abstract reference or identifier used to access or manipulate a resource, such as a file, memory location, object, or data structure. Handles are often used to maintain abstraction layers and encapsulate the details of resource management

Wow64 - WOW64 (Windows 32-bit on Windows 64-bit) is a subsystem of the Windows operating system that enables 32-bit applications to run seamlessly on 64-bit versions of Windows.

CreateTime - In operating systems, create time typically refers to the timestamp associated with the creation of a file or directory. File systems record metadata attributes for each file or directory, including the time when it was created. This information is useful for file management, auditing, and version control purposes.

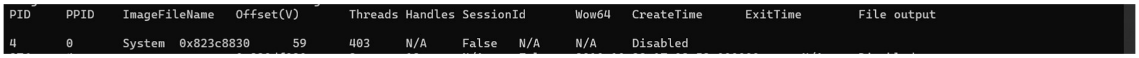
Exit time - typically refers to the moment when a process or program stops running or terminates. In the context of operating systems, including Windows, Linux, or macOS, when a process completes its execution or is forcefully terminated

File Output - typically refers to the process of exporting or saving forensic artifacts, evidence, or analysis results to files.



```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\stuxnet.vmem\stuxnet.vmem" windows.pslist
Volatility 3 Framework 2.4.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x823c8830      59      403     N/A     False   N/A     N/A     Disabled
376     4       smss.exe        0x820df020      3       19      N/A     False   2010-10-29 17:08:53.000000      N/A     Disabled
600     376     csrss.exe       0x821a2da0      11      395     0       False   2010-10-29 17:08:54.000000      N/A     Disabled
624     376     winlogon.exe    0x81da5650      19      570     0       False   2010-10-29 17:08:54.000000      N/A     Disabled
668     624     services.exe    0x82073020      21      431     0       False   2010-10-29 17:08:54.000000      N/A     Disabled
680     624     lsass.exe       0x81e70020      19      342     0       False   2010-10-29 17:08:54.000000      N/A     Disabled
844     668     vmacthlp.exe    0x823315d8      1       25      0       False   2010-10-29 17:08:55.000000      N/A     Disabled
856     668     svchost.exe     0x81db8da0      17      193     0       False   2010-10-29 17:08:55.000000      N/A     Disabled
940     668     svchost.exe     0x81e61da0      13      312     0       False   2010-10-29 17:08:55.000000      N/A     Disabled
1032    668     svchost.exe     0x822843e8      61      1169    0       False   2010-10-29 17:08:55.000000      N/A     Disabled
1080    668     svchost.exe     0x81e18b28      5       80      0       False   2010-10-29 17:08:55.000000      N/A     Disabled
1200    668     svchost.exe     0x81ff7020      14      197     0       False   2010-10-29 17:08:55.000000      N/A     Disabled
1412    668     spoolsv.exe     0x81fee8b0      10      118     0       False   2010-10-29 17:08:56.000000      N/A     Disabled
1580    668     jqs.exe 0x81e0eda0      5       148     0       False   2010-10-29 17:09:05.000000      N/A     Disabled
1664    668     vmtoolsd.exe    0x81fe52d0      5       284     0       False   2010-10-29 17:09:05.000000      N/A     Disabled
1816    668     VMUpgradeHelper 0x821a0568      3       96      0       False   2010-10-29 17:09:08.000000      N/A     Disabled
188     668     alg.exe 0x8205ada0      6       107     0       False   2010-10-29 17:09:09.000000      N/A     Disabled
1196    1728    explorer.exe    0x820ec7e8      16      582     0       False   2010-10-29 17:11:49.000000      N/A     Disabled
2040    1032    wscntfy.exe     0x820ecc10      1       28      0       False   2010-10-29 17:11:49.000000      N/A     Disabled
324     1196    TSVNCache.exe   0x81e86978      7       54      0       False   2010-10-29 17:11:49.000000      N/A     Disabled
1912    1196    VMwareTray.exe  0x81fc5da0      1       50      0       False   2010-10-29 17:11:50.000000      N/A     Disabled
1356    1196    VMwareUser.exe  0x81e6b660      9       251     0       False   2010-10-29 17:11:50.000000      N/A     Disabled
1712    1196    jusched.exe     0x8210d478      1       26      0       False   2010-10-29 17:11:50.000000      N/A     Disabled
756     668     imapi.exe       0x82279998      4       116     0       False   2010-10-29 17:11:54.000000      N/A     Disabled
976     1032    wuauclt.exe     0x822b9a10      3       133     0       False   2010-10-29 17:12:03.000000      N/A     Disabled
660     1196    Procmon.exe     0x81c543a0      13      189     0       False   2011-06-03 04:25:56.000000      N/A     Disabled
1872    856     wmiprvse.exe    0x81fa5390      5       134     0       False   2011-06-03 04:25:58.000000      N/A     Disabled
868     668     lsass.exe       0x81c498c8      2       23      0       False   2011-06-03 04:26:55.000000      N/A     Disabled
1928    668     lsass.exe       0x81c47c00      4       65      0       False   2011-06-03 04:26:55.000000      N/A     Disabled
968     1664    cmd.exe 0x81c0cda0      0       -       0       False   2011-06-03 04:31:35.000000      2011-06-03 04:31:36.000000      Disabled
304     968     ipconfig.exe    0x81f14938      0       -       0       False   2011-06-03 04:31:35.000000      2011-06-03 04:31:36.000000      Disabled
```

It shows System is the 1st processor

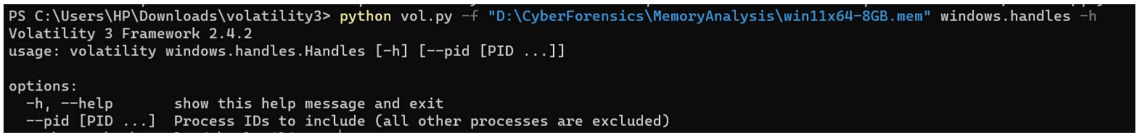


```
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x823c8830      59      403     N/A     False   N/A     N/A     Disabled
```

Windows.handles plugin :

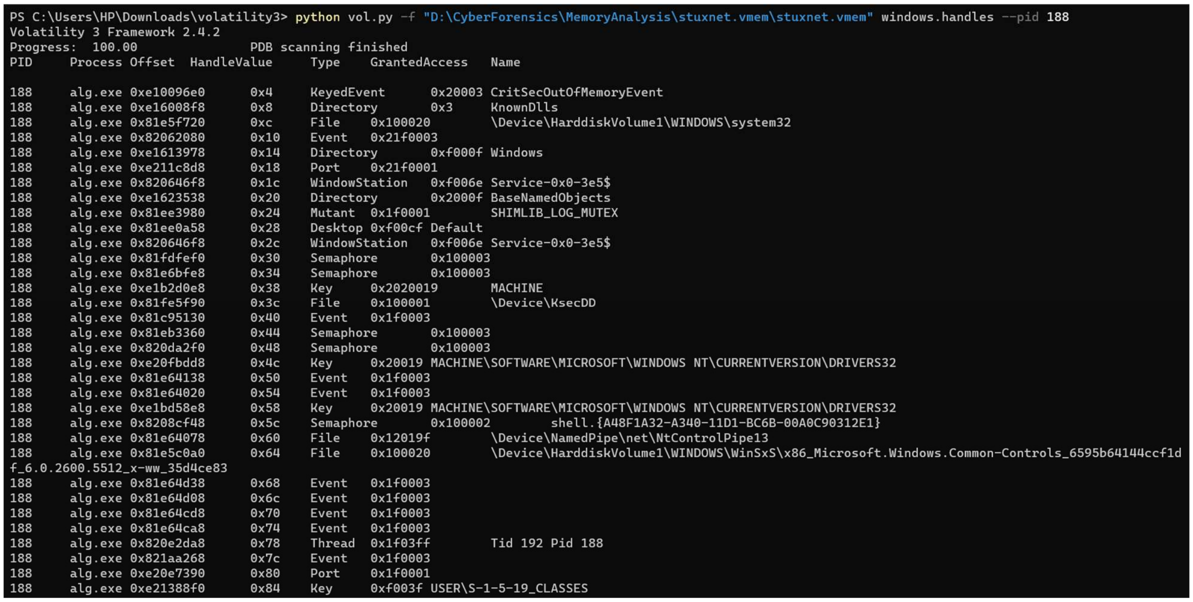
To know what handles

windows.handles -h (Help menu for windows handles)

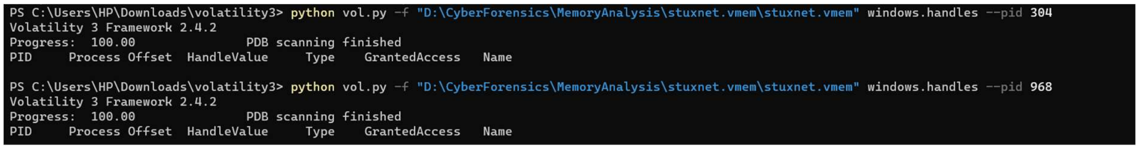


```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\win11x64-8GB.mem" windows.handles -h
Volatility 3 Framework 2.4.2
usage: volatility windows.handles.Handles [-h] [--pid [PID ...]]

options:
  -h, --help        show this help message and exit
  --pid [PID ...]   Process IDs to include (all other processes are excluded)
```

If you don’t use pid it gives all of handles not only file handles in the memory image its going to be a lot of data

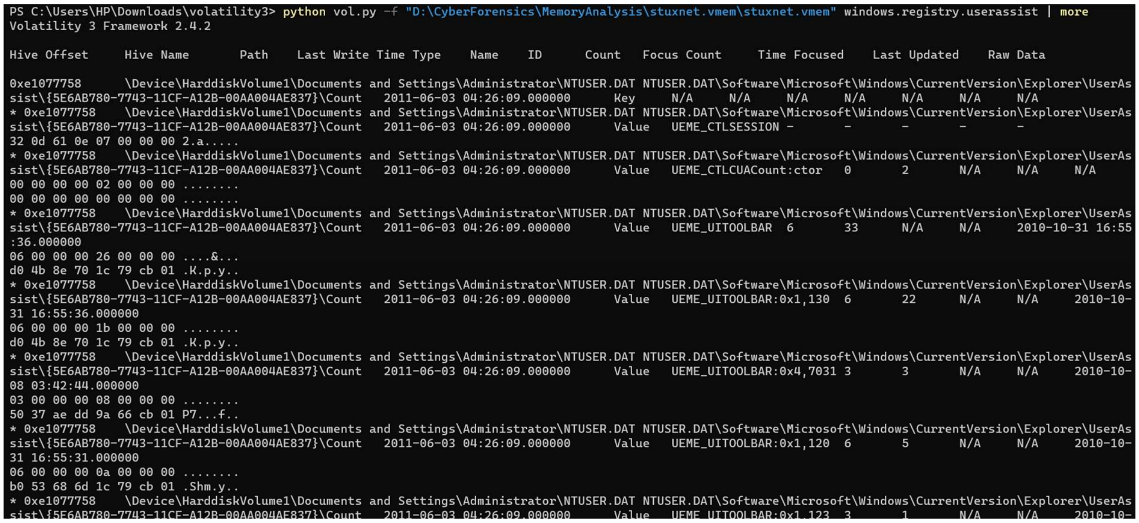


```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\stuxnet.vmem\stuxnet.vmem" windows.handles --pid 188
Volatility 3 Framework 2.4.2
Progress:  100.00               PDB scanning finished
PID     Process Offset  HandleValue     Type    GrantedAccess   Name

188     alg.exe 0xe10096e0      0x4     KeyedEvent      0x20003 CritSecOutOfMemoryEvent
188     alg.exe 0xe16008f8      0x8     Directory       0x3     KnownDlls
188     alg.exe 0x81e5f720      0xc     File    0x100020        \Device\HarddiskVolume1\WINDOWS\system32
188     alg.exe 0x82062080      0x10    Event   0x21f0003
188     alg.exe 0xe1613978      0x14    Directory       0xf000f Windows
188     alg.exe 0xe211c8d8      0x18    Port    0x21f0001
188     alg.exe 0x820646f8      0x1c    WindowStation   0xf006e Service-0x0-3e5$
188     alg.exe 0xe1623538      0x20    Directory       0x2000f BaseNamedObjects
188     alg.exe 0x81ee3980      0x24    Mutant  0x1f0001        SHIMLIB_LOG_MUTEX
188     alg.exe 0x81ee0a58      0x28    Desktop 0xf00cf Default
188     alg.exe 0x820646f8      0x2c    WindowStation   0xf006e Service-0x0-3e5$
188     alg.exe 0x81fdfef0      0x30    Semaphore       0x100003
188     alg.exe 0x81e6bfe8      0x34    Semaphore       0x100003
188     alg.exe 0xe1b2d0e8      0x38    Key     0x2020019       MACHINE
188     alg.exe 0x81fe5f90      0x3c    File    0x100001        \Device\KsecDD
188     alg.exe 0x81c95130      0x40    Event   0x1f0003
188     alg.exe 0x81eb3360      0x44    Semaphore       0x100003
188     alg.exe 0x820da2f0      0x48    Semaphore       0x100003
188     alg.exe 0xe20fbdd8      0x4c    Key     0x20019 MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\DRIVERS32
188     alg.exe 0x81e64138      0x50    Event   0x1f0003
188     alg.exe 0x81e64020      0x54    Event   0x1f0003
188     alg.exe 0xe1bd58e8      0x58    Key     0x20019 MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\DRIVERS32
188     alg.exe 0x8208cf48      0x5c    Semaphore       0x100002        shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
188     alg.exe 0x81e64078      0x60    File    0x12019f        \Device\NamedPipe\net\NtControlPipe13
188     alg.exe 0x81e5c0a0      0x64    File    0x100020        \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d
f_6.0.2600.5512_x-ww_35d4ce83
188     alg.exe 0x81e64d38      0x68    Event   0x1f0003
188     alg.exe 0x81e64d08      0x6c    Event   0x1f0003
188     alg.exe 0x81e64cd8      0x70    Event   0x1f0003
188     alg.exe 0x81e64ca8      0x74    Event   0x1f0003
188     alg.exe 0x820e2da8      0x78    Thread  0x1f03ff        Tid 192 Pid 188
188     alg.exe 0x821aa268      0x7c    Event   0x1f0003
188     alg.exe 0xe20e7390      0x80    Port    0x1f0001
188     alg.exe 0xe21388f0      0x84    Key     0xf003f USER\S-1-5-19_CLASSES
```



```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\stuxnet.vmem\stuxnet.vmem" windows.handles --pid 304
Volatility 3 Framework 2.4.2
Progress:  100.00               PDB scanning finished
PID     Process Offset  HandleValue     Type    GrantedAccess   Name

PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\stuxnet.vmem\stuxnet.vmem" windows.handles --pid 968
Volatility 3 Framework 2.4.2
Progress:  100.00               PDB scanning finished
PID     Process Offset  HandleValue     Type    GrantedAccess   Name
```

Windows.registry.userassist pluggin is used for to know the user activities



```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\stuxnet.vmem\stuxnet.vmem" windows.registry.userassist | more
Volatility 3 Framework 2.4.2

Hive Offset     Hive Name       Path    Last Write Time Type    Name    ID      Count   Focus Count     Time Focused    Last Updated    Raw Data

0xe1077758      \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAs
sist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count   2011-06-03 04:26:09.000000      Key     N/A     N/A     N/A     N/A     N/A     N/A     N/A
* 0xe1077758    \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAs
sist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count   2011-06-03 04:26:09.000000      Value   UEME_CTLSESSION -       -       -       -       -
32 0d 61 0e 07 00 00 00 2.a.....
* 0xe1077758    \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAs
sist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count   2011-06-03 04:26:09.000000      Value   UEME_CTLCUACount:ctor   0       2       N/A     N/A     N/A
00 00 00 00 02 00 00 00 ........
00 00 00 00 00 00 00 00 ........
* 0xe1077758    \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAs
sist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count   2011-06-03 04:26:09.000000      Value   UEME_UITOOLBAR  6       33      N/A     N/A     2010-10-31 16:55
:36.000000
06 00 00 00 26 00 00 00 ....&...
d0 4b 8e 70 1c 79 cb 01 .K.p.y..
* 0xe1077758    \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAs
sist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count   2011-06-03 04:26:09.000000      Value   UEME_UITOOLBAR:0x1,130  6       22      N/A     N/A     2010-10-
31 16:55:36.000000
06 00 00 00 1b 00 00 00 ........
d0 4b 8e 70 1c 79 cb 01 .K.p.y..
* 0xe1077758    \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAs
sist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count   2011-06-03 04:26:09.000000      Value   UEME_UITOOLBAR:0x4,7031 3       3       N/A     N/A     2010-10-
08 03:42:44.000000
03 00 00 00 08 00 00 00 ........
50 37 ae dd 9a 66 cb 01 P7...f..
* 0xe1077758    \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAs
sist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count   2011-06-03 04:26:09.000000      Value   UEME_UITOOLBAR:0x1,120  6       5       N/A     N/A     2010-10-
31 16:55:31.000000
06 00 00 00 0a 00 00 00 ........
b0 53 68 6d 1c 79 cb 01 .Shm.y..
* 0xe1077758    \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAs
sist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count   2011-06-03 04:26:09.000000      Value   UEME_UITOOLBAR:0x1,123  3       1       N/A     N/A     2010-10-
```

Here we get

Hive Offset and Hive Name where we are getting all this information

Last write – last time that action took place related to key by user

Count – no : of times the program is run

Focus count – no : of times that user focus on the window for the program

Time Focus – the total amount of time that user was looking over time

About Hive –

Windows Registry hive files to gather information about system configuration, user activity, installed software, and other artifacts.

hive offsets to extract specific registry keys or values from hive files

hive offsets may be used in data recovery efforts to extract registry data from damaged or corrupted hive files

By correlating timestamps with hive offsets, analysts can determine when specific registry keys or values were created, modified, or deleted.