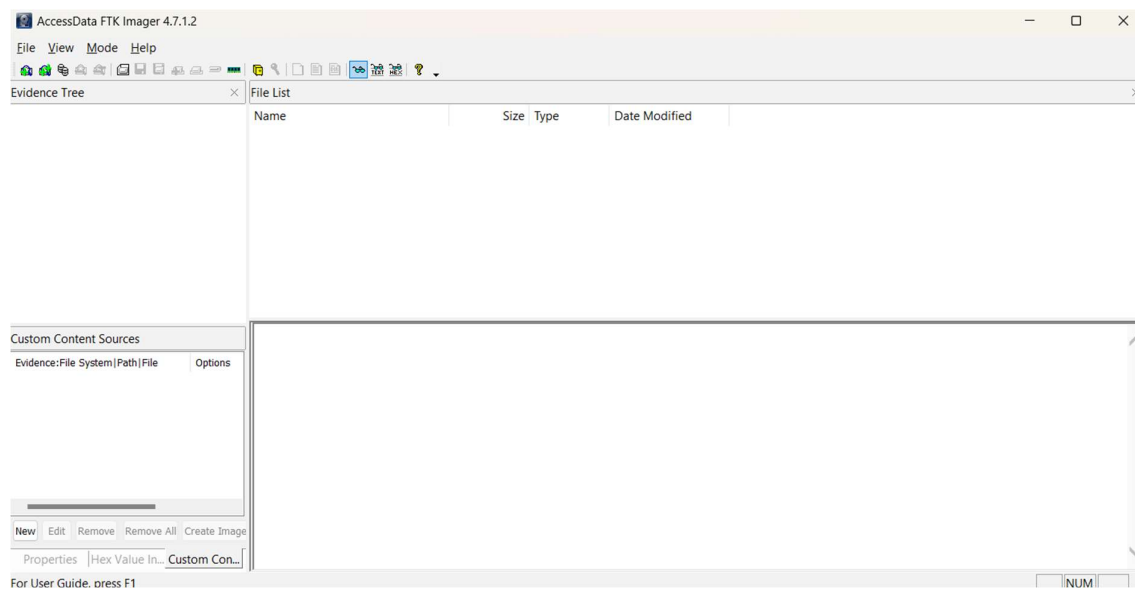
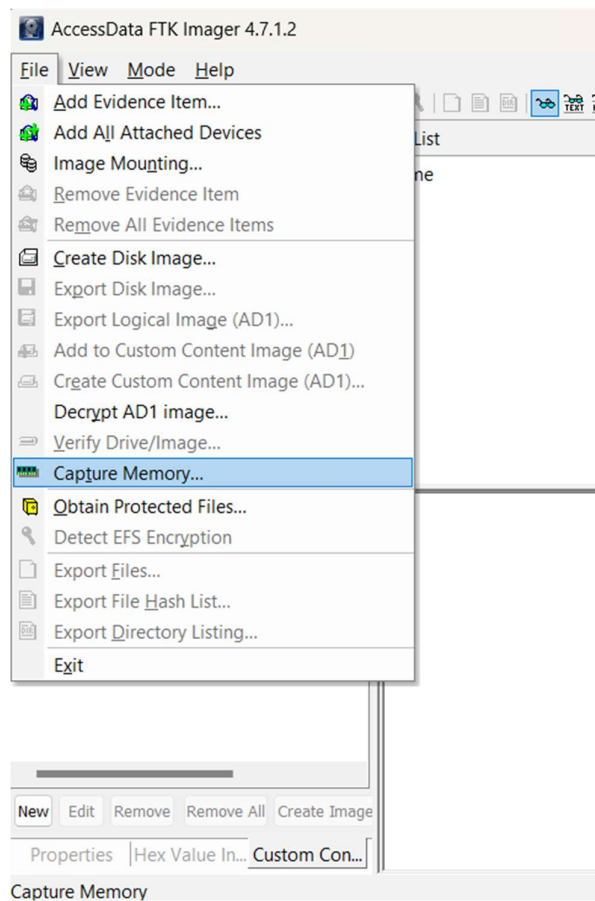
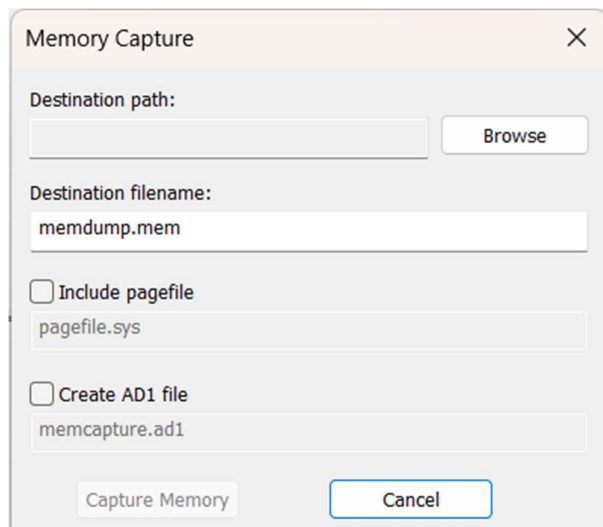


Taking a memory dump(RAM) :

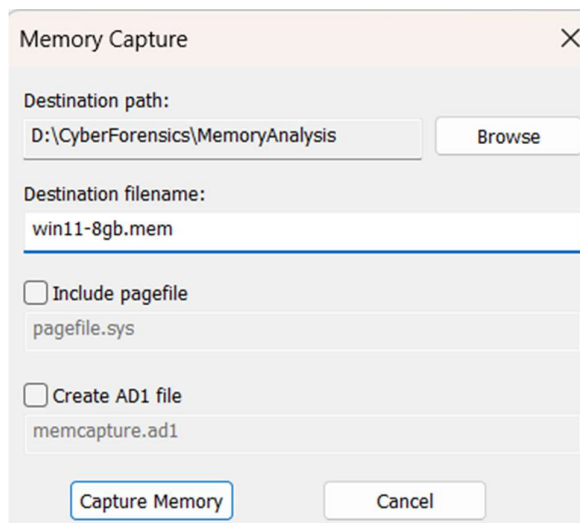


Go to File - > capture memory



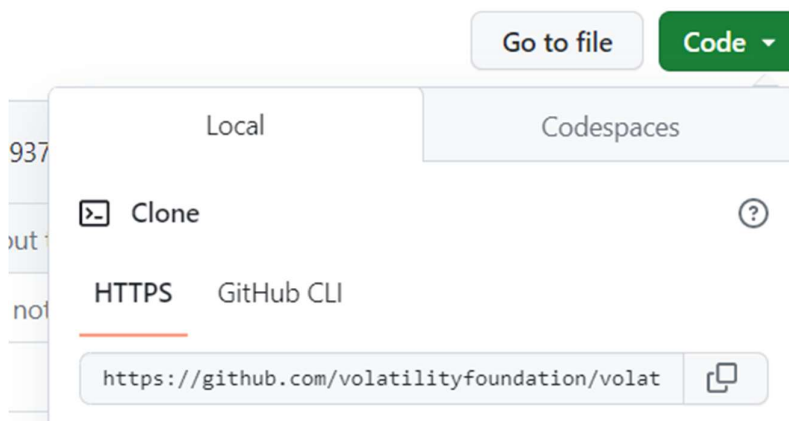


Give a required destination path and you can give file name manually ,next click on capture memory :



Go to volatility GitHub Link :

<https://github.com/volatilityfoundation/volatility3>



Using git clone can download that all file in your 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-cp310-cp310-win_amd64.whl
Defaulting to user installation because normal site-packages is not writeable
Processing c:\users\hp\downloads\python_snappy-0.6.1-cp310-cp310-win_amd64.whl
Installing collected packages: python-snappy
Successfully installed python-snappy-0.6.1

[notice] A new release of pip is available: 23.0.1 -> 23.1.2
[notice] To update, run: python.exe -m pip install --upgrade pip
PS C:\Users\HP\Downloads> python.exe -m pip install --upgrade pip
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: pip in c:\program files\python310\lib\site-packages (23.0.1)
Collecting pip
  Using cached pip-23.1.2-py3-none-any.whl (2.1 MB)
Installing collected packages: pip
  WARNING: The scripts pip.exe, pip3.10.exe and pip3.exe are installed in 'C:\Users\HP\AppData\Roaming\Python\Python310\Scripts' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
Successfully installed pip-23.1.2

[notice] A new release of pip is available: 23.0.1 -> 23.1.2
[notice] To update, run: python.exe -m pip install --upgrade pip
PS C:\Users\HP\Downloads> python.exe -m pip install --upgrade pip
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: pip in c:\users\hp\appdata\roaming\python\python310\site-packages (23.1.2)
```

 python_snappy-0.6.1-cp310-cp310-win_a...	03-05-2023 16:44	Python Wheel	30 KB
 vs_BuildTools	03-05-2023 16:35	Application	3,622 KB
 python-3.11.3-amd64	03-05-2023 17:22	Application	24,753 KB
 python-3.10.11-amd64	03-05-2023 17:31	Application	28,357 KB
▼ Yesterday			
 volatility3	02-05-2023 11:19	File folder	

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\HP> cd .\Downloads\
PS C:\Users\HP\Downloads> pip install C:\Users\HP\Downloads\python_snappy-0.6.1-cp311-cp311-win_amd64.whl
Defaulting to user installation because normal site-packages is not writeable
ERROR: python_snappy-0.6.1-cp311-cp311-win_amd64.whl is not a supported wheel on this platform.
PS C:\Users\HP\Downloads> pip install C:\Users\HP\Downloads\python_snappy-0.6.1-cp310-cp310-win_amd64.whl
Defaulting to user installation because normal site-packages is not writeable
Processing c:\users\hp\downloads\python_snappy-0.6.1-cp310-cp310-win_amd64.whl
python-snappy is already installed with the same version as the provided wheel. Use --force-reinstall to force an installation of the wheel.
PS C:\Users\HP\Downloads> cd .\volatility3\
```

Go to volatility directory and list all the files

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

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-----          02-05-2023     11:19        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
```

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-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 a memory dump file and take its path

Gives information which taken from memory

In this command : python vol.py -f D:\CyberForensics\MemoryAnalysis\win11x64-8GB.mem windows.info

python vol.py → to Check Volatility

-f → to get file path

D:\CyberForensics\MemoryAnalysis\win11x64-8GB.mem → Path where dump file is there

windows.info → name of plugin

```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f D:\CyberForensics\MemoryAnalysis\win11x64-8GB.mem windows.info
Volatility 3 Framework 2.4.2
Progress: 100.00 PDB scanning finished
Variable      Value
-----
Kernel Base   0xf80286200000
DTB           0x1ae000
Symbols file: //C:/Users/HP/Downloads/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/D60B01EB7A8A7D46D5EF38DD5556547C-1.json.xz
Is64Bit       True
IsPAE         False
Layer_name    0 WindowsIntel32e
memory_layer  1 FileLayer
KdVersionBlock 0xf80286e099b0
Major/Minor   15.22621
MachineType   34404
KeNumberProcessors 8
SystemTime    2023-05-04 04:56:05
NtSystemRoot  C:\WINDOWS
NtProductType NtProductWinNt
NtMajorVersion 10
NtMinorVersion 0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine     34404
PE TimeDateStamp Sun Jul 24 04:13:48 1977
```

To check what are the plugins :

To check what are available plugins

```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\win11x64-8GB.mem" windows
Volatility 3 Framework 2.4.2
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-a 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.cachedump.Cachedump, windows.callbacks.Callb
acks, windows.cmdline.CmdLine, windows.crashinfo.CrashInfo, windows.devicetree.DeviceTree, windows.dllexport.DllList, windows.driverirp.DriverIrp, windows.dri
vermodule.DriverModule, windows.driverscan.DriverScan, windows.dumpfiles.DumpFiles, windows.envvars.Envvars, windows.filescan.FileScan, windows.getservicesids
.GetServiceSids, windows.getuids.GetUIDs, windows.handles.Handles, windows.hashdump.Hashdump, windows.info.Info, windows.joblinks.JobLinks, windows.ldrmodul
es.LdrModules, windows.lsadump.Lsadump, windows.malfind.Malfind, windows.mbrscan.MBRScan, windows.memmap.Memmap, windows.mftscan.MFTScan, windows.modscan.Mo
dScan, windows.modules.Modules, windows.mutantscan.MutantScan, windows.netstat.NetStat, windows.poolscanner.PoolScanner, windows.pr
ivileges.Privs, windows.pslist.PsList, windows.psscan.PsScan, windows.pstree.PsTree, windows.registry.certificates.Certificates, windows.registry.hivelist.Hi
veList, windows.registry.hivescan.HiveScan, windows.registry.printkey.PrintKey, windows.registry.userassist.UserAssist, windows.sessions.Sessions, windows.s
keleton_key_check.SkeletonKeyCheck, windows.ssd.SSD, windows.statistics.Statistics, windows.strings.Strings, windows.svcscan.SvcScan, windows.symlinksca
n.SymlinkScan, windows.vadinfo.VadInfo, windows.vadwalk.VadWalk, windows.vadvarscan.VadVarScan, windows.verinfo.VerInfo, windows.virtmap.VirtMap)
```

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

```
PS C:\Users\WP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\win11x64-8GB.mem" windows.pslist | more
Volatility 3 Framework 2.4.2
```

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
4	0	System	0x860eeb2f5040 291	-	N/A	False	2023-05-03 12:16:29.000000	N/A	Disabled140	4 Registry
0eeb3ef040	4	-	N/A	False	2023-05-03 12:16:23.000000	N/A	Disabled			
636	4	smss.exe	0x860f063aa080	2	-	N/A	False	2023-05-03 12:16:29.000000	N/A	Disabled
868	636	smss.exe	0x860f084f2080	0	-	0	False	2023-05-03 12:16:30.000000	2023-05-03 12:16:34.000000	Dis
788	868	csrss.exe	0x860f0931e140	11	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
580	868	wininit.exe	0x860f0b475080	2	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1052	580	services.exe	0x860f0b53e080	8	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1080	580	lsass.exe	0x860f0b5c7080	10	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1152	1012	winlogon.exe	0x860f0b5d9080	0	-	1	False	2023-05-03 12:16:34.000000	2023-05-03 12:17:49.000000	Dis
1268	1052	svchost.exe	0x860f0b68b080	16	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1296	1152	fontdrvhost.exe	0x860f0b6b0800	0	-	1	False	2023-05-03 12:16:34.000000	2023-05-03 12:17:49.000000	Dis
1300	580	fontdrvhost.exe	0x860f0b6b4080	5	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1384	1052	WUDFHost.exe	0x860f0b7340c0	14	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1440	1052	svchost.exe	0x860f0b7be0c0	10	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1492	1052	svchost.exe	0x860f0b7d5080	5	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1588	1052	svchost.exe	0x860f0cc5b080	3	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1596	1052	svchost.exe	0x860f0cc54080	3	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1620	1052	svchost.exe	0x860f0cc56080	3	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1628	1052	WUDFHost.exe	0x860f0cc80080	5	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1640	1052	svchost.exe	0x860f0cc8a080	4	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1664	1052	svchost.exe	0x860f0cc8c080	10	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1676	1052	svchost.exe	0x860f0cc900c0	7	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1796	1052	svchost.exe	0x860f0ccc0080	6	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1812	1052	svchost.exe	0x860f0ccc0080	4	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1832	1052	svchost.exe	0x860f0ccf2080	2	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
2024	1052	svchost.exe	0x860f0cdd6080	3	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
844	1052	IntelCpHDCPSvc	0x860f0ce4730c0	3	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1204	1052	svchost.exe	0x860f0ce47080	10	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1488	1052	svchost.exe	0x860f0ce4d080	19	-	0	False	2023-05-03 12:16:35.000000	N/A	Disabled
1936	1052	svchost.exe	0x860f0cf3d080	4	-	0	False	2023-05-03 12:16:35.000000	N/A	Disabled
1980	1052	svchost.exe	0x860f0cf3c080	0	-	0	False	2023-05-03 12:16:35.000000	2023-05-03 16:31:05.000000	Dis

It shows System is the 1st processor

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
4	0	System	0x860eeb2f5040 291	-	N/A	False	2023-05-03 12:16:29.000000	N/A	Disabled140	4 Registry 0x86

To get entire information at a time

```
> python vol.py -f "D:\CyberForensics\MemoryAnalysis\win11x64-8GB.mem" 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	0x860eeb2f5040 291	-	N/A	False	2023-05-03 12:16:29.000000	N/A	Disabled140	4 Registry 0x86
0eeb3ef040	4	-	N/A	False	2023-05-03 12:16:23.000000	N/A	Disabled			
636	4	smss.exe	0x860f063aa080	2	-	N/A	False	2023-05-03 12:16:29.000000	N/A	Disabled
868	636	smss.exe	0x860f084f2080	0	-	0	False	2023-05-03 12:16:30.000000	2023-05-03 12:16:34.000000	Disabled
788	868	csrss.exe	0x860f0931e140	11	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
580	868	wininit.exe	0x860f0b475080	2	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1052	580	services.exe	0x860f0b53e080	8	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1080	580	lsass.exe	0x860f0b5c7080	10	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1152	1012	winlogon.exe	0x860f0b5d9080	0	-	1	False	2023-05-03 12:16:34.000000	2023-05-03 12:17:49.000000	Disabled
1268	1052	svchost.exe	0x860f0b68b080	16	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1296	1152	fontdrvhost.exe	0x860f0b6b0800	0	-	1	False	2023-05-03 12:16:34.000000	2023-05-03 12:17:49.000000	Disabled
1300	580	fontdrvhost.exe	0x860f0b6b4080	5	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1384	1052	WUDFHost.exe	0x860f0b7340c0	14	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1440	1052	svchost.exe	0x860f0b7be0c0	10	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled
1492	1052	svchost.exe	0x860f0b7d5080	5	-	0	False	2023-05-03 12:16:34.000000	N/A	Disabled

For filtering purpose we use Select-String

Analysing chrome

```
PS C:\Users\HP\Downloads\volatility3> python vol.py -f "D:\CyberForensics\MemoryAnalysis\win11x64-8GB.mem" windows.pslist | Select-String chrome
Progress: 100.00      PDB scanning finished
12796 11544 chrome.exe 0x860f155f7140 55 - 2 False 2023-05-03 16:52:58.000000 N/A Disabled
1400 12796 chrome.exe 0x860f162de0c0 8 - 2 False 2023-05-03 16:52:58.000000 N/A Disabled
14420 12796 chrome.exe 0x860f168b80c0 27 - 2 False 2023-05-03 16:52:58.000000 N/A Disabled
9140 12796 chrome.exe 0x860f16bda0c0 20 - 2 False 2023-05-03 16:52:58.000000 N/A Disabled
16772 12796 chrome.exe 0x860f171ec0c0 10 - 2 False 2023-05-03 16:52:58.000000 N/A Disabled
19428 12796 chrome.exe 0x860f162790c0 19 - 2 False 2023-05-03 16:52:58.000000 N/A Disabled
9940 12796 chrome.exe 0x860f15e450c0 19 - 2 False 2023-05-03 16:52:58.000000 N/A Disabled
11456 12796 chrome.exe 0x860f170020c0 16 - 2 False 2023-05-03 16:52:58.000000 N/A Disabled
4188 12796 chrome.exe 0x860f163670c0 20 - 2 False 2023-05-03 16:52:58.000000 N/A Disabled
8752 12796 chrome.exe 0x860f16faf0c0 17 - 2 False 2023-05-03 16:52:58.000000 N/A Disabled
576 12796 chrome.exe 0x860f16dda0c0 16 - 2 False 2023-05-03 16:52:58.000000 N/A Disabled
10816 12796 chrome.exe 0x860f15f980c0 17 - 2 False 2023-05-03 16:52:58.000000 N/A Disabled
19028 12796 chrome.exe 0x860f160eb0c0 19 - 2 False 2023-05-03 16:52:58.000000 N/A Disabled
8128 12796 chrome.exe 0x860f160790c0 17 - 2 False 2023-05-03 16:52:58.000000 N/A Disabled
1616 12796 chrome.exe 0x860f164570c0 19 - 2 False 2023-05-03 16:52:58.000000 N/A Disabled
2444 12796 chrome.exe 0x860f097020c0 19 - 2 False 2023-05-03 16:52:58.000000 N/A Disabled
3208 12796 chrome.exe 0x860f110c6080 12 - 2 False 2023-05-03 16:53:07.000000 N/A Disabled
3300 12796 chrome.exe 0x860f17a020c0 19 - 2 False 2023-05-03 16:57:36.000000 N/A Disabled
10636 12796 chrome.exe 0x860f1a433080 21 - 2 False 2023-05-03 17:26:02.000000 N/A Disabled
26996 12796 chrome.exe 0x860f1de350c0 22 - 2 False 2023-05-03 21:19:22.000000 N/A Disabled
15256 12796 chrome.exe 0x860f1baf2080 22 - 2 False 2023-05-04 03:57:30.000000 N/A Disabled
26252 12796 chrome.exe 0x860f1794c080 20 - 2 False 2023-05-04 04:06:54.000000 N/A Disabled
23920 12796 chrome.exe 0x860f187920c0 19 - 2 False 2023-05-04 04:08:36.000000 N/A Disabled
1636 12796 chrome.exe 0x860f09a180c0 21 - 2 False 2023-05-04 04:11:17.000000 N/A Disabled
6048 12796 chrome.exe 0x860f1a39b0c0 18 - 2 False 2023-05-04 04:17:30.000000 N/A Disabled
24152 12796 chrome.exe 0x860f16a130c0 19 - 2 False 2023-05-04 04:19:58.000000 N/A Disabled
15948 12796 chrome.exe 0x860f1b00c080 18 - 2 False 2023-05-04 04:20:04.000000 N/A Disabled
24040 12796 chrome.exe 0x860f18bd10c0 20 - 2 False 2023-05-04 04:20:06.000000 N/A Disabled
28488 12796 chrome.exe 0x860f1ae8c080 19 - 2 False 2023-05-04 04:48:01.000000 N/A Disabled
3704 12796 chrome.exe 0x860f18bf3080 8 - 2 False 2023-05-04 04:49:29.000000 N/A Disabled
11096 12796 chrome.exe 0x860f1d615080 22 - 2 False 2023-05-04 04:49:30.000000 N/A Disabled
17916 12796 chrome.exe 0x860f1e888080 13 - 2 False 2023-05-04 04:49:32.000000 N/A Disabled
23232 12796 chrome.exe 0x860f1d7b4080 16 - 2 False 2023-05-04 04:54:43.000000 N/A Disabled
```

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