Sanjana Asrani — Digital Forensics
D17B/ 01/ Batch B — Lab-03

AIM: Performing RAM Forensics

OBJECTIVE:

- Capture an image of RAM of victim machine
- Use volatility tool to analyze memory images to find traces of an attack.

THEORY:

- ➢ RAM capture is the process of capturing live memory from a running computer system. RAM analysis consists of performing forensic analysis on the data gathered from the live computer.
- ➢ After conducting a memory dump on any live machine to capture RAM, the memory image can be used to determine information about running programs, the operating system, and the overall state of a computer, as well as to locate deleted or temporary information that might otherwise not be found on a normal image.
- ➢ Until recently, RAM analysis and capture was not a mandatory step in investigations, or even in triage situations where analysts were attempting to gather forensic data on site.
- ➢ However, with new tools that allow entry into locked systems and with the growing importance of temporary files, RAM analysis is quickly becoming a pivotal and mandatory part of the digital forensics process.
- ➢ Volatile memory access is useful in law enforcement situations where data would be lost by powering off a suspect machine.
- ➢ The longer a machine is off, the more data becomes lost.
  The following can be found using RAM capture: Processes, Network connections, Open files /Configurations/Encryption keys,Open/Active Registry keys,Exploit-related information, Zero-day attacks and root-kits, and kernel-level structures.

Tools:

1. Volatility:

- Volatility is a powerful open-source memory forensics framework used to analyze volatile memory dumps. It is a powerful memory forensics tool used for analyzing volatile memory dumps. RAM analysis involves extracting and analyzing data from volatile memory dumps to investigate security incidents and identify malicious activities. It allows forensic investigators and incident responders to extract valuable information from memory images, including running processes, open network connections, loaded kernel modules, registry artifacts, and more.

- Supports analysis of memory dumps from various operating systems, including Windows, Linux, macOS, and Android.

- Provides a wide range of plugins for analyzing different aspects of memory, such as processes, network connections, registry, and file system artifacts.
- Offers scripting and automation capabilities through its Python API, allowing users to create custom analysis workflows and automate repetitive tasks.

2. **VolatilityBot:**
- VolatilityBot is an automation framework built on top of Volatility. It is designed to simplify the process of analyzing memory dumps by automating the execution of multiple Volatility plugins and aggregating the results into a unified report.
- Automates the execution of Volatility plugins against memory dumps, saving time and effort for analysts.
- Supports the creation of custom analysis workflows by chaining together multiple Volatility plugins.
- Provides a unified HTML report summarizing the findings from all executed plugins, making it easier for analysts to interpret the results.

3. **DumpIt:**
- DumpIt is a lightweight and easy-to-use tool for creating memory dumps on Windows systems. It is commonly used by forensic investigators and incident responders to acquire the physical memory of a suspect system for subsequent analysis.
- Creates a memory dump of the entire physical memory (RAM) of a Windows system, including kernel space and user space.
- Runs directly from a USB drive without requiring installation, making it portable and convenient to use in the field.
- Supports both 32-bit and 64-bit versions of Windows..

4**. LiME (Linux Memory Extractor):**
- LiME is a loadable kernel module for Linux that allows for the acquisition of volatile memory from a Linux system. It enables forensic investigators and incident responders to capture memory dumps for analysis without disrupting the running system.
- Acquires physical memory (RAM) from a Linux system by loading as a kernel module, ensuring minimal impact on system operations.
- Generates memory dumps in raw or Lime format, which can be analyzed using memory forensics tools like Volatility or Rekall.
- Supports both 32-bit and 64-bit Linux kernels.

Here are some options available in Volatility for the cmd: python3 vol.py -f <filename.raw> windows.option-name:

windows.pstree: This command displays the process tree, showing parent-child relationships between processes on a Windows system.

windows.pslist: This command lists running processes on a Windows system.

windows.psscan: This command scans for processes that might have been terminated or hidden from the pslist plugin.

windows.psxview: This command reveals hidden and terminated processes by analyzing various process lists and kernel objects.

windows.callbacks: Lists registered callback functions in the kernel, which can provide insights into the activities of certain malware or rootkits.

windows.lsadump: Extracts security account information from the Security Account Manager (SAM) hive.

windows.netstat: Displays network connections, similar to the netstat command in Windows.

windows.filescan: Scans for file handles within the memory dump.

windows.dlllist: Lists loaded DLLs within processes.

windows.driverirp: Examines Windows kernel drivers and their associated IRP (I/O Request Packet) structures.

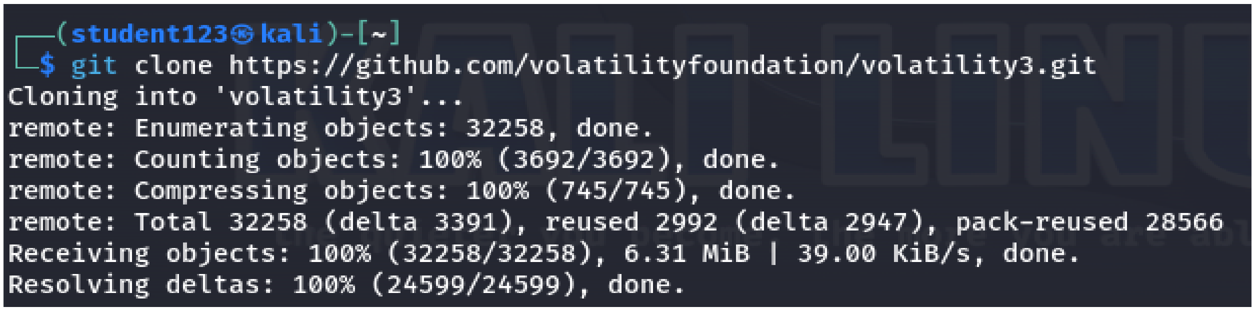
windows.consoles: Lists information about console windows.

windows.modules: Lists loaded kernel modules and drivers, helping to identify potentially malicious or suspicious drivers.

windows.sessions: Lists active user sessions on the system, including interactive logon sessions and remote desktop sessions.

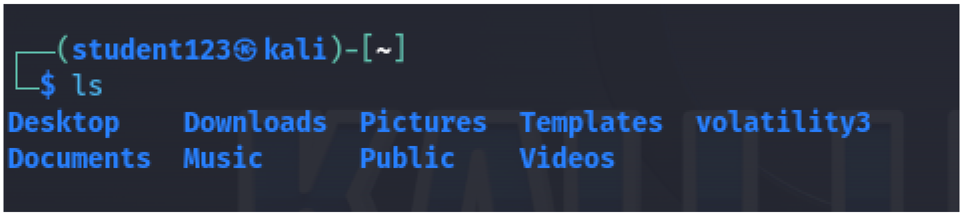
STEPS:

Refer to:
https://www.varonis.com/blog/how-to-use-volatility
cmd: git clone https://github.com/volatilityfoundation/volatility3.git



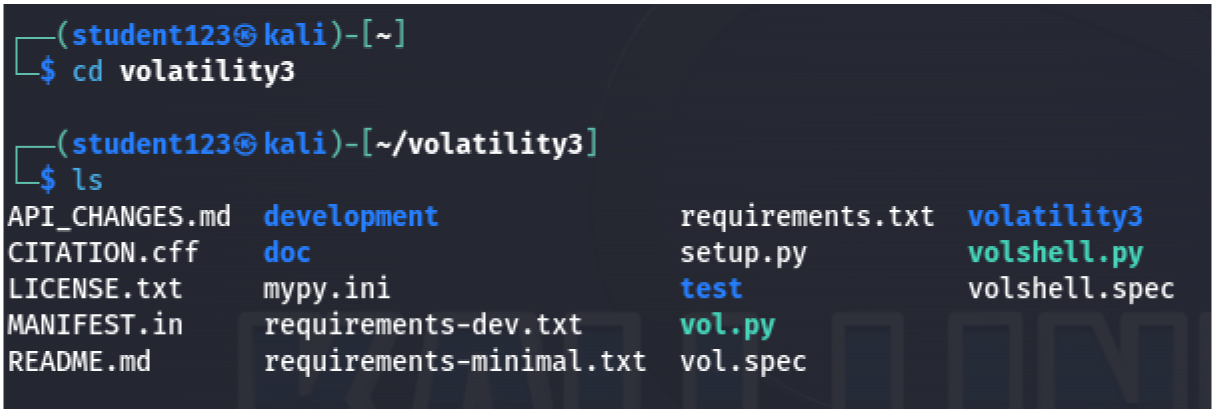
```
┌──(student123㉿kali)-[~]
└─$ git clone https://github.com/volatilityfoundation/volatility3.git
Cloning into 'volatility3'...
remote: Enumerating objects: 32258, done.
remote: Counting objects: 100% (3692/3692), done.
remote: Compressing objects: 100% (745/745), done.
remote: Total 32258 (delta 3391), reused 2992 (delta 2947), pack-reused 28566
Receiving objects: 100% (32258/32258), 6.31 MiB | 39.00 KiB/s, done.
Resolving deltas: 100% (24599/24599), done.
```

Repo has been cloned:



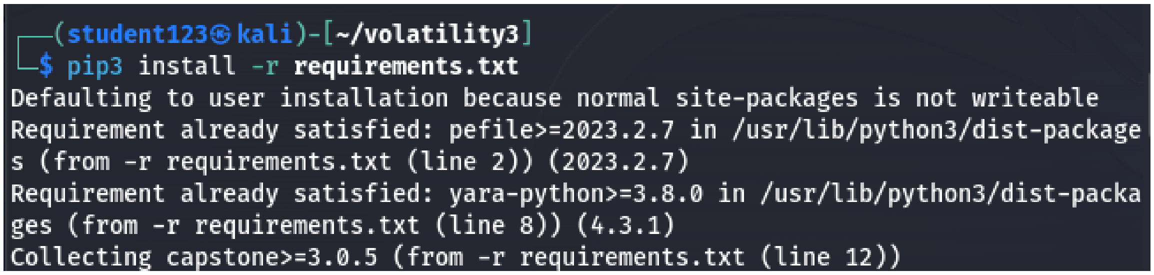
```
┌──(student123㉿kali)-[~]
└─$ ls
Desktop    Downloads  Pictures  Templates  volatility3
Documents  Music      Public    Videos
```

Go to that directory:



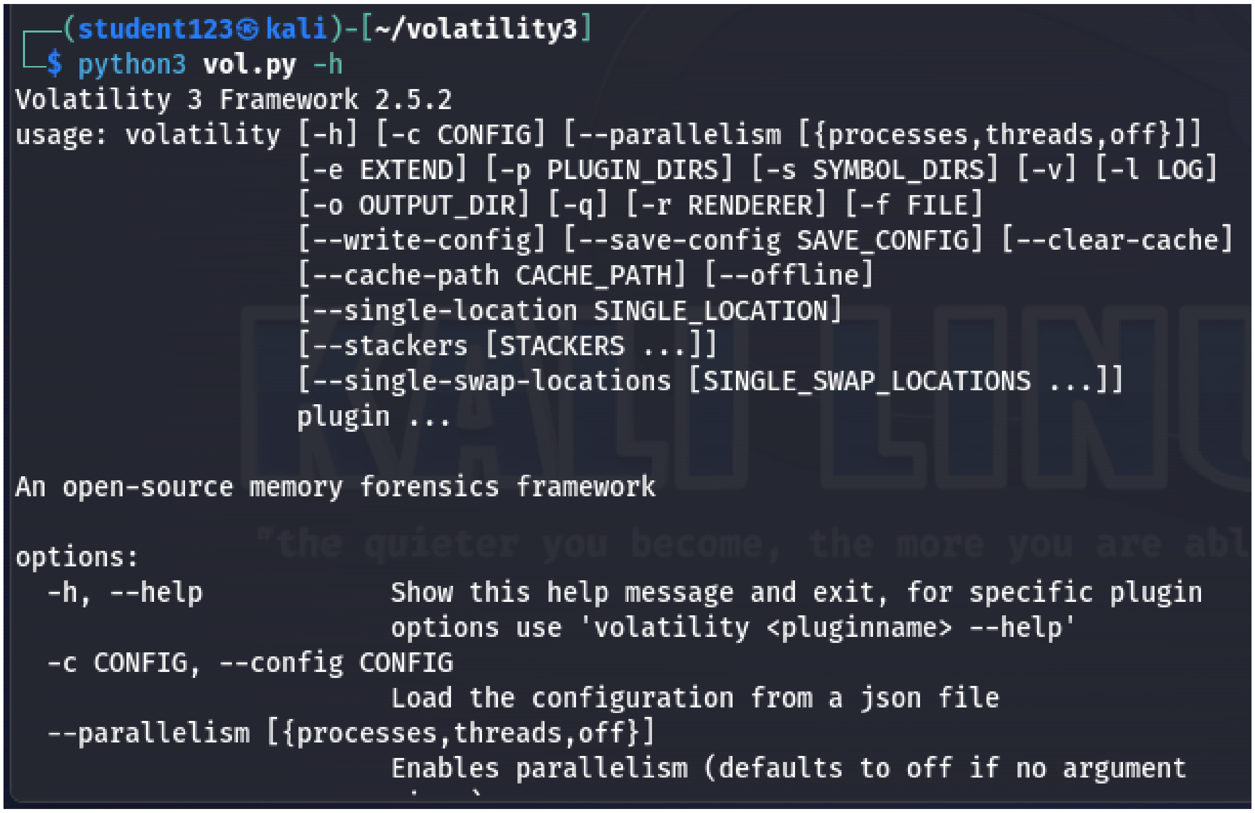
```
┌──(student123㉿kali)-[~]
└─$ cd volatility3

┌──(student123㉿kali)-[~/volatility3]
└─$ ls
API_CHANGES.md  development               requirements.txt  volatility3
CITATION.cff    doc                       setup.py          volshell.py
LICENSE.txt     mypy.ini                  test              volshell.spec
MANIFEST.in     requirements-dev.txt      vol.py
README.md       requirements-minimal.txt  vol.spec
```

Cmd: pip3 install -r requirements.txt



```
┌──(student123㉿kali)-[~/volatility3]
└─$ pip3 install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: pefile>=2023.2.7 in /usr/lib/python3/dist-package
s (from -r requirements.txt (line 2)) (2023.2.7)
Requirement already satisfied: yara-python>=3.8.0 in /usr/lib/python3/dist-packa
ges (from -r requirements.txt (line 8)) (4.3.1)
Collecting capstone>=3.0.5 (from -r requirements.txt (line 12))
```

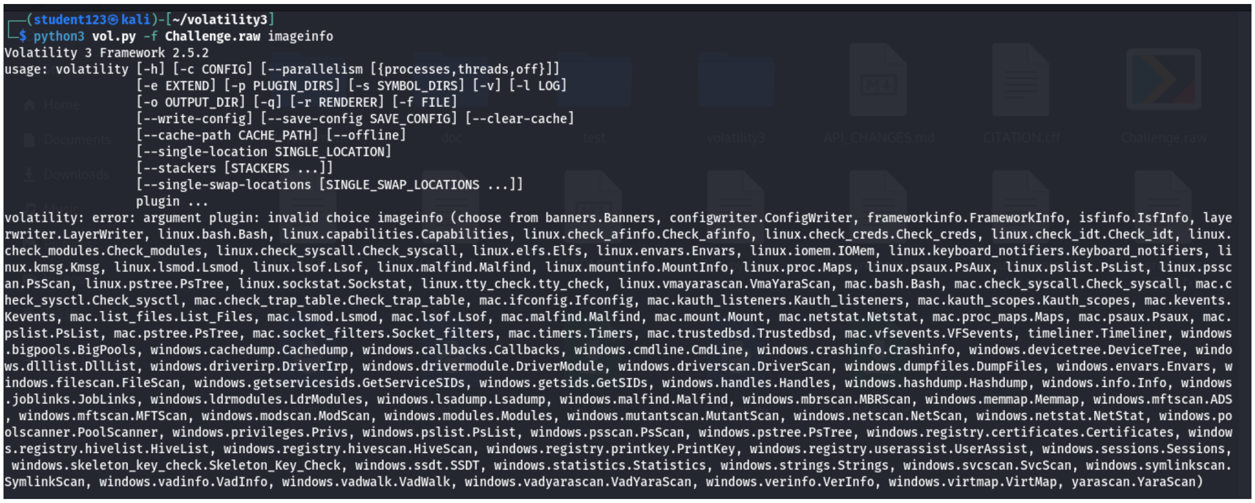
Run the vol.py file:



```
┌──(student123㉿kali)-[~/volatility3]
└─$ python3 vol.py -h
Volatility 3 Framework 2.5.2
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 ...

An open-source memory forensics framework

options:
  -h, --help            Show this help message and exit, for specific plugin
                        options use 'volatility <pluginname> --help'
  -c CONFIG, --config CONFIG
                        Load the configuration from a json file
  --parallelism [{processes,threads,off}]
                        Enables parallelism (defaults to off if no argument
```

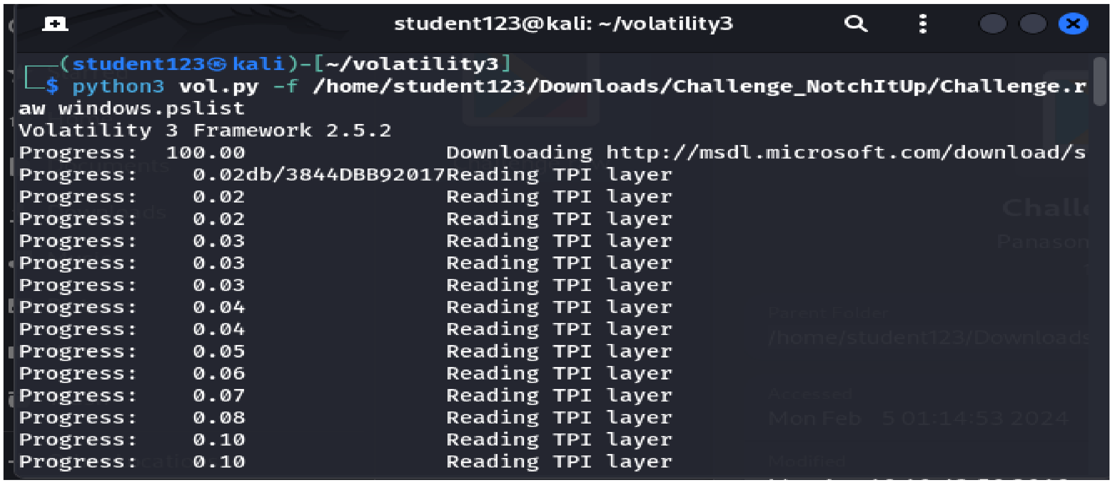
Download the Raw file from
https://drive.usercontent.google.com/download?id=1bER4wmHP_LAMgdB52LGkb8x2Mf8hG3V6&export=download

Python3 vol.py -f filename.raw imageinfo

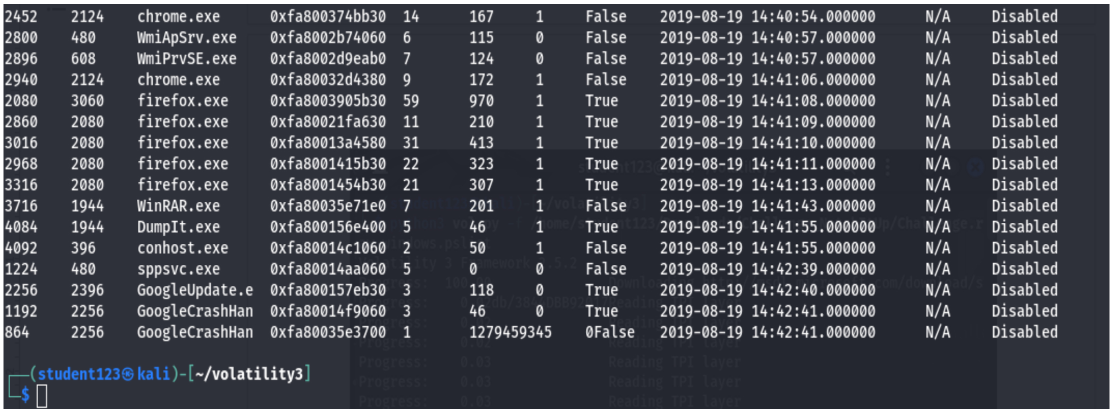


```
┌──(student123㉿kali)-[~/volatility3]
└─$ python3 vol.py -f Challenge.raw imageinfo
Volatility 3 Framework 2.5.2
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]]
                  [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG]
                  [-o OUTPUT_DIR] [-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: invalid choice imageinfo (choose from banners.Banners, configwriter.ConfigWriter, frameworkinfo.FrameworkInfo, isfinfo.IsfInfo, laye
rwriter.LayerWriter, linux.bash.Bash, linux.capabilities.Capabilities, linux.check_afinfo.Check_afinfo, linux.check_creds.Check_creds, linux.check_idt.Check_idt, linux.
check_modules.Check_modules, linux.check_syscall.Check_syscall, linux.elfs.Elfs, linux.envars.Envars, linux.iomem.IOMem, linux.keyboard_notifiers.Keyboard_notifiers, li
nux.kmsg.Kmsg, linux.lsmod.Lsmod, linux.lsof.Lsof, linux.malfind.Malfind, linux.mountinfo.MountInfo, linux.proc.Maps, linux.psaux.PsAux, linux.pslist.PsList, linux.pssc
an.PsScan, linux.pstree.PsTree, linux.sockstat.Sockstat, linux.tty_check.tty_check, linux.vmayarascan.VmaYaraScan, mac.bash.Bash, mac.check_syscall.Check_syscall, mac.c
heck_sysctl.Check_sysctl, mac.check_trap_table.Check_trap_table, mac.ifconfig.Ifconfig, mac.kauth_listeners.Kauth_listeners, mac.kauth_scopes.Kauth_scopes, mac.kevents.
Kevents, mac.list_files.List_Files, mac.lsmod.Lsmod, mac.lsof.Lsof, mac.malfind.Malfind, mac.mount.Mount, mac.netstat.Netstat, mac.proc_maps.Maps, mac.psaux.Psaux, mac.
pslist.PsList, mac.pstree.PsTree, mac.socket_filters.Socket_filters, mac.timers.Timers, mac.trustedbsd.Trustedbsd, mac.vfsevents.VFSevents, timeliner.Timeliner, windows
.bigpools.BigPools, windows.cachedump.Cachedump, windows.callbacks.Callbacks, windows.cmdline.CmdLine, windows.crashinfo.Crashinfo, windows.devicetree.DeviceTree, windo
ws.dlllist.DllList, windows.driverirp.DriverIrp, windows.drivermodule.DriverModule, windows.driverscan.DriverScan, windows.dumpfiles.DumpFiles, windows.envars.Envars, w
indows.filescan.FileScan, windows.getservicesids.GetServiceSIDs, windows.getsids.GetSIDs, windows.handles.Handles, windows.hashdump.Hashdump, windows.info.Info, windows
.joblinks.JobLinks, windows.ldrmodules.LdrModules, windows.lsadump.Lsadump, windows.malfind.Malfind, windows.mbrscan.MBRScan, windows.memmap.Memmap, windows.mftscan.ADS
, windows.mftscan.MFTScan, windows.modscan.ModScan, windows.modules.Modules, windows.mutantscan.MutantScan, windows.netscan.NetScan, windows.netstat.NetStat, windows.po
olscanner.PoolScanner, windows.privileges.Privs, windows.pslist.PsList, windows.psscan.PsScan, windows.pstree.PsTree, windows.registry.certificates.Certificates, window
s.registry.hivelist.HiveList, windows.registry.hivescan.HiveScan, windows.registry.printkey.PrintKey, windows.registry.userassist.UserAssist, windows.sessions.Sessions,
 windows.skeleton_key_check.Skeleton_Key_Check, windows.ssdt.SSDT, windows.statistics.Statistics, windows.strings.Strings, windows.svcscan.SvcScan, windows.symlinkscan.
SymlinkScan, windows.vadinfo.VadInfo, windows.vadwalk.VadWalk, windows.vadyarascan.VadYaraScan, windows.verinfo.VerInfo, windows.virtmap.VirtMap, yarascan.YaraScan)
```

python3 vol.py -f <filename.raw> windows.pslist

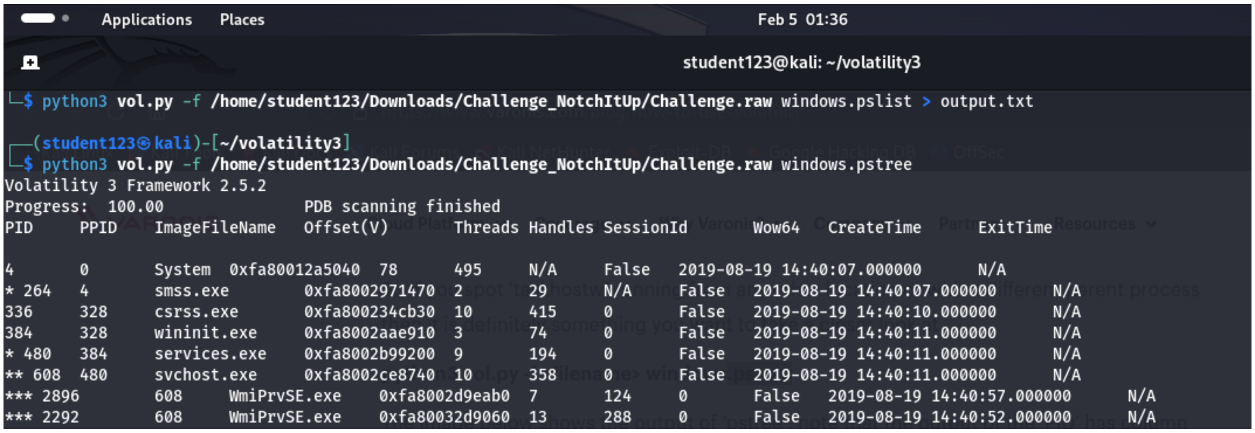


```
┌──(student123㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/student123/Downloads/Challenge_NotchItUp/Challenge.r
aw windows.pslist
Volatility 3 Framework 2.5.2
Progress:  100.00               Downloading http://msdl.microsoft.com/download/s
Progress:    0.02db/3844DBB92017Reading TPI layer
Progress:    0.02               Reading TPI layer
Progress:    0.02               Reading TPI layer
Progress:    0.03               Reading TPI layer
Progress:    0.03               Reading TPI layer
Progress:    0.03               Reading TPI layer
Progress:    0.04               Reading TPI layer
Progress:    0.04               Reading TPI layer
Progress:    0.05               Reading TPI layer
Progress:    0.06               Reading TPI layer
Progress:    0.07               Reading TPI layer
Progress:    0.08               Reading TPI layer
Progress:    0.10               Reading TPI layer
Progress:    0.10               Reading TPI layer
```

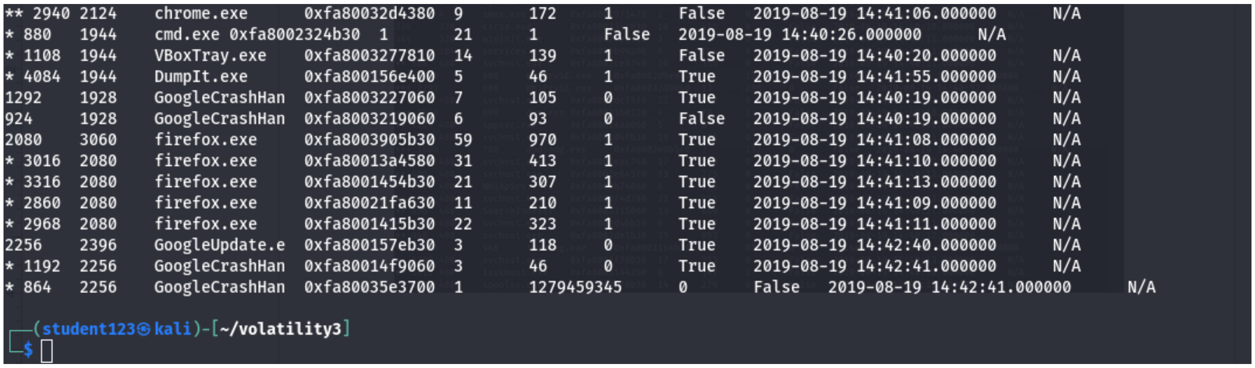


```
2452    2124    chrome.exe      0xfa800374bb30  14      167     1       False   2019-08-19 14:40:54.000000      N/A     Disabled
2800    480     WmiApSrv.exe    0xfa8002b74060  6       115     0       False   2019-08-19 14:40:57.000000      N/A     Disabled
2896    608     WmiPrvSE.exe    0xfa8002d9eab0  7       124     0       False   2019-08-19 14:40:57.000000      N/A     Disabled
2940    2124    chrome.exe      0xfa80032d4380  9       172     1       False   2019-08-19 14:41:06.000000      N/A     Disabled
2080    3060    firefox.exe     0xfa8003905b30  59      970     1       True    2019-08-19 14:41:08.000000      N/A     Disabled
2860    2080    firefox.exe     0xfa80021fa630  11      210     1       True    2019-08-19 14:41:09.000000      N/A     Disabled
3016    2080    firefox.exe     0xfa80013a4580  31      413     1       True    2019-08-19 14:41:10.000000      N/A     Disabled
2968    2080    firefox.exe     0xfa8001415b30  22      323     1       True    2019-08-19 14:41:11.000000      N/A     Disabled
3316    2080    firefox.exe     0xfa8001454b30  21      307     1       True    2019-08-19 14:41:13.000000      N/A     Disabled
3716    1944    WinRAR.exe      0xfa80035e71e0  7       201     1       False   2019-08-19 14:41:43.000000      N/A     Disabled
4084    1944    DumpIt.exe      0xfa800156e400  5       46      1       True    2019-08-19 14:41:55.000000      N/A     Disabled
4092    396     conhost.exe     0xfa80014c1060  2       50      1       False   2019-08-19 14:41:55.000000      N/A     Disabled
1224    480     sppsvc.exe      0xfa80014aa060  5       0       0       False   2019-08-19 14:42:39.000000      N/A     Disabled
2256    2396    GoogleUpdate.e  0xfa800157eb30  3       118     0       True    2019-08-19 14:42:40.000000      N/A     Disabled
1192    2256    GoogleCrashHan  0xfa80014f9060  3       46      0       True    2019-08-19 14:42:41.000000      N/A     Disabled
864     2256    GoogleCrashHan  0xfa80035e3700  1       1279459345      0False  2019-08-19 14:42:41.000000      N/A     Disabled

┌──(student123㉿kali)-[~/volatility3]
└─$ 
```

This cmd stores the output of the cmd in a file: python3 vol.py -f <filename.raw> windows.pslist > output.txt

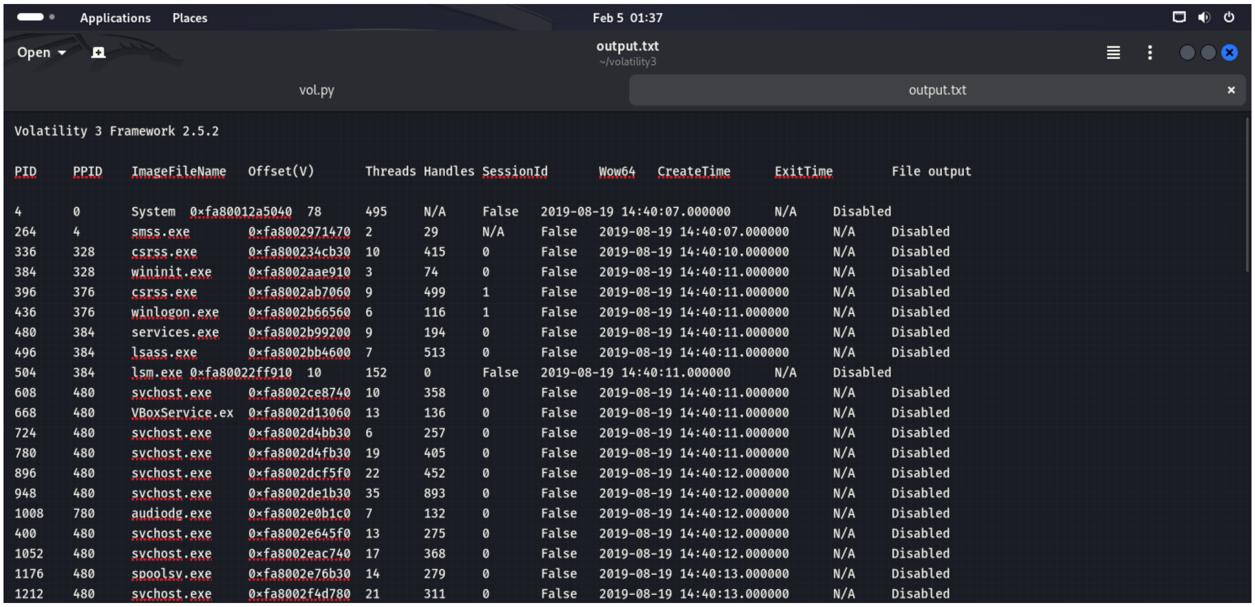


```
└─$ python3 vol.py -f /home/student123/Downloads/Challenge_NotchItUp/Challenge.raw windows.pslist > output.txt

┌──(student123㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/student123/Downloads/Challenge_NotchItUp/Challenge.raw windows.pstree
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0xfa80012a5040  78      495     N/A     False   2019-08-19 14:40:07.000000      N/A
* 264   4       smss.exe        0xfa8002971470  2       29      N/A     False   2019-08-19 14:40:07.000000      N/A
336     328     csrss.exe       0xfa800234cb30  10      415     0       False   2019-08-19 14:40:10.000000      N/A
384     328     wininit.exe     0xfa8002aae910  3       74      0       False   2019-08-19 14:40:11.000000      N/A
* 480   384     services.exe    0xfa8002b99200  9       194     0       False   2019-08-19 14:40:11.000000      N/A
** 608  480     svchost.exe     0xfa8002ce8740  10      358     0       False   2019-08-19 14:40:11.000000      N/A
*** 2896        608     WmiPrvSE.exe    0xfa8002d9eab0  7       124     0       False   2019-08-19 14:40:57.000000      N/A
*** 2292        608     WmiPrvSE.exe    0xfa80032d9060  13      288     0       False   2019-08-19 14:40:52.000000      N/A
```



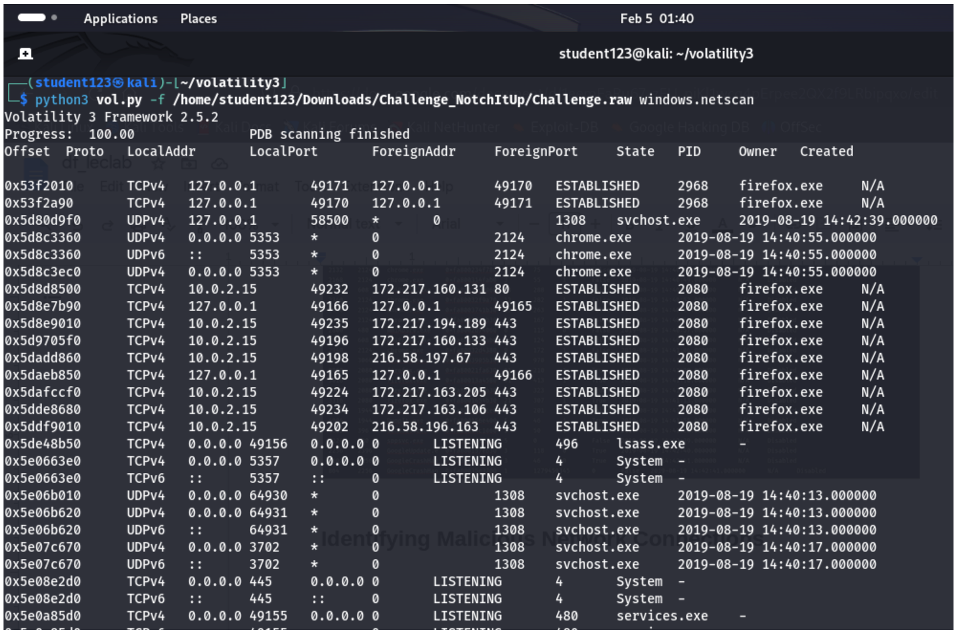
```
** 2940 2124    chrome.exe      0xfa80032d4380  9       172     1       False   2019-08-19 14:41:06.000000      N/A
* 880   1944    cmd.exe 0xfa8002324b30  1       21      1       False   2019-08-19 14:40:26.000000      N/A
* 1108  1944    VBoxTray.exe    0xfa8003277810  14      139     1       False   2019-08-19 14:40:20.000000      N/A
* 4084  1944    DumpIt.exe      0xfa800156e400  5       46      1       True    2019-08-19 14:41:55.000000      N/A
1292    1928    GoogleCrashHan  0xfa8003227060  7       105     0       True    2019-08-19 14:40:19.000000      N/A
924     1928    GoogleCrashHan  0xfa8003219060  6       93      0       False   2019-08-19 14:40:19.000000      N/A
2080    3060    firefox.exe     0xfa8003905b30  59      970     1       True    2019-08-19 14:41:08.000000      N/A
* 3016  2080    firefox.exe     0xfa80013a4580  31      413     1       True    2019-08-19 14:41:10.000000      N/A
* 3316  2080    firefox.exe     0xfa8001454b30  21      307     1       True    2019-08-19 14:41:13.000000      N/A
* 2860  2080    firefox.exe     0xfa80021fa630  11      210     1       True    2019-08-19 14:41:09.000000      N/A
* 2968  2080    firefox.exe     0xfa8001415b30  22      323     1       True    2019-08-19 14:41:11.000000      N/A
2256    2396    GoogleUpdate.e  0xfa800157eb30  3       118     0       True    2019-08-19 14:42:40.000000      N/A
* 1192  2256    GoogleCrashHan  0xfa80014f9060  3       46      0       True    2019-08-19 14:42:41.000000      N/A
* 864   2256    GoogleCrashHan  0xfa80035e3700  1       1279459345      0       False   2019-08-19 14:42:41.000000      N/A

┌──(student123㉿kali)-[~/volatility3]
└─$ 
```

Open the file which stores the output:



```
Volatility 3 Framework 2.5.2

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

4       0       System  0xfa80012a5040  78      495     N/A     False   2019-08-19 14:40:07.000000      N/A     Disabled
264     4       smss.exe        0xfa8002971470  2       29      N/A     False   2019-08-19 14:40:07.000000      N/A     Disabled
336     328     csrss.exe       0xfa800234cb30  10      415     0       False   2019-08-19 14:40:10.000000      N/A     Disabled
384     328     wininit.exe     0xfa8002aae910  3       74      0       False   2019-08-19 14:40:11.000000      N/A     Disabled
396     376     csrss.exe       0xfa8002ab7060  9       499     1       False   2019-08-19 14:40:11.000000      N/A     Disabled
436     376     winlogon.exe    0xfa8002b66560  6       116     1       False   2019-08-19 14:40:11.000000      N/A     Disabled
480     384     services.exe    0xfa8002b99200  9       194     0       False   2019-08-19 14:40:11.000000      N/A     Disabled
496     384     lsass.exe       0xfa8002bb4600  7       513     0       False   2019-08-19 14:40:11.000000      N/A     Disabled
504     384     lsm.exe 0xfa80022ff910  10      152     0       False   2019-08-19 14:40:11.000000      N/A     Disabled
608     480     svchost.exe     0xfa8002ce8740  10      358     0       False   2019-08-19 14:40:11.000000      N/A     Disabled
668     480     VBoxService.ex  0xfa8002d13060  13      136     0       False   2019-08-19 14:40:11.000000      N/A     Disabled
724     480     svchost.exe     0xfa8002d4bb30  6       257     0       False   2019-08-19 14:40:11.000000      N/A     Disabled
780     480     svchost.exe     0xfa8002d4fb30  19      405     0       False   2019-08-19 14:40:11.000000      N/A     Disabled
896     480     svchost.exe     0xfa8002dcf5f0  22      452     0       False   2019-08-19 14:40:12.000000      N/A     Disabled
948     480     svchost.exe     0xfa8002de1b30  35      893     0       False   2019-08-19 14:40:12.000000      N/A     Disabled
1008    780     audiodg.exe     0xfa8002e0b1c0  7       132     0       False   2019-08-19 14:40:12.000000      N/A     Disabled
400     480     svchost.exe     0xfa8002e645f0  13      275     0       False   2019-08-19 14:40:12.000000      N/A     Disabled
1052    480     svchost.exe     0xfa8002eac740  17      368     0       False   2019-08-19 14:40:12.000000      N/A     Disabled
1176    480     spoolsv.exe     0xfa8002e76b30  14      279     0       False   2019-08-19 14:40:13.000000      N/A     Disabled
1212    480     svchost.exe     0xfa8002f4d780  21      311     0       False   2019-08-19 14:40:13.000000      N/A     Disabled
```

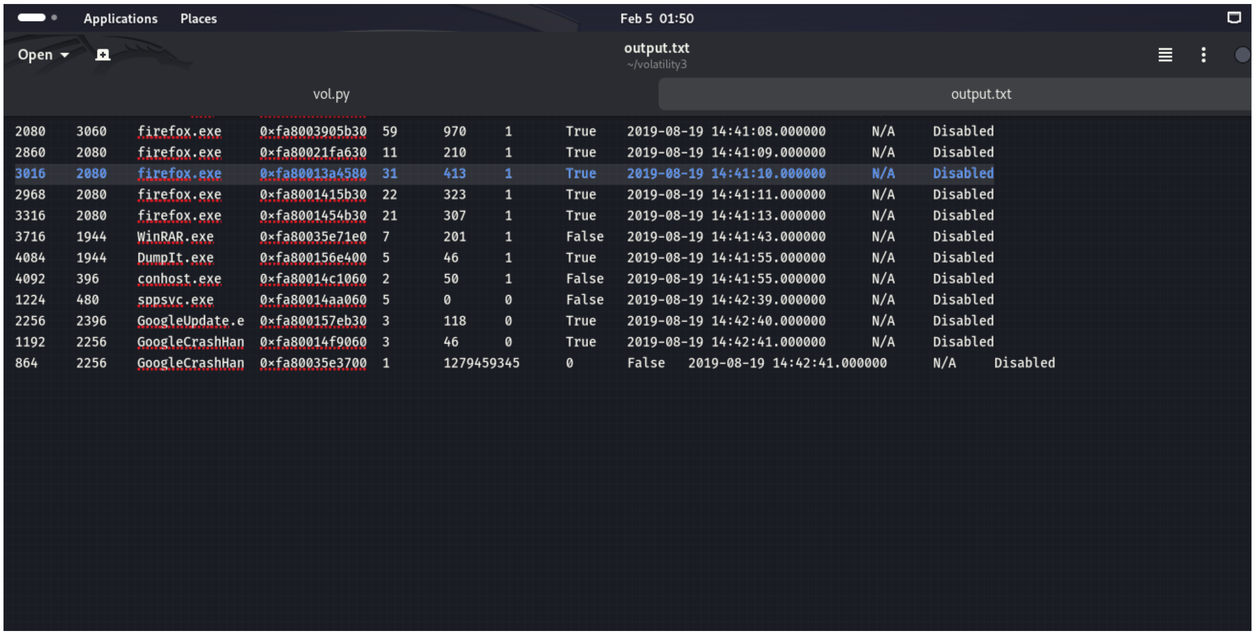
Identifying Malicious Network Connections



```
┌──(student123㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/student123/Downloads/Challenge_NotchItUp/Challenge.raw windows.netscan
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0x53f2010       TCPv4   127.0.0.1       49171   127.0.0.1       49170   ESTABLISHED     2968    firefox.exe     N/A
0x53f2a90       TCPv4   127.0.0.1       49170   127.0.0.1       49171   ESTABLISHED     2968    firefox.exe     N/A
0x5d80d9f0      UDPv4   127.0.0.1       58500   *       0               1308    svchost.exe     2019-08-19 14:42:39.000000
0x5d8c3360      UDPv4   0.0.0.0 5353    *       0               2124    chrome.exe      2019-08-19 14:40:55.000000
0x5d8c3360      UDPv6   ::      5353    *       0               2124    chrome.exe      2019-08-19 14:40:55.000000
0x5d8c3ec0      UDPv4   0.0.0.0 5353    *       0               2124    chrome.exe      2019-08-19 14:40:55.000000
0x5d8d8500      TCPv4   10.0.2.15       49232   172.217.160.131 80      ESTABLISHED     2080    firefox.exe     N/A
0x5d8e7b90      TCPv4   127.0.0.1       49166   127.0.0.1       49165   ESTABLISHED     2080    firefox.exe     N/A
0x5d8e9010      TCPv4   10.0.2.15       49235   172.217.194.189 443     ESTABLISHED     2080    firefox.exe     N/A
0x5d9705f0      TCPv4   10.0.2.15       49196   172.217.160.133 443     ESTABLISHED     2080    firefox.exe     N/A
0x5dadd860      TCPv4   10.0.2.15       49198   216.58.197.67   443     ESTABLISHED     2080    firefox.exe     N/A
0x5daeb850      TCPv4   127.0.0.1       49165   127.0.0.1       49166   ESTABLISHED     2080    firefox.exe     N/A
0x5dafccf0      TCPv4   10.0.2.15       49224   172.217.163.205 443     ESTABLISHED     2080    firefox.exe     N/A
0x5dde8680      TCPv4   10.0.2.15       49234   172.217.163.106 443     ESTABLISHED     2080    firefox.exe     N/A
0x5ddf9010      TCPv4   10.0.2.15       49202   216.58.196.163  443     ESTABLISHED     2080    firefox.exe     N/A
0x5de48b50      TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       496     lsass.exe       -
0x5e0663e0      TCPv4   0.0.0.0 5357    0.0.0.0 0       LISTENING       4       System  -
0x5e0663e0      TCPv6   ::      5357    ::      0       LISTENING       4       System  -
0x5e06b010      UDPv4   0.0.0.0 64930   *       0               1308    svchost.exe     2019-08-19 14:40:13.000000
0x5e06b620      UDPv4   0.0.0.0 64931   *       0               1308    svchost.exe     2019-08-19 14:40:13.000000
0x5e06b620      UDPv6   ::      64931   *       0               1308    svchost.exe     2019-08-19 14:40:13.000000
0x5e07c670      UDPv4   0.0.0.0 3702    *       0               1308    svchost.exe     2019-08-19 14:40:17.000000
0x5e07c670      UDPv6   ::      3702    *       0               1308    svchost.exe     2019-08-19 14:40:17.000000
0x5e08e2d0      TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  -
0x5e08e2d0      TCPv6   ::      445     ::      0       LISTENING       4       System  -
0x5e0a85d0      TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       480     services.exe    -
```

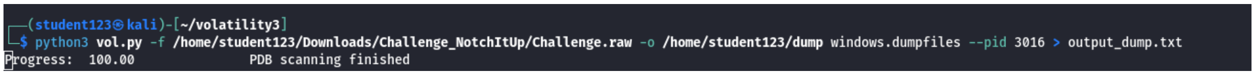
Create a folder dump in home

Select a random pid from here:

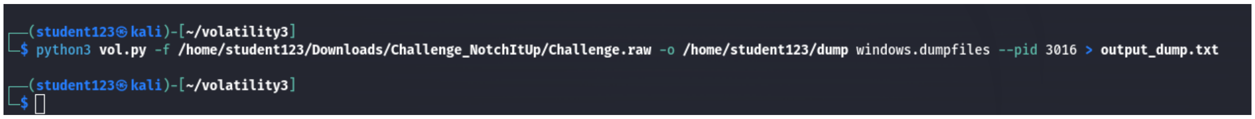


```
2080    3060    firefox.exe     0xfa8003905b30  59      970     1       True    2019-08-19 14:41:08.000000      N/A     Disabled
2860    2080    firefox.exe     0xfa80021fa630  11      210     1       True    2019-08-19 14:41:09.000000      N/A     Disabled
3016    2080    firefox.exe     0xfa80013a4580  31      413     1       True    2019-08-19 14:41:10.000000      N/A     Disabled
2968    2080    firefox.exe     0xfa8001415b30  22      323     1       True    2019-08-19 14:41:11.000000      N/A     Disabled
3316    2080    firefox.exe     0xfa8001454b30  21      307     1       True    2019-08-19 14:41:13.000000      N/A     Disabled
3716    1944    WinRAR.exe      0xfa80035e71e0  7       201     1       False   2019-08-19 14:41:43.000000      N/A     Disabled
4084    1944    DumpIt.exe      0xfa800156e400  5       46      1       True    2019-08-19 14:41:55.000000      N/A     Disabled
4092    396     conhost.exe     0xfa80014c1060  2       50      1       False   2019-08-19 14:41:55.000000      N/A     Disabled
1224    480     sppsvc.exe      0xfa80014aa060  5       0       0       False   2019-08-19 14:42:39.000000      N/A     Disabled
2256    2396    GoogleUpdate.e  0xfa800157eb30  3       118     0       True    2019-08-19 14:42:40.000000      N/A     Disabled
1192    2256    GoogleCrashHan  0xfa80014f9060  3       46      0       True    2019-08-19 14:42:41.000000      N/A     Disabled
864     2256    GoogleCrashHan  0xfa80035e3700  1       1279459345      0       False   2019-08-19 14:42:41.000000      N/A     Disabled
```

Then run:

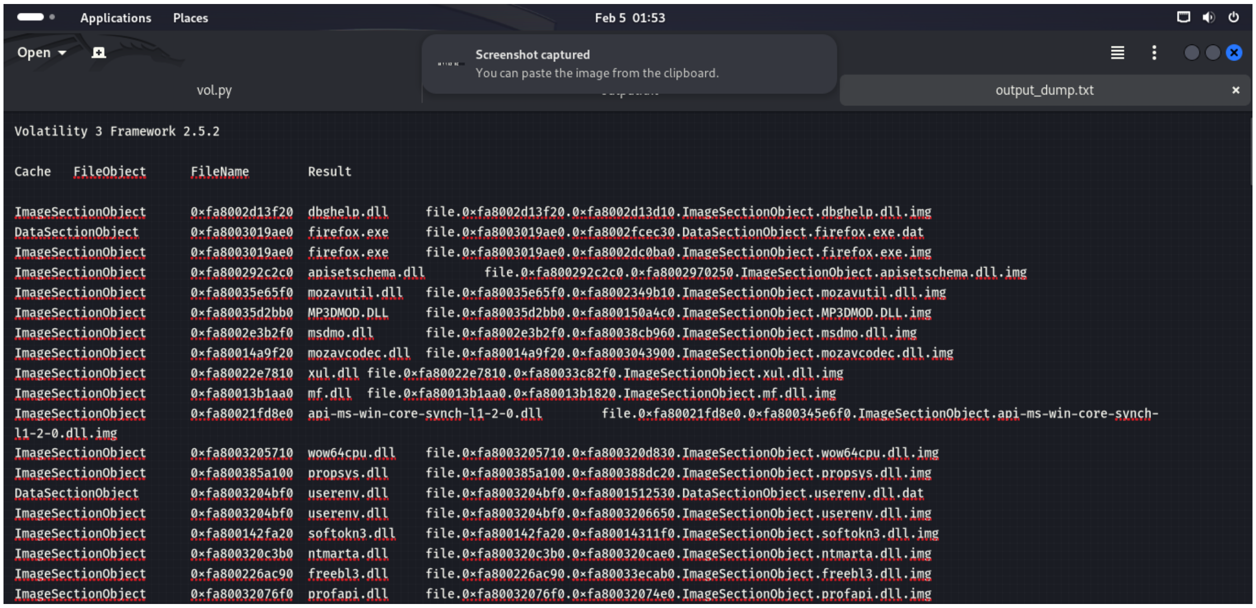


```
┌──(student123㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/student123/Downloads/Challenge_NotchItUp/Challenge.raw -o /home/student123/dump windows.dumpfiles --pid 3016 > output_dump.txt
Progress:  100.00               PDB scanning finished
```



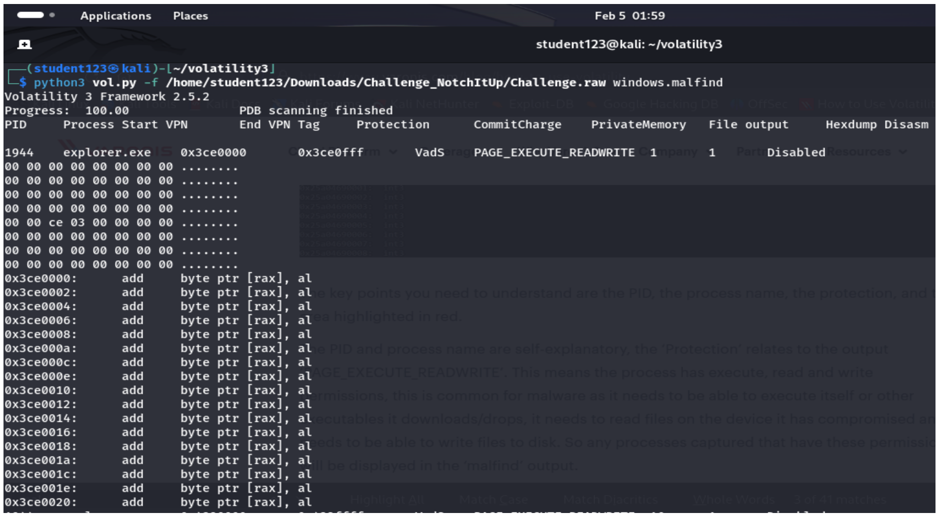
```
┌──(student123㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/student123/Downloads/Challenge_NotchItUp/Challenge.raw -o /home/student123/dump windows.dumpfiles --pid 3016 > output_dump.txt

┌──(student123㉿kali)-[~/volatility3]
└─$ 
```

Output in the dump file:

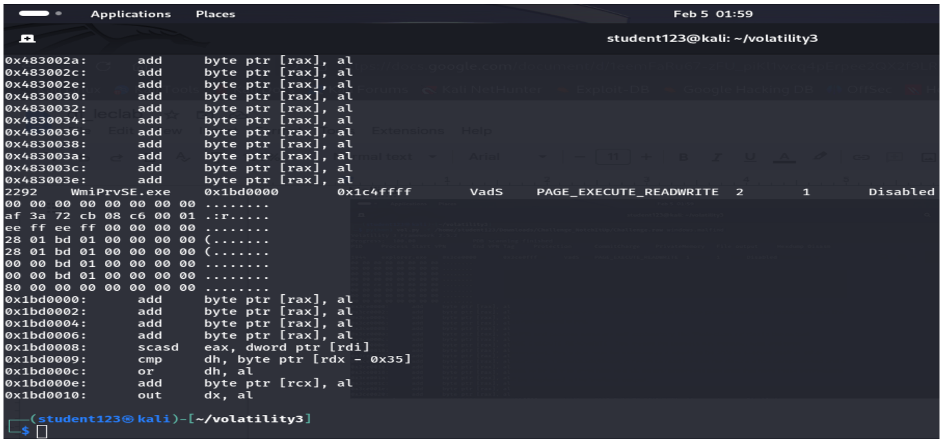


```
Volatility 3 Framework 2.5.2

Cache	FileObject	FileName	Result

ImageSectionObject	0xfa8002d13f20	dbghelp.dll	file.0xfa8002d13f20.0xfa8002d13d10.ImageSectionObject.dbghelp.dll.img
DataSectionObject	0xfa8003019ae0	firefox.exe	file.0xfa8003019ae0.0xfa8002fcec30.DataSectionObject.firefox.exe.dat
ImageSectionObject	0xfa8003019ae0	firefox.exe	file.0xfa8003019ae0.0xfa8002dc0ba0.ImageSectionObject.firefox.exe.img
ImageSectionObject	0xfa800292c2c0	apisetschema.dll	file.0xfa800292c2c0.0xfa8002970250.ImageSectionObject.apisetschema.dll.img
ImageSectionObject	0xfa80035e65f0	mozavutil.dll	file.0xfa80035e65f0.0xfa8002349b10.ImageSectionObject.mozavutil.dll.img
ImageSectionObject	0xfa80035d2bb0	MP3DMOD.DLL	file.0xfa80035d2bb0.0xfa800150a4c0.ImageSectionObject.MP3DMOD.DLL.img
ImageSectionObject	0xfa8002e3b2f0	msdmo.dll	file.0xfa8002e3b2f0.0xfa80038cb960.ImageSectionObject.msdmo.dll.img
ImageSectionObject	0xfa80014a9f20	mozavcodec.dll	file.0xfa80014a9f20.0xfa8003043900.ImageSectionObject.mozavcodec.dll.img
ImageSectionObject	0xfa80022e7810	xul.dll file.0xfa80022e7810.0xfa80033c82f0.ImageSectionObject.xul.dll.img
ImageSectionObject	0xfa80013b1aa0	mf.dll	file.0xfa80013b1aa0.0xfa80013b1820.ImageSectionObject.mf.dll.img
ImageSectionObject	0xfa80021fd8e0	api-ms-win-core-synch-l1-2-0.dll	file.0xfa80021fd8e0.0xfa800345e6f0.ImageSectionObject.api-ms-win-core-synch-
l1-2-0.dll.img
ImageSectionObject	0xfa8003205710	wow64cpu.dll	file.0xfa8003205710.0xfa800320d830.ImageSectionObject.wow64cpu.dll.img
ImageSectionObject	0xfa800385a100	propsys.dll	file.0xfa800385a100.0xfa800388dc20.ImageSectionObject.propsys.dll.img
DataSectionObject	0xfa8003204bf0	userenv.dll	file.0xfa8003204bf0.0xfa8001512530.DataSectionObject.userenv.dll.dat
ImageSectionObject	0xfa8003204bf0	userenv.dll	file.0xfa8003204bf0.0xfa8003206650.ImageSectionObject.userenv.dll.img
ImageSectionObject	0xfa800142fa20	softokn3.dll	file.0xfa800142fa20.0xfa80014311f0.ImageSectionObject.softokn3.dll.img
ImageSectionObject	0xfa800320c3b0	ntmarta.dll	file.0xfa800320c3b0.0xfa800320cae0.ImageSectionObject.ntmarta.dll.img
ImageSectionObject	0xfa800226ac90	freebl3.dll	file.0xfa800226ac90.0xfa80033ecab0.ImageSectionObject.freebl3.dll.img
ImageSectionObject	0xfa80032076f0	profapi.dll	file.0xfa80032076f0.0xfa80032074e0.ImageSectionObject.profapi.dll.img
```

python3 vol.py -f <filename> windows.malfind

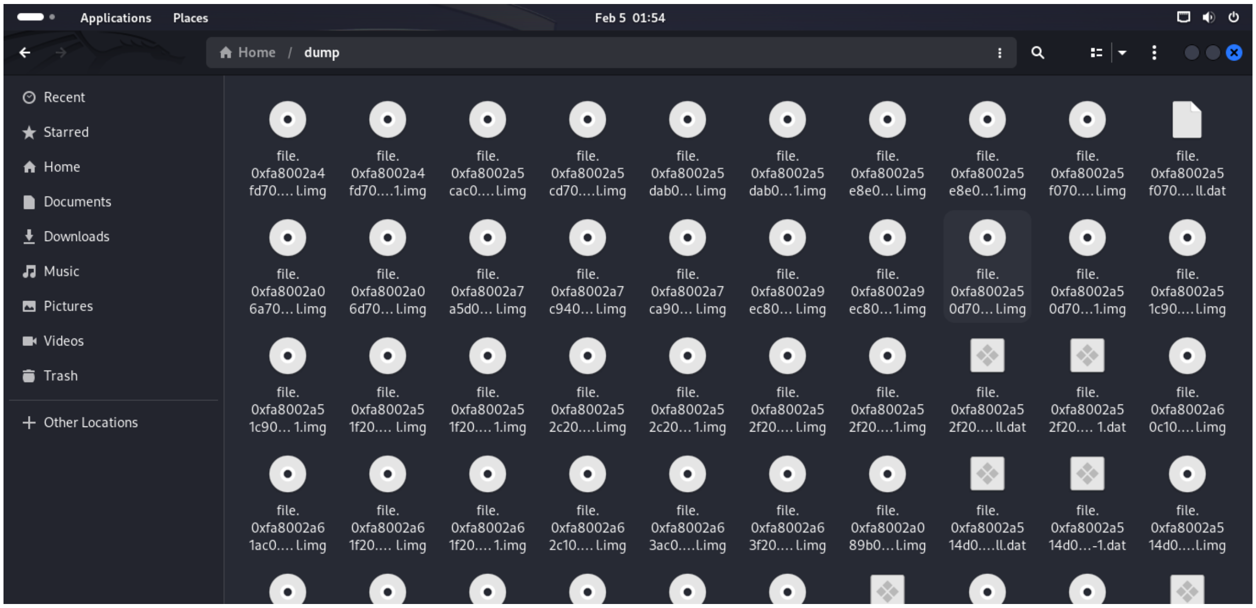


```
┌──(student123㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/student123/Downloads/Challenge_NotchItUp/Challenge.raw windows.malfind
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Hexdump Disasm

1944    explorer.exe    0x3ce0000       0x3ce0fff       VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 ce 03 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
0x3ce0000:      add     byte ptr [rax], al
0x3ce0002:      add     byte ptr [rax], al
0x3ce0004:      add     byte ptr [rax], al
0x3ce0006:      add     byte ptr [rax], al
0x3ce0008:      add     byte ptr [rax], al
0x3ce000a:      add     byte ptr [rax], al
0x3ce000c:      add     byte ptr [rax], al
0x3ce000e:      add     byte ptr [rax], al
0x3ce0010:      add     byte ptr [rax], al
0x3ce0012:      add     byte ptr [rax], al
0x3ce0014:      add     byte ptr [rax], al
0x3ce0016:      add     byte ptr [rax], al
0x3ce0018:      add     byte ptr [rax], al
0x3ce001a:      add     byte ptr [rax], al
0x3ce001c:      add     byte ptr [rax], al
0x3ce001e:      add     byte ptr [rax], al
0x3ce0020:      add     byte ptr [rax], al
```



```
0x483002a:      add     byte ptr [rax], al
0x483002c:      add     byte ptr [rax], al
0x483002e:      add     byte ptr [rax], al
0x4830030:      add     byte ptr [rax], al
0x4830032:      add     byte ptr [rax], al
0x4830034:      add     byte ptr [rax], al
0x4830036:      add     byte ptr [rax], al
0x4830038:      add     byte ptr [rax], al
0x483003a:      add     byte ptr [rax], al
0x483003c:      add     byte ptr [rax], al
0x483003e:      add     byte ptr [rax], al
2292    WmiPrvSE.exe    0x1bd0000       0x1c4ffff       VadS    PAGE_EXECUTE_READWRITE  2       1       Disabled
00 00 00 00 00 00 00 00 ........
af 3a 72 cb 08 c6 00 01 .:r.....
ee ff ee ff 00 00 00 00 ........
28 01 bd 01 00 00 00 00 (.......
28 01 bd 01 00 00 00 00 (.......
00 00 bd 01 00 00 00 00 ........
00 00 bd 01 00 00 00 00 ........
80 00 00 00 00 00 00 00 ........
0x1bd0000:      add     byte ptr [rax], al
0x1bd0002:      add     byte ptr [rax], al
0x1bd0004:      add     byte ptr [rax], al
0x1bd0006:      add     byte ptr [rax], al
0x1bd0008:      scasd   eax, dword ptr [rdi]
0x1bd0009:      cmp     dh, byte ptr [rdx - 0x35]
0x1bd000c:      or      dh, al
0x1bd000e:      add     byte ptr [rcx], al
0x1bd0010:      out     dx, al

┌──(student123㉿kali)-[~/volatility3]
└─$ 
```

Inside that dump folder:



```
file.0xfa8002a4fd70....l.img
file.0xfa8002a4fd70....1.img
file.0xfa8002a5cac0....l.img
file.0xfa8002a5cd70....l.img
file.0xfa8002a5dab0... l.img
file.0xfa8002a5dab0...1.img
file.0xfa8002a5e8e0... l.img
file.0xfa8002a5e8e0...1.img
file.0xfa8002a5f070....l.img
file.0xfa8002a5f070....ll.dat
file.0xfa8002a06a70... l.img
file.0xfa8002a06d70... l.img
file.0xfa8002a7a5d0... l.img
file.0xfa8002a7c940... l.img
file.0xfa8002a7ca90... l.img
file.0xfa8002a9ec80... l.img
file.0xfa8002a9ec80...1.img
file.0xfa8002a50d70... l.img
file.0xfa8002a50d70...1.img
file.0xfa8002a51c90....l.img
file.0xfa8002a51c90... 1.img
file.0xfa8002a51f20.... l.img
file.0xfa8002a51f20.... 1.img
file.0xfa8002a52c20....l.img
file.0xfa8002a52c20... 1.img
file.0xfa8002a52f20.... l.img
file.0xfa8002a52f20....1.img
file.0xfa8002a52f20.... ll.dat
file.0xfa8002a52f20.... 1.dat
file.0xfa8002a60c10....l.img
file.0xfa8002a61ac0....l.img
file.0xfa8002a61f20.... l.img
file.0xfa8002a61f20.... 1.img
file.0xfa8002a62c10.... l.img
file.0xfa8002a63ac0....l.img
file.0xfa8002a63f20.... l.img
file.0xfa8002a089b0...l.img
file.0xfa8002a514d0....ll.dat
file.0xfa8002a514d0...-1.dat
file.0xfa8002a514d0....l.img
```

CONCLUSION:

____

____

____

____.