Digital Forensics Experiments Report

Exp. 1

DD Command is one of the most basic and traditional command used to make a bit by bit copy of the drive/image.

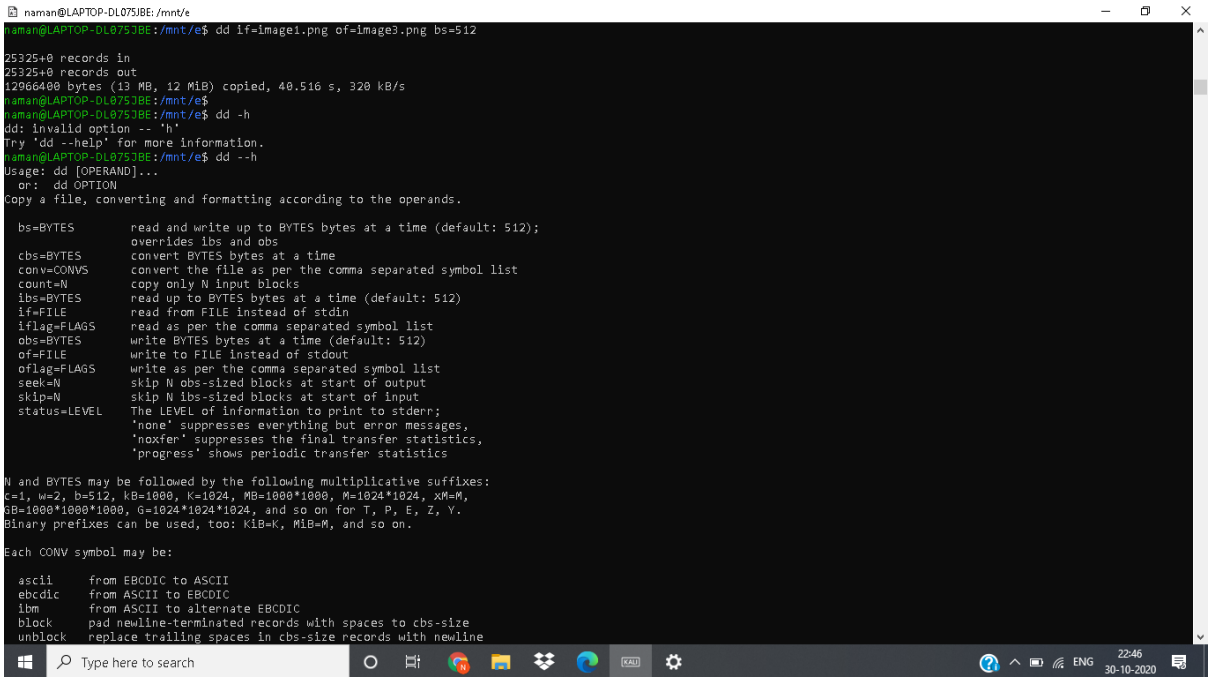
We can mention the input file and the output file for copying the image.

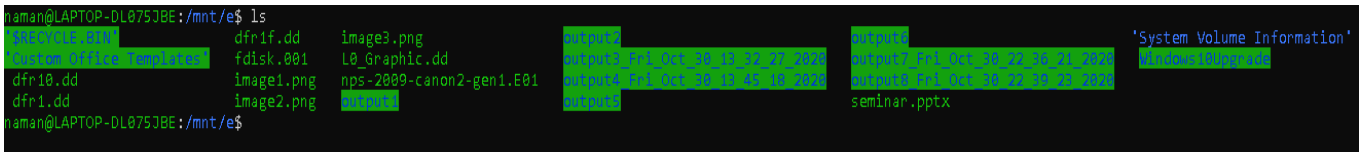
dd if = /media/naman/h of = /mnt/f bs = 512

dd if = /mnt/f/image1.png of = /mnt/f/image2.png bs = 512

dd command can also be used for copying files.

Here bs = block size i.e. the amount of bytes it copies each time until all blocks all copied.





Exp. 2

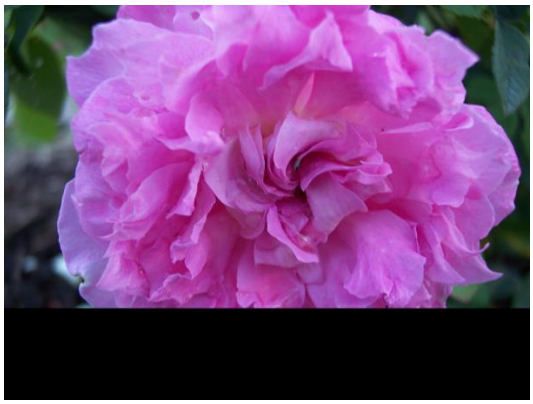
DD Command for Data Carving.

DD can be used for data carving also. All we need to do is to specify a skip & count offset to tell it to start from the position we want to carve the data and how much to carve.

```
naman@LAPTOP-DL075JBE: /mnt/e
  count_bytes  treat 'count=N' as a byte count (iflag only)
  skip_bytes  treat 'skip=N' as a byte count (iflag only)
  seek_bytes  treat 'seek=N' as a byte count (oflag only)

Sending a USR1 signal to a running 'dd' process makes it
print I/O statistics to standard error and then resume copying.

Options are:

      --help     display this help and exit
      --version  output version information and exit

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation <https://www.gnu.org/software/coreutils/dd>
or available locally via: info '(coreutils) dd invocation'
naman@LAPTOP-DL075JBE:/mnt/e$ dd if=L0_Graphic.dd of=image1.png bs=512 skip=10000 count=25325
25325+0 records in
25325+0 records out
12966400 bytes (13 MB, 12 MiB) copied, 34.1163 s, 380 kB/s
naman@LAPTOP-DL075JBE:/mnt/e$ dd if=L0_Graphic.dd of=image2.png bs=512 skip=10000 count=20000
20000+0 records in
20000+0 records out
10240000 bytes (10 MB, 9.8 MiB) copied, 30.3863 s, 337 kB/s
naman@LAPTOP-DL075JBE:/mnt/e$ ls
'$RECYCLE.BIN'              fdisk.001                 output1                          seminar.pptx
'Custom Office Templates'   image1.png                output2                         'System Volume Information'
 dfr10.dd                   image2.png                output3_Fri_Oct_30_13_32_27_202   Windows10Upgrade
 dfr1.dd                    L0_Graphic.dd             output4_Fri_Oct_30_13_45_10_2020
 dfr1f.dd                   nps-2009-canon2-gen1.E01  output5
naman@LAPTOP-DL075JBE:/mnt/e$
```

$ dd if = L0_Graphic.dd of = image2.png bs = 512 count = 25325

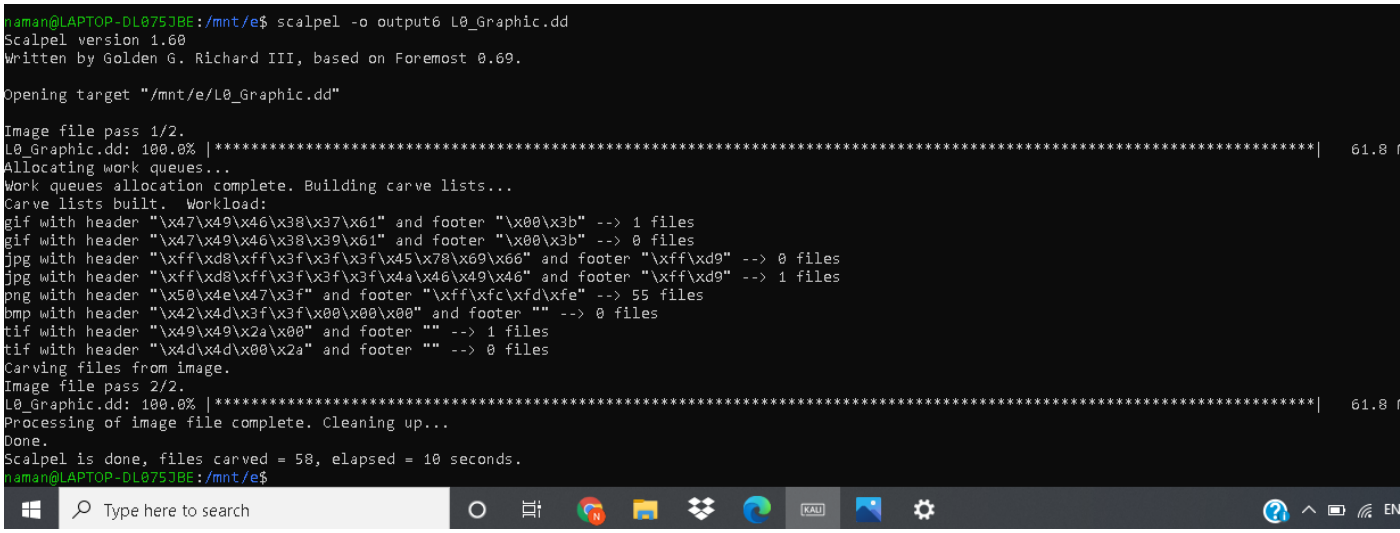
$ dd if = L0_Graphic.dd of = image2.png bs = 512 count = 20000

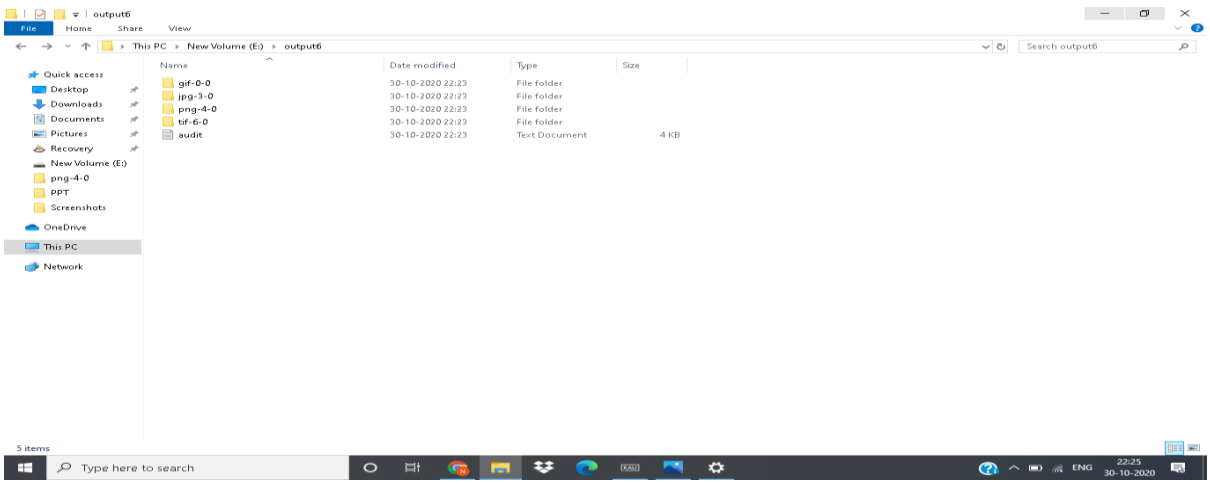


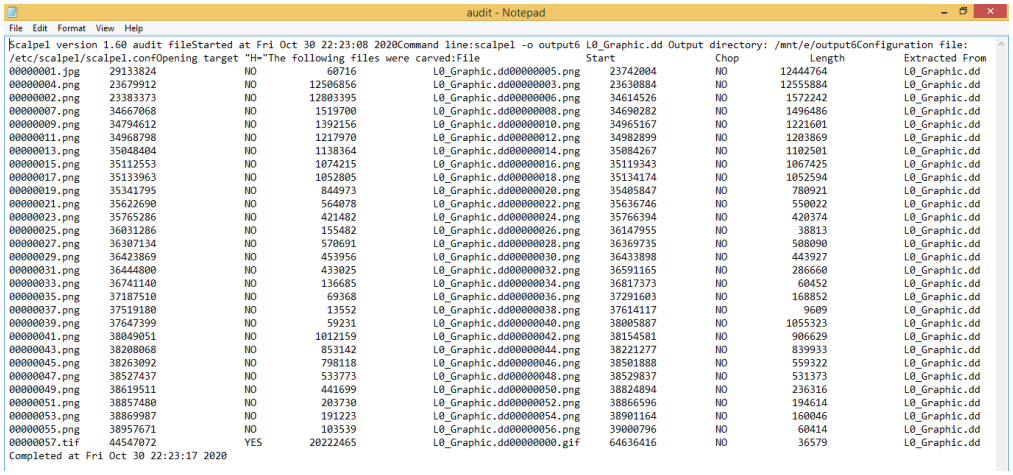
Exp. 3

Scalpel is an open-source tool used for data carving. It has a config file which contains all the predefined headers which we need to uncomment in order to carve files of those formats.

1. Sudo apt-get install scalpel.
2. Nano /etc/scalpel/scalpel.config > Uncomment #jpg,#tif,#gif,#png
3. Scalpel -o output6 L0_Graphic.dd
   (-o offset specifies the output file)





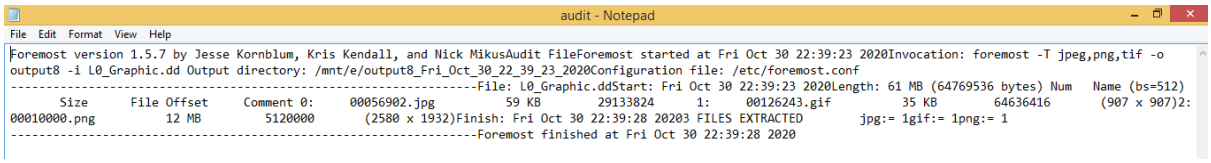


Foremost :

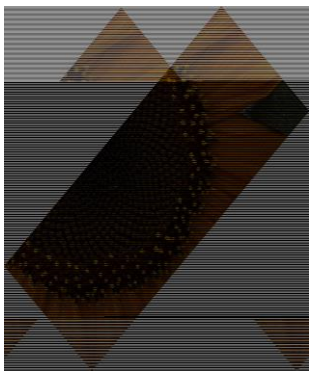
It's also an open source tool for file carving like scalpel. It differs in it's output file an execution command offset.

$ foremost –T jpeg,png,tif -o output8 -i L_0Graphic.dd

```
naman@LAPTOP-DL075JBE:/mnt/e$ foremost -h
foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w-d] [-t <type>] [-s <blocks>] [-k <size>]
        [-b <size>] [-c <file>] [-o <dir>] [-i <file]

-V  - display copyright information and exit
-t  - specify file type.  (-t jpeg,pdf ...)
-d  - turn on indirect block detection (for UNIX file-systems)
-i  - specify input file (default is stdin)
-a  - Write all headers, perform no error detection (corrupted files)
-w  - Only write the audit file, do not write any detected files to the disk
-o  - set output directory (defaults to output)
-c  - set configuration file to use (defaults to foremost.conf)
-q  - enables quick mode. Search are performed on 512 byte boundaries.
-Q  - enables quiet mode. Suppress output messages.
-v  - verbose mode. Logs all messages to screen
naman@LAPTOP-DL075JBE:/mnt/e$ foremost -T jpeg,png,tif -o output7 -i nps-2009-canon2-gen1.E01
Processing: nps-2009-canon2-gen1.E01
|*|
naman@LAPTOP-DL075JBE:/mnt/e$ ls
 $RECYCLE.BIN                dfr1f.dd     L0_Graphic.dd              output3_Fri_Oct_30_13_32_27_2020   output7_Fri_Oct_30_22_38_21_2020
'Custom Office Templates'    fdisk.001    nps-2009-canon2-gen1.E01   output4_Fri_Oct_30_13_45_10_2020   seminar.pptx
 dfr10.dd                    image1.png   output1                    output5                            'System Volume Information'
 dfr1.dd                     image2.png   output2                    output6                            Windows10Upgrade
naman@LAPTOP-DL075JBE:/mnt/e$ foremost -T jpeg,png,tif -o output8 -i L0_Graphic.dd
Processing: L0_Graphic.dd
|*|
naman@LAPTOP-DL075JBE:/mnt/e$
```



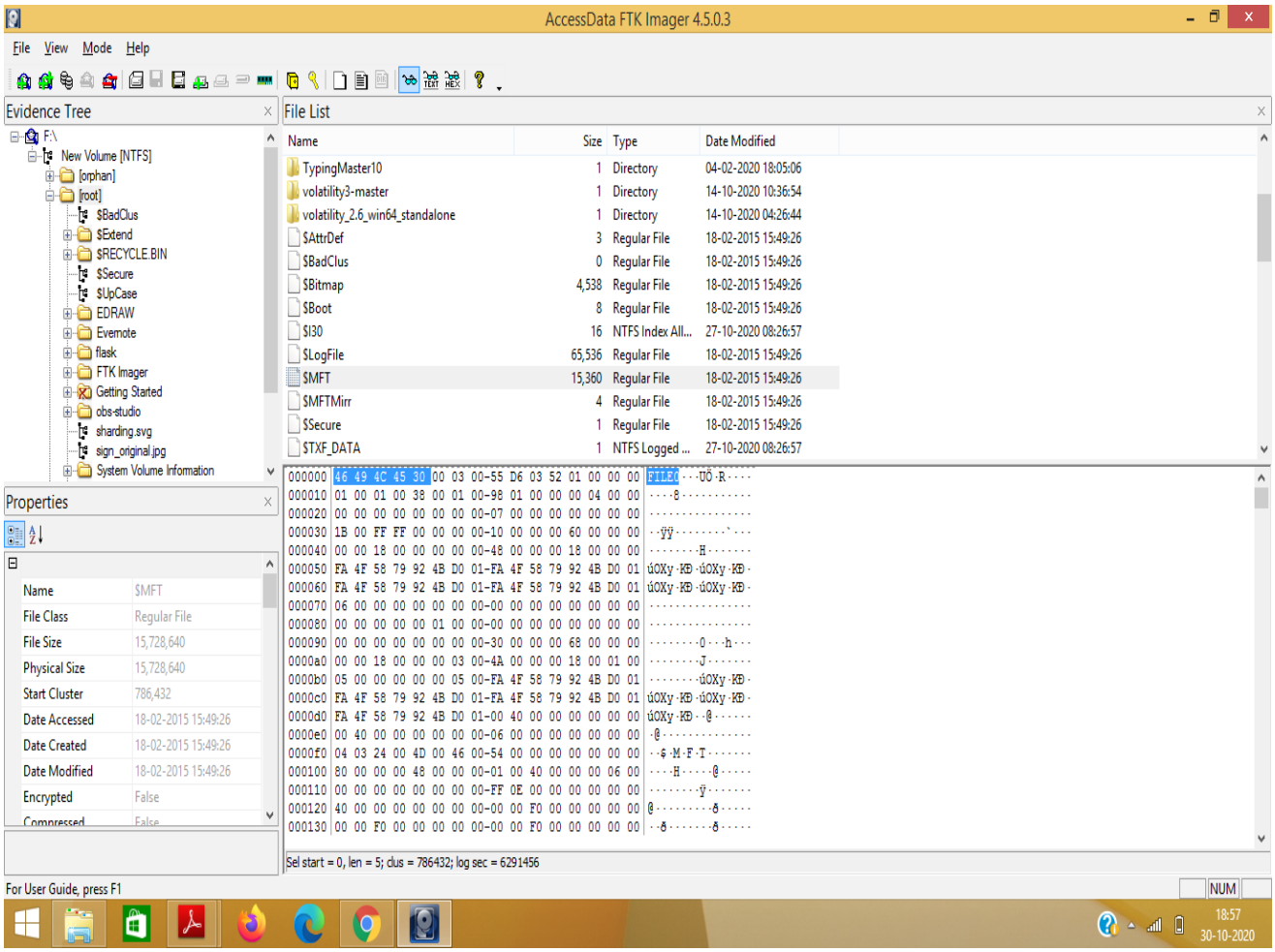
Outputs of Both :

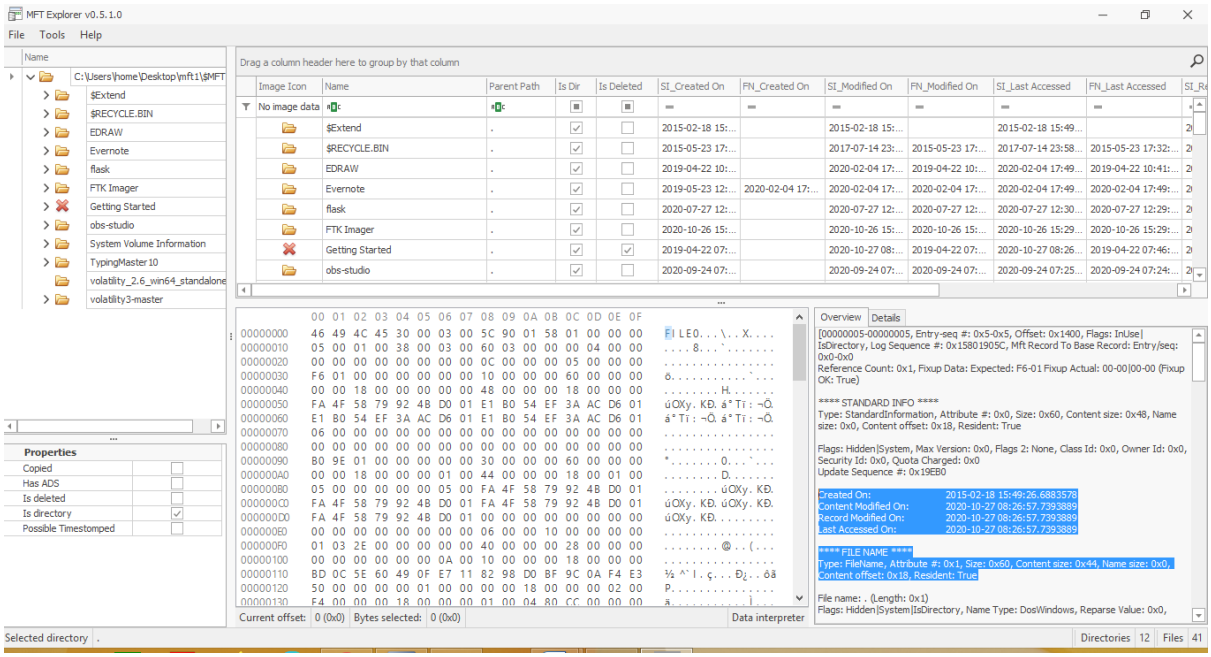


Exp. - 4 FTK Imager tool is used for forensic investigation. Using this we can extract file artifacts of different drives/images etc.

The MFT Table is an important part of NTFS file system and contains the entry of each and every file on the drive which is crucial for any digital investigation. Each entry contains important attributes of the file like type, size, date/time of creation, date/time of most recent modification etc. are stored in MFT.

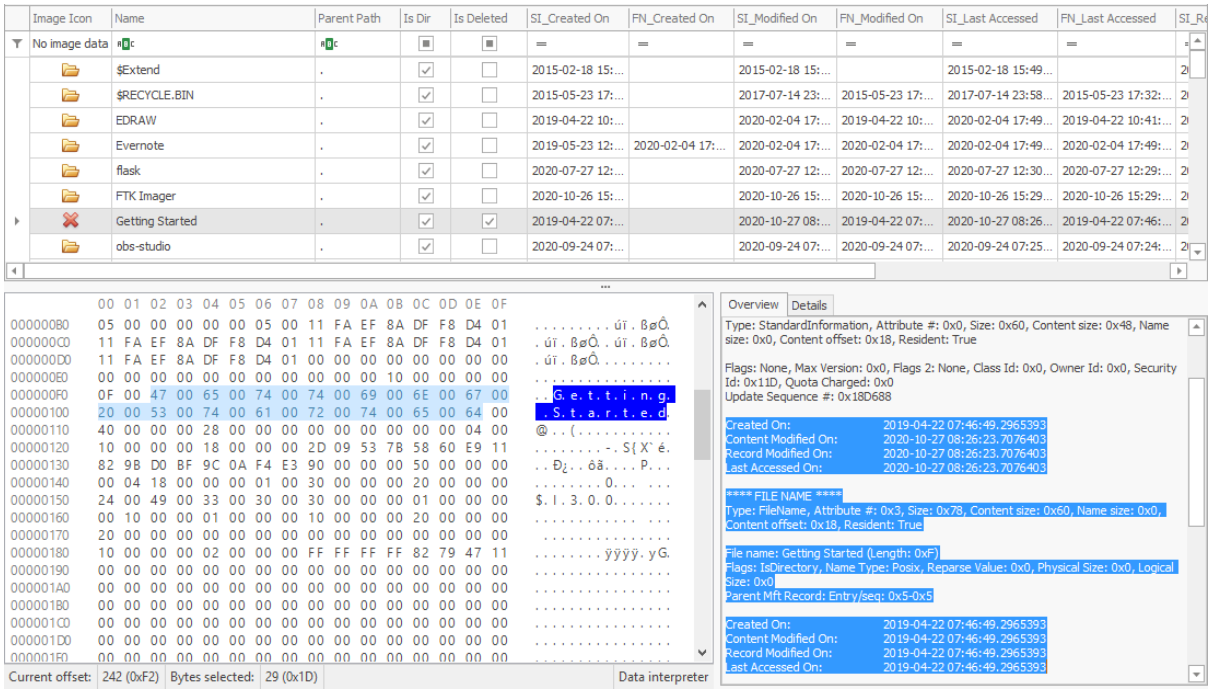
a. Open FTK Imager.
b. Add Evidence Item.
c. Select Logical Drive F:\
d. Select root>MFT
e. This shows the MFT Table in Hex Format.
f. Different File Attrbutes like Last Access Time, Size, Name etc. can be extracted from the is table for all the files.
g. They can be then interpreted in a HxD Editor or a dedicated tool like MFT Explorer can be used.
h. FILe0 denotes the start of each new entry in MFT
i. The first entry in MFT is the MFT Table itself.





In the MFT file, We can see entries of all the files in F:/ drive even the deleted ones.(above image)

Now we analyse a deleted folder named “Getting Started” which contained some videos. We can see it’s entry in the MFT although it’s deleted. We can extract information/metadata about it.

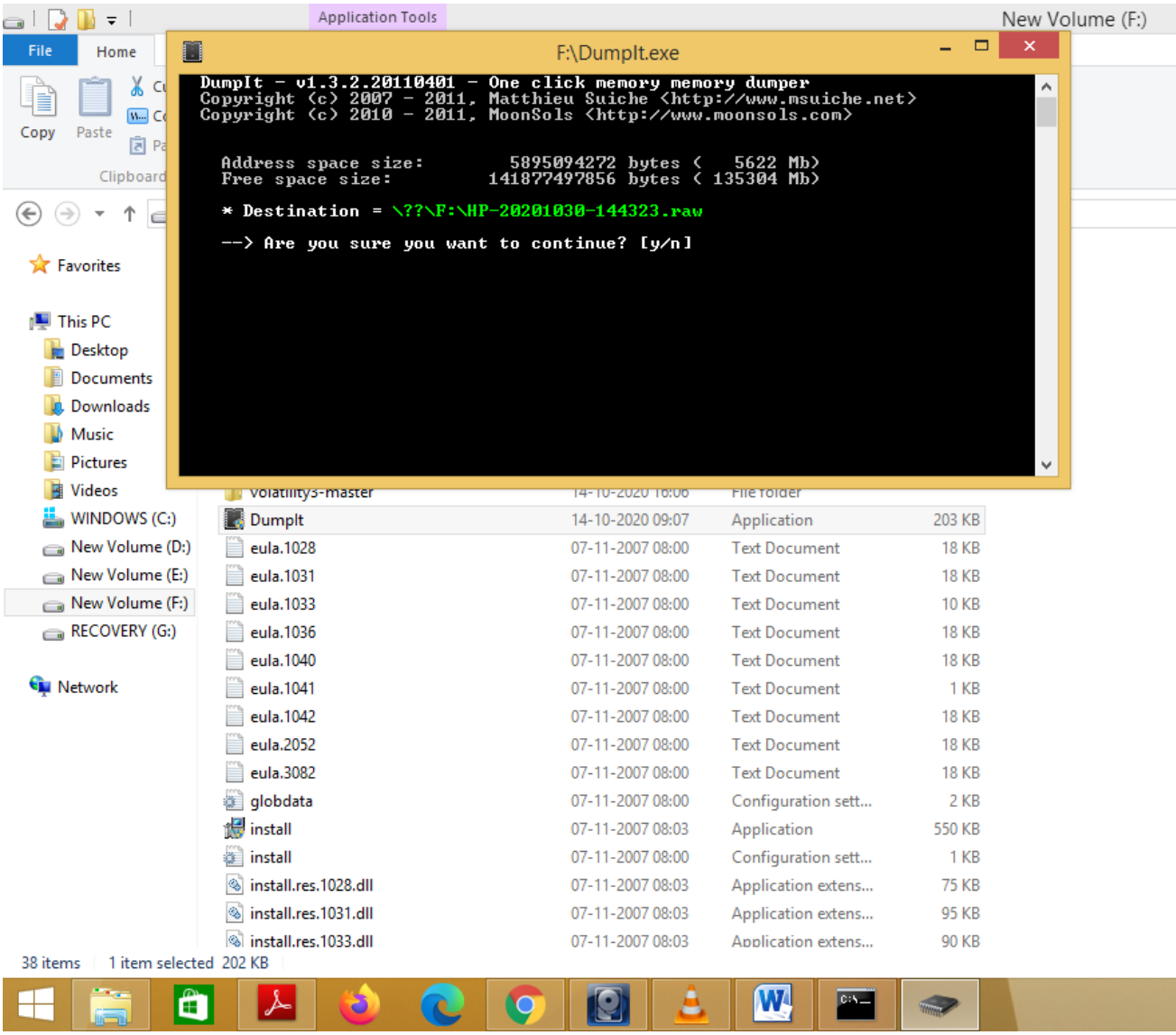


We clearly see that the entries in **SI attribute(0x10)** have changed but the entries in **FN attribute(0x30) have not changed** and remain as it is. Also the name of the folder is stored in MFT entry.

Exp. 5 Using DumpIt.exe we capture the RAM image. We can then use it for forensic analysis using Volatility tool.

Dumpit is a free tool which is easy to use.

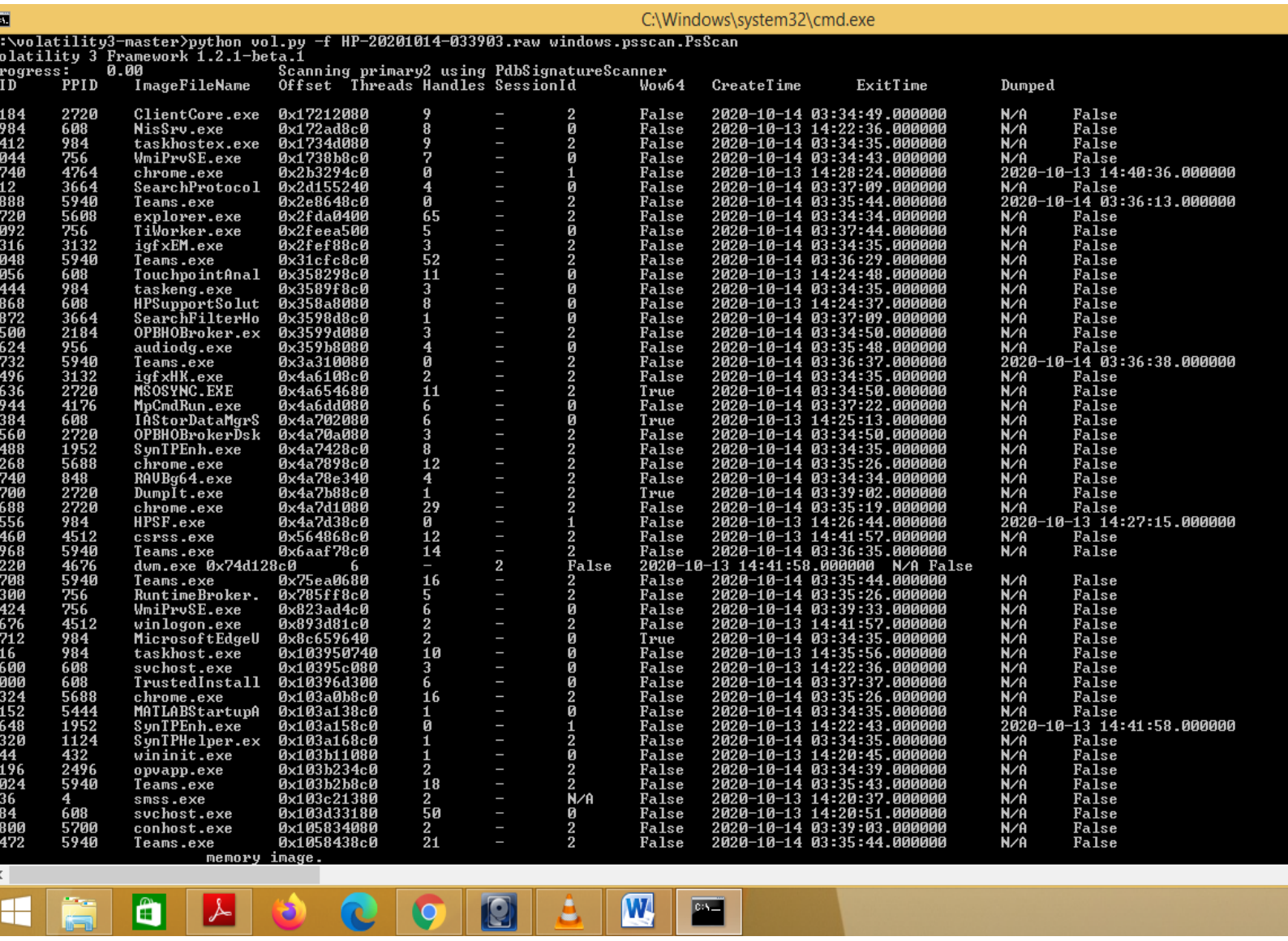
1. Download Dumpit.exe from Github
2. Open Dumpit.exe
3. Check the destination folder.
4. Type y to make the image.



Exp.6 Volatility 3 as it's name suggests is a volatile memory (RAM) Analysis tool. It's written in python. It takes as input the RAM image and has different command to show different details like Basic active process listing, terminated processes scan etc.

The major commands are :

1. Python vol.py –f HP-20201014-033903.raw windows.psscan.PsScan
   This cmd shows Basic active process listing along with scanning for hidden or terminated pr

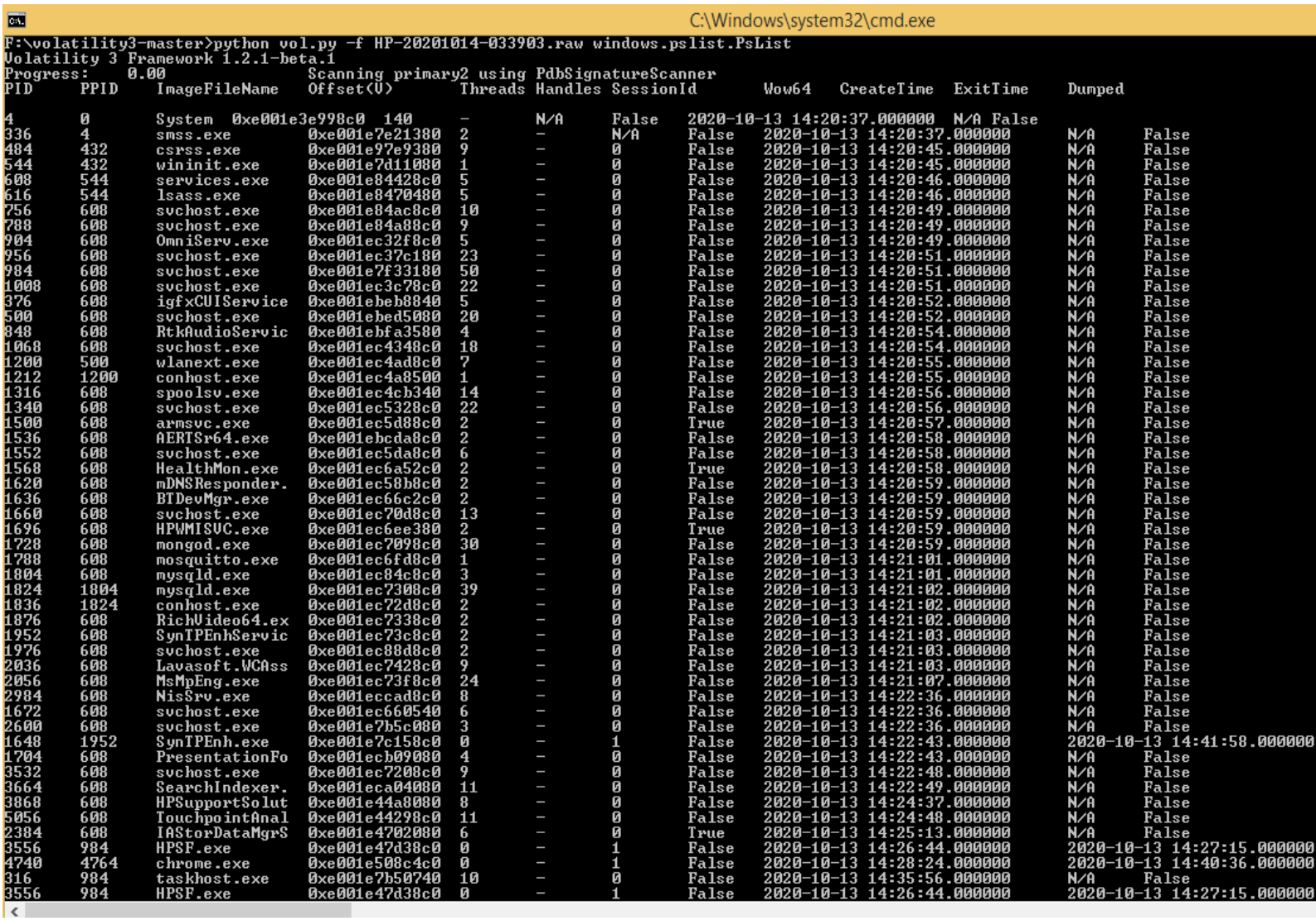


As here we can see, PID = Process ID, PPID = Parent PID, No. of thread by each process, start time, end time, Session Id.

System has PPID = 0, as it's the first process to start.

System has Session ID = N/A because the System starts before sessions are established.

2. Python vol.py –f HP-20201014-033903.raw windows.pslist.PsList
   This shows basic active process listing.

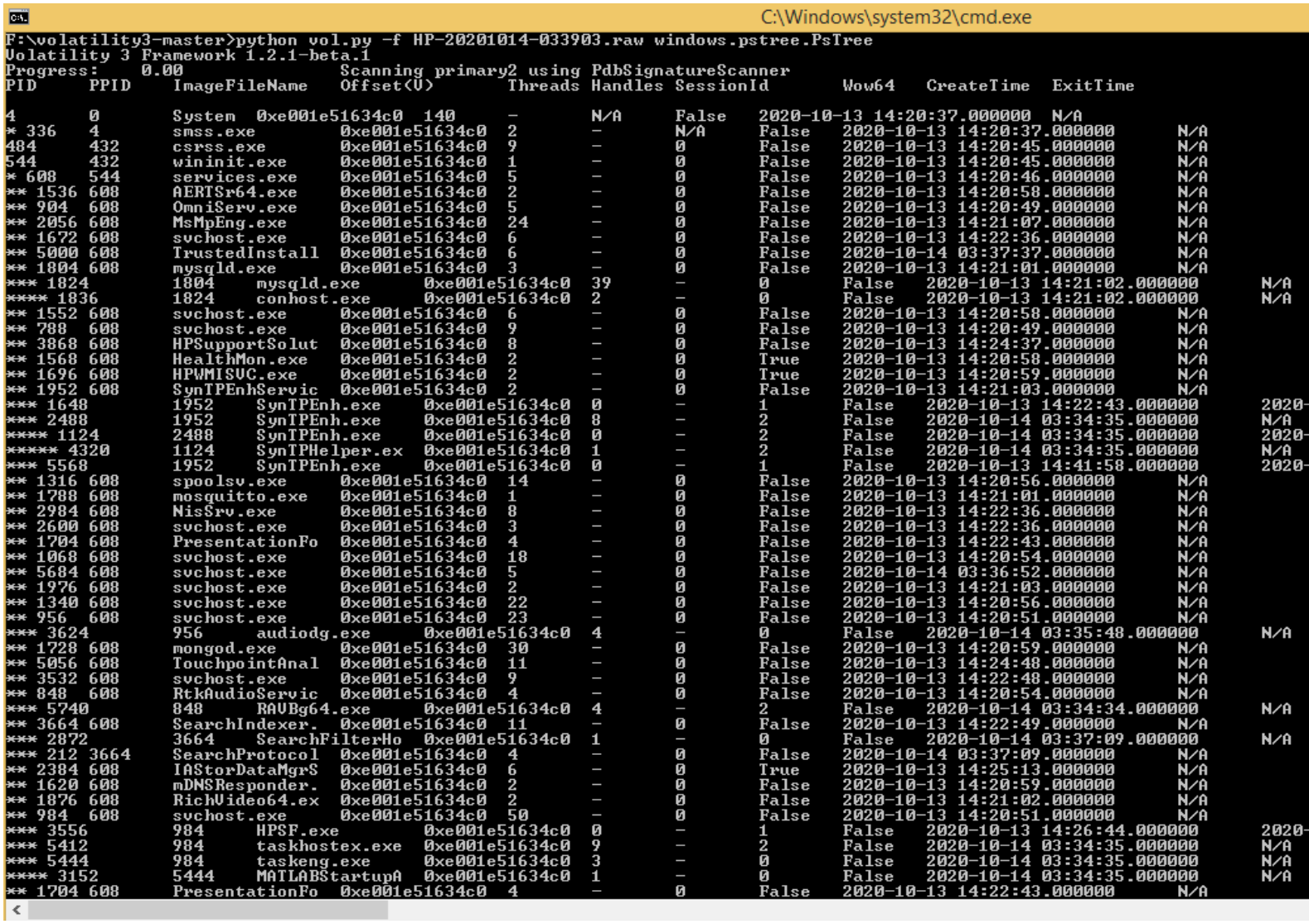


```
C:\Windows\system32\cmd.exe
F:\volatility3-master>python vol.py -f HP-20201014-033903.raw windows.pslist.PsList
Volatility 3 Framework 1.2.1-beta.1
Progress:  0.00         Scanning primary2 using PdbSignatureScanner
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        Dumped

4       0       System  0xe001e3e998c0  140     -       N/A     False   2020-10-13 14:20:37.000000      N/A False
336     4       smss.exe        0xe001e7e21380  2       -       N/A     False   2020-10-13 14:20:37.000000      N/A     False
484     432     csrss.exe       0xe001e97e9380  9       -       0       False   2020-10-13 14:20:45.000000      N/A     False
544     432     wininit.exe     0xe001e7d11080  1       -       0       False   2020-10-13 14:20:45.000000      N/A     False
608     544     services.exe    0xe001e84428c0  5       -       0       False   2020-10-13 14:20:46.000000      N/A     False
616     544     lsass.exe       0xe001e8470480  5       -       0       False   2020-10-13 14:20:46.000000      N/A     False
756     608     svchost.exe     0xe001e84ac8c0  10      -       0       False   2020-10-13 14:20:49.000000      N/A     False
788     608     svchost.exe     0xe001e84a88c0  9       -       0       False   2020-10-13 14:20:49.000000      N/A     False
904     608     OmniServ.exe    0xe001ec32f8c0  5       -       0       False   2020-10-13 14:20:49.000000      N/A     False
956     608     svchost.exe     0xe001ec37c180  23      -       0       False   2020-10-13 14:20:51.000000      N/A     False
984     608     svchost.exe     0xe001e7f33180  50      -       0       False   2020-10-13 14:20:51.000000      N/A     False
1008    608     svchost.exe     0xe001ec3c78c0  22      -       0       False   2020-10-13 14:20:51.000000      N/A     False
376     608     igfxCUIService  0xe001ebeb8840  5       -       0       False   2020-10-13 14:20:52.000000      N/A     False
500     608     svchost.exe     0xe001ebed5080  20      -       0       False   2020-10-13 14:20:52.000000      N/A     False
848     608     RtkAudioServic  0xe001ebfa3580  4       -       0       False   2020-10-13 14:20:54.000000      N/A     False
1068    608     svchost.exe     0xe001ec4348c0  18      -       0       False   2020-10-13 14:20:54.000000      N/A     False
1200    500     wlanext.exe     0xe001ec4ad8c0  7       -       0       False   2020-10-13 14:20:55.000000      N/A     False
1212    1200    conhost.exe     0xe001ec4a8500  1       -       0       False   2020-10-13 14:20:55.000000      N/A     False
1316    608     spoolsv.exe     0xe001ec4cb340  14      -       0       False   2020-10-13 14:20:56.000000      N/A     False
1340    608     svchost.exe     0xe001ec5328c0  22      -       0       False   2020-10-13 14:20:56.000000      N/A     False
1500    608     armsvc.exe      0xe001ec5d88c0  2       -       0       True    2020-10-13 14:20:57.000000      N/A     False
1536    608     AERTSr64.exe    0xe001ebcda8c0  2       -       0       False   2020-10-13 14:20:58.000000      N/A     False
1552    608     svchost.exe     0xe001ec5da8c0  6       -       0       False   2020-10-13 14:20:58.000000      N/A     False
1568    608     HealthMon.exe   0xe001ec6a52c0  2       -       0       True    2020-10-13 14:20:58.000000      N/A     False
1620    608     mDNSResponder.  0xe001ec58b8c0  2       -       0       False   2020-10-13 14:20:59.000000      N/A     False
1636    608     BTDevMgr.exe    0xe001ec66c2c0  2       -       0       False   2020-10-13 14:20:59.000000      N/A     False
1660    608     svchost.exe     0xe001ec70d8c0  13      -       0       False   2020-10-13 14:20:59.000000      N/A     False
1696    608     HPWMISVC.exe    0xe001ec6ee380  2       -       0       True    2020-10-13 14:20:59.000000      N/A     False
1728    608     mongod.exe      0xe001ec7098c0  30      -       0       False   2020-10-13 14:20:59.000000      N/A     False
1788    608     mosquitto.exe   0xe001ec6fd8c0  1       -       0       False   2020-10-13 14:21:01.000000      N/A     False
1804    608     mysqld.exe      0xe001ec84c8c0  3       -       0       False   2020-10-13 14:21:01.000000      N/A     False
1824    1804    mysqld.exe      0xe001ec7308c0  39      -       0       False   2020-10-13 14:21:02.000000      N/A     False
1836    1824    conhost.exe     0xe001ec72d8c0  2       -       0       False   2020-10-13 14:21:02.000000      N/A     False
1876    608     RichVideo64.ex  0xe001ec7338c0  2       -       0       False   2020-10-13 14:21:02.000000      N/A     False
1952    608     SynTPEnhServic  0xe001ec73c8c0  2       -       0       False   2020-10-13 14:21:03.000000      N/A     False
1976    608     svchost.exe     0xe001ec88d8c0  2       -       0       False   2020-10-13 14:21:03.000000      N/A     False
2036    608     Lavasoft.WCAss  0xe001ec7428c0  9       -       0       False   2020-10-13 14:21:03.000000      N/A     False
2056    608     MsMpEng.exe     0xe001ec73f8c0  24      -       0       False   2020-10-13 14:21:07.000000      N/A     False
2984    608     NisSrv.exe      0xe001eccad8c0  8       -       0       False   2020-10-13 14:22:36.000000      N/A     False
1672    608     svchost.exe     0xe001ec660540  6       -       0       False   2020-10-13 14:22:36.000000      N/A     False
2600    608     svchost.exe     0xe001e7b5c080  3       -       0       False   2020-10-13 14:22:36.000000      N/A     False
1648    1952    SynTPEnh.exe    0xe001e7c158c0  0       -       1       False   2020-10-13 14:22:43.000000      2020-10-13 14:41:58.000000
1704    608     PresentationFo  0xe001ecb09080  4       -       0       False   2020-10-13 14:22:43.000000      N/A     False
3532    608     svchost.exe     0xe001ec7208c0  9       -       0       False   2020-10-13 14:22:48.000000      N/A     False
3664    608     SearchIndexer.  0xe001eca04080  11      -       0       False   2020-10-13 14:22:49.000000      N/A     False
3868    608     HPSupportSolut  0xe001e44a8080  8       -       0       False   2020-10-13 14:24:37.000000      N/A     False
5056    608     TouchpointAnal  0xe001e44298c0  11      -       0       False   2020-10-13 14:24:48.000000      N/A     False
2384    608     IAStorDataMgrS  0xe001e4702080  6       -       0       True    2020-10-13 14:25:13.000000      N/A     False
3556    984     HPSF.exe        0xe001e47d38c0  0       -       1       False   2020-10-13 14:26:44.000000      2020-10-13 14:27:15.000000
4740    4764    chrome.exe      0xe001e508c4c0  0       -       1       False   2020-10-13 14:28:24.000000      2020-10-13 14:40:36.000000
316     984     taskhost.exe    0xe001e7b50740  10      -       0       False   2020-10-13 14:35:56.000000      N/A     False
3556    984     HPSF.exe        0xe001e47d38c0  0       -       1       False   2020-10-13 14:26:44.000000      2020-10-13 14:27:15.000000
```

Here we can see some processes (hidden processes) as compared to last one.

3. Python vol.py –f HP-20201014-033903.raw windows.pstree.PsTree
   This shows processes in parent-child tree format.

   Here we can see parent processes and child processes clearly with starts as levels o f=f the child tree.
   System is the parent process.
   Services is a parent process which has so many children.



4. Python vol.py –f HP-20201014-033903.raw windows.dlllist.DllList –pid 5940
   Shows list of all processes used by the process with –pid mentioned.
   Here the output shows the list of DLLs used by Microsoft Teams.exe pid = 5940.


C:\Windows\system32\cmd.exe
PID Process Base Size Name Path LoadTime Dumped
5940 Teams.exe 0x7ff6d4db0000 0x58b1000 Teams.exe C:\Users\home\AppData\Local\Microsoft\Teams\current\Teams.exe 2020-10-14 03:35:40.0
5940 Teams.exe 0x7ffcf6ce0000 0x1ad000 ntdll.dll C:\Windows\SYSTEM32\ntdll.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf6050000 0x13f000 KERNEL32.DLL C:\Windows\system32\KERNEL32.DLL 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf4240000 0x115000 KERNELBASE.dll C:\Windows\system32\KERNELBASE.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcd6bb0000 0x31c000 ffmpeg.dll C:\Users\home\AppData\Local\Microsoft\Teams\current\ffmpeg.dll 2020-10-14 03:35:40.0
5940 Teams.exe 0x7ffcf1600000 0x27b000 COMCTL32.dll C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9600.1
5940 Teams.exe 0x7ffcf43d0000 0xaa000 ADVAPI32.dll C:\Windows\system32\ADVAPI32.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf63b0000 0x14d000 GDI32.dll C:\Windows\system32\GDI32.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf6500000 0xc7000 OLEAUT32.dll C:\Windows\system32\OLEAUT32.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf4360000 0x7000 PSAPI.DLL C:\Windows\system32\PSAPI.DLL 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf4840000 0x152e000 SHELL32.dll C:\Windows\system32\SHELL32.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf4480000 0x177000 USER32.dll C:\Windows\system32\USER32.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcec8e0000 0x4ac000 WININET.dll C:\Windows\SYSTEM32\WININET.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffceeba0000 0x22000 WINMM.dll C:\Windows\SYSTEM32\WINMM.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf6190000 0x5a000 WS2_32.dll C:\Windows\system32\WS2_32.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf6a80000 0x195000 ole32.dll C:\Windows\system32\ole32.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf2060000 0x2a000 IPHLPAPI.DLL C:\Windows\SYSTEM32\IPHLPAPI.DLL 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffceef50000 0x6a000 OLEACC.dll C:\Windows\SYSTEM32\OLEACC.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcef300000 0xd000 msdmo.dll C:\Windows\SYSTEM32\msdmo.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf2ff0000 0xd000 HID.DLL C:\Windows\SYSTEM32\HID.DLL 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf6860000 0xb6000 COMDLG32.dll C:\Windows\system32\COMDLG32.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcec440000 0x189000 dbghelp.dll C:\Windows\SYSTEM32\dbghelp.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcee3a0000 0xa000 VERSION.dll C:\Windows\SYSTEM32\VERSION.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf4370000 0x54000 SHLWAPI.dll C:\Windows\system32\SHLWAPI.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf33d0000 0x21000 USERENV.dll C:\Windows\SYSTEM32\USERENV.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffceec00000 0x17f000 PROPSYS.dll C:\Windows\SYSTEM32\PROPSYS.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffceb080000 0x16000 USP10.dll C:\Windows\SYSTEM32\USP10.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffceefc0000 0x1ec000 DWrite.dll C:\Windows\SYSTEM32\DWrite.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf5f50000 0x36000 IMM32.dll C:\Windows\system32\IMM32.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf1b70000 0x21000 dwmapi.dll C:\Windows\SYSTEM32\dwmapi.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf2020000 0x12000 WTSAPI32.dll C:\Windows\SYSTEM32\WTSAPI32.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffceea60000 0x82000 WINSPOOL.DRV C:\Windows\SYSTEM32\WINSPOOL.DRV 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcebcb0000 0xc9000 WINHTTP.dll C:\Windows\SYSTEM32\WINHTTP.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf1ac0000 0x87000 dxgi.dll C:\Windows\SYSTEM32\dxgi.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcd8c10000 0x221000 d3d9.dll C:\Windows\SYSTEM32\d3d9.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffce4920000 0x24000 dxva2.dll C:\Windows\SYSTEM32\dxva2.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf1de0000 0x233000 d3d11.dll C:\Windows\SYSTEM32\d3d11.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcec090000 0x85000 wer.dll C:\Windows\SYSTEM32\wer.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf4060000 0x1df000 CRYPT32.dll C:\Windows\system32\CRYPT32.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffced0e0000 0x18a000 urlmon.dll C:\Windows\SYSTEM32\urlmon.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf2090000 0xc000 Secur32.dll C:\Windows\SYSTEM32\Secur32.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf3910000 0x25000 ncrypt.dll C:\Windows\SYSTEM32\ncrypt.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcee2d0000 0x1a000 dhcpcsvc.DLL C:\Windows\SYSTEM32\dhcpcsvc.DLL 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffced700000 0x135000 UIAutomationCore.DLL C:\Windows\SYSTEM32\UIAutomationCore.DLL 2020-10-14 03:35:40.000000
5940 Teams.exe 0x7ffcf20a0000 0x7000 MSIMG32.dll C:\Windows\SYSTEM32\MSIMG32.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf2a70000 0x129000 UxTheme.dll C:\Windows\SYSTEM32\UxTheme.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf6c30000 0xaa000 msvcrt.dll C:\Windows\system32\msvcrt.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf4670000 0x58000 sechost.dll C:\Windows\SYSTEM32\sechost.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf6920000 0x140000 RPCRT4.dll C:\Windows\system32\RPCRT4.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf65d0000 0x211000 combase.dll C:\Windows\system32\combase.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcece10000 0x2cc000 iertutil.dll C:\Windows\SYSTEM32\iertutil.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffceeb70000 0x2a000 WINMMBASE.dll C:\Windows\SYSTEM32\WINMMBASE.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf6c20000 0x9000 NSI.dll C:\Windows\system32\NSI.dll 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf1bb0000 0xa000 WINNSI.DLL C:\Windows\SYSTEM32\WINNSI.DLL 2020-10-14 03:35:40.000000 False
5940 Teams.exe 0x7ffcf1bb0000 0xa000 WINNSI.DLL C:\Windows\SYSTEM32\WINNSI.DLL 2020-10-14 03:35:40.000000 False

C:\Windows\system32\cmd.exe
5940 Teams.exe 0x7ffceff00000 0x70000 MMDevAPI.DLL C:\Windows\system32\MMDevAPI.DLL 2020-10-14 03:35:43.000000 False
5940 Teams.exe 0x7ffcf5f90000 0xb6000 clbcatq.dll C:\Windows\SYSTEM32\clbcatq.dll 2020-10-14 03:35:43.000000 False
5940 Teams.exe 0x7ffcefd10000 0x32000 ntmarta.dll C:\Windows\SYSTEM32\ntmarta.dll 2020-10-14 03:35:43.000000 False
5940 Teams.exe 0x7ffcebb10000 0x15000 napinsp.dll C:\Windows\system32\napinsp.dll 2020-10-14 03:35:43.000000 False
5940 Teams.exe 0x7ffceba f0000 0x1a000 pnrpnsp.dll C:\Windows\system32\pnrpnsp.dll 2020-10-14 03:35:43.000000 False
5940 Teams.exe 0x7ffcf3440000 0xa4000 DNSAPI.dll C:\Windows\SYSTEM32\DNSAPI.dll 2020-10-14 03:35:43.000000 False
5940 Teams.exe 0x7ffcebd80000 0xd000 winrnr.dll C:\Windows\System32\winrnr.dll 2020-10-14 03:35:43.000000 False
5940 Teams.exe 0x71e00000 0x26000 mdnsNSP.dll C:\Program Files\Bonjour\mdnsNSP.dll 2020-10-14 03:35:43.000000 False
5940 Teams.exe 0x7ffcec120000 0x14000 wshbth.dll C:\Windows\system32\wshbth.dll 2020-10-14 03:35:43.000000 False
5940 Teams.exe 0x7ffce6e40000 0xa000 rasadhlp.dll C:\Windows\System32\rasadhlp.dll 2020-10-14 03:35:43.000000 False
5940 Teams.exe 0x7ffcee2f0000 0x6b000 fwpuclnt.dll C:\Windows\System32\fwpuclnt.dll 2020-10-14 03:35:43.000000 False
5940 Teams.exe 0x7ffcf36a0000 0x20000 CRYPTSP.dll C:\Windows\SYSTEM32\CRYPTSP.dll 2020-10-14 03:35:43.000000 False
5940 Teams.exe 0x7ffcf32c0000 0x36000 rsaenh.dll C:\Windows\system32\rsaenh.dll 2020-10-14 03:35:43.000000 False
5940 Teams.exe 0x7ffce3f60000 0xf000 atlthunk.dll C:\Windows\SYSTEM32\atlthunk.dll 2020-10-14 03:35:43.000000 False
5940 Teams.exe 0x7ffcc2170000 0xd000 LINKINFO.dll C:\Windows\SYSTEM32\LINKINFO.dll 2020-10-14 03:35:44.000000 False
5940 Teams.exe 0x7ffcf5f70000 0xda000 SETUPAPI.dll C:\Windows\system32\SETUPAPI.dll 2020-10-14 03:35:44.000000 False
5940 Teams.exe 0x7ffcdb990000 0xba000 ntshrui.dll C:\Windows\SYSTEM32\ntshrui.dll 2020-10-14 03:35:44.000000 False
5940 Teams.exe 0x7ffcf3a00000 0x26000 srvcli.dll C:\Windows\SYSTEM32\srvcli.dll 2020-10-14 03:35:44.000000 False
5940 Teams.exe 0x7ffce5f10000 0x12000 cscapi.dll C:\Windows\SYSTEM32\cscapi.dll 2020-10-14 03:35:44.000000 False
5940 Teams.exe 0x7ffce47b0000 0x9000 IconCodecService.dll C:\Windows\system32\IconCodecService.dll 2020-10-14 03:35:44.000000 False
5940 Teams.exe 0x7ffce1360000 0x1af000 WindowsCodecs.dll C:\Windows\SYSTEM32\WindowsCodecs.dll 2020-10-14 03:35:44.000000 False
5940 Teams.exe 0x7ffcdf3a0000 0x2fe000 explorerframe.dll C:\Windows\system32\explorerframe.dll 2020-10-14 03:35:44.000000 False
5940 Teams.exe 0x7ffceffa0000 0xa4000 DUser.dll C:\Windows\system32\DUser.dll 2020-10-14 03:35:44.000000 False
5940 Teams.exe 0x7ffcf1bc0000 0x1c1000 DUI70.dll C:\Windows\system32\DUI70.dll 2020-10-14 03:35:44.000000 False
5940 Teams.exe 0x7ffcdaef0000 0x22000 adal-win.node \\?\C:\Users\home\AppData\Local\Microsoft\Teams\current\resources\app.asar.unpacked\node_modules\adal3-w
5940 Teams.exe 0x7ffcd69e0000 0x1c7000 adal.dll \\?\C:\Users\home\AppData\Local\Microsoft\Teams\current\resources\app.asar.unpacked\node_modules
5940 Teams.exe 0x7ffcdf250000 0x1f000 keytar.node \\?\C:\Users\home\AppData\Local\Microsoft\Teams\current\resources\app.asar.unpacked\node_modules\keytar3
5940 Teams.exe 0x7ffcf2a60000 0xa000 DPAPI.dll C:\Windows\SYSTEM32\DPAPI.dll 2020-10-14 03:35:45.000000 False
5940 Teams.exe 0x7ffcf2fc0000 0x24000 gpapi.dll C:\Windows\SYSTEM32\gpapi.dll 2020-10-14 03:35:46.000000 False
5940 Teams.exe 0x7ffce9600000 0x33000 cryptnet.dll C:\Windows\System32\cryptnet.dll 2020-10-14 03:35:46.000000 False
5940 Teams.exe 0x7ffcf4610000 0x5c000 WLDAP32.dll C:\Windows\system32\WLDAP32.dll 2020-10-14 03:35:46.000000 False
5940 Teams.exe 0x7ffce9020000 0xc000 ondemandconnroutehelper.dll C:\Windows\SYSTEM32\ondemandconnroutehelper.dll 2020-10-14 03:35:46.000000 False
5940 Teams.exe 0x7ffcf3210000 0x6e000 schannel.DLL C:\Windows\system32\schannel.DLL 2020-10-14 03:35:47.000000 False
5940 Teams.exe 0x7ffce3f40000 0x1d000 ncryptsslp.dll C:\Windows\system32\ncryptsslp.dll 2020-10-14 03:35:47.000000 False
5940 Teams.exe 0x7ffcde6f0000 0x3e000 wdmaud.drv C:\Windows\SYSTEM32\wdmaud.drv 2020-10-14 03:35:48.000000 False
5940 Teams.exe 0x7ffceebf0000 0x8000 ksuser.dll C:\Windows\SYSTEM32\ksuser.dll 2020-10-14 03:35:48.000000 False
5940 Teams.exe 0x7ffcf2050000 0xc000 AVRT.dll C:\Windows\SYSTEM32\AVRT.dll 2020-10-14 03:35:48.000000 False
5940 Teams.exe 0x7ffce47a0000 0xb000 msacm32.drv C:\Windows\SYSTEM32\msacm32.drv 2020-10-14 03:35:48.000000 False
5940 Teams.exe 0x7ffce2b20000 0x1c000 MSACM32.dll C:\Windows\SYSTEM32\MSACM32.dll 2020-10-14 03:35:48.000000 False
5940 Teams.exe 0x7ffce42f0000 0xa000 midimap.dll C:\Windows\SYSTEM32\midimap.dll 2020-10-14 03:35:48.000000 False
5940 Teams.exe 0x7ffcf3d50000 0x99000 sxs.dll C:\Windows\SYSTEM32\sxs.dll 2020-10-14 03:36:10.000000 False
5940 Teams.exe 0x7ffcf23f0000 0x1d000 sharing-indicator.node \\?\C:\Users\home\AppData\Local\Microsoft\Teams\current\resources\app.asar.unpacked\node_modules
5940 Teams.exe 0x7ffcf23c0000 0x25000 RtmControl.dll \\?\C:\Users\home\AppData\Local\Microsoft\Teams\current\resources\app.asar.unpacked\node_modules\slimcor
5940 Teams.exe 0x7ffcd22f0000 0x32e000 skypert.dll \\?\C:\Users\home\AppData\Local\Microsoft\Teams\current\resources\app.asar.unpacked\node_modules
5940 Teams.exe 0x7ffcf0160000 0x1b1000 gdiplus.dll C:\Windows\WinSxS\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.9600.19812_none_932b02e94
5940 Teams.exe 0x7ffcf23b0000 0xb000 VCRUNTIME140_1.dll C:\Users\home\AppData\Local\Microsoft\Teams\current\VCRUNTIME140_1.dll 2020-10-14 03:36:26.0000
5940 Teams.exe 0x7ffcda050000 0xd2000 RtmPal.dll \\?\C:\Users\home\AppData\Local\Microsoft\Teams\current\resources\app.asar.unpacked\node_modules\slimcor
5940 Teams.exe 0x7ffcec040000 0x4f000 pdh.dll C:\Windows\SYSTEM32\pdh.dll 2020-10-14 03:36:26.000000 False
5940 Teams.exe 0x7ffccbcc0000 0xb1000 RASAPI32.dll C:\Windows\SYSTEM32\RASAPI32.dll 2020-10-14 03:36:26.000000 False
5940 Teams.exe 0x7ffccbc90000 0x30000 rasman.dll C:\Windows\SYSTEM32\rasman.dll 2020-10-14 03:36:26.000000 False
5940 Teams.exe 0x7ffcf2380000 0x2c000 keyboard-layout-manager.node \\?\C:\Users\home\AppData\Local\Microsoft\Teams\current\resources\app.asar.unpacked\node
5940 Teams.exe 0x7ffcd9fd0000 0x7f000 spellchecker.node \\?\C:\Users\home\AppData\Local\Microsoft\Teams\current\resources\app.asar.unpacked\node_modules
5940 Teams.exe 0x7ffce0540000 0xfa000 MsSpellCheckingFacility.dll C:\Windows\System32\MsSpellCheckingFacility.dll 2020-10-14 03:36:30.000000 False
5940 Teams.exe 0x7ffcef7a0000 0x66000 Bcp47Langs.dll C:\Windows\System32\Bcp47Langs.dll 2020-10-14 03:36:30.000000 False
5940 Teams.exe 0x7ffcf4030000 0x5000 Normaliz.dll C:\Windows\system32\Normaliz.dll 2020-10-14 03:36:30.000000 False
5940 Teams.exe 0x7ffcdc050000 0x2c4000 actxprxy.dll C:\Windows\System32\actxprxy.dll 2020-10-14 03:36:30.000000 False

5. Python vol.py –f HP-20201014-033903.raw windows.netscan.NetScan
   Gives Network Info like open & closed ports, processes using them, IP address, port ID etc.