# Memory Forensics

***Task 1:*** With the Triage.mem shared in class, conduct a forensic analysis, and write a report on this memory dump when you perform a memory forensic analysis in 2 and 3

Notes: Analysis done on Triage.mem on Volatility 2 and Volatility 3 with your justification and conclusion needed. Analyzing the Triage.mem memory dump using Volatility – 2:

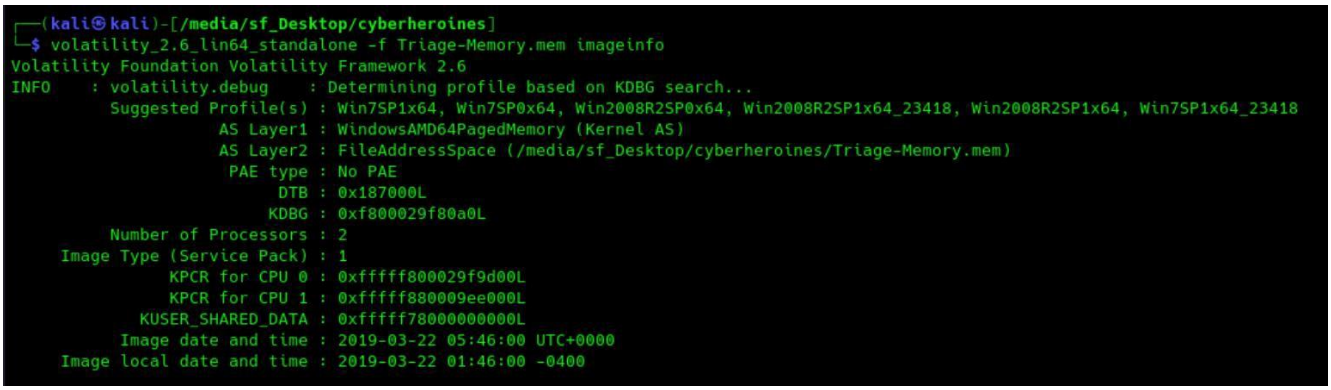
***Calculating md5sum of the memory dump:***


Analyzing profile for memory image:

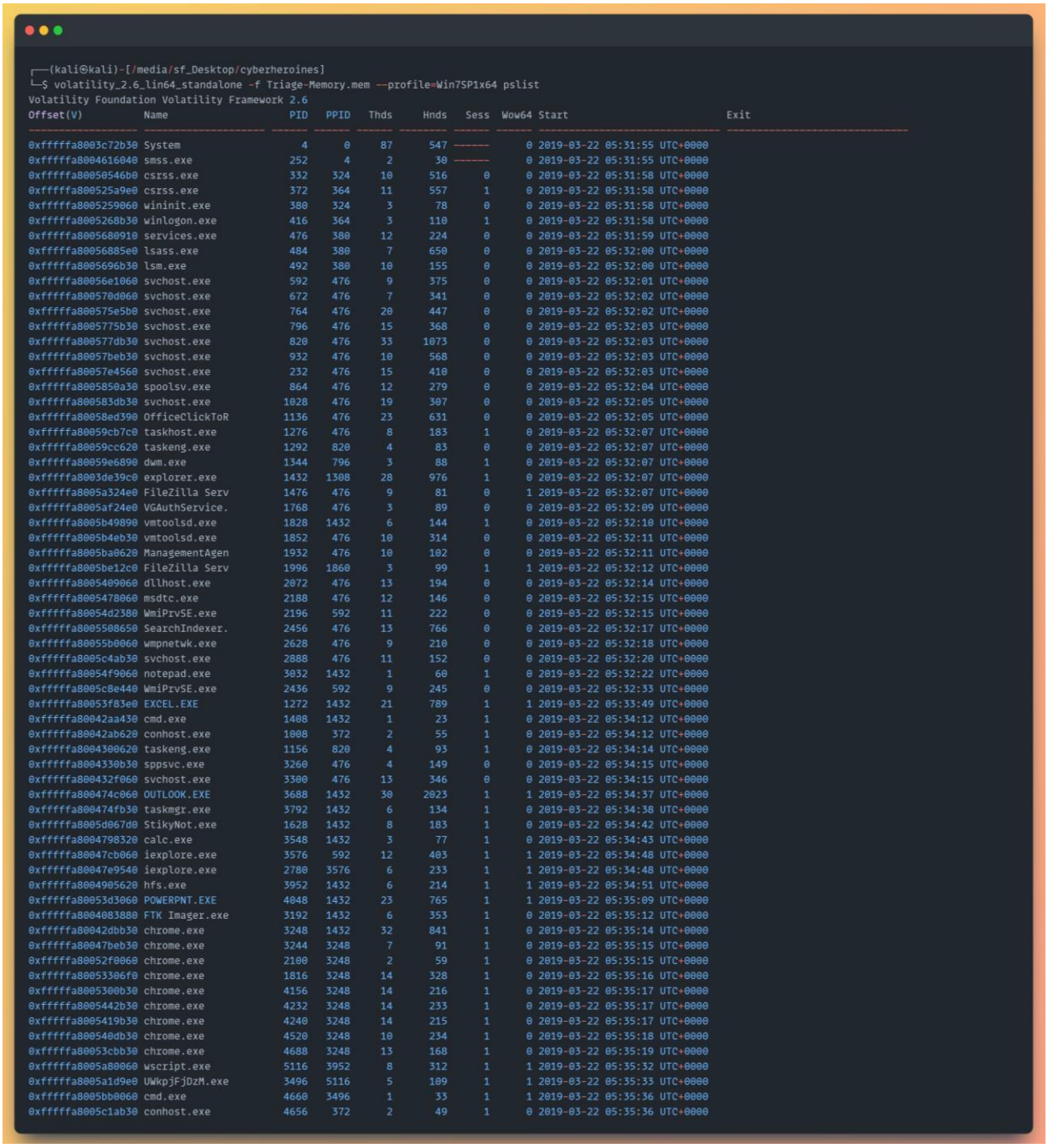
By using the “imageinfo” plugin, the most important task is to determine the profile of the memory dump. In this case, the profile is “Win7SP1x64”. "Win7SP1x64" refers to the operating system profile suggested by the Volatility memory forensics framework based on the analysis of the memory image. In this case, it indicates the following:

- Operating System: Windows 7
- Service Pack: Service Pack 1 (SP1)
- Architecture: 64-bit (x64)

Besides this critical information, we can also know at what time the memory dump was taken. A time zone offset of UTC-04:00 hours corresponds to the Eastern Daylight Time (EDT) zone in North America and Canada.



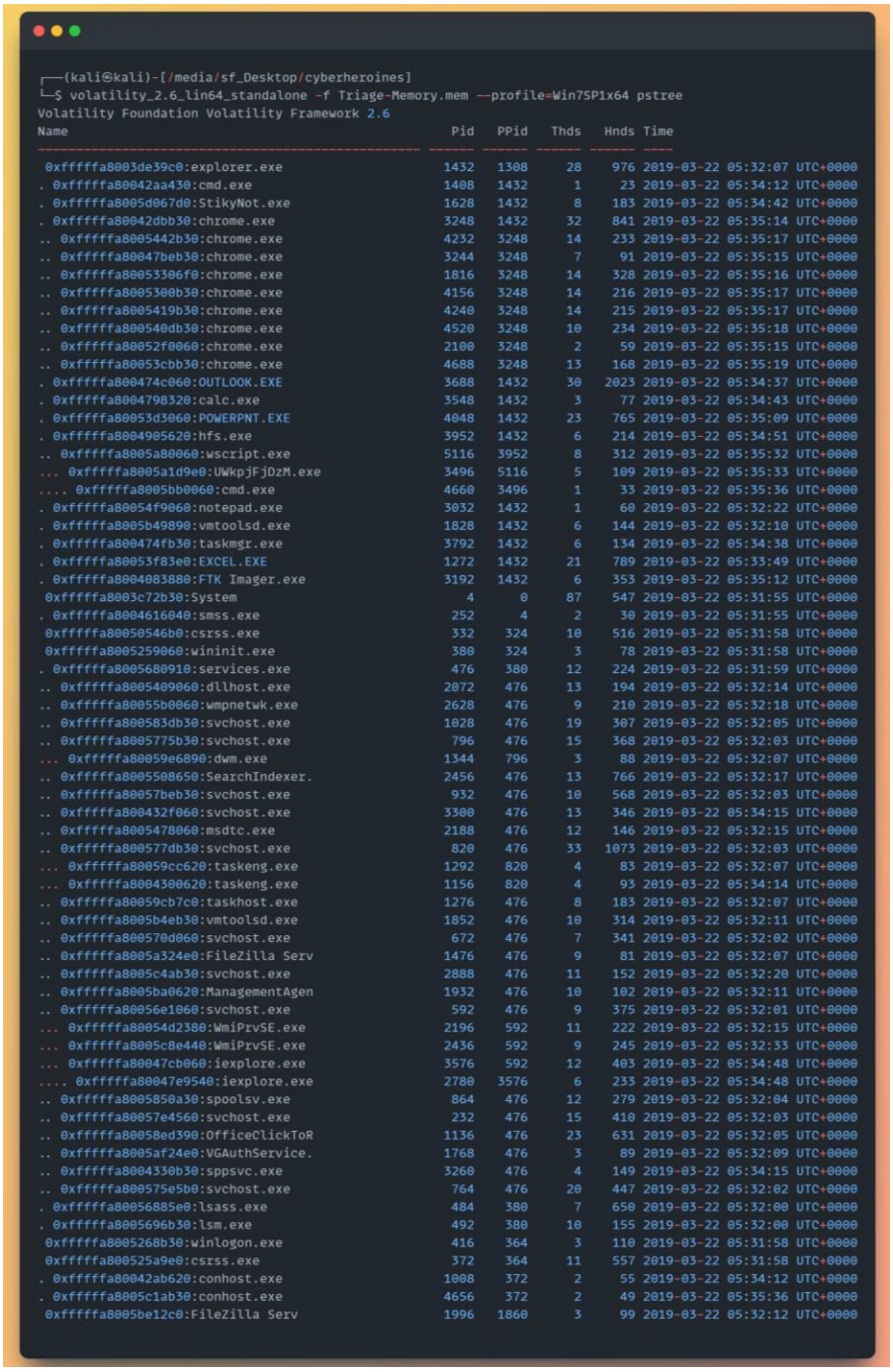
Listing out the processes using PSLIST plugin:



```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ volatility_2.6_lin64_standalone -f Triage-Memory.mem --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8003c72b30 System                    4      0     87      547 ------      0 2019-03-22 05:31:55 UTC+0000
0xfffffa8004616040 smss.exe                252      4      2       30 ------      0 2019-03-22 05:31:55 UTC+0000
0xfffffa80050546b0 csrss.exe               332    324     10      516      0      0 2019-03-22 05:31:58 UTC+0000
0xfffffa800525a9e0 csrss.exe               372    364     11      557      1      0 2019-03-22 05:31:58 UTC+0000
0xfffffa8005259060 wininit.exe             380    324      3       78      0      0 2019-03-22 05:31:58 UTC+0000
0xfffffa8005268b30 winlogon.exe            416    364      3      110      1      0 2019-03-22 05:31:58 UTC+0000
0xfffffa8005680910 services.exe            476    380     12      224      0      0 2019-03-22 05:31:59 UTC+0000
0xfffffa80056885e0 lsass.exe               484    380      7      650      0      0 2019-03-22 05:32:00 UTC+0000
0xfffffa8005696b30 lsm.exe                 492    380     10      155      0      0 2019-03-22 05:32:00 UTC+0000
0xfffffa80056e1060 svchost.exe             592    476      9      375      0      0 2019-03-22 05:32:01 UTC+0000
0xfffffa800570d060 svchost.exe             672    476      7      341      0      0 2019-03-22 05:32:02 UTC+0000
0xfffffa800575e5b0 svchost.exe             764    476     20      447      0      0 2019-03-22 05:32:02 UTC+0000
0xfffffa8005775b30 svchost.exe             796    476     15      368      0      0 2019-03-22 05:32:03 UTC+0000
0xfffffa800577db30 svchost.exe             820    476     33     1073      0      0 2019-03-22 05:32:03 UTC+0000
0xfffffa80057beb30 svchost.exe             932    476     10      568      0      0 2019-03-22 05:32:03 UTC+0000
0xfffffa80057e4560 svchost.exe             232    476     15      410      0      0 2019-03-22 05:32:03 UTC+0000
0xfffffa8005850a30 spoolsv.exe             864    476     12      279      0      0 2019-03-22 05:32:04 UTC+0000
0xfffffa800583db30 svchost.exe            1028    476     19      307      0      0 2019-03-22 05:32:05 UTC+0000
0xfffffa80058ed390 OfficeClickToR         1136    476     23      631      0      0 2019-03-22 05:32:05 UTC+0000
0xfffffa80059cb7c0 taskhost.exe           1276    476      8      183      1      0 2019-03-22 05:32:07 UTC+0000
0xfffffa80059cc620 taskeng.exe            1292    820      4       83      0      0 2019-03-22 05:32:07 UTC+0000
0xfffffa80059e6890 dwm.exe                1344    796      3       88      1      0 2019-03-22 05:32:07 UTC+0000
0xfffffa8003de39c0 explorer.exe           1432   1308     28      976      1      0 2019-03-22 05:32:07 UTC+0000
0xfffffa8005a324e0 FileZilla Serv         1476    476      9       81      0      1 2019-03-22 05:32:07 UTC+0000
0xfffffa8005af24e0 VGAuthService.         1768    476      3       89      0      0 2019-03-22 05:32:09 UTC+0000
0xfffffa8005b49890 vmtoolsd.exe           1828   1432      6      144      1      0 2019-03-22 05:32:10 UTC+0000
0xfffffa8005b4eb30 vmtoolsd.exe           1852    476     10      314      0      0 2019-03-22 05:32:11 UTC+0000
0xfffffa8005ba0620 ManagementAgen         1932    476     10      102      0      0 2019-03-22 05:32:11 UTC+0000
0xfffffa8005be12c0 FileZilla Serv         1996   1860      3       99      1      1 2019-03-22 05:32:12 UTC+0000
0xfffffa8005409060 dllhost.exe            2072    476     13      194      0      0 2019-03-22 05:32:14 UTC+0000
0xfffffa8005478060 msdtc.exe              2188    476     12      146      0      0 2019-03-22 05:32:15 UTC+0000
0xfffffa80054d2380 WmiPrvSE.exe           2196    592     11      222      0      0 2019-03-22 05:32:15 UTC+0000
0xfffffa8005508650 SearchIndexer.         2456    476     13      766      0      0 2019-03-22 05:32:17 UTC+0000
0xfffffa80055b0060 wmpnetwk.exe           2628    476      9      210      0      0 2019-03-22 05:32:18 UTC+0000
0xfffffa8005c4ab30 svchost.exe            2888    476     11      152      0      0 2019-03-22 05:32:20 UTC+0000
0xfffffa80054f9060 notepad.exe            3032   1432      1       60      1      0 2019-03-22 05:32:22 UTC+0000
0xfffffa8005c8e440 WmiPrvSE.exe           2436    592      9      245      0      0 2019-03-22 05:32:33 UTC+0000
0xfffffa80053f83e0 EXCEL.EXE              1272   1432     21      789      1      1 2019-03-22 05:33:49 UTC+0000
0xfffffa80042aa430 cmd.exe                1408   1432      1       23      1      0 2019-03-22 05:34:12 UTC+0000
0xfffffa80042ab620 conhost.exe            1008    372      2       55      1      0 2019-03-22 05:34:12 UTC+0000
0xfffffa8004300620 taskeng.exe            1156    820      4       93      1      0 2019-03-22 05:34:14 UTC+0000
0xfffffa8004330b30 sppsvc.exe             3260    476      4      149      0      0 2019-03-22 05:34:15 UTC+0000
0xfffffa800432f060 svchost.exe            3300    476     13      346      0      0 2019-03-22 05:34:15 UTC+0000
0xfffffa800474c060 OUTLOOK.EXE            3688   1432     30     2023      1      1 2019-03-22 05:34:37 UTC+0000
0xfffffa800474fb30 taskmgr.exe            3792   1432      6      134      1      0 2019-03-22 05:34:38 UTC+0000
0xfffffa8005d067d0 StikyNot.exe           1628   1432      8      183      1      0 2019-03-22 05:34:42 UTC+0000
0xfffffa8004798320 calc.exe               3548   1432      3       77      1      0 2019-03-22 05:34:43 UTC+0000
0xfffffa80047cb060 iexplore.exe           3576    592     12      403      1      1 2019-03-22 05:34:48 UTC+0000
0xfffffa80047e9540 iexplore.exe           2780   3576      6      233      1      1 2019-03-22 05:34:48 UTC+0000
0xfffffa8004905620 hfs.exe                3952   1432      6      214      1      1 2019-03-22 05:34:51 UTC+0000
0xfffffa80053d3060 POWERPNT.EXE           4048   1432     23      765      1      1 2019-03-22 05:35:09 UTC+0000
0xfffffa8004083880 FTK Imager.exe         3192   1432      6      353      1      0 2019-03-22 05:35:12 UTC+0000
0xfffffa80042dbb30 chrome.exe             3248   1432     32      841      1      0 2019-03-22 05:35:14 UTC+0000
0xfffffa80047beb30 chrome.exe             3244   3248      7       91      1      0 2019-03-22 05:35:15 UTC+0000
0xfffffa80052f0060 chrome.exe             2100   3248      2       59      1      0 2019-03-22 05:35:15 UTC+0000
0xfffffa80053306f0 chrome.exe             1816   3248     14      328      1      0 2019-03-22 05:35:16 UTC+0000
0xfffffa8005300b30 chrome.exe             4156   3248     14      216      1      0 2019-03-22 05:35:17 UTC+0000
0xfffffa8005442b30 chrome.exe             4232   3248     14      233      1      0 2019-03-22 05:35:17 UTC+0000
0xfffffa8005419b30 chrome.exe             4240   3248     14      215      1      0 2019-03-22 05:35:17 UTC+0000
0xfffffa800540db30 chrome.exe             4520   3248     10      234      1      0 2019-03-22 05:35:18 UTC+0000
0xfffffa80053cbb30 chrome.exe             4688   3248     13      168      1      0 2019-03-22 05:35:19 UTC+0000
0xfffffa8005a80060 wscript.exe            5116   3952      8      312      1      1 2019-03-22 05:35:32 UTC+0000
0xfffffa8005a1d9e0 UWkpjFjDzM.exe         3496   5116      5      109      1      1 2019-03-22 05:35:33 UTC+0000
0xfffffa8005bb0060 cmd.exe                4660   3496      1       33      1      1 2019-03-22 05:35:36 UTC+0000
0xfffffa8005c1ab30 conhost.exe            4656    372      2       49      1      0 2019-03-22 05:35:36 UTC+0000
```

From the above process list, I find “UWkpjFjDzM.exe” process as malicious because of its suspicious file name. Furthermore, analysis is required to conclude it. Basically, the pslist is useful for quickly listing all processes in a straightforward manner. It's a starting point for process analysis and can help identify suspicious or unusual processes.

***Listing the processes including child processes using PSTREE plugin:***



```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ volatility_2.6_lin64_standalone -f Triage-Memory.mem --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa8003de39c0:explorer.exe                     1432   1308     28    976 2019-03-22 05:32:07 UTC+0000
. 0xfffffa80042aa430:cmd.exe                         1408   1432      1     23 2019-03-22 05:34:12 UTC+0000
. 0xfffffa8005d067d0:StikyNot.exe                    1628   1432      8    183 2019-03-22 05:34:42 UTC+0000
. 0xfffffa80042dbb30:chrome.exe                      3248   1432     32    841 2019-03-22 05:35:14 UTC+0000
.. 0xfffffa8005442b30:chrome.exe                     4232   3248     14    233 2019-03-22 05:35:17 UTC+0000
.. 0xfffffa80047beb30:chrome.exe                     3244   3248      7     91 2019-03-22 05:35:15 UTC+0000
.. 0xfffffa80053306f0:chrome.exe                     1816   3248     14    328 2019-03-22 05:35:16 UTC+0000
.. 0xfffffa8005300b30:chrome.exe                     4156   3248     14    216 2019-03-22 05:35:17 UTC+0000
.. 0xfffffa8005419b30:chrome.exe                     4240   3248     14    215 2019-03-22 05:35:17 UTC+0000
.. 0xfffffa800540db30:chrome.exe                     4520   3248     10    234 2019-03-22 05:35:18 UTC+0000
.. 0xfffffa80052f0060:chrome.exe                     2100   3248      2     59 2019-03-22 05:35:15 UTC+0000
.. 0xfffffa80053cbb30:chrome.exe                     4688   3248     13    168 2019-03-22 05:35:19 UTC+0000
. 0xfffffa800474c060:OUTLOOK.EXE                     3688   1432     30   2023 2019-03-22 05:34:37 UTC+0000
. 0xfffffa8004798320:calc.exe                        3548   1432      3     77 2019-03-22 05:34:43 UTC+0000
. 0xfffffa80053d3060:POWERPNT.EXE                    4048   1432     23    765 2019-03-22 05:35:09 UTC+0000
. 0xfffffa8004905620:hfs.exe                         3952   1432      6    214 2019-03-22 05:34:51 UTC+0000
.. 0xfffffa8005a80060:wscript.exe                    5116   3952      8    312 2019-03-22 05:35:32 UTC+0000
... 0xfffffa8005a1d9e0:UWkpjFjDzM.exe                3496   5116      5    109 2019-03-22 05:35:33 UTC+0000
.... 0xfffffa8005bb0060:cmd.exe                      4660   3496      1     33 2019-03-22 05:35:36 UTC+0000
. 0xfffffa80054f9060:notepad.exe                     3032   1432      1     60 2019-03-22 05:32:22 UTC+0000
. 0xfffffa8005b49890:vmtoolsd.exe                    1828   1432      6    144 2019-03-22 05:32:10 UTC+0000
. 0xfffffa800474fb30:taskmgr.exe                     3792   1432      6    134 2019-03-22 05:34:38 UTC+0000
. 0xfffffa80053f83e0:EXCEL.EXE                       1272   1432     21    789 2019-03-22 05:33:49 UTC+0000
. 0xfffffa8004083880:FTK Imager.exe                  3192   1432      6    353 2019-03-22 05:35:12 UTC+0000
 0xfffffa8003c72b30:System                              4      0     87    547 2019-03-22 05:31:55 UTC+0000
. 0xfffffa8004616040:smss.exe                        252      4      2     30 2019-03-22 05:31:55 UTC+0000
 0xfffffa80050546b0:csrss.exe                        332    324     10    516 2019-03-22 05:31:58 UTC+0000
 0xfffffa8005259060:wininit.exe                      380    324      3     78 2019-03-22 05:31:58 UTC+0000
. 0xfffffa8005680910:services.exe                    476    380     12    224 2019-03-22 05:31:59 UTC+0000
.. 0xfffffa8005409060:dllhost.exe                   2072    476     13    194 2019-03-22 05:32:14 UTC+0000
.. 0xfffffa80055b0060:wmpnetwk.exe                  2628    476      9    210 2019-03-22 05:32:18 UTC+0000
.. 0xfffffa800583db30:svchost.exe                   1028    476     19    307 2019-03-22 05:32:05 UTC+0000
.. 0xfffffa8005775b30:svchost.exe                    796    476     15    368 2019-03-22 05:32:03 UTC+0000
... 0xfffffa80059e6890:dwm.exe                      1344    796      3     88 2019-03-22 05:32:07 UTC+0000
.. 0xfffffa8005508650:SearchIndexer.                2456    476     13    766 2019-03-22 05:32:17 UTC+0000
.. 0xfffffa80057beb30:svchost.exe                    932    476     10    568 2019-03-22 05:32:03 UTC+0000
.. 0xfffffa800432f060:svchost.exe                   3300    476     13    346 2019-03-22 05:34:15 UTC+0000
.. 0xfffffa8005478060:msdtc.exe                     2188    476     12    146 2019-03-22 05:32:15 UTC+0000
.. 0xfffffa800577db30:svchost.exe                    820    476     33   1073 2019-03-22 05:32:03 UTC+0000
... 0xfffffa80059cc620:taskeng.exe                  1292    820      4     83 2019-03-22 05:32:07 UTC+0000
... 0xfffffa8004300620:taskeng.exe                  1156    820      4     93 2019-03-22 05:34:14 UTC+0000
.. 0xfffffa80059cb7c0:taskhost.exe                  1276    476      8    183 2019-03-22 05:32:07 UTC+0000
.. 0xfffffa8005b4eb30:vmtoolsd.exe                  1852    476     10    314 2019-03-22 05:32:11 UTC+0000
.. 0xfffffa800570d060:svchost.exe                    672    476      7    341 2019-03-22 05:32:02 UTC+0000
.. 0xfffffa8005a324e0:FileZilla Serv                1476    476      9     81 2019-03-22 05:32:07 UTC+0000
.. 0xfffffa8005c4ab30:svchost.exe                   2888    476     11    152 2019-03-22 05:32:20 UTC+0000
.. 0xfffffa8005ba0620:ManagementAgen                1932    476     10    102 2019-03-22 05:32:11 UTC+0000
.. 0xfffffa80056e1060:svchost.exe                    592    476      9    375 2019-03-22 05:32:01 UTC+0000
... 0xfffffa80054d2380:WmiPrvSE.exe                 2196    592     11    222 2019-03-22 05:32:15 UTC+0000
... 0xfffffa8005c8e440:WmiPrvSE.exe                 2436    592      9    245 2019-03-22 05:32:33 UTC+0000
... 0xfffffa80047cb060:iexplore.exe                 3576    592     12    403 2019-03-22 05:34:48 UTC+0000
.... 0xfffffa80047e9540:iexplore.exe                2780   3576      6    233 2019-03-22 05:34:48 UTC+0000
.. 0xfffffa8005850a30:spoolsv.exe                    864    476     12    279 2019-03-22 05:32:04 UTC+0000
.. 0xfffffa80057e4560:svchost.exe                    232    476     15    410 2019-03-22 05:32:03 UTC+0000
.. 0xfffffa80058ed390:OfficeClickToR                1136    476     23    631 2019-03-22 05:32:05 UTC+0000
.. 0xfffffa8005af24e0:VGAuthService.                1768    476      3     89 2019-03-22 05:32:09 UTC+0000
.. 0xfffffa8004330b30:sppsvc.exe                    3260    476      4    149 2019-03-22 05:34:15 UTC+0000
.. 0xfffffa800575e5b0:svchost.exe                    764    476     20    447 2019-03-22 05:32:02 UTC+0000
. 0xfffffa80056885e0:lsass.exe                       484    380      7    650 2019-03-22 05:32:00 UTC+0000
. 0xfffffa8005696b30:lsm.exe                         492    380     10    155 2019-03-22 05:32:00 UTC+0000
 0xfffffa8005268b30:winlogon.exe                     416    364      3    110 2019-03-22 05:31:58 UTC+0000
 0xfffffa800525a9e0:csrss.exe                        372    364     11    557 2019-03-22 05:31:58 UTC+0000
. 0xfffffa80042ab620:conhost.exe                    1008    372      2     55 2019-03-22 05:34:12 UTC+0000
. 0xfffffa8005c1ab30:conhost.exe                    4656    372      2     49 2019-03-22 05:35:36 UTC+0000
 0xfffffa8005be12c0:FileZilla Serv                  1996   1860      3     99 2019-03-22 05:32:12 UTC+0000
```

Pslist is not enough while analyzing the memory dump. Pstree is valuable for understanding the relationships between processes. It helps visualize how processes are spawned and connected in the system. This is particularly useful for identifying process chains that might indicate malicious activity, like a suspicious parent process spawning a suspicious child process.

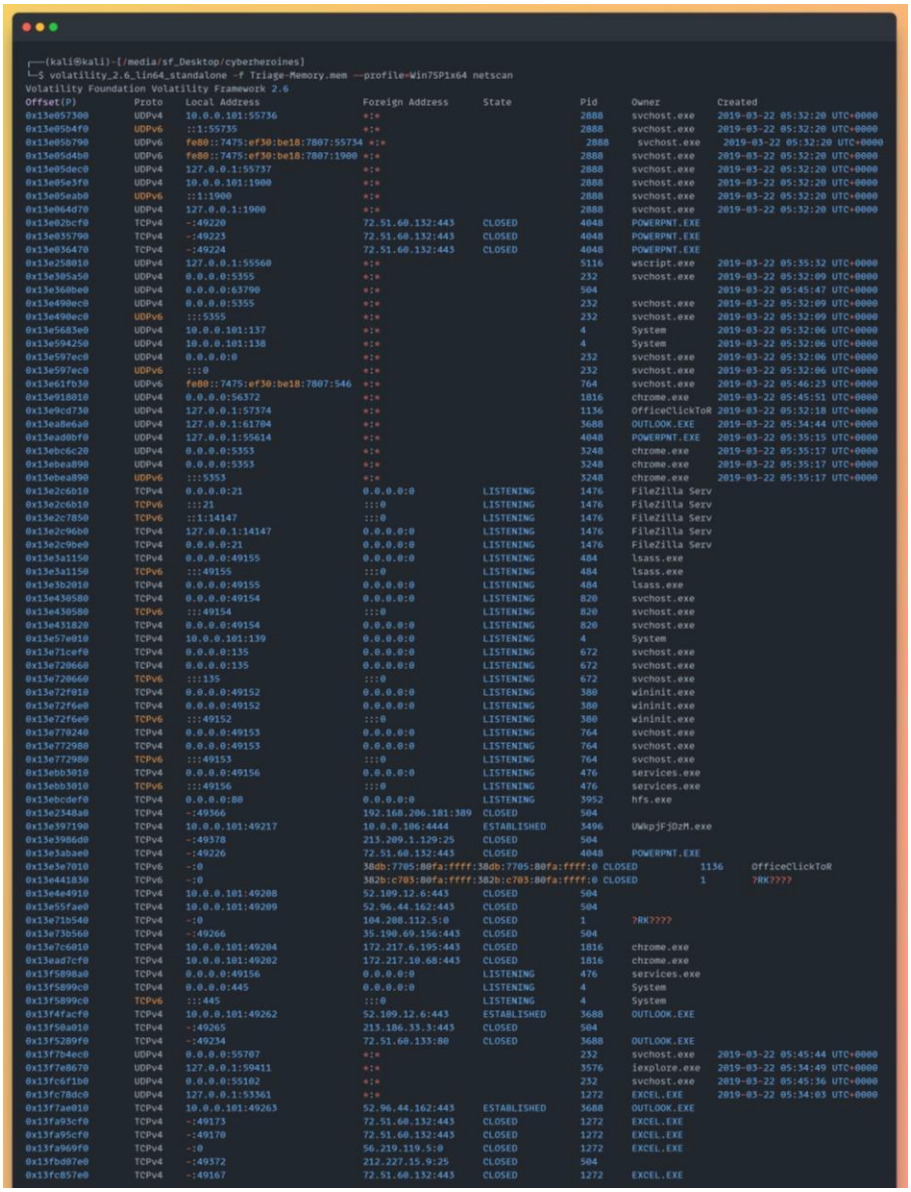
***Dumping a process with Volatility - 2:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ volatility_2.6_lin64_standalone -f Triage-Memory.mem --profile=Win7SP1x64 procdump -p3496 --dump-dir dumps/
Volatility Foundation Volatility Framework 2.6
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
0xfffffa8005a1d9e0 0x0000000000400000 UWkpjFjDzM.exe       OK: executable.3496.exe
```

***Scanning for all the processes using PSSCAN plugin:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ volatility_2.6_lin64_standalone -f Triage-Memory.mem --profile=Win7SP1x64 psscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                PID   PPID PDB                Time created                   Time exited
------------------ ---------------- ------ ------ ------------------ ------------------------------ ------------------------------
0x0000000007072b30 System                4      0 0x0000000000187000 2019-03-22 05:31:55 UTC+0000
0x00000000071e39c0 explorer.exe       1432   1308 0x0000000093db1000 2019-03-22 05:32:07 UTC+0000
0x000000013e01ab30 conhost.exe        4656    372 0x000000011b768000 2019-03-22 05:35:36 UTC+0000
0x000000013e04ab30 svchost.exe        2888    476 0x000000007f819000 2019-03-22 05:32:20 UTC+0000
0x000000013e08e440 WmiPrvSE.exe       2436    592 0x000000007d1ce000 2019-03-22 05:32:33 UTC+0000
0x000000013e1067d0 StikyNot.exe       1628   1432 0x000000003edbb000 2019-03-22 05:34:42 UTC+0000
0x000000013e21d9e0 UWkpjFjDzM.exe     3496   5116 0x000000010ef40000 2019-03-22 05:35:33 UTC+0000
0x000000013e2324e0 FileZilla Serv     1476    476 0x0000000093828000 2019-03-22 05:32:07 UTC+0000
0x000000013e280060 wscript.exe        5116   3952 0x000000012e80000 2019-03-22 05:35:32 UTC+0000
0x000000013e2f24e0 VGAuthService.     1768    476 0x0000000009037e000 2019-03-22 05:32:09 UTC+0000
0x000000013e349890 vmtoolsd.exe       1828   1432 0x000000008f68c000 2019-03-22 05:32:10 UTC+0000
0x000000013e34eb30 vmtoolsd.exe       1852    476 0x000000008f1d0000 2019-03-22 05:32:11 UTC+0000
0x000000013e3a0620 ManagementAgen     1932    476 0x000000008dd27000 2019-03-22 05:32:11 UTC+0000
0x000000013e3b0060 cmd.exe            4660   3496 0x000000011c8a9000 2019-03-22 05:35:36 UTC+0000
0x000000013e3e12c0 FileZilla Serv     1996   1860 0x000000008c66a000 2019-03-22 05:32:12 UTC+0000
0x000000013e43db30 svchost.exe        1028    476 0x0000000097dbf000 2019-03-22 05:32:05 UTC+0000
0x000000013e450a30 spoolsv.exe         864    476 0x00000000982e5000 2019-03-22 05:32:04 UTC+0000
0x000000013e4ed390 OfficeClickToR     1136    476 0x0000000009729f000 2019-03-22 05:32:05 UTC+0000
0x000000013e5cb7c0 taskhost.exe       1276    476 0x0000000094d46000 2019-03-22 05:32:07 UTC+0000
0x000000013e5cc620 taskeng.exe        1292    820 0x00000000948bd000 2019-03-22 05:32:07 UTC+0000
0x000000013e5e6890 dwm.exe            1344    796 0x0000000094422000 2019-03-22 05:32:07 UTC+0000
0x000000013e680910 services.exe        476    380 0x000000009cccc000 2019-03-22 05:31:59 UTC+0000
0x000000013e6885e0 lsass.exe           484    380 0x000000009ce2c000 2019-03-22 05:32:00 UTC+0000
0x000000013e696b30 lsm.exe             492    380 0x000000009ce72000 2019-03-22 05:32:00 UTC+0000
0x000000013e6e1060 svchost.exe         592    476 0x000000009c255000 2019-03-22 05:32:01 UTC+0000
0x000000013e70d060 svchost.exe         672    476 0x000000009bdfb000 2019-03-22 05:32:02 UTC+0000
0x000000013e75e5b0 svchost.exe         764    476 0x000000009b3a6000 2019-03-22 05:32:02 UTC+0000
0x000000013e775b30 svchost.exe         796    476 0x000000009b5f6000 2019-03-22 05:32:03 UTC+0000
0x000000013e77db30 svchost.exe         820    476 0x000000009b13b000 2019-03-22 05:32:03 UTC+0000
0x000000013e7beb30 svchost.exe         932    476 0x000000009aac6000 2019-03-22 05:32:03 UTC+0000
0x000000013e7e4560 svchost.exe         232    476 0x000000009a08e000 2019-03-22 05:32:03 UTC+0000
0x000000013e809060 dllhost.exe        2072    476 0x0000000087586000 2019-03-22 05:32:14 UTC+0000
0x000000013e80db30 chrome.exe         4520   3248 0x000000001f476000 2019-03-22 05:35:18 UTC+0000
0x000000013e819b30 chrome.exe         4240   3248 0x000000001e874000 2019-03-22 05:35:17 UTC+0000
0x000000013e842b30 chrome.exe         4232   3248 0x000000001d296000 2019-03-22 05:35:17 UTC+0000
0x000000013e878060 msdtc.exe          2188    476 0x0000000084ece000 2019-03-22 05:32:15 UTC+0000
0x000000013e8d2380 WmiPrvSE.exe       2196    592 0x0000000085107000 2019-03-22 05:32:15 UTC+0000
0x000000013e8f9060 notepad.exe        3032   1432 0x000000007de76000 2019-03-22 05:32:22 UTC+0000
0x000000013e908650 SearchIndexer.     2456    476 0x000000008298a000 2019-03-22 05:32:17 UTC+0000
0x000000013e9b0060 wmpnetwk.exe       2628    476 0x000000008f14000 2019-03-22 05:32:18 UTC+0000
0x000000013ea59060 wininit.exe         380    324 0x000000009ef8a000 2019-03-22 05:31:58 UTC+0000
0x000000013ea5a9e0 csrss.exe           372    364 0x000000009f383000 2019-03-22 05:31:58 UTC+0000
0x000000013ea68b30 winlogon.exe        416    364 0x000000009e209000 2019-03-22 05:31:58 UTC+0000
0x000000013eaf0060 chrome.exe         2100   3248 0x000000002a0a4000 2019-03-22 05:35:15 UTC+0000
0x000000013eaf0710 OfficeC2RClien     3612   1292 0x000000003e049000 2019-03-22 05:37:07 UTC+0000   2019-03-22 05:37:26 UTC+0000
0x000000013eb00b30 chrome.exe         4156   3248 0x000000001eae6000 2019-03-22 05:35:17 UTC+0000
0x000000013eb306f0 chrome.exe         1816   3248 0x0000000028d98000 2019-03-22 05:35:16 UTC+0000
0x000000013ebcbb30 chrome.exe         4688   3248 0x0000000133480000 2019-03-22 05:35:19 UTC+0000
0x000000013ebd3060 POWERPNT.EXE       4048   1432 0x0000000025a00000 2019-03-22 05:35:09 UTC+0000
0x000000013ebf83e0 EXCEL.EXE          1272   1432 0x00000000a985a000 2019-03-22 05:33:49 UTC+0000
0x000000013ec546b0 csrss.exe           332    324 0x000000009f644000 2019-03-22 05:31:58 UTC+0000
0x000000013f505620 hfs.exe            3952   1432 0x000000000364bc000 2019-03-22 05:34:51 UTC+0000
0x000000013f616040 smss.exe            252      4 0x00000000a8495000 2019-03-22 05:31:55 UTC+0000
0x000000013f74c060 OUTLOOK.EXE        3688   1432 0x0000000004251a000 2019-03-22 05:34:37 UTC+0000
0x000000013f74fb30 taskmgr.exe        3792   1432 0x0000000041304000 2019-03-22 05:34:38 UTC+0000
0x000000013f798320 calc.exe           3548   1432 0x000000003d5f0000 2019-03-22 05:34:43 UTC+0000
0x000000013f7beb30 chrome.exe         3244   3248 0x000000002e722000 2019-03-22 05:35:15 UTC+0000
0x000000013f7cb060 iexplore.exe       3576    592 0x000000003a8ea000 2019-03-22 05:34:48 UTC+0000
0x000000013f7e9540 iexplore.exe       2780   3576 0x0000000038bd0000 2019-03-22 05:34:48 UTC+0000
0x000000013faaa430 cmd.exe            1408   1432 0x0000000006b9bb000 2019-03-22 05:34:12 UTC+0000
0x000000013faab620 conhost.exe        1008    372 0x0000000064122000 2019-03-22 05:34:12 UTC+0000
0x000000013fadbb30 chrome.exe         3248   1432 0x000000002ea4b000 2019-03-22 05:35:14 UTC+0000
0x000000013fb00620 taskeng.exe        1156    820 0x0000000064267000 2019-03-22 05:34:14 UTC+0000
0x000000013fb2f060 svchost.exe        3300    476 0x0000000006301f000 2019-03-22 05:34:15 UTC+0000
0x000000013fb30b30 sppsvc.exe         3260    476 0x000000006630da000 2019-03-22 05:34:15 UTC+0000
0x000000013fc83880 FTK Imager.exe     3192   1432 0x0000000030bb2000 2019-03-22 05:35:12 UTC+0000
```

***Volatility with netscan:***



```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ volatility_2.6_lin64_standalone -f Tziage-Memory.mem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State          Pid      Owner          Created
0x13e057300        UDPv4    10.0.0.101:55736               *:*                                 2888     svchost.exe    2019-03-22 05:32:20 UTC+0000
0x13e05b4f0        UDPv6    ::1:55735                      *:*                                 2888     svchost.exe    2019-03-22 05:32:20 UTC+0000
0x13e05b790        UDPv6    fe80::7475:ef30:be18:7807:55734 *:*                                 2888     svchost.exe    2019-03-22 05:32:20 UTC+0000
0x13e05d4b0        UDPv6    fe80::7475:ef30:be18:7807:1900 *:*                                  2888     svchost.exe    2019-03-22 05:32:20 UTC+0000
0x13e05dec0        UDPv4    127.0.0.1:55737                *:*                                 2888     svchost.exe    2019-03-22 05:32:20 UTC+0000
0x13e05e3f0        UDPv4    10.0.0.101:1900                *:*                                 2888     svchost.exe    2019-03-22 05:32:20 UTC+0000
0x13e05eab0        UDPv6    ::1:1900                       *:*                                 2888     svchost.exe    2019-03-22 05:32:20 UTC+0000
0x13e064d70        UDPv4    127.0.0.1:1900                 *:*                                 2888     svchost.exe    2019-03-22 05:32:20 UTC+0000
0x13e02bcf0        TCPv4    -:49220                        72.51.60.132:443     CLOSED         4048     POWERPNT.EXE
0x13e035790        TCPv4    -:49223                        72.51.60.132:443     CLOSED         4048     POWERPNT.EXE
0x13e036470        TCPv4    -:49224                        72.51.60.132:443     CLOSED         4048     POWERPNT.EXE
0x13e258010        UDPv4    127.0.0.1:55560                *:*                                 5116     wscript.exe    2019-03-22 05:35:32 UTC+0000
0x13e305a50        UDPv4    0.0.0.0:5355                   *:*                                 232      svchost.exe    2019-03-22 05:32:09 UTC+0000
0x13e360be0        UDPv4    0.0.0.0:63790                  *:*                                 504                     2019-03-22 05:45:47 UTC+0000
0x13e490ec0        UDPv4    0.0.0.0:5355                   *:*                                 232      svchost.exe    2019-03-22 05:32:09 UTC+0000
0x13e490ec0        UDPv6    :::5355                        *:*                                 232      svchost.exe    2019-03-22 05:32:09 UTC+0000
0x13e5683e0        UDPv4    10.0.0.101:137                 *:*                                 4        System         2019-03-22 05:32:06 UTC+0000
0x13e594250        UDPv4    10.0.0.101:138                 *:*                                 4        System         2019-03-22 05:32:06 UTC+0000
0x13e597ec0        UDPv4    0.0.0.0:0                      *:*                                 232      svchost.exe    2019-03-22 05:32:06 UTC+0000
0x13e597ec0        UDPv6    :::0                           *:*                                 232      svchost.exe    2019-03-22 05:32:06 UTC+0000
0x13e61fb30        UDPv6    fe80::7475:ef30:be18:7807:546  *:*                                 764      svchost.exe    2019-03-22 05:46:23 UTC+0000
0x13e918010        UDPv4    0.0.0.0:56372                  *:*                                 1816     chrome.exe     2019-03-22 05:45:51 UTC+0000
0x13e9cd730        UDPv4    127.0.0.1:57374                *:*                                 1136     OfficeClickToR 2019-03-22 05:32:18 UTC+0000
0x13ea8e6a0        UDPv4    127.0.0.1:61704                *:*                                 3688     OUTLOOK.EXE    2019-03-22 05:34:44 UTC+0000
0x13ead0bf0        UDPv4    127.0.0.1:55614                *:*                                 4048     POWERPNT.EXE   2019-03-22 05:35:15 UTC+0000
0x13ebc6c20        UDPv4    0.0.0.0:5353                   *:*                                 3248     chrome.exe     2019-03-22 05:35:17 UTC+0000
0x13ebea890        UDPv4    0.0.0.0:5353                   *:*                                 3248     chrome.exe     2019-03-22 05:35:17 UTC+0000
0x13ebea890        UDPv6    :::5353                        *:*                                 3248     chrome.exe     2019-03-22 05:35:17 UTC+0000
0x13e2c6b10        TCPv4    0.0.0.0:21                     0.0.0.0:0            LISTENING      1476     FileZilla Serv
0x13e2c6b10        TCPv6    :::21                          :::0                 LISTENING      1476     FileZilla Serv
0x13e2c7850        TCPv6    ::1:14147                      :::0                 LISTENING      1476     FileZilla Serv
0x13e2c96b0        TCPv4    127.0.0.1:14147                0.0.0.0:0            LISTENING      1476     FileZilla Serv
0x13e2c9be0        TCPv4    0.0.0.0:21                     0.0.0.0:0            LISTENING      1476     FileZilla Serv
0x13e3a1150        TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING      484      lsass.exe
0x13e3a1150        TCPv6    :::49155                       :::0                 LISTENING      484      lsass.exe
0x13e3b2010        TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING      484      lsass.exe
0x13e430580        TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING      820      svchost.exe
0x13e430580        TCPv6    :::49154                       :::0                 LISTENING      820      svchost.exe
0x13e431820        TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING      820      svchost.exe
0x13e57e010        TCPv4    10.0.0.101:139                 0.0.0.0:0            LISTENING      4        System
0x13e71cef0        TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING      672      svchost.exe
0x13e720660        TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING      672      svchost.exe
0x13e720660        TCPv6    :::135                         :::0                 LISTENING      672      svchost.exe
0x13e72f010        TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING      380      wininit.exe
0x13e72f6e0        TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING      380      wininit.exe
0x13e72f6e0        TCPv6    :::49152                       :::0                 LISTENING      380      wininit.exe
0x13e770240        TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING      764      svchost.exe
0x13e772980        TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING      764      svchost.exe
0x13e772980        TCPv6    :::49153                       :::0                 LISTENING      764      svchost.exe
0x13ebb3010        TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING      476      services.exe
0x13ebb3010        TCPv6    :::49156                       :::0                 LISTENING      476      services.exe
0x13ebcdef0        TCPv4    0.0.0.0:80                     0.0.0.0:0            LISTENING      3952     hfs.exe
0x13e2348a8        TCPv4    -:49366                        192.168.206.181:389  CLOSED         504
0x13e397190        TCPv4    10.0.0.101:49217               10.0.0.106:4444      ESTABLISHED    5496     UWkpjFjDzM.exe
0x13e3986d0        TCPv4    -:49378                        213.209.1.129:25     CLOSED         504
0x13e3abae0        TCPv4    -:49226                        72.51.60.132:443     CLOSED         4048     POWERPNT.EXE
0x13e3e7010        TCPv6    -:0                            38db:7705:80fa:ffff:38db:7705:80fa:ffff:0 CLOSED          1136     OfficeClickToR
0x13e441830        TCPv6    -:0                            382b:c703:80fa:ffff:382b:c703:80fa:ffff:0 CLOSED          1        ?RK????
0x13e4e4910        TCPv4    10.0.0.101:49208               52.109.12.6:443      CLOSED         504
0x13e55fae0        TCPv4    10.0.0.101:49209               52.96.44.162:443     CLOSED         504
0x13e71b540        TCPv4    -:0                            184.208.112.5:0      CLOSED         1        ?RK????
0x13e73b560        TCPv4    -:49266                        35.190.69.156:443    CLOSED         504
0x13e7c6010        TCPv4    10.0.0.101:49204               172.217.6.195:443    CLOSED         1816     chrome.exe
0x13ead7cf0        TCPv4    10.0.0.101:49202               172.217.10.68:443    CLOSED         1816     chrome.exe
0x13f5898a0        TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING      476      services.exe
0x13f5899c0        TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING      4        System
0x13f5899c0        TCPv6    :::445                         :::0                 LISTENING      4        System
0x13f4facf0        TCPv4    10.0.0.101:49262               52.109.12.6:443      ESTABLISHED    3688     OUTLOOK.EXE
0x13f50a010        TCPv4    -:49265                        213.186.33.3:443     CLOSED         504
0x13f5289f0        TCPv4    -:49234                        72.51.60.133:80      CLOSED         3688     OUTLOOK.EXE
0x13f7b4ec0        UDPv4    0.0.0.0:55707                  *:*                                 232      svchost.exe    2019-03-22 05:45:44 UTC+0000
0x13f7e8670        UDPv4    127.0.0.1:59411                *:*                                 3576     iexplore.exe   2019-03-22 05:34:49 UTC+0000
0x13fc6f1b0        UDPv4    0.0.0.0:55102                  *:*                                 232      svchost.exe    2019-03-22 05:45:36 UTC+0000
0x13fc78dc0        UDPv4    127.0.0.1:53361                *:*                                 1272     EXCEL.EXE      2019-03-22 05:34:03 UTC+0000
0x13f7ae010        TCPv4    10.0.0.101:49263               52.96.44.162:443     ESTABLISHED    3688     OUTLOOK.EXE
0x13fa93cf0        TCPv4    -:49173                        72.51.60.132:443     CLOSED         1272     EXCEL.EXE
0x13fa95cf0        TCPv4    -:49170                        72.51.60.132:443     CLOSED         1272     EXCEL.EXE
0x13fa969f0        TCPv4    -:0                            56.219.119.5:0       CLOSED         1272     EXCEL.EXE
0x13fbd87e0        TCPv4    -:49372                        212.227.15.9:25      CLOSED         504
0x13fc857e0        TCPv4    -:49167                        72.51.60.132:443     CLOSED         1272     EXCEL.EXE
```

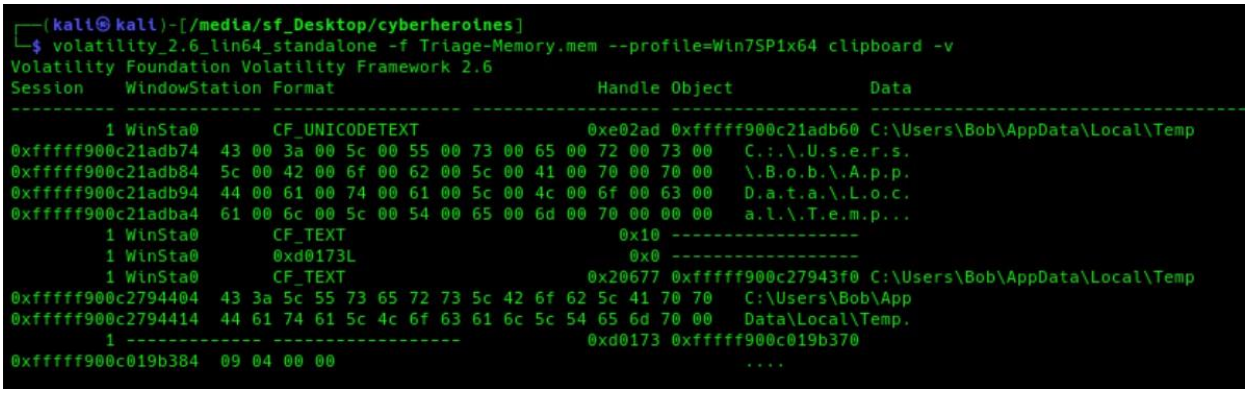
- Purpose: Analyzes network-related information in memory dumps.
- Functions: Identifies active network connections, listening ports, associated processes, and connection states.
- Use Case: Valuable for investigating network activity on compromised systems and understanding security incidents.

***Volatility with hashdump:***

- Purpose: Extracts password hashes from memory dumps.
- Functions: Retrieves hashed passwords stored in memory, which can be used for offline password cracking.
- Use Case: Useful for recovering passwords and assessing the security of a system.


***Volatility with clipboard Plugin:***

- Purpose: Captures data from the system's clipboard.
- Functions: Extracts text or other data that users have copied to the clipboard.
- Use Case: Helps gather potentially sensitive information that users have interacted with on the system.




***Volatility with cmdline:***

- Purpose: Retrieves information about executed command-line commands.
- Functions: Collects a history of executed commands and associated processes.
- Use Case: Aids in understanding the actions and operations performed on the system.

***Volatility with vadinfo:***

Purpose: Provides details about Virtual Address Descriptors (VADs) in memory.

Functions: Offers information on memory regions, permissions, and usage.

Use Case: Helps in memory analysis, identifying memory-mapped files, and understanding memory layout.

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ volatility_2.6_lin64_standalone -f Triage-Memory.mem --profile=Win7SP1x64 vadinfo -p 3496 | head -n 100
Volatility Foundation Volatility Framework 2.6
**********************************************************************
Pid:   3496
VAD node @ 0xfffffa8005af78f0 Start 0x0000000068540000 End 0x0000000068597fff Tag Vad
Flags: CommitCharge: 2, Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @fffffa80042849b0 Segment fffff8a0029ba990
NumberOfSectionReferences:          0 NumberOfPfnReferences:          49
NumberOfMappedViews:                4 NumberOfUserReferences:          4
Control Flags: Accessed: 1, File: 1, Image: 1
FileObject @fffffa8005bdf260, Name: \Device\HarddiskVolume2\Windows\SysWOW64\winhttp.dll
First prototype PTE: fffff8a0029ba9d8 Last contiguous PTE: fffffffffffffffc
Flags2: Inherit: 1

VAD node @ 0xfffffa8005a19b00 Start 0x0000000002150000 End 0x000000000218ffff Tag VadS
Flags: CommitCharge: 1, PrivateMemory: 1, Protection: 4
Protection: PAGE_READWRITE
Vad Type: VadNone

VAD node @ 0xfffffa8005c18dc0 Start 0x0000000000400000 End 0x0000000000415fff Tag Vad
Flags: CommitCharge: 9, Protection: 7, VadType: 2
Protection: PAGE_EXECUTE_WRITECOPY
Vad Type: VadImageMap
ControlArea @fffffa8005b55ba0 Segment fffff8a003e11070
NumberOfSectionReferences:          1 NumberOfPfnReferences:          15
NumberOfMappedViews:                1 NumberOfUserReferences:          2
Control Flags: Accessed: 1, File: 1, Image: 1
FileObject @fffffa8005a55f20, Name: \Device\HarddiskVolume2\Users\Bob\AppData\Local\Temp\rad93398.tmp\UWkpjFjDzM.exe
First prototype PTE: fffff8a003e110b8 Last contiguous PTE: fffffffffffffffc
Flags2: Inherit: 1
```

**VAD node address:** This is the address of the VAD node in memory, which uniquely identifies it.

**Start and End Addresses:** The VAD covers the virtual memory address range from 0x0000000000400000 to 0x0000000000415fff. This is a relatively small memory range.

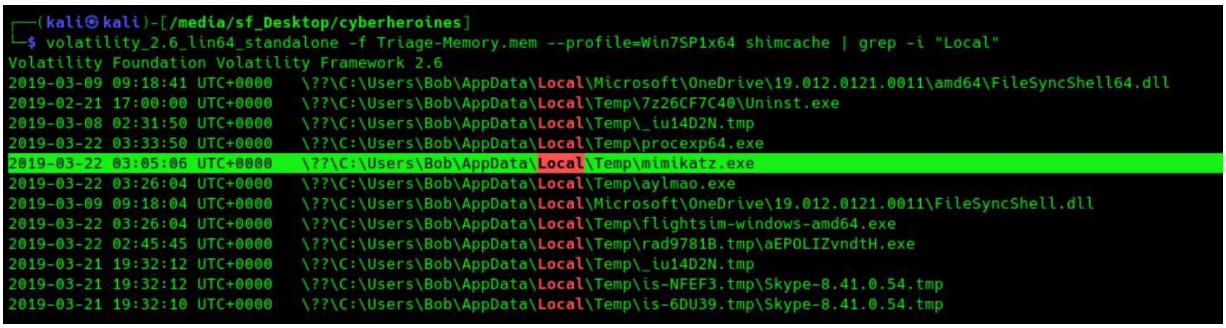
**Tag Vad:** The "Tag" field specifies that this is a standard VAD.

**Flags:** CommitCharge: 9: The CommitCharge value of 9 indicates that this VAD has a relatively low commitment of virtual memory. This means that a small amount of virtual memory has been committed for this region.

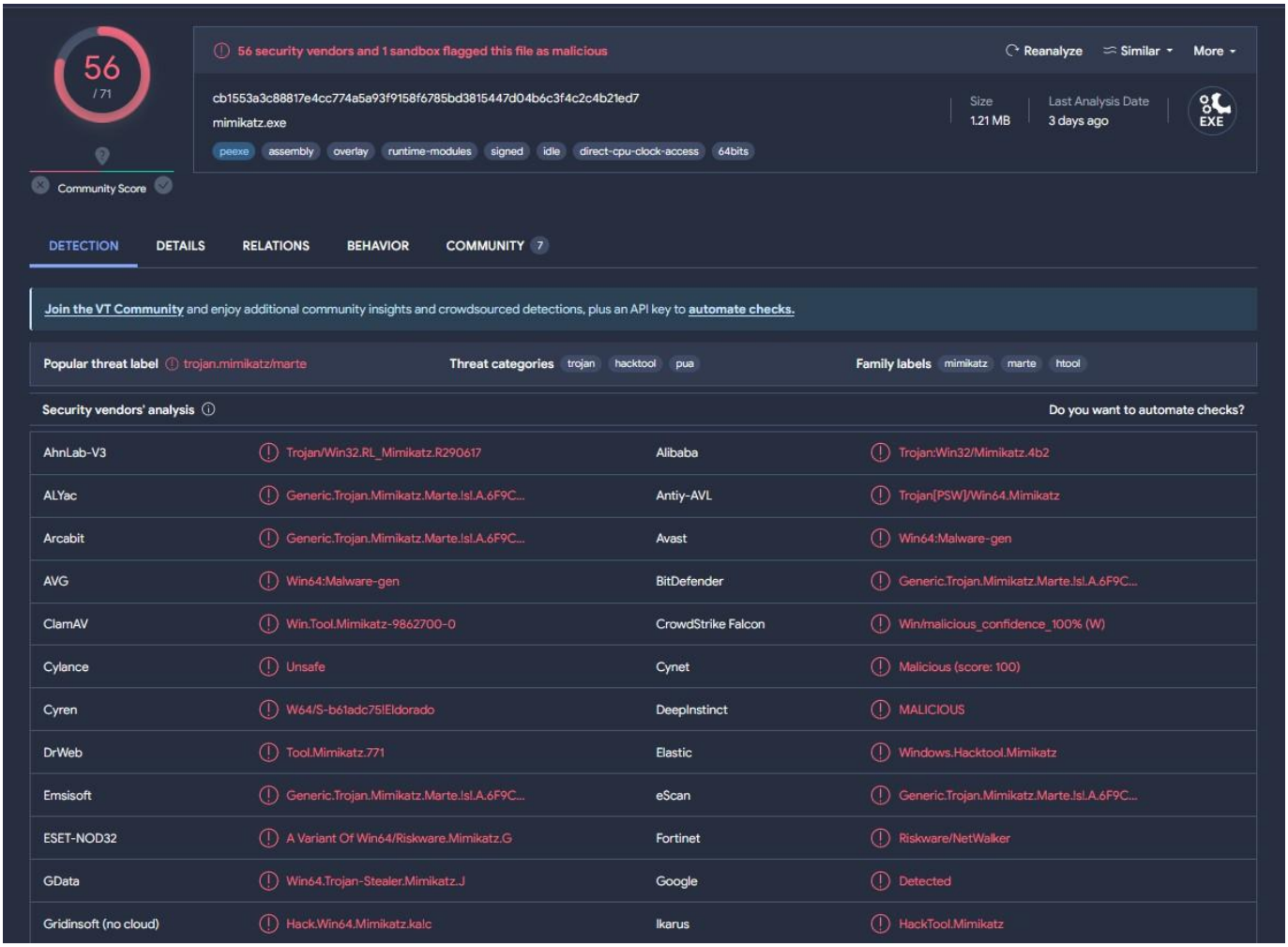
**Protection**: PAGE_EXECUTE_WRITECOPY: The Protection field indicates that this memory region is executable and writeable. This combination can be used for self-modifying code, which is not uncommon in legitimate applications. However, it can also be used by malware to modify its code at runtime.

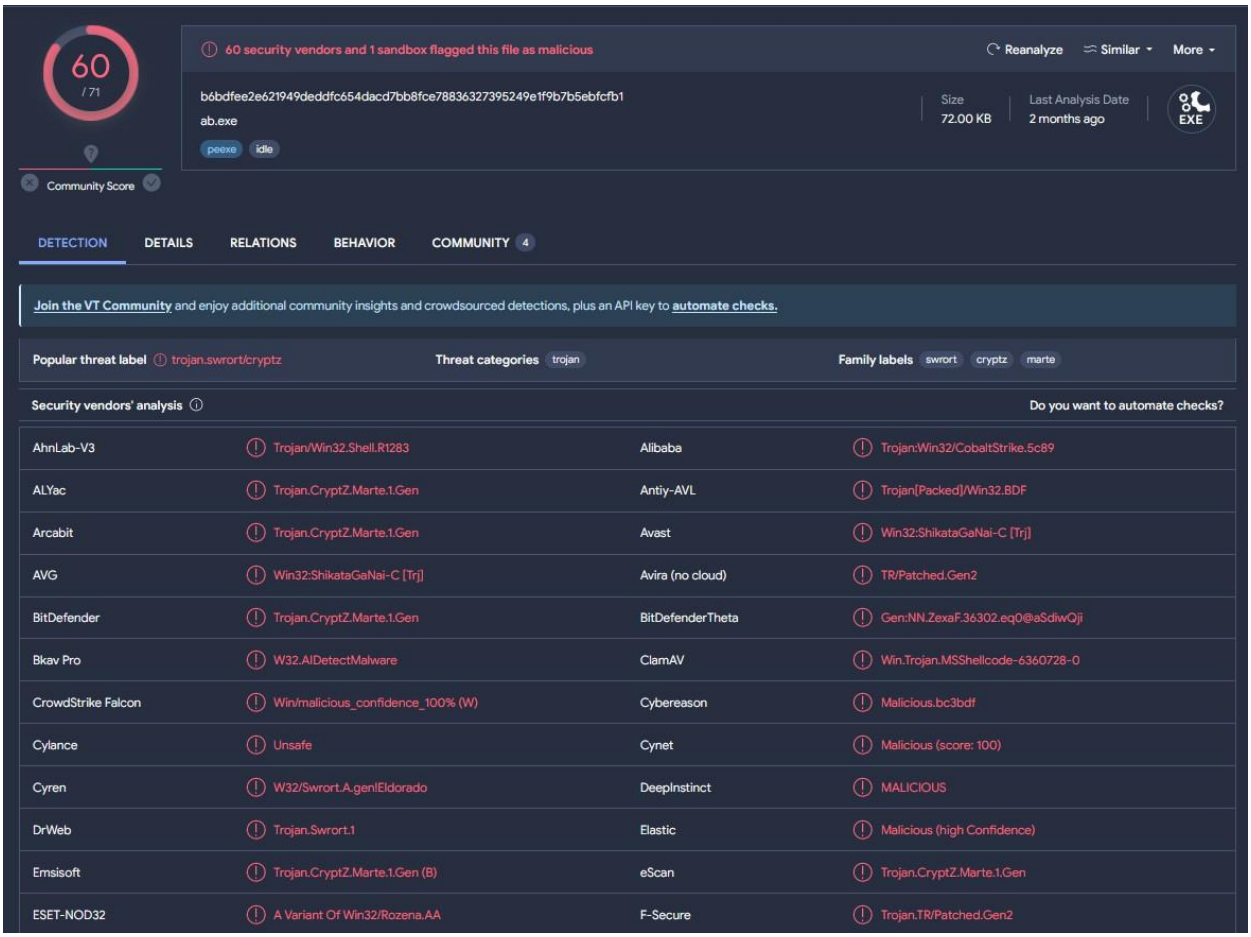
***Volatility with shimcache:***

- Purpose: Shimcache, short for "Application Compatibility Cache," is a Windows OS feature designed to improve application compatibility.
- Functions: It records information about executed programs and libraries, storing it in a cache. This includes timestamps, paths, and other execution details.
- Use Case: Shimcache is used to help older applications run smoothly on newer Windows versions by identifying compatibility issues and applying compatibility fixes. It is valuable in forensic analysis for tracking program execution and potentially identifying suspicious or malicious activity.



***Analyzing the dumped process with Virus total:***






***Extracting the notepad process dump using volatility – 2:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ volatility_2.6_lin64_standalone -f Triage-Memory.mem --profile=Win7SP1x64 procdump -p3032 --dump-dir dumps/
Volatility Foundation Volatility Framework 2.6
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
0xfffffa80054f9060 0x00000000ff6b0000 notepad.exe          OK: executable.3032.exe
```

***Using strings to extract any valuable information from the notepad process:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines/dumps]
└─$ strings executable.3032.exe
!This program cannot be run in DOS mode.
\zRich
.text
`.rdata
@.data
.pdata
@.rsrc
@.reloc
ADVAPI32.dll
KERNEL32.dll
NTDLL.DLL
GDI32.dll
USER32.dll
msvcrt.dll
COMDLG32.dll
SHELL32.dll
WINSPOOL.DRV
ole32.dll
SHLWAPI.dll
COMCTL32.dll
OLEAUT32.dll
VERSION.dll
d$0L
L$@E3
```

***Dumping the memory of the notepad process:***

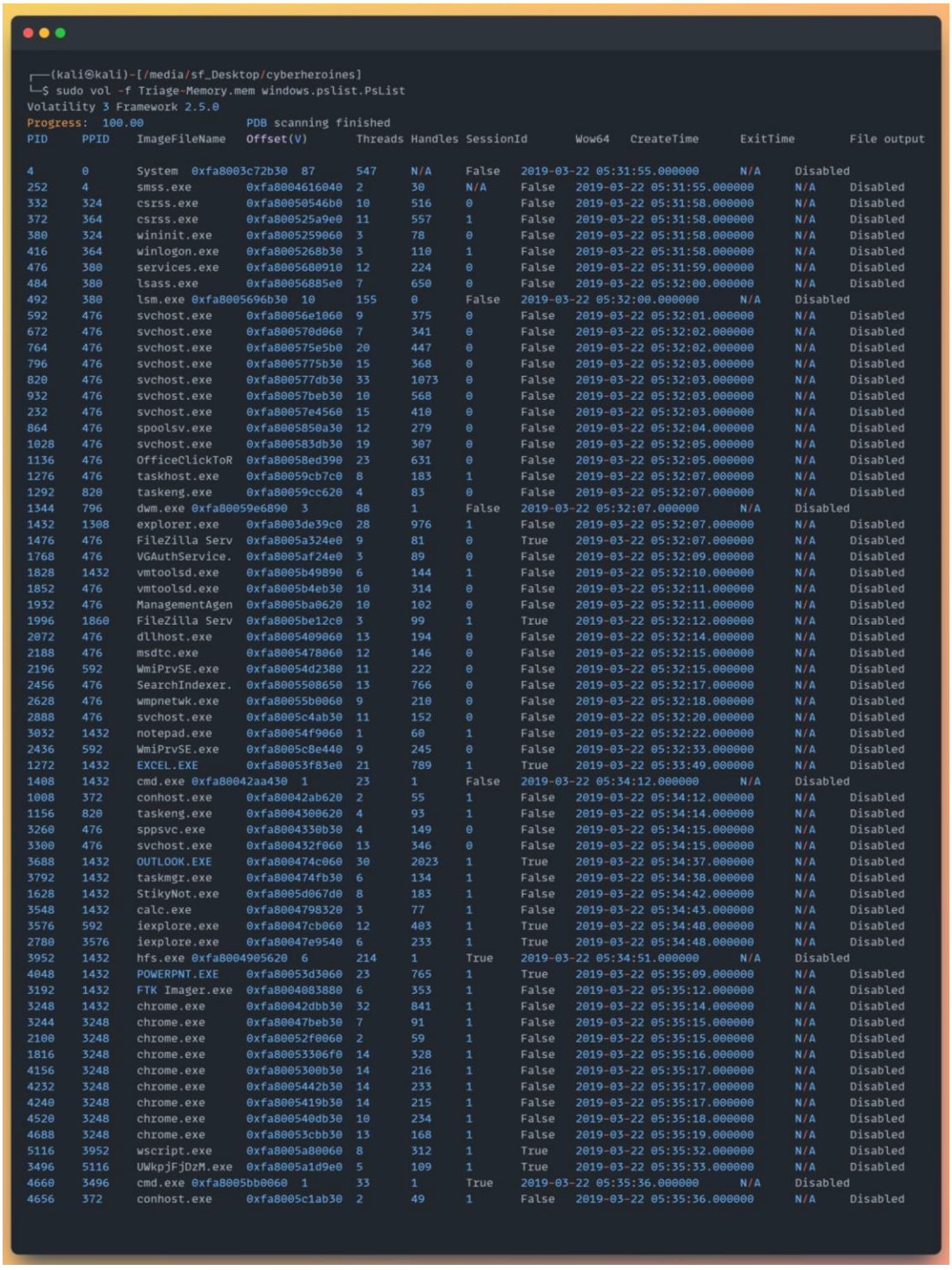
```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ volatility_2.6_lin64_standalone -f Triage-Memory.mem --profile=Win7SP1x64 memdump -p 3032 -D dumps/
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing notepad.exe [  3032] to 3032.dmp
```

***Using strings to find any data from the notepad memory dump:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines/dumps]
└─$ strings -e l 3032.dmp | grep -i "Flag" | head -n 25
flag<REDBULL_IS_LIFE>
AppCompatFlags\Layers
ShutdownFlags
TracingFlags
VerifierFlags
PageHeapFlags
\Registry\Machine\Software\Microsoft\Windows nt\currentversion\appcompatflags\AIT
dwFlags
dwFlags
  dwFlags: 0x%x
Allow flag to be passed with CreateFile call that indicates to perform downgrade if applicable.
FFlags
RpcVerifierFlags
thread_flags
activation_flags
thread_flags
activation_flags
flags
flags
ResourceCheckFlags
TimerCheckFlags
PoCleanShutdownFlags
GlobalFlag
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags
FLAG_INSTALL
```

# Analyzing the Triage-Memory dump with Volatility – 3

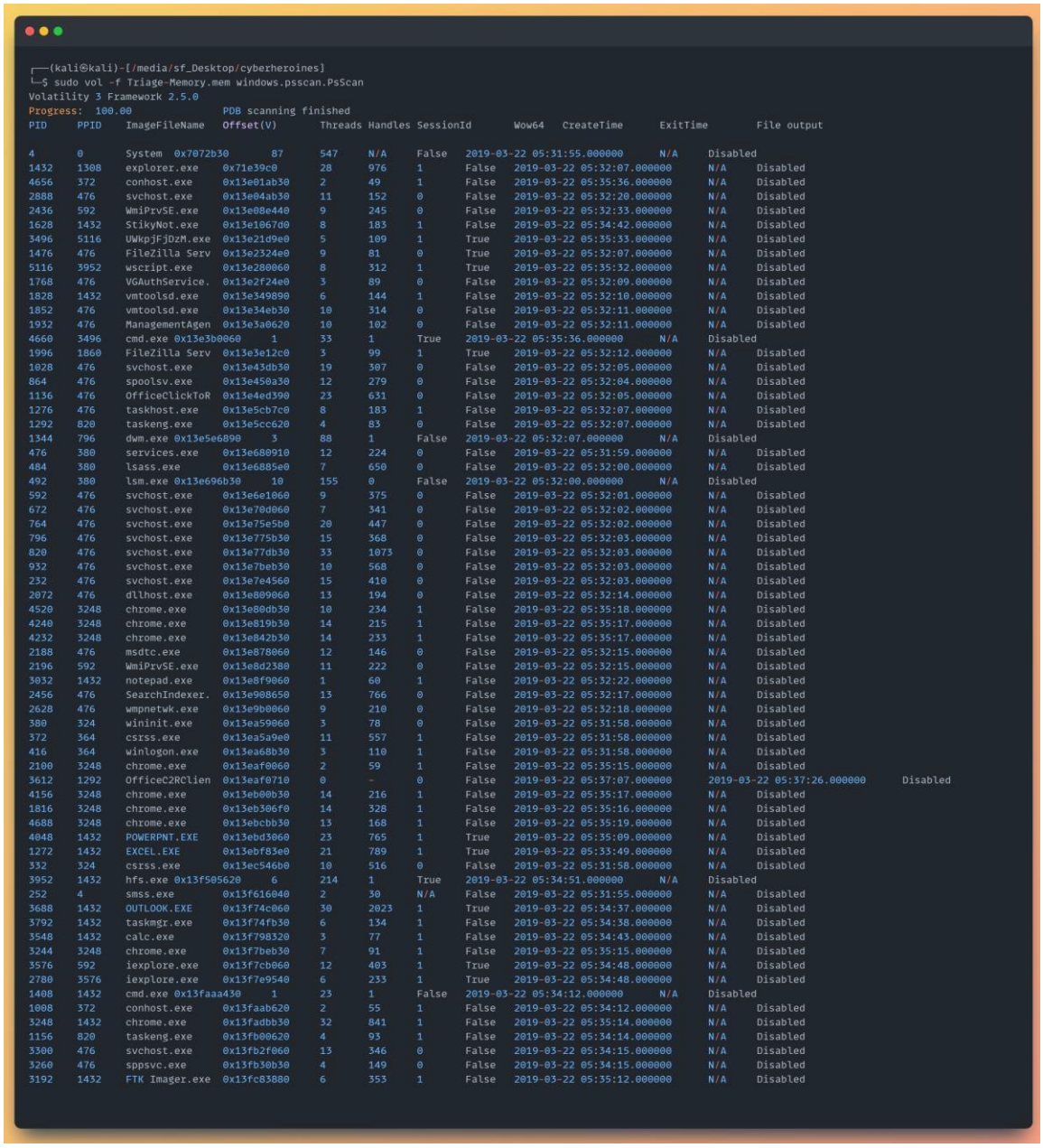
***Volatility – 3 with pslist:***



```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Triage-Memory.mem windows.pslist.PsList
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xfa8003c72b30  87      547     N/A     False   2019-03-22 05:31:55.000000      N/A     Disabled
252     4       smss.exe        0xfa8004616040  2       30      N/A     False   2019-03-22 05:31:55.000000      N/A     Disabled
332     324     csrss.exe       0xfa80050546b0  10      516     0       False   2019-03-22 05:31:58.000000      N/A     Disabled
372     364     csrss.exe       0xfa800525a9e0  11      557     1       False   2019-03-22 05:31:58.000000      N/A     Disabled
380     324     wininit.exe     0xfa8005259060  3       78      0       False   2019-03-22 05:31:58.000000      N/A     Disabled
416     364     winlogon.exe    0xfa8005268b30  3       110     1       False   2019-03-22 05:31:58.000000      N/A     Disabled
476     380     services.exe    0xfa8005680910  12      224     0       False   2019-03-22 05:31:59.000000      N/A     Disabled
484     380     lsass.exe       0xfa80056885e0  7       650     0       False   2019-03-22 05:32:00.000000      N/A     Disabled
492     380     lsm.exe 0xfa8005696b30  10      155     0       False   2019-03-22 05:32:00.000000      N/A     Disabled
592     476     svchost.exe     0xfa80056e1060  9       375     0       False   2019-03-22 05:32:01.000000      N/A     Disabled
672     476     svchost.exe     0xfa800570d060  7       341     0       False   2019-03-22 05:32:02.000000      N/A     Disabled
764     476     svchost.exe     0xfa800575e5b0  20      447     0       False   2019-03-22 05:32:02.000000      N/A     Disabled
796     476     svchost.exe     0xfa8005775b30  15      368     0       False   2019-03-22 05:32:03.000000      N/A     Disabled
820     476     svchost.exe     0xfa800577db30  33      1073    0       False   2019-03-22 05:32:03.000000      N/A     Disabled
932     476     svchost.exe     0xfa80057beb30  10      568     0       False   2019-03-22 05:32:03.000000      N/A     Disabled
232     476     svchost.exe     0xfa80057e4560  15      410     0       False   2019-03-22 05:32:03.000000      N/A     Disabled
864     476     spoolsv.exe     0xfa8005850a30  12      279     0       False   2019-03-22 05:32:04.000000      N/A     Disabled
1028    476     svchost.exe     0xfa800583db30  19      307     0       False   2019-03-22 05:32:05.000000      N/A     Disabled
1136    476     OfficeClickToR  0xfa80058ed390  23      631     0       False   2019-03-22 05:32:05.000000      N/A     Disabled
1276    476     taskhost.exe    0xfa80059cb7c0  8       183     1       False   2019-03-22 05:32:07.000000      N/A     Disabled
1292    820     taskeng.exe     0xfa80059cc620  4       83      0       False   2019-03-22 05:32:07.000000      N/A     Disabled
1344    796     dwm.exe 0xfa80059e6890  3       88      1       False   2019-03-22 05:32:07.000000      N/A     Disabled
1432    1308    explorer.exe    0xfa8003de39c0  28      976     1       False   2019-03-22 05:32:07.000000      N/A     Disabled
1476    476     FileZilla Serv  0xfa8005a324e0  9       81      0       True    2019-03-22 05:32:07.000000      N/A     Disabled
1768    476     VGAuthService.  0xfa8005af24e0  3       89      0       False   2019-03-22 05:32:09.000000      N/A     Disabled
1828    1432    vmtoolsd.exe    0xfa8005b49890  6       144     1       False   2019-03-22 05:32:10.000000      N/A     Disabled
1852    476     vmtoolsd.exe    0xfa8005b4eb30  10      314     0       False   2019-03-22 05:32:11.000000      N/A     Disabled
1932    476     ManagementAgen  0xfa8005ba0620  10      102     0       False   2019-03-22 05:32:11.000000      N/A     Disabled
1996    1860    FileZilla Serv  0xfa8005be12c0  3       99      1       True    2019-03-22 05:32:12.000000      N/A     Disabled
2072    476     dllhost.exe     0xfa8005409060  13      194     0       False   2019-03-22 05:32:14.000000      N/A     Disabled
2188    476     msdtc.exe       0xfa8005478060  12      146     0       False   2019-03-22 05:32:15.000000      N/A     Disabled
2196    592     WmiPrvSE.exe    0xfa80054d2380  11      222     0       False   2019-03-22 05:32:15.000000      N/A     Disabled
2456    476     SearchIndexer.  0xfa8005508650  13      766     0       False   2019-03-22 05:32:17.000000      N/A     Disabled
2628    476     wmpnetwk.exe    0xfa80055b0060  9       210     0       False   2019-03-22 05:32:18.000000      N/A     Disabled
2888    476     svchost.exe     0xfa8005c4ab30  11      152     0       False   2019-03-22 05:32:20.000000      N/A     Disabled
3032    1432    notepad.exe     0xfa80054f9060  1       60      1       False   2019-03-22 05:32:22.000000      N/A     Disabled
2436    592     WmiPrvSE.exe    0xfa8005c8e440  9       245     0       False   2019-03-22 05:32:33.000000      N/A     Disabled
1272    1432    EXCEL.EXE       0xfa80053f83e0  21      789     1       True    2019-03-22 05:33:49.000000      N/A     Disabled
1408    1432    cmd.exe 0xfa80042aa430  1       23      1       False   2019-03-22 05:34:12.000000      N/A     Disabled
1008    372     conhost.exe     0xfa80042ab620  2       55      1       False   2019-03-22 05:34:12.000000      N/A     Disabled
1156    820     taskeng.exe     0xfa8004300620  4       93      1       False   2019-03-22 05:34:14.000000      N/A     Disabled
3260    476     sppsvc.exe      0xfa8004330b30  4       149     0       False   2019-03-22 05:34:15.000000      N/A     Disabled
3300    476     svchost.exe     0xfa800432f060  13      346     0       False   2019-03-22 05:34:15.000000      N/A     Disabled
3688    1432    OUTLOOK.EXE     0xfa800474c060  30      2023    1       True    2019-03-22 05:34:37.000000      N/A     Disabled
3792    1432    taskmgr.exe     0xfa800474fb30  6       134     1       False   2019-03-22 05:34:38.000000      N/A     Disabled
1628    1432    StikyNot.exe    0xfa8005d067d0  8       183     1       False   2019-03-22 05:34:42.000000      N/A     Disabled
3548    1432    calc.exe        0xfa800479b320  3       77      1       False   2019-03-22 05:34:43.000000      N/A     Disabled
3576    592     iexplore.exe    0xfa80047cb060  12      403     1       True    2019-03-22 05:34:48.000000      N/A     Disabled
2780    3576    iexplore.exe    0xfa80047e9540  6       233     1       True    2019-03-22 05:34:48.000000      N/A     Disabled
3952    1432    hfs.exe 0xfa8004905620  6       214     1       True    2019-03-22 05:34:51.000000      N/A     Disabled
4048    1432    POWERPNT.EXE    0xfa80053d3060  23      765     1       True    2019-03-22 05:35:09.000000      N/A     Disabled
3192    1432    FTK Imager.exe  0xfa8004083880  6       353     1       False   2019-03-22 05:35:12.000000      N/A     Disabled
3248    1432    chrome.exe      0xfa80042dbb30  32      841     1       False   2019-03-22 05:35:14.000000      N/A     Disabled
3244    3248    chrome.exe      0xfa80047beb30  7       91      1       False   2019-03-22 05:35:15.000000      N/A     Disabled
2100    3248    chrome.exe      0xfa80052f0060  2       59      1       False   2019-03-22 05:35:15.000000      N/A     Disabled
1816    3248    chrome.exe      0xfa80053306f0  14      328     1       False   2019-03-22 05:35:16.000000      N/A     Disabled
4156    3248    chrome.exe      0xfa8005300b30  14      216     1       False   2019-03-22 05:35:17.000000      N/A     Disabled
4232    3248    chrome.exe      0xfa8005442b30  14      233     1       False   2019-03-22 05:35:17.000000      N/A     Disabled
4240    3248    chrome.exe      0xfa8005419b30  14      215     1       False   2019-03-22 05:35:17.000000      N/A     Disabled
4520    3248    chrome.exe      0xfa800540db30  10      234     1       False   2019-03-22 05:35:18.000000      N/A     Disabled
4688    3248    chrome.exe      0xfa80053cbb30  13      168     1       False   2019-03-22 05:35:19.000000      N/A     Disabled
5116    3952    wscript.exe     0xfa8005a80060  8       312     1       True    2019-03-22 05:35:32.000000      N/A     Disabled
3496    5116    UWkpjFjDzM.exe  0xfa8005a1d9e0  5       109     1       True    2019-03-22 05:35:33.000000      N/A     Disabled
4660    3496    cmd.exe 0xfa8005bb0060  1       33      1       True    2019-03-22 05:35:36.000000      N/A     Disabled
4656    372     conhost.exe     0xfa8005c1ab30  2       49      1       False   2019-03-22 05:35:36.000000      N/A     Disabled
```

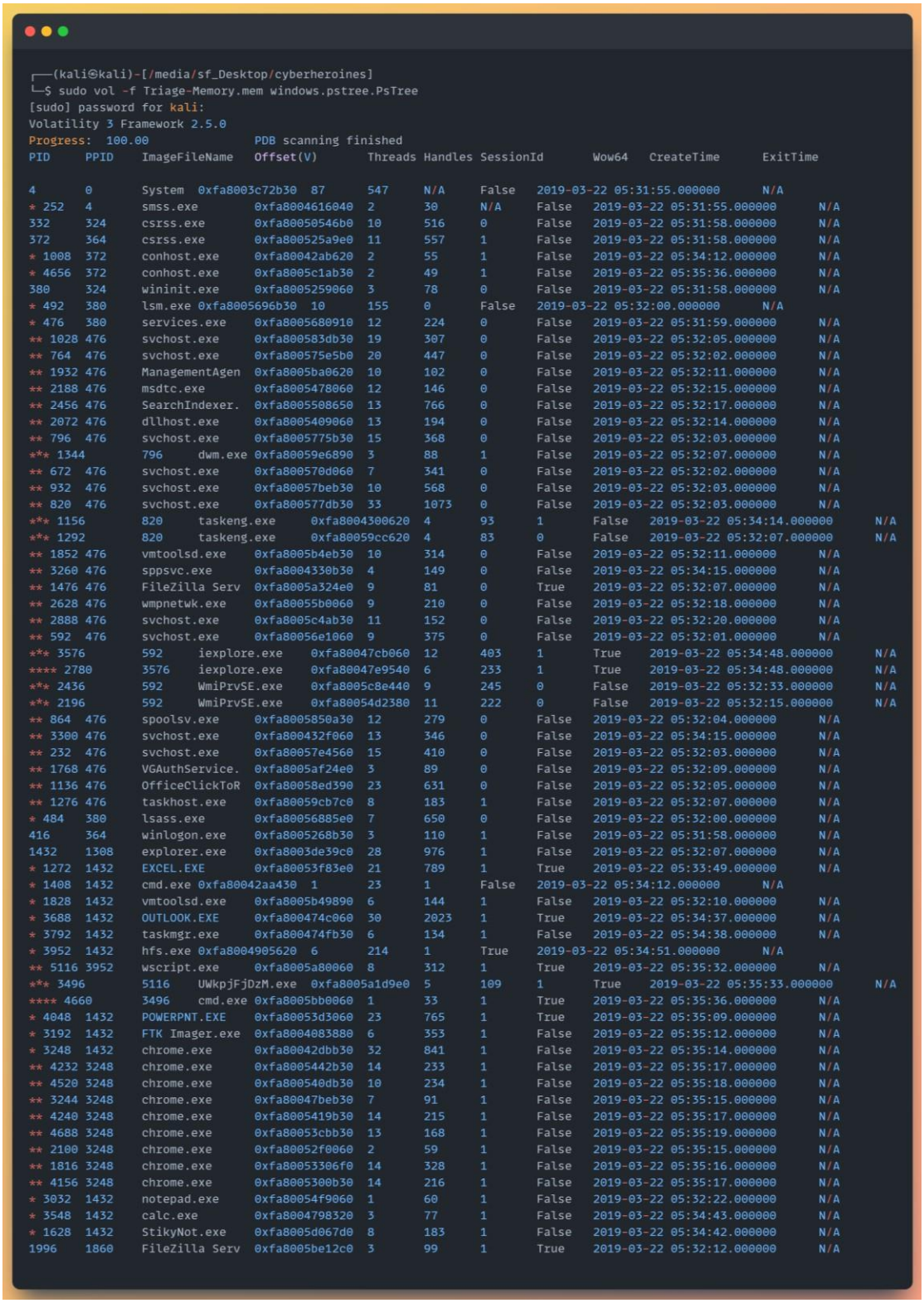
From the above process list, I find “UWkpjFjDzM.exe” process as malicious because of its suspicious file name. Furthermore, analysis is required to conclude it. Basically, the pslist is useful for quickly listing all processes in a straightforward manner. It's a starting point for process analysis and can help identify suspicious or unusual processes.

***Volatility – 3 with psscan:***



```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Triage-Memory.mem windows.psscan.PsScan
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x7072b30       87      547     N/A     False   2019-03-22 05:31:55.000000      N/A     Disabled
1432    1308    explorer.exe    0x71e39c0       28      976     1       False   2019-03-22 05:32:07.000000      N/A     Disabled
4656    372     conhost.exe     0x13e01ab30     2       49      1       False   2019-03-22 05:35:36.000000      N/A     Disabled
2888    476     svchost.exe     0x13e04ab30     11      152     0       False   2019-03-22 05:32:20.000000      N/A     Disabled
2436    592     WmiPrvSE.exe    0x13e08e440     9       245     0       False   2019-03-22 05:32:33.000000      N/A     Disabled
1628    1432    StikyNot.exe    0x13e1067d0     8       183     1       False   2019-03-22 05:34:42.000000      N/A     Disabled
3496    5116    UWkpjFjDzM.exe  0x13e21d9e0     5       109     1       True    2019-03-22 05:35:33.000000      N/A     Disabled
1476    476     FileZilla Serv  0x13e2324e0     9       81      0       True    2019-03-22 05:32:07.000000      N/A     Disabled
5116    3952    wscript.exe     0x13e280060     8       312     1       True    2019-03-22 05:35:32.000000      N/A     Disabled
1768    476     VGAuthService.  0x13e2f24e0     3       89      0       False   2019-03-22 05:32:09.000000      N/A     Disabled
1828    1432    vmtoolsd.exe    0x13e349890     6       144     1       False   2019-03-22 05:32:10.000000      N/A     Disabled
1852    476     vmtoolsd.exe    0x13e34eb30     10      314     0       False   2019-03-22 05:32:11.000000      N/A     Disabled
1932    476     ManagementAgen  0x13e3a0620     10      102     0       False   2019-03-22 05:32:11.000000      N/A     Disabled
4660    3496    cmd.exe 0x13e3b0060     1       33      1       True    2019-03-22 05:35:36.000000      N/A     Disabled
1996    1860    FileZilla Serv  0x13e3e12c0     3       99      1       True    2019-03-22 05:32:12.000000      N/A     Disabled
1028    476     svchost.exe     0x13e43db30     19      307     0       False   2019-03-22 05:32:05.000000      N/A     Disabled
864     476     spoolsv.exe     0x13e450a30     12      279     0       False   2019-03-22 05:32:04.000000      N/A     Disabled
1136    476     OfficeClickToR  0x13e4ed390     23      631     0       False   2019-03-22 05:32:05.000000      N/A     Disabled
1276    476     taskhost.exe    0x13e5cb7c0     8       183     1       False   2019-03-22 05:32:07.000000      N/A     Disabled
1292    820     taskeng.exe     0x13e5cc620     4       83      0       False   2019-03-22 05:32:07.000000      N/A     Disabled
1344    796     dwm.exe 0x13e5e6890     3       88      1       False   2019-03-22 05:32:07.000000      N/A     Disabled
476     380     services.exe    0x13e680910     12      224     0       False   2019-03-22 05:31:59.000000      N/A     Disabled
484     380     lsass.exe       0x13e6885e0     7       650     0       False   2019-03-22 05:32:00.000000      N/A     Disabled
492     380     lsm.exe 0x13e696b30     10      155     0       False   2019-03-22 05:32:00.000000      N/A     Disabled
592     476     svchost.exe     0x13e6e1060     9       375     0       False   2019-03-22 05:32:01.000000      N/A     Disabled
672     476     svchost.exe     0x13e70d060     7       341     0       False   2019-03-22 05:32:02.000000      N/A     Disabled
764     476     svchost.exe     0x13e75e5b0     20      447     0       False   2019-03-22 05:32:02.000000      N/A     Disabled
796     476     svchost.exe     0x13e775b30     15      368     0       False   2019-03-22 05:32:03.000000      N/A     Disabled
820     476     svchost.exe     0x13e77db30     33      1073    0       False   2019-03-22 05:32:03.000000      N/A     Disabled
932     476     svchost.exe     0x13e7beb30     10      568     0       False   2019-03-22 05:32:03.000000      N/A     Disabled
232     476     svchost.exe     0x13e7e4560     15      410     0       False   2019-03-22 05:32:03.000000      N/A     Disabled
2072    476     dllhost.exe     0x13e809060     13      194     0       False   2019-03-22 05:32:14.000000      N/A     Disabled
4520    3248    chrome.exe      0x13e80db30     10      234     1       False   2019-03-22 05:35:18.000000      N/A     Disabled
4240    3248    chrome.exe      0x13e819b30     14      215     1       False   2019-03-22 05:35:17.000000      N/A     Disabled
4232    3248    chrome.exe      0x13e842b30     14      233     1       False   2019-03-22 05:35:17.000000      N/A     Disabled
2188    476     msdtc.exe       0x13e878060     12      146     0       False   2019-03-22 05:32:15.000000      N/A     Disabled
2196    592     WmiPrvSE.exe    0x13e8d2380     11      222     0       False   2019-03-22 05:32:15.000000      N/A     Disabled
3032    1432    notepad.exe     0x13e8f9060     1       60      1       False   2019-03-22 05:32:22.000000      N/A     Disabled
2456    476     SearchIndexer.  0x13e908650     13      766     0       False   2019-03-22 05:32:17.000000      N/A     Disabled
2628    476     wmpnetwk.exe    0x13e9b0060     9       210     0       False   2019-03-22 05:32:18.000000      N/A     Disabled
380     324     wininit.exe     0x13ea59060     3       78      0       False   2019-03-22 05:31:58.000000      N/A     Disabled
372     364     csrss.exe       0x13ea5a9e0     11      557     1       False   2019-03-22 05:31:58.000000      N/A     Disabled
416     364     winlogon.exe    0x13ea68b30     3       110     1       False   2019-03-22 05:31:58.000000      N/A     Disabled
2100    3248    chrome.exe      0x13eaf0060     2       59      1       False   2019-03-22 05:35:15.000000      N/A     Disabled
3612    1292    OfficeC2RClien  0x13eaf0710     0       -       0       False   2019-03-22 05:37:07.000000      2019-03-22 05:37:26.000000      Disabled
4156    3248    chrome.exe      0x13eb00b30     14      216     1       False   2019-03-22 05:35:17.000000      N/A     Disabled
1816    3248    chrome.exe      0x13eb306f0     14      328     1       False   2019-03-22 05:35:16.000000      N/A     Disabled
4688    3248    chrome.exe      0x13ebcbb30     13      168     1       False   2019-03-22 05:35:19.000000      N/A     Disabled
4048    1432    POWERPNT.EXE    0x13ebd3060     23      765     1       True    2019-03-22 05:35:09.000000      N/A     Disabled
1272    1432    EXCEL.EXE       0x13ebf83e0     21      789     1       True    2019-03-22 05:33:49.000000      N/A     Disabled
332     324     csrss.exe       0x13ec546b0     10      516     0       False   2019-03-22 05:31:58.000000      N/A     Disabled
3952    1432    hfs.exe 0x13f505620     6       214     1       True    2019-03-22 05:34:51.000000      N/A     Disabled
252     4       smss.exe        0x13f616040     2       30      N/A     False   2019-03-22 05:31:55.000000      N/A     Disabled
3688    1432    OUTLOOK.EXE     0x13f74c060     30      2023    1       True    2019-03-22 05:34:37.000000      N/A     Disabled
3792    1432    taskmgr.exe     0x13f74fb30     6       134     1       False   2019-03-22 05:34:38.000000      N/A     Disabled
3548    1432    calc.exe        0x13f798320     3       77      1       False   2019-03-22 05:34:43.000000      N/A     Disabled
3244    3248    chrome.exe      0x13f7beb30     7       91      1       False   2019-03-22 05:35:15.000000      N/A     Disabled
3576    592     iexplore.exe    0x13f7cb060     12      403     1       True    2019-03-22 05:34:48.000000      N/A     Disabled
2780    3576    iexplore.exe    0x13f7e9540     6       233     1       True    2019-03-22 05:34:48.000000      N/A     Disabled
1408    1432    cmd.exe 0x13faaa430     1       23      1       False   2019-03-22 05:34:12.000000      N/A     Disabled
1008    372     conhost.exe     0x13faab620     2       55      1       False   2019-03-22 05:34:12.000000      N/A     Disabled
3248    1432    chrome.exe      0x13fadbb30     32      841     1       False   2019-03-22 05:35:14.000000      N/A     Disabled
1156    820     taskeng.exe     0x13fb00620     4       93      1       False   2019-03-22 05:34:14.000000      N/A     Disabled
3300    476     svchost.exe     0x13fb2f060     13      346     0       False   2019-03-22 05:34:15.000000      N/A     Disabled
3260    476     sppsvc.exe      0x13fb30b30     4       149     0       False   2019-03-22 05:34:15.000000      N/A     Disabled
3192    1432    FTK Imager.exe  0x13fc83880     6       353     1       False   2019-03-22 05:35:12.000000      N/A     Disabled
```

***Volatility – 3 with pstree:***



```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Triage-Memory.mem windows.pstree.PsTree
[sudo] password for kali:
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0xfa8003c72b30  87      547     N/A     False   2019-03-22 05:31:55.000000      N/A
* 252   4       smss.exe        0xfa8004616040  2       30      N/A     False   2019-03-22 05:31:55.000000      N/A
332     324     csrss.exe       0xfa80050546b0  10      516     0       False   2019-03-22 05:31:58.000000      N/A
372     364     csrss.exe       0xfa800525a9e0  11      557     1       False   2019-03-22 05:31:58.000000      N/A
* 1008  372     conhost.exe     0xfa80042ab620  2       55      1       False   2019-03-22 05:34:12.000000      N/A
* 4656  372     conhost.exe     0xfa8005c1ab30  2       49      1       False   2019-03-22 05:35:36.000000      N/A
380     324     wininit.exe     0xfa8005259060  3       78      0       False   2019-03-22 05:31:58.000000      N/A
* 492   380     lsm.exe 0xfa8005696b30  10      155     0       False   2019-03-22 05:32:00.000000      N/A
* 476   380     services.exe    0xfa8005680910  12      224     0       False   2019-03-22 05:31:59.000000      N/A
** 1028 476     svchost.exe     0xfa800583db30  19      307     0       False   2019-03-22 05:32:05.000000      N/A
** 764  476     svchost.exe     0xfa800575e5b0  20      447     0       False   2019-03-22 05:32:02.000000      N/A
** 1932 476     ManagementAgen  0xfa8005ba0620  10      102     0       False   2019-03-22 05:32:11.000000      N/A
** 2188 476     msdtc.exe       0xfa8005478060  12      146     0       False   2019-03-22 05:32:15.000000      N/A
** 2456 476     SearchIndexer.  0xfa8005508650  13      766     0       False   2019-03-22 05:32:17.000000      N/A
** 2072 476     dllhost.exe     0xfa8005409060  13      194     0       False   2019-03-22 05:32:14.000000      N/A
** 796  476     svchost.exe     0xfa8005775b30  15      368     0       False   2019-03-22 05:32:03.000000      N/A
**** 1344       796     dwm.exe 0xfa80059e6890  3       88      1       False   2019-03-22 05:32:07.000000      N/A
** 672  476     svchost.exe     0xfa800570d060  7       341     0       False   2019-03-22 05:32:02.000000      N/A
** 932  476     svchost.exe     0xfa80057beb30  10      568     0       False   2019-03-22 05:32:03.000000      N/A
** 820  476     svchost.exe     0xfa800577db30  33      1073    0       False   2019-03-22 05:32:03.000000      N/A
**** 1156       820     taskeng.exe     0xfa8004300620  4       93      1       False   2019-03-22 05:34:14.000000      N/A
**** 1292       820     taskeng.exe     0xfa80059cc620  4       83      0       False   2019-03-22 05:32:07.000000      N/A
** 1852 476     vmtoolsd.exe    0xfa8005b4eb30  10      314     0       False   2019-03-22 05:32:11.000000      N/A
** 3260 476     sppsvc.exe      0xfa8004330b30  4       149     0       False   2019-03-22 05:34:15.000000      N/A
** 1476 476     FileZilla Serv  0xfa8005a324e0  9       81      0       True    2019-03-22 05:32:07.000000      N/A
** 2628 476     wmpnetwk.exe    0xfa80055b0060  9       210     0       False   2019-03-22 05:32:18.000000      N/A
** 2888 476     svchost.exe     0xfa8005c4ab30  11      152     0       False   2019-03-22 05:32:20.000000      N/A
** 592  476     svchost.exe     0xfa80056e1060  9       375     0       False   2019-03-22 05:32:01.000000      N/A
**** 3576       592     iexplore.exe    0xfa80047cb060  12      403     1       True    2019-03-22 05:34:48.000000      N/A
****** 2780      3576    iexplore.exe    0xfa80047e9540  6       233     1       True    2019-03-22 05:34:48.000000      N/A
**** 2436       592     WmiPrvSE.exe    0xfa8005c8e440  9       245     0       False   2019-03-22 05:32:33.000000      N/A
**** 2196       592     WmiPrvSE.exe    0xfa80054d2380  11      222     0       False   2019-03-22 05:32:15.000000      N/A
** 864  476     spoolsv.exe     0xfa8005850a30  12      279     0       False   2019-03-22 05:32:04.000000      N/A
** 3300 476     svchost.exe     0xfa800432f060  13      346     0       False   2019-03-22 05:34:15.000000      N/A
** 232  476     svchost.exe     0xfa80057e4560  15      410     0       False   2019-03-22 05:32:03.000000      N/A
** 1768 476     VGAuthService.  0xfa8005af24e0  3       89      0       False   2019-03-22 05:32:09.000000      N/A
** 1136 476     OfficeClickToR  0xfa80058ed390  23      631     0       False   2019-03-22 05:32:05.000000      N/A
** 1276 476     taskhost.exe    0xfa80059cb7c0  8       183     1       False   2019-03-22 05:32:07.000000      N/A
* 484   380     lsass.exe       0xfa80056885e0  7       650     0       False   2019-03-22 05:32:00.000000      N/A
416     364     winlogon.exe    0xfa8005268b30  3       110     1       False   2019-03-22 05:31:58.000000      N/A
1432    1308    explorer.exe    0xfa8003de39c0  28      976     1       False   2019-03-22 05:32:07.000000      N/A
* 1272  1432    EXCEL.EXE       0xfa80053f83e0  21      789     1       True    2019-03-22 05:33:49.000000      N/A
* 1408  1432    cmd.exe 0xfa80042aa430  1       23      1       False   2019-03-22 05:34:12.000000      N/A
* 1828  1432    vmtoolsd.exe    0xfa8005b49890  6       144     1       False   2019-03-22 05:32:10.000000      N/A
* 3688  1432    OUTLOOK.EXE     0xfa800474c060  30      2023    1       True    2019-03-22 05:34:37.000000      N/A
* 3792  1432    taskmgr.exe     0xfa800474fb30  6       134     1       False   2019-03-22 05:34:38.000000      N/A
* 3952  1432    hfs.exe 0xfa8004905620  6       214     1       True    2019-03-22 05:34:51.000000      N/A
** 5116 3952    wscript.exe     0xfa8005a80060  8       312     1       True    2019-03-22 05:35:32.000000      N/A
**** 3496       5116    UWkpjFjDzM.exe  0xfa8005a1d9e0  5       109     1       True    2019-03-22 05:35:33.000000      N/A
****** 4660      3496    cmd.exe 0xfa8005bb0060  1       33      1       True    2019-03-22 05:35:36.000000      N/A
* 4048  1432    POWERPNT.EXE    0xfa80053d3060  23      765     1       True    2019-03-22 05:35:09.000000      N/A
* 3192  1432    FTK Imager.exe  0xfa8004083880  6       353     1       False   2019-03-22 05:35:12.000000      N/A
* 3248  1432    chrome.exe      0xfa80042dbb30  32      841     1       False   2019-03-22 05:35:14.000000      N/A
** 4232 3248    chrome.exe      0xfa8005442b30  14      233     1       False   2019-03-22 05:35:17.000000      N/A
** 4520 3248    chrome.exe      0xfa800540db30  10      234     1       False   2019-03-22 05:35:18.000000      N/A
** 3244 3248    chrome.exe      0xfa80047beb30  7       91      1       False   2019-03-22 05:35:15.000000      N/A
** 4240 3248    chrome.exe      0xfa8005419b30  14      215     1       False   2019-03-22 05:35:17.000000      N/A
** 4688 3248    chrome.exe      0xfa80053cbb30  13      168     1       False   2019-03-22 05:35:19.000000      N/A
** 2100 3248    chrome.exe      0xfa80052f0060  2       59      1       False   2019-03-22 05:35:15.000000      N/A
** 1816 3248    chrome.exe      0xfa80053306f0  14      328     1       False   2019-03-22 05:35:16.000000      N/A
** 4156 3248    chrome.exe      0xfa8005300b30  14      216     1       False   2019-03-22 05:35:17.000000      N/A
* 3032  1432    notepad.exe     0xfa80054f9060  1       60      1       False   2019-03-22 05:32:22.000000      N/A
* 3548  1432    calc.exe        0xfa8004798320  3       77      1       False   2019-03-22 05:34:43.000000      N/A
* 1628  1432    StikyNot.exe    0xfa8005d067d0  8       183     1       False   2019-03-22 05:34:42.000000      N/A
1996    1860    FileZilla Serv  0xfa8005be12c0  3       99      1       True    2019-03-22 05:32:12.000000      N/A
```

***Volatility – 3 with Netstat (not in Volatility 2):***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Triage-Memory.mem windows.netstat.NetStat
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xfa8005ac6b10  TCPv4   0.0.0.0 21      0.0.0.0 0       LISTENING       1476    FileZilla Serv  -
0xfa8005ac6b10  TCPv6   ::      21      ::      0       LISTENING       1476    FileZilla Serv  -
0xfa8005ac9be0  TCPv4   0.0.0.0 21      0.0.0.0 0       LISTENING       1476    FileZilla Serv  -
0xfa80053cdef0  TCPv4   0.0.0.0 80      0.0.0.0 0       LISTENING       3952    hfs.exe -
0xfa8005720660  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       672     svchost.exe     -
0xfa8005720660  TCPv6   ::      135     ::      0       LISTENING       672     svchost.exe     -
0xfa800571cef0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       672     svchost.exe     -
0xfa800597e010  TCPv4   10.0.0.101      139     0.0.0.0 0       LISTENING       4       System  -
0xfa80049899c0  TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  -
0xfa80049899c0  TCPv6   ::      445     ::      0       LISTENING       4       System  -
0xfa8005ac7850  TCPv6   ::1     14147   ::      0       LISTENING       1476    FileZilla Serv  -
0xfa8005ac96b0  TCPv4   127.0.0.1       14147   0.0.0.0 0       LISTENING       1476    FileZilla Serv  -
0xfa800572f6e0  TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       380     wininit.exe     -
0xfa800572f6e0  TCPv6   ::      49152   ::      0       LISTENING       380     wininit.exe     -
0xfa800572f010  TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       380     wininit.exe     -
0xfa8005772980  TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       764     svchost.exe     -
0xfa8005772980  TCPv6   ::      49153   ::      0       LISTENING       764     svchost.exe     -
0xfa8005770240  TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       764     svchost.exe     -
0xfa8005830580  TCPv4   0.0.0.0 49154   0.0.0.0 0       LISTENING       820     svchost.exe     -
0xfa8005830580  TCPv6   ::      49154   ::      0       LISTENING       820     svchost.exe     -
0xfa8005831820  TCPv4   0.0.0.0 49154   0.0.0.0 0       LISTENING       820     svchost.exe     -
0xfa8005ba1150  TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       484     lsass.exe       -
0xfa8005ba1150  TCPv6   ::      49155   ::      0       LISTENING       484     lsass.exe       -
0xfa8005bb2010  TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       484     lsass.exe       -
0xfa80053b3010  TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       476     services.exe    -
0xfa80053b3010  TCPv6   ::      49156   ::      0       LISTENING       476     services.exe    -
0xfa80049898a0  TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       476     services.exe    -
0xfa80052d8580  TCPv4   0.0.0.0 49202   0.0.0.0 0       LISTENING       -       -       -
0xfa80054c1cf0  TCPv4   0.0.0.0 49204   0.0.0.0 0       LISTENING       -       -       -
0xfa8004399010  TCPv4   0.0.0.0 49217   0.0.0.0 0       LISTENING       -       -       -
0xfa80053fc790  TCPv4   0.0.0.0 49262   0.0.0.0 0       LISTENING       -       -       -
0xfa800481a570  TCPv4   0.0.0.0 49263   0.0.0.0 0       LISTENING       -       -       -
0xfa80059683e0  UDPv4   10.0.0.101      137     *       0               4       System  2019-03-22 05:32:06.000000
0xfa8005994250  UDPv4   10.0.0.101      138     *       0               4       System  2019-03-22 05:32:06.000000
0xfa800561fb30  UDPv6   fe80::7475:ef30:be18:7807       546     *       0               764     svchost.exe     2019-03-22 05:46:23.000000
0xfa8005c5d4b0  UDPv6   fe80::7475:ef30:be18:7807       1900    *       0               2888    svchost.exe     2019-03-22 05:32:20.000000
0xfa8005c5eab0  UDPv6   ::1     1900    *       0               2888    svchost.exe     2019-03-22 05:32:20.000000
0xfa8005c5e3f0  UDPv4   10.0.0.101      1900    *       0               2888    svchost.exe     2019-03-22 05:32:20.000000
0xfa8005c64d70  UDPv4   127.0.0.1       1900    *       0               2888    svchost.exe     2019-03-22 05:32:20.000000
0xfa80053c6c20  UDPv4   0.0.0.0 5353    *       0               3248    chrome.exe      2019-03-22 05:35:17.000000
0xfa80053ea890  UDPv4   0.0.0.0 5353    *       0               3248    chrome.exe      2019-03-22 05:35:17.000000
0xfa80053ea890  UDPv6   ::      5353    *       0               3248    chrome.exe      2019-03-22 05:35:17.000000
0xfa8005890ec0  UDPv4   0.0.0.0 5355    *       0               232     svchost.exe     2019-03-22 05:32:09.000000
0xfa8005890ec0  UDPv6   ::      5355    *       0               232     svchost.exe     2019-03-22 05:32:09.000000
0xfa8005b05a50  UDPv4   0.0.0.0 5355    *       0               232     svchost.exe     2019-03-22 05:32:09.000000
0xfa8004078dc0  UDPv4   127.0.0.1       53361   *       0               1272    EXCEL.EXE       2019-03-22 05:34:03.000000
0xfa8005a58010  UDPv4   127.0.0.1       55560   *       0               5116    wscript.exe     2019-03-22 05:35:32.000000
0xfa80052d0bf0  UDPv4   127.0.0.1       55614   *       0               4048    POWERPNT.EXE    2019-03-22 05:35:15.000000
0xfa8005c5b790  UDPv6   fe80::7475:ef30:be18:7807       55734   *       0               2888    svchost.exe     2019-03-22 05:32:20.000000
0xfa8005c5b4f0  UDPv6   ::1     55735   *       0               2888    svchost.exe     2019-03-22 05:32:20.000000
0xfa8005c57300  UDPv4   10.0.0.101      55736   *       0               2888    svchost.exe     2019-03-22 05:32:20.000000
0xfa8005c5dec0  UDPv4   127.0.0.1       55737   *       0               2888    svchost.exe     2019-03-22 05:32:20.000000
0xfa8005518010  UDPv4   0.0.0.0 56372   *       0               1816    chrome.exe      2019-03-22 05:45:51.000000
0xfa80055cd730  UDPv4   127.0.0.1       57374   *       0               1136    OfficeClickToR  2019-03-22 05:32:18.000000
0xfa80047e8670  UDPv4   127.0.0.1       59411   *       0               3576    iexplore.exe    2019-03-22 05:34:49.000000
0xfa800528e6a0  UDPv4   127.0.0.1       61704   *       0               3688    OUTLOOK.EXE     2019-03-22 05:34:44.000000
```

***Volatility – 3 with Netscan:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Triage-Memory.mem windows.netscan.NetScan
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0x13e02bcf0     TCPv4   -       49220   72.51.60.132    443     CLOSED  4048    POWERPNT.EXE    -
0x13e035790     TCPv4   -       49223   72.51.60.132    443     CLOSED  4048    POWERPNT.EXE    -
0x13e036470     TCPv4   -       49224   72.51.60.132    443     CLOSED  4048    POWERPNT.EXE    -
0x13e057300     UDPv4   10.0.0.101      55736   *       0               2888    svchost.exe     2019-03-22 05:32:20.000000
0x13e05b4f0     UDPv6   ::1     55735   *       0               2888    svchost.exe     2019-03-22 05:32:20.000000
0x13e05b790     UDPv6   fe80::7475:ef30:be18:7807       55734   *       0               2888    svchost.exe     2019-03-22 05:32:20.000000
0x13e05d4b0     UDPv6   fe80::7475:ef30:be18:7807       1900    *       0               2888    svchost.exe     2019-03-22 05:32:20.000000
0x13e05dec0     UDPv4   127.0.0.1       55737   *       0               2888    svchost.exe     2019-03-22 05:32:20.000000
0x13e05e3f0     UDPv4   10.0.0.101      1900    *       0               2888    svchost.exe     2019-03-22 05:32:20.000000
0x13e05eab0     UDPv6   ::1     1900    *       0               2888    svchost.exe     2019-03-22 05:32:20.000000
0x13e064d70     UDPv4   127.0.0.1       1900    *       0               2888    svchost.exe     2019-03-22 05:32:20.000000
0x13e2348a0     TCPv4   -       49366   192.168.206.181 389     CLOSED  -       -       N/A
0x13e258010     UDPv4   127.0.0.1       55560   *       0               5116    wscript.exe     2019-03-22 05:35:32.000000
0x13e2c6b10     TCPv4   0.0.0.0 21      0.0.0.0 0       LISTENING       1476    FileZilla Serv  -
0x13e2c6b10     TCPv6   ::      21      ::      0       LISTENING       1476    FileZilla Serv  -
0x13e2c7850     TCPv6   ::1     14147   ::      0       LISTENING       1476    FileZilla Serv  -
0x13e2c96b0     TCPv4   127.0.0.1       14147   0.0.0.0 0       LISTENING       1476    FileZilla Serv  -
0x13e2c9be0     TCPv4   0.0.0.0 21      0.0.0.0 0       LISTENING       1476    FileZilla Serv  -
0x13e305a50     UDPv4   0.0.0.0 5355    *       0               232     svchost.exe     2019-03-22 05:32:09.000000
0x13e360be0     UDPv4   0.0.0.0 63790   *       0               -       -       2019-03-22 05:45:47.000000
0x13e397190     TCPv4   10.0.0.101      49217   10.0.0.106      4444    ESTABLISHED     3496    UWkpjFjDzM.exe  N/A
0x13e3986d0     TCPv4   -       49378   213.209.1.129   25      CLOSED  -       -       -
0x13e3a1150     TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       484     lsass.exe       -
0x13e3a1150     TCPv6   ::      49155   ::      0       LISTENING       484     lsass.exe       -
0x13e3abae0     TCPv4   -       49226   72.51.60.132    443     CLOSED  4048    POWERPNT.EXE    -
0x13e3b2010     TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       484     lsass.exe       -
0x13e3e7010     TCPv6   -       0       38db:7705:80fa:ffff:38db:7705:80fa:ffff 0       CLOSED  1136    OfficeClickToR  N/A
0x13e430580     TCPv4   0.0.0.0 49154   0.0.0.0 0       LISTENING       820     svchost.exe     -
0x13e430580     TCPv6   ::      49154   ::      0       LISTENING       820     svchost.exe     -
0x13e431820     TCPv4   0.0.0.0 49154   0.0.0.0 0       LISTENING       820     svchost.exe     -
0x13e490ec0     UDPv4   0.0.0.0 5355    *       0               232     svchost.exe     2019-03-22 05:32:09.000000
0x13e490ec0     UDPv6   ::      5355    *       0               232     svchost.exe     2019-03-22 05:32:09.000000
0x13e4e4910     TCPv4   10.0.0.101      49208   52.109.12.6     443     CLOSED  -       -       -
0x13e55fae0     TCPv4   10.0.0.101      49209   52.96.44.162    443     CLOSED  -       -       -
0x13e5683e0     UDPv4   10.0.0.101      137     *       0               4       System  2019-03-22 05:32:06.000000
0x13e57e010     TCPv4   10.0.0.101      139     0.0.0.0 0       LISTENING       4       System  -
0x13e594250     UDPv4   10.0.0.101      138     *       0               4       System  2019-03-22 05:32:06.000000
0x13e597ec0     UDPv4   0.0.0.0 0       *       0               232     svchost.exe     2019-03-22 05:32:06.000000
0x13e597ec0     UDPv6   ::      0       *       0               232     svchost.exe     2019-03-22 05:32:06.000000
0x13e61fb30     UDPv6   fe80::7475:ef30:be18:7807       546     *       0               764     svchost.exe     2019-03-22 05:46:23.000000
0x13e71cef0     TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       672     svchost.exe     -
0x13e720660     TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       672     svchost.exe     -
0x13e720660     TCPv6   ::      135     ::      0       LISTENING       672     svchost.exe     -
0x13e72f010     TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       380     wininit.exe     -
0x13e72f6e0     TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       380     wininit.exe     -
0x13e72f6e0     TCPv6   ::      49152   ::      0       LISTENING       380     wininit.exe     -
0x13e73b560     TCPv4   -       49266   35.190.69.156   443     CLOSED  -       -       -
0x13e770240     TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       764     svchost.exe     -
0x13e772980     TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       764     svchost.exe     -
0x13e772980     TCPv6   ::      49153   ::      0       LISTENING       764     svchost.exe     -
0x13e7c6010     TCPv4   10.0.0.101      49204   172.217.6.195   443     CLOSED  1816    chrome.exe      N/A
0x13e918010     UDPv4   0.0.0.0 56372   *       0               1816    chrome.exe      2019-03-22 05:45:51.000000
0x13e9cd730     UDPv4   127.0.0.1       57374   *       0               1136    OfficeClickToR  2019-03-22 05:32:18.000000
0x13ea8e6a0     UDPv4   127.0.0.1       61704   *       0               3688    OUTLOOK.EXE     2019-03-22 05:34:44.000000
0x13ead0bf0     UDPv4   127.0.0.1       55614   *       0               4048    POWERPNT.EXE    2019-03-22 05:35:15.000000
0x13ead7cf0     TCPv4   10.0.0.101      49202   172.217.10.68   443     CLOSED  1816    chrome.exe      N/A
0x13ebb3010     TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       476     services.exe    -
0x13ebb3010     TCPv6   ::      49156   ::      0       LISTENING       476     services.exe    -
0x13ebc6c20     UDPv4   0.0.0.0 5353    *       0               3248    chrome.exe      2019-03-22 05:35:17.000000
0x13ebcdef0     TCPv4   0.0.0.0 80      0.0.0.0 0       LISTENING       3952    hfs.exe -
0x13ebea890     UDPv4   0.0.0.0 5353    *       0               3248    chrome.exe      2019-03-22 05:35:17.000000
0x13ebea890     UDPv6   ::      5353    *       0               3248    chrome.exe      2019-03-22 05:35:17.000000
0x13f4facf0     TCPv4   10.0.0.101      49262   52.109.12.6     443     ESTABLISHED     3688    OUTLOOK.EXE     N/A
0x13f50a010     TCPv4   -       49265   213.186.33.3    443     CLOSED  -       -       -
0x13f5289f0     TCPv4   -       49234   72.51.60.133    80      CLOSED  3688    OUTLOOK.EXE     -
0x13f5898a0     TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       476     services.exe    -
0x13f5899c0     TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  -
0x13f5899c0     TCPv6   ::      445     ::      0       LISTENING       4       System  -
0x13f7ae010     TCPv4   10.0.0.101      49263   52.96.44.162    443     ESTABLISHED     3688    OUTLOOK.EXE     N/A
0x13f7b4ec0     UDPv4   0.0.0.0 55707   *       0               232     svchost.exe     2019-03-22 05:45:44.000000
0x13f7e8670     UDPv4   127.0.0.1       59411   *       0               3576    iexplore.exe    2019-03-22 05:34:49.000000
0x13fa93cf0     TCPv4   -       49173   72.51.60.132    443     CLOSED  1272    EXCEL.EXE       -
0x13fa95cf0     TCPv4   -       49170   72.51.60.132    443     CLOSED  1272    EXCEL.EXE       -
0x13fa969f0     TCPv4   -       0       56.219.119.5    0       CLOSED  1272    EXCEL.EXE       N/A
0x13fbd07e0     TCPv4   -       49372   212.227.15.9    25      CLOSED  -       -       N/A
0x13fc6f1b0     UDPv4   0.0.0.0 55102   *       0               232     svchost.exe     2019-03-22 05:45:36.000000
0x13fc78dc0     UDPv4   127.0.0.1       53361   *       0               1272    EXCEL.EXE       2019-03-22 05:34:03.000000
0x13fc857e0     TCPv4   -       49167   72.51.60.132    443     CLOSED  1272    EXCEL.EXE       -
```

***Volatility 3 with cmdline:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Triage-Memory.mem windows.cmdline.CmdLine | grep -E "vbs"
5116resswscript.exe     "C:\Windows\System32\wscript.exe" //B //NOLOGO %TEMP%\vhjReUDEuumrX.vbs
```

***Volatility 3 with memdump:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Triage-Memory.mem -o dumps/ windows.memmap --dump --pid 3032
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Virtual Physical        Size    Offset in File  File output

0x10000 0x7dfee000      0x1000  0x0     pid.3032.dmp
0x11000 0x7e663000      0x1000  0x1000  pid.3032.dmp
0x20000 0x82606000      0x1000  0x2000  pid.3032.dmp
0x21000 0x82207000      0x1000  0x3000  pid.3032.dmp
0x22000 0x81788000      0x1000  0x4000  pid.3032.dmp
0x30000 0x9429d000      0x1000  0x5000  pid.3032.dmp
0x31000 0x945de000      0x1000  0x6000  pid.3032.dmp
0x32000 0x9475f000      0x1000  0x7000  pid.3032.dmp
0x33000 0x946a0000      0x1000  0x8000  pid.3032.dmp
0x40000 0x820e7000      0x1000  0x9000  pid.3032.dmp
0x41000 0x81e68000      0x1000  0xa000  pid.3032.dmp
0x50000 0x7da93000      0x1000  0xb000  pid.3032.dmp
0x60000 0x7d7a4000      0x1000  0xc000  pid.3032.dmp
0x70000 0x7e4a5000      0x1000  0xd000  pid.3032.dmp
0xfa000 0x7d5f9000      0x1000  0xe000  pid.3032.dmp
0xfb000 0x7e469000      0x1000  0xf000  pid.3032.dmp
0xfc000 0x7e802000      0x1000  0x10000 pid.3032.dmp
0xfd000 0x7d868000      0x1000  0x11000 pid.3032.dmp
0xfe000 0x7d8dd000      0x1000  0x12000 pid.3032.dmp
0xff000 0x7e419000      0x1000  0x13000 pid.3032.dmp
0x100000        0x936ab000      0x1000  0x14000 pid.3032.dmp
```

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines/dumps]
└─$ strings -e l pid.3032.dmp | grep -i "Flag"
flag<REDBULL_IS_LIFE>
AppCompatFlags\Layers
ShutdownFlags
TracingFlags
VerifierFlags
PageHeapFlags
\Registry\Machine\Software\Microsoft\Windows nt\currentversion\appcompatflags\AIT
dwFlags
dwFlags
  dwFlags: 0x%x
Allow flag to be passed with CreateFile call that indicates to perform downgrade if applicable.
FFlags
RpcVerifierFlags
thread_flags
activation_flags
thread_flags
activation_flags
```

***Volatility – 3 with malfind:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Triage-Memory.mem windows.malfind | grep -i "UWk"
3496ressUWkpjFjDzM.exe  0x20000 0x20fff VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled
3496    UWkpjFjDzM.exe  0x230000        0x25bfff        VadS    PAGE_EXECUTE_READWRITE  44      1       Disabled
3496    UWkpjFjDzM.exe  0x280000        0x2b0fff        VadS    PAGE_EXECUTE_READWRITE  49      1       Disabled
3496    UWkpjFjDzM.exe  0x350000        0x3b0fff        VadS    PAGE_EXECUTE_READWRITE  97      1       Disabled
3496    UWkpjFjDzM.exe  0x820000        0x840fff        VadS    PAGE_EXECUTE_READWRITE  33      1       Disabled
3496    UWkpjFjDzM.exe  0x2950000       0x2981fff       VadS    PAGE_EXECUTE_READWRITE  50      1       Disabled
3496    UWkpjFjDzM.exe  0x2ad0000       0x2b06fff       VadS    PAGE_EXECUTE_READWRITE  55      1       Disabled
```

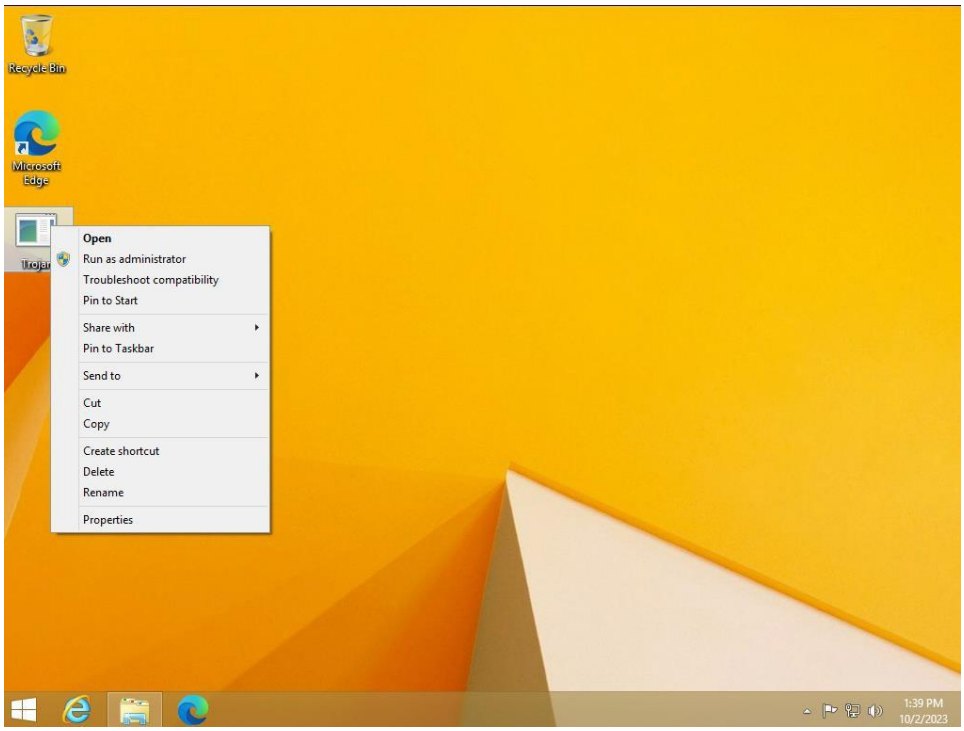
```
3496    UWkpjFjDzM.exe  0x350000        0x3b0fff        VadS    PAGE_EXECUTE_READWRITE  97      1       Disabled
4d 5a 90 00 03 00 00 00 MZ......
04 00 00 00 ff ff 00 00 ........
b8 00 00 00 00 00 00 00 ........
40 00 00 00 00 00 00 00 @.......
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 10 01 00 00 ........
0x350000:       dec     ebp
0x350001:       pop     edx
0x350002:       nop
0x350003:       add     byte ptr [ebx], al
0x350005:       add     byte ptr [eax], al
0x350007:       add     byte ptr [eax + eax], al
0x35000a:       add     byte ptr [eax], al
3496    UWkpjFjDzM.exe  0x820000        0x840fff        VadS    PAGE_EXECUTE_READWRITE  33      1       Disabled
4d 5a 90 00 03 00 00 00 MZ......
04 00 00 00 ff ff 00 00 ........
b8 00 00 00 00 00 00 00 ........
40 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 00 e8 00 00 00 ........
0x820000:       dec     ebp
0x820001:       pop     edx
0x820002:       nop
0x820003:       add     byte ptr [ebx], al
0x820005:       add     byte ptr [eax], al
0x820007:       add     byte ptr [eax + eax], al
0x82000a:       add     byte ptr [eax], al
3496    UWkpjFjDzM.exe  0x2950000       0x2981fff       VadS    PAGE_EXECUTE_READWRITE  50      1       Disabled
4d 5a 90 00 03 00 00 00 MZ......
```

# Executing a njRAT - Trojan virus on Windows 8 virtual machine

In a controlled and isolated environment within my Windows 8 virtual machine, I deliberately executed the njRAT trojan. njRAT is a type of remote access trojan often used for unauthorized remote access and control of infected systems. I acquired the trojan for analysis purposes from a trusted and legitimate source dedicated to cybersecurity research and analysis. To perform a comprehensive analysis, I followed these steps:

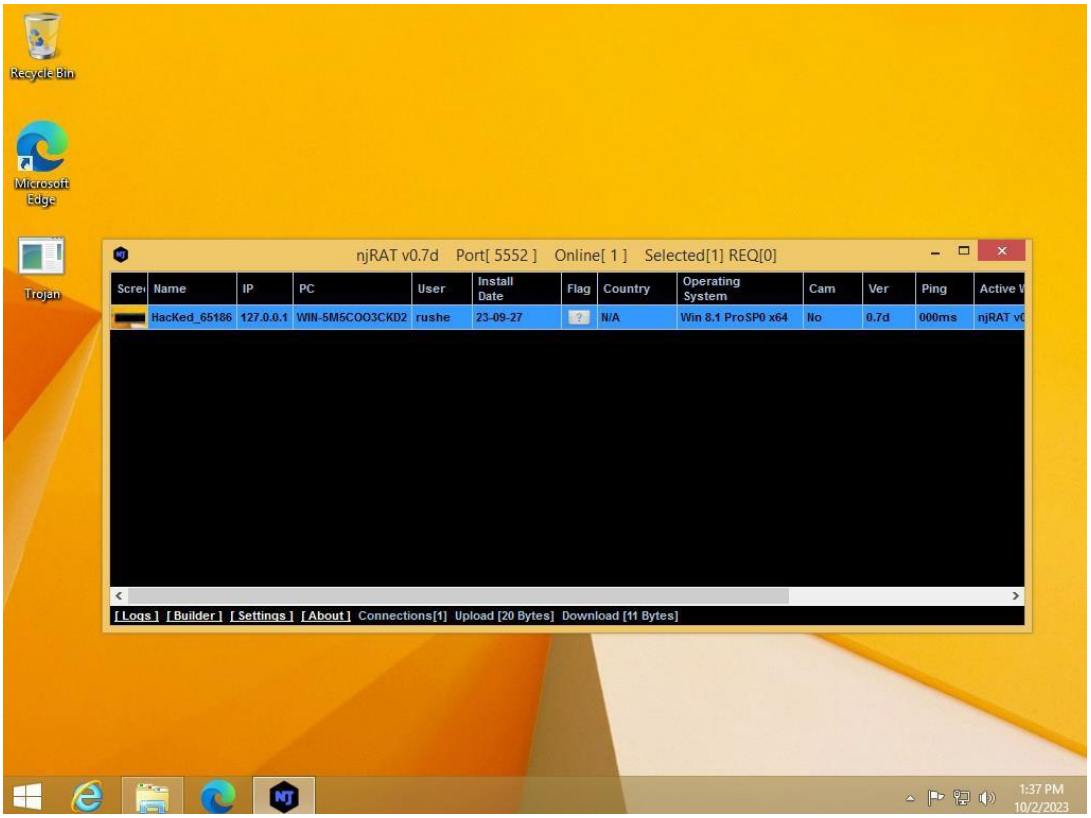
- Isolated Environment: I set up a Windows 8 virtual machine solely for this analysis, ensuring that the trojan's activities would not affect my actual system or network.
- njRAT Execution: I executed the njRAT trojan within this controlled environment to closely monitor its behavior and interactions with the operating system.
- Memory Dump: After njRAT had been active for a period, I extracted a memory dump from the virtual machine. This memory dump captured the state of the system's memory at that particular moment.
- Volatility 3 Analysis: With the memory dump in hand, I initiated the analysis using Volatility 3, a robust memory forensics tool.

***<u>Executing the Trojan.exe in Windows 8 Virtual machine:</u>***

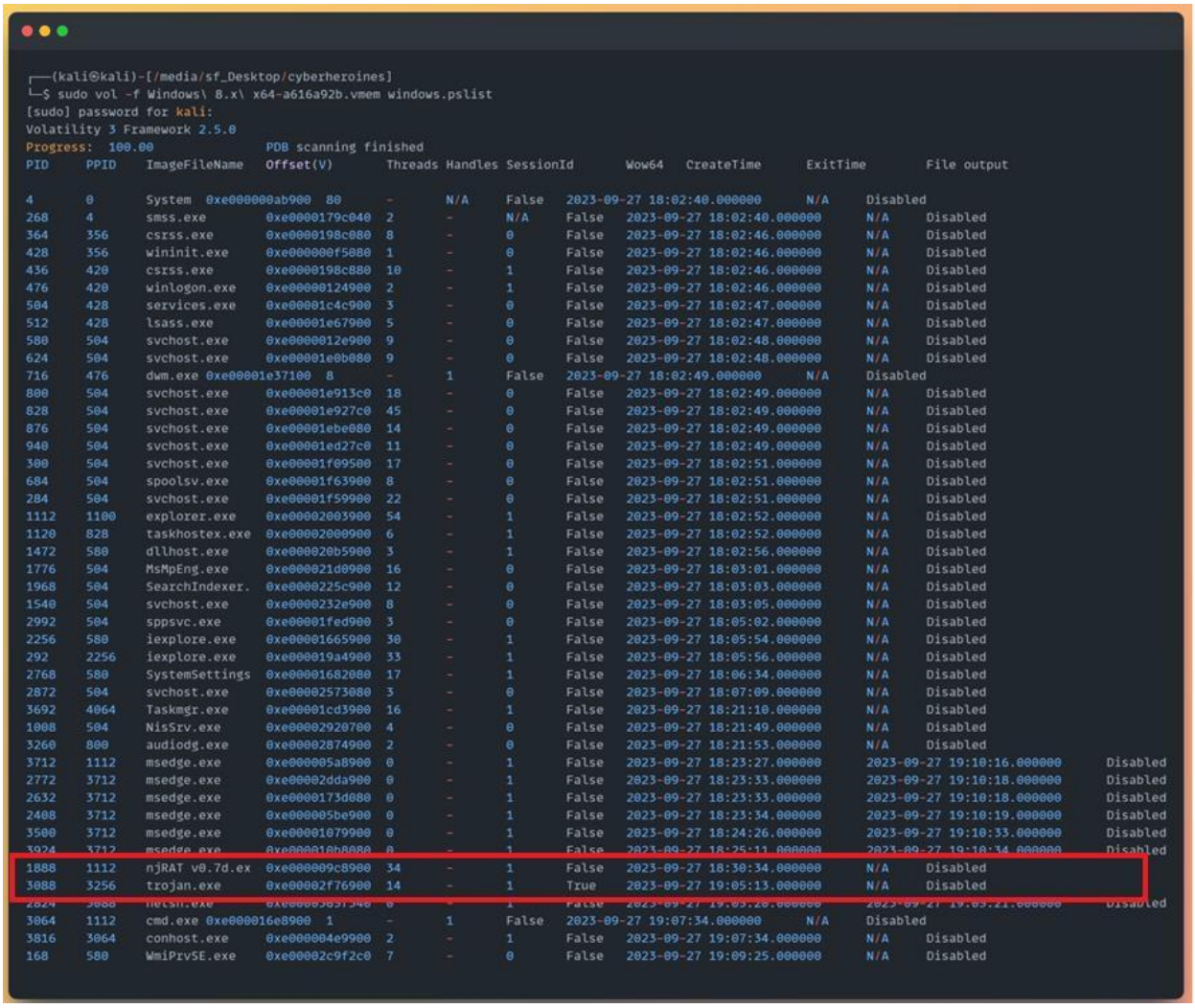


***After successfully running, we can access the machine via this njRAT GUI:***

We can observe, that the Trojan.exe which ran in the VM has been communicating with this njRAT process, and thereby full system access is the hands of the attacker. He has root level privileges.

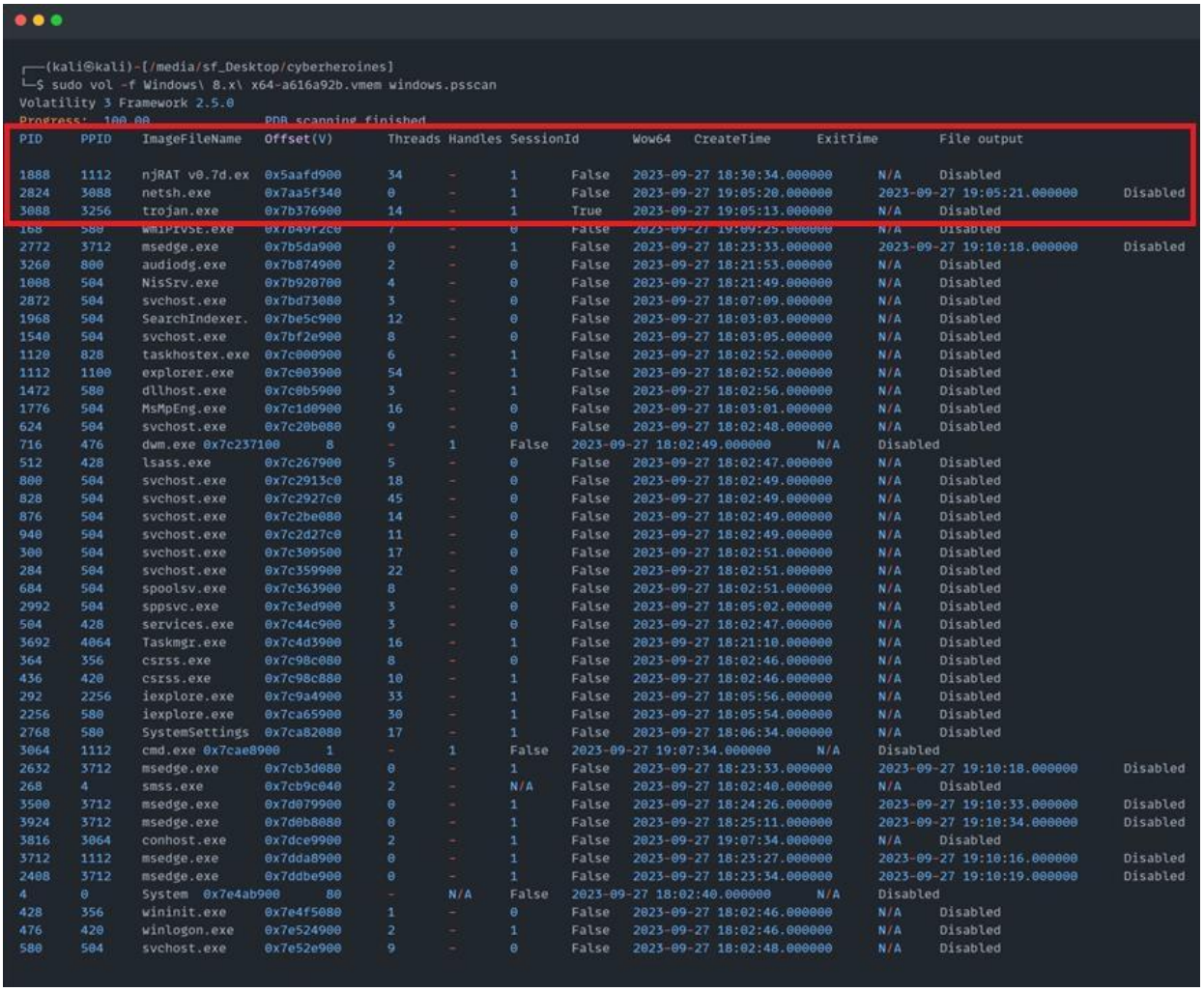


***Volatility – 3 with pslist:***



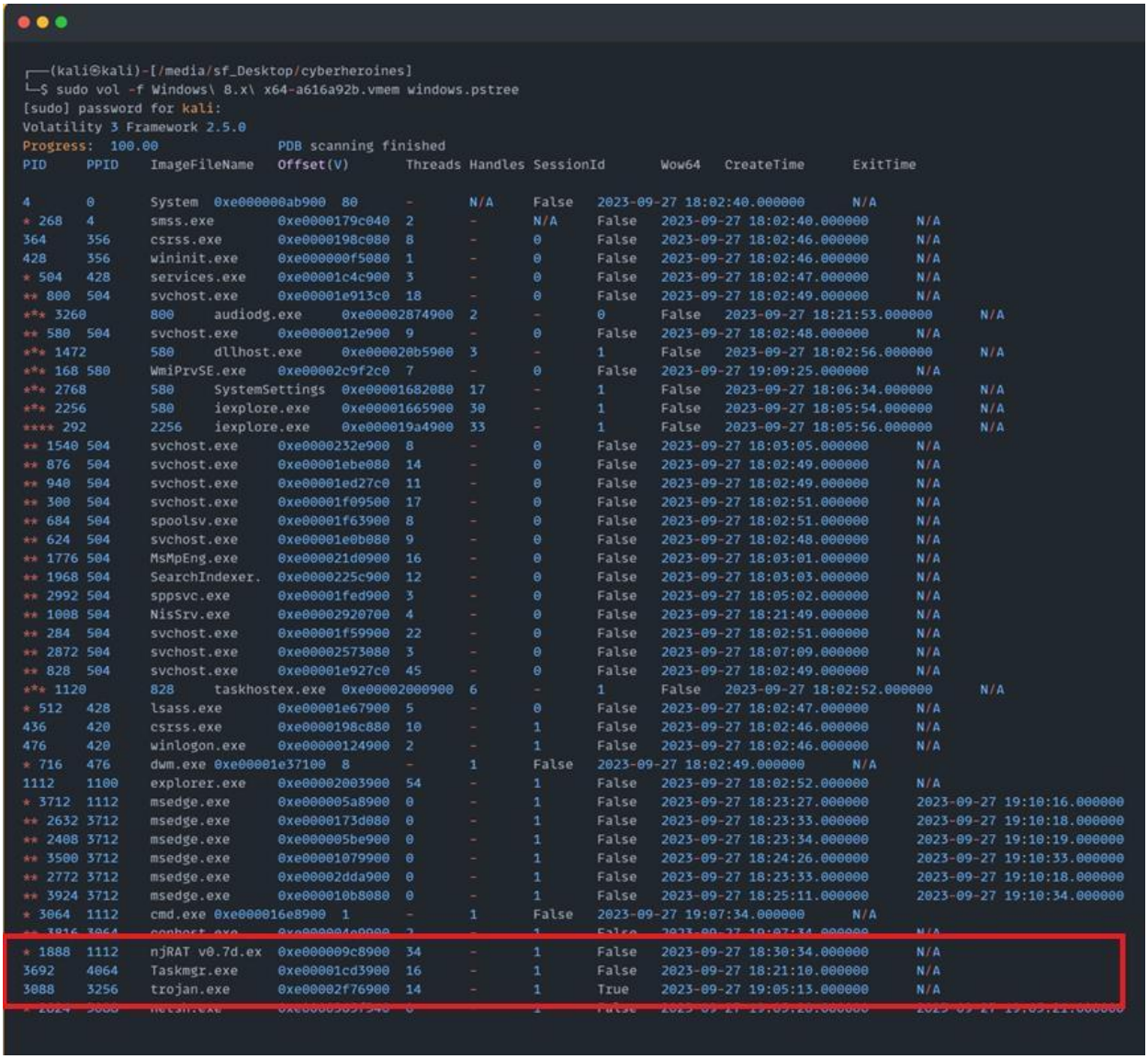
```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem windows.pslist
[sudo] password for kali:
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xe000000ab900  80      -       N/A     False   2023-09-27 18:02:40.000000      N/A     Disabled
268     4       smss.exe        0xe0000179c040  2       -       N/A     False   2023-09-27 18:02:40.000000      N/A     Disabled
364     356     csrss.exe       0xe0000198c080  8       -       0       False   2023-09-27 18:02:46.000000      N/A     Disabled
428     356     wininit.exe     0xe000000f5080  1       -       0       False   2023-09-27 18:02:46.000000      N/A     Disabled
436     420     csrss.exe       0xe0000198c880  10      -       1       False   2023-09-27 18:02:46.000000      N/A     Disabled
476     420     winlogon.exe    0xe00000124900  2       -       1       False   2023-09-27 18:02:46.000000      N/A     Disabled
504     428     services.exe    0xe00001c4c900  3       -       0       False   2023-09-27 18:02:47.000000      N/A     Disabled
512     428     lsass.exe       0xe00001e67900  5       -       0       False   2023-09-27 18:02:47.000000      N/A     Disabled
580     504     svchost.exe     0xe0000012e900  9       -       0       False   2023-09-27 18:02:48.000000      N/A     Disabled
624     504     svchost.exe     0xe00001e0b080  9       -       0       False   2023-09-27 18:02:48.000000      N/A     Disabled
716     476     dwm.exe 0xe00001e37100  8       -       1       False   2023-09-27 18:02:49.000000      N/A     Disabled
800     504     svchost.exe     0xe00001e913c0  18      -       0       False   2023-09-27 18:02:49.000000      N/A     Disabled
828     504     svchost.exe     0xe00001e927c0  45      -       0       False   2023-09-27 18:02:49.000000      N/A     Disabled
876     504     svchost.exe     0xe00001ebe080  14      -       0       False   2023-09-27 18:02:49.000000      N/A     Disabled
948     504     svchost.exe     0xe00001ed27c0  11      -       0       False   2023-09-27 18:02:49.000000      N/A     Disabled
300     504     svchost.exe     0xe00001f09500  17      -       0       False   2023-09-27 18:02:51.000000      N/A     Disabled
684     504     spoolsv.exe     0xe00001f63900  8       -       0       False   2023-09-27 18:02:51.000000      N/A     Disabled
284     504     svchost.exe     0xe00001f59900  22      -       0       False   2023-09-27 18:02:51.000000      N/A     Disabled
1112    1100    explorer.exe    0xe00002003900  54      -       1       False   2023-09-27 18:02:52.000000      N/A     Disabled
1120    828     taskhostex.exe  0xe00002000900  6       -       1       False   2023-09-27 18:02:52.000000      N/A     Disabled
1472    580     dllhost.exe     0xe000020b5900  3       -       1       False   2023-09-27 18:02:56.000000      N/A     Disabled
1776    504     MsMpEng.exe     0xe000021d0900  16      -       0       False   2023-09-27 18:03:01.000000      N/A     Disabled
1968    504     SearchIndexer.  0xe0000225c900  12      -       0       False   2023-09-27 18:03:03.000000      N/A     Disabled
1540    504     svchost.exe     0xe0000232e900  8       -       0       False   2023-09-27 18:03:05.000000      N/A     Disabled
2992    504     sppsvc.exe      0xe00001fed900  3       -       0       False   2023-09-27 18:05:02.000000      N/A     Disabled
2256    580     iexplore.exe    0xe00001665900  30      -       1       False   2023-09-27 18:05:54.000000      N/A     Disabled
292     2256    iexplore.exe    0xe000019a4900  33      -       1       False   2023-09-27 18:05:56.000000      N/A     Disabled
2768    580     SystemSettings  0xe00001682080  17      -       1       False   2023-09-27 18:06:34.000000      N/A     Disabled
2872    504     svchost.exe     0xe00002573080  3       -       0       False   2023-09-27 18:07:09.000000      N/A     Disabled
3692    4064    Taskmgr.exe     0xe00001cd3900  16      -       1       False   2023-09-27 18:21:10.000000      N/A     Disabled
1008    504     NisSrv.exe      0xe00002920700  4       -       0       False   2023-09-27 18:21:49.000000      N/A     Disabled
3260    800     audiodg.exe     0xe00002874900  2       -       0       False   2023-09-27 18:21:53.000000      N/A     Disabled
3712    1112    msedge.exe      0xe000005a8900  0       -       1       False   2023-09-27 18:23:27.000000      2023-09-27 19:10:16.000000      Disabled
2772    3712    msedge.exe      0xe00002dda900  0       -       1       False   2023-09-27 18:23:33.000000      2023-09-27 19:10:18.000000      Disabled
2632    3712    msedge.exe      0xe0000173d080  0       -       1       False   2023-09-27 18:23:33.000000      2023-09-27 19:10:18.000000      Disabled
2408    3712    msedge.exe      0xe000005be900  0       -       1       False   2023-09-27 18:23:34.000000      2023-09-27 19:10:19.000000      Disabled
3500    3712    msedge.exe      0xe00001079900  0       -       1       False   2023-09-27 18:24:26.000000      2023-09-27 19:10:33.000000      Disabled
3924    3712    msedge.exe      0xe000010b8080  0       -       1       False   2023-09-27 18:25:11.000000      2023-09-27 19:10:34.000000      Disabled
1888    1112    njRAT v0.7d.ex  0xe000009c8900  34      -       1       False   2023-09-27 18:30:34.000000      N/A     Disabled
3088    3256    trojan.exe      0xe00002f76900  14      -       1       True    2023-09-27 19:05:13.000000      N/A     Disabled
2824    3088    netsh.exe       0xe0000365f340  6       -       1       False   2023-09-27 19:05:20.000000      2023-09-27 19:05:21.000000      Disabled
3064    1112    cmd.exe 0xe000016e8900  1       -       1       False   2023-09-27 19:07:34.000000      N/A     Disabled
3816    3064    conhost.exe     0xe000004e9900  2       -       1       False   2023-09-27 19:07:34.000000      N/A     Disabled
168     580     WmiPrvSE.exe    0xe00002c9f2c0  7       -       0       False   2023-09-27 19:09:25.000000      N/A     Disabled
```

***Volatility – 3 with psscan:***



```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem windows.psscan
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

1888    1112    njRAT v0.7d.ex  0x5aafd900      34      -       1       False   2023-09-27 18:30:34.000000      N/A     Disabled
2824    3088    netsh.exe       0x7aa5f340      0       -       1       False   2023-09-27 19:05:20.000000      2023-09-27 19:05:21.000000      Disabled
3088    3256    trojan.exe      0x7b376900      14      -       1       True    2023-09-27 19:05:13.000000      N/A     Disabled
168     580     WmiPrvSE.exe    0x7b49f2c0      7       -       0       False   2023-09-27 19:09:25.000000      N/A     Disabled
2772    3712    msedge.exe      0x7b5da900      0       -       1       False   2023-09-27 18:23:33.000000      2023-09-27 19:10:18.000000      Disabled
3260    800     audiodg.exe     0x7b874900      2       -       0       False   2023-09-27 18:21:53.000000      N/A     Disabled
1008    504     NisSrv.exe      0x7b920700      4       -       0       False   2023-09-27 18:21:49.000000      N/A     Disabled
2872    504     svchost.exe     0x7bd73080      3       -       0       False   2023-09-27 18:07:09.000000      N/A     Disabled
1968    504     SearchIndexer.  0x7be5c900      12      -       0       False   2023-09-27 18:03:03.000000      N/A     Disabled
1540    504     svchost.exe     0x7bf2e900      8       -       0       False   2023-09-27 18:03:05.000000      N/A     Disabled
1120    828     taskhostex.exe  0x7c000900      6       -       1       False   2023-09-27 18:02:52.000000      N/A     Disabled
1112    1100    explorer.exe    0x7c003900      54      -       1       False   2023-09-27 18:02:52.000000      N/A     Disabled
1472    580     dllhost.exe     0x7c0b5900      3       -       1       False   2023-09-27 18:02:56.000000      N/A     Disabled
1776    504     MsMpEng.exe     0x7c1d0900      16      -       0       False   2023-09-27 18:03:01.000000      N/A     Disabled
624     504     svchost.exe     0x7c20b080      9       -       0       False   2023-09-27 18:02:48.000000      N/A     Disabled
716     476     dwm.exe 0x7c237100      8       -       1       False   2023-09-27 18:02:49.000000      N/A     Disabled
512     428     lsass.exe       0x7c267900      5       -       0       False   2023-09-27 18:02:47.000000      N/A     Disabled
800     504     svchost.exe     0x7c2913c0      18      -       0       False   2023-09-27 18:02:49.000000      N/A     Disabled
828     504     svchost.exe     0x7c2927c0      45      -       0       False   2023-09-27 18:02:49.000000      N/A     Disabled
876     504     svchost.exe     0x7c2be080      14      -       0       False   2023-09-27 18:02:49.000000      N/A     Disabled
940     504     svchost.exe     0x7c2d27c0      11      -       0       False   2023-09-27 18:02:49.000000      N/A     Disabled
300     504     svchost.exe     0x7c309500      17      -       0       False   2023-09-27 18:02:51.000000      N/A     Disabled
284     504     svchost.exe     0x7c359900      22      -       0       False   2023-09-27 18:02:51.000000      N/A     Disabled
684     504     spoolsv.exe     0x7c363900      8       -       0       False   2023-09-27 18:02:51.000000      N/A     Disabled
2992    504     sppsvc.exe      0x7c3ed900      3       -       0       False   2023-09-27 18:05:02.000000      N/A     Disabled
504     428     services.exe    0x7c44c900      3       -       0       False   2023-09-27 18:02:47.000000      N/A     Disabled
3692    4064    Taskmgr.exe     0x7c4d3900      16      -       1       False   2023-09-27 18:21:10.000000      N/A     Disabled
364     356     csrss.exe       0x7c98c080      8       -       0       False   2023-09-27 18:02:46.000000      N/A     Disabled
436     420     csrss.exe       0x7c98c880      10      -       1       False   2023-09-27 18:02:46.000000      N/A     Disabled
292     2256    iexplore.exe    0x7c9a4900      33      -       1       False   2023-09-27 18:05:56.000000      N/A     Disabled
2256    580     iexplore.exe    0x7ca65900      30      -       1       False   2023-09-27 18:05:54.000000      N/A     Disabled
2768    580     SystemSettings  0x7ca82080      17      -       1       False   2023-09-27 18:06:34.000000      N/A     Disabled
3064    1112    cmd.exe 0x7cae8900      1       -       1       False   2023-09-27 19:07:34.000000      N/A     Disabled
2632    3712    msedge.exe      0x7cb3d080      0       -       1       False   2023-09-27 18:23:33.000000      2023-09-27 19:10:18.000000      Disabled
268     4       smss.exe        0x7cb9c040      2       -       N/A     False   2023-09-27 18:02:40.000000      N/A     Disabled
3500    3712    msedge.exe      0x7d079900      0       -       1       False   2023-09-27 18:24:26.000000      2023-09-27 19:10:33.000000      Disabled
3924    3712    msedge.exe      0x7d0b8080      0       -       1       False   2023-09-27 18:25:11.000000      2023-09-27 19:10:34.000000      Disabled
3816    3064    conhost.exe     0x7dce9900      2       -       1       False   2023-09-27 19:07:34.000000      N/A     Disabled
3712    1112    msedge.exe      0x7dda8900      0       -       1       False   2023-09-27 18:23:27.000000      2023-09-27 19:10:16.000000      Disabled
2408    3712    msedge.exe      0x7ddbe900      0       -       1       False   2023-09-27 18:23:34.000000      2023-09-27 19:10:19.000000      Disabled
4       0       System  0x7e4ab900      80      -       N/A     False   2023-09-27 18:02:40.000000      N/A     Disabled
428     356     wininit.exe     0x7e4f5080      1       -       0       False   2023-09-27 18:02:46.000000      N/A     Disabled
476     420     winlogon.exe    0x7e524900      2       -       1       False   2023-09-27 18:02:46.000000      N/A     Disabled
580     504     svchost.exe     0x7e52e900      9       -       0       False   2023-09-27 18:02:48.000000      N/A     Disabled
```

***Volatility – 3 with pstree:***

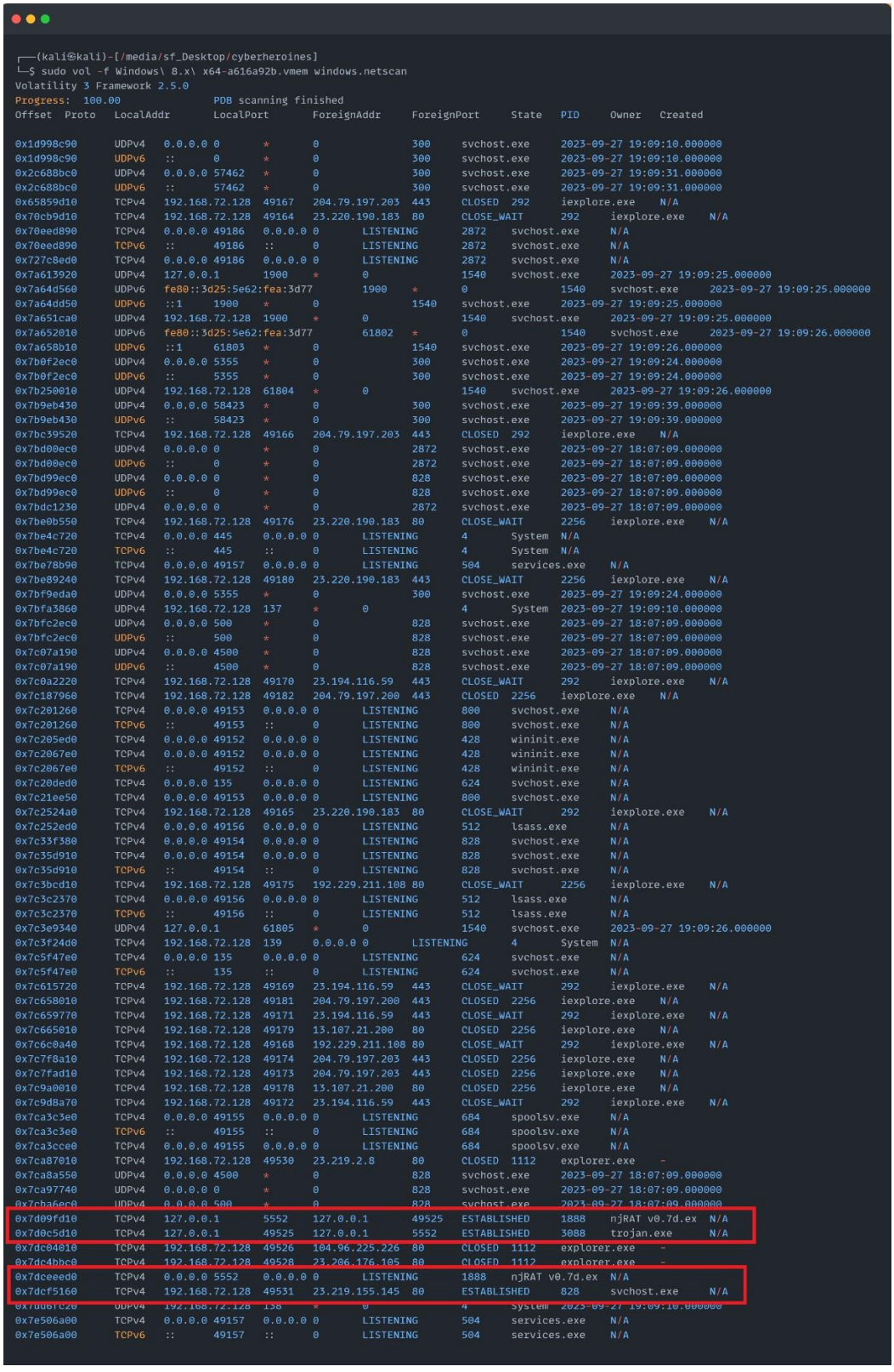


```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem windows.pstree
[sudo] password for kali:
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0xe000000ab900  80      -       N/A     False   2023-09-27 18:02:40.000000      N/A
* 268   4       smss.exe        0xe0000179c040  2       -       N/A     False   2023-09-27 18:02:40.000000      N/A
364     356     csrss.exe       0xe0000198c080  8       -       0       False   2023-09-27 18:02:46.000000      N/A
428     356     wininit.exe     0xe000000f5080  1       -       0       False   2023-09-27 18:02:46.000000      N/A
* 504   428     services.exe    0xe00001c4c900  3       -       0       False   2023-09-27 18:02:47.000000      N/A
** 800  504     svchost.exe     0xe00001e913c0  18      -       0       False   2023-09-27 18:02:49.000000      N/A
*** 3260        800     audiodg.exe     0xe00002874900  2       -       0       False   2023-09-27 18:21:53.000000      N/A
** 580  504     svchost.exe     0xe0000012e900  9       -       0       False   2023-09-27 18:02:48.000000      N/A
*** 1472        580     dllhost.exe     0xe000020b5900  3       -       1       False   2023-09-27 18:02:56.000000      N/A
*** 168 580     WmiPrvSE.exe    0xe00002c9f2c0  7       -       0       False   2023-09-27 19:09:25.000000      N/A
*** 2768        580     SystemSettings  0xe00001682080  17      -       1       False   2023-09-27 18:06:34.000000      N/A
*** 2256        580     iexplore.exe    0xe00001665900  30      -       1       False   2023-09-27 18:05:54.000000      N/A
**** 292        2256    iexplore.exe    0xe000019a4900  33      -       1       False   2023-09-27 18:05:56.000000      N/A
** 1540 504     svchost.exe     0xe0000232e900  8       -       0       False   2023-09-27 18:03:05.000000      N/A
** 876  504     svchost.exe     0xe00001ebe080  14      -       0       False   2023-09-27 18:02:49.000000      N/A
** 940  504     svchost.exe     0xe00001ed27c0  11      -       0       False   2023-09-27 18:02:49.000000      N/A
** 300  504     svchost.exe     0xe00001f09500  17      -       0       False   2023-09-27 18:02:51.000000      N/A
** 684  504     spoolsv.exe     0xe00001f63900  8       -       0       False   2023-09-27 18:02:51.000000      N/A
** 624  504     svchost.exe     0xe00001e0b080  9       -       0       False   2023-09-27 18:02:48.000000      N/A
** 1776 504     MsMpEng.exe     0xe000021d0900  16      -       0       False   2023-09-27 18:03:01.000000      N/A
** 1968 504     SearchIndexer.  0xe0000225c900  12      -       0       False   2023-09-27 18:03:03.000000      N/A
** 2992 504     sppsvc.exe      0xe00001fed900  3       -       0       False   2023-09-27 18:05:02.000000      N/A
** 1008 504     NisSrv.exe      0xe00002920700  4       -       0       False   2023-09-27 18:21:49.000000      N/A
** 284  504     svchost.exe     0xe00001f59900  22      -       0       False   2023-09-27 18:02:51.000000      N/A
** 2872 504     svchost.exe     0xe00002573080  3       -       0       False   2023-09-27 18:07:09.000000      N/A
** 828  504     svchost.exe     0xe00001e927c0  45      -       0       False   2023-09-27 18:02:49.000000      N/A
*** 1120        828     taskhostex.exe  0xe00002000900  6       -       1       False   2023-09-27 18:02:52.000000      N/A
* 512   428     lsass.exe       0xe00001e67900  5       -       0       False   2023-09-27 18:02:47.000000      N/A
436     420     csrss.exe       0xe0000198c880  10      -       1       False   2023-09-27 18:02:46.000000      N/A
476     420     winlogon.exe    0xe00000124900  2       -       1       False   2023-09-27 18:02:46.000000      N/A
* 716   476     dwm.exe 0xe00001e37100  8       -       1       False   2023-09-27 18:02:49.000000      N/A
1112    1100    explorer.exe    0xe00002003900  54      -       1       False   2023-09-27 18:02:52.000000      N/A
* 3712  1112    msedge.exe      0xe000005a8900  0       -       1       False   2023-09-27 18:23:27.000000      2023-09-27 19:10:16.000000
** 2632 3712    msedge.exe      0xe0000173d080  0       -       1       False   2023-09-27 18:23:33.000000      2023-09-27 19:10:18.000000
** 2408 3712    msedge.exe      0xe000005be900  0       -       1       False   2023-09-27 18:23:34.000000      2023-09-27 19:10:19.000000
** 3500 3712    msedge.exe      0xe00001079900  0       -       1       False   2023-09-27 18:24:26.000000      2023-09-27 19:10:33.000000
** 2772 3712    msedge.exe      0xe00002dda900  0       -       1       False   2023-09-27 18:23:33.000000      2023-09-27 19:10:18.000000
** 3924 3712    msedge.exe      0xe000010b8080  0       -       1       False   2023-09-27 18:25:11.000000      2023-09-27 19:10:34.000000
* 3064  1112    cmd.exe 0xe000016e8900  1       -       1       False   2023-09-27 19:07:34.000000      N/A
** 3816 3064    conhost.exe     0xe000004e0900  2       -       1       False   2023-09-27 19:07:34.000000      N/A
* 1888  1112    njRAT v0.7d.ex  0xe000009c8900  34      -       1       False   2023-09-27 18:30:34.000000      N/A
3692    4064    Taskmgr.exe     0xe00001cd3900  16      -       1       False   2023-09-27 18:21:10.000000      N/A
3088    3256    trojan.exe      0xe00002f76900  14      -       1       True    2023-09-27 19:05:13.000000      N/A
* 2024  3088    netsh.exe       0xe00005b37540  6       -       1       False   2023-09-27 19:09:20.000000      2023-09-27 19:09:21.000000
```

***Volatility – 3 with netstat:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem windows.netstat
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xe000019d8a70  TCPv4   192.168.72.128  49172   23.194.116.59   443     CLOSE_WAIT      292     iexplore.exe    N/A
0xe00002289240  TCPv4   192.168.72.128  49180   23.220.190.183  443     CLOSE_WAIT      2256    iexplore.exe    N/A
0xe00001a59770  TCPv4   192.168.72.128  49171   23.194.116.59   443     CLOSE_WAIT      292     iexplore.exe    N/A
0xe0000220b550  TCPv4   192.168.72.128  49176   23.220.190.183  80      CLOSE_WAIT      2256    iexplore.exe    N/A
0xe00001ac0a40  TCPv4   192.168.72.128  49168   192.229.211.108 80      CLOSE_WAIT      292     iexplore.exe    N/A
0xe000020a2220  TCPv4   192.168.72.128  49170   23.194.116.59   443     CLOSE_WAIT      292     iexplore.exe    N/A
0xe000010c5d10  TCPv4   127.0.0.1       49525   127.0.0.1       5552    ESTABLISHED     3088    trojan.exe      N/A
0xe00001a15720  TCPv4   192.168.72.128  49169   23.194.116.59   443     CLOSE_WAIT      292     iexplore.exe    N/A
0xe00007f7dd10  TCPv4   192.168.72.128  49164   23.220.190.183  80      CLOSE_WAIT      292     iexplore.exe    N/A
0xe00001fbcd10  TCPv4   192.168.72.128  49175   192.229.211.108 80      CLOSE_WAIT      2256    iexplore.exe    N/A
0xe00001e524a0  TCPv4   192.168.72.128  49165   23.220.190.183  80      CLOSE_WAIT      292     iexplore.exe    N/A
0xe0000109fd10  TCPv4   127.0.0.1       5552    127.0.0.1       49525   ESTABLISHED     1888    njRAT v0.7d.ex  N/A
0xe000004f5160  TCPv4   192.168.72.128  49531   23.219.155.145  80      ESTABLISHED     828     svchost.exe     N/A
0xe00001df47e0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       624     svchost.exe     N/A
0xe00001df47e0  TCPv6   ::      135     ::      0       LISTENING       624     svchost.exe     N/A
0xe00001e0ded0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       624     svchost.exe     N/A
0xe00001ff24d0  TCPv4   192.168.72.128  139     0.0.0.0 0       LISTENING       4       System  N/A
0xe0000224c720  TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  N/A
0xe0000224c720  TCPv6   ::      445     ::      0       LISTENING       4       System  N/A
```

***Volatility – 3 with netscan:***



```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem windows.netscan
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0x1d998c90      UDPv4   0.0.0.0 0       *       0               300     svchost.exe     2023-09-27 19:09:10.000000
0x1d998c90      UDPv6   ::      0       *       0               300     svchost.exe     2023-09-27 19:09:10.000000
0x2c688bc0      UDPv4   0.0.0.0 57462   *       0               300     svchost.exe     2023-09-27 19:09:31.000000
0x2c688bc0      UDPv6   ::      57462   *       0               300     svchost.exe     2023-09-27 19:09:31.000000
0x65859d10      TCPv4   192.168.72.128  49167   204.79.197.203  443     CLOSED  292     iexplore.exe    N/A
0x70cb9d10      TCPv4   192.168.72.128  49164   23.220.190.183  80      CLOSE_WAIT      292     iexplore.exe    N/A
0x70eed890      TCPv4   0.0.0.0 49186   0.0.0.0 0       LISTENING       2872    svchost.exe     N/A
0x70eed890      TCPv6   ::      49186   ::      0       LISTENING       2872    svchost.exe     N/A
0x727c8ed0      TCPv4   0.0.0.0 49186   0.0.0.0 0       LISTENING       2872    svchost.exe     N/A
0x7a613920      UDPv4   127.0.0.1       1900    *       0               1540    svchost.exe     2023-09-27 19:09:25.000000
0x7a64d560      UDPv6   fe80::3d25:5e62:fea:3d77        1900    *       0               1540    svchost.exe     2023-09-27 19:09:25.000000
0x7a64dd50      UDPv6   ::1     1900    *       0               1540    svchost.exe     2023-09-27 19:09:25.000000
0x7a651ca0      UDPv4   192.168.72.128  1900    *       0               1540    svchost.exe     2023-09-27 19:09:25.000000
0x7a652010      UDPv6   fe80::3d25:5e62:fea:3d77        61802   *       0               1540    svchost.exe     2023-09-27 19:09:26.000000
0x7a658b10      UDPv6   ::1     61803   *       0               1540    svchost.exe     2023-09-27 19:09:26.000000
0x7b0f2ec0      UDPv4   0.0.0.0 5355    *       0               300     svchost.exe     2023-09-27 19:09:24.000000
0x7b0f2ec0      UDPv6   ::      5355    *       0               300     svchost.exe     2023-09-27 19:09:24.000000
0x7b250010      UDPv4   192.168.72.128  61804   *       0               1540    svchost.exe     2023-09-27 19:09:26.000000
0x7b9eb430      UDPv4   0.0.0.0 58423   *       0               300     svchost.exe     2023-09-27 19:09:39.000000
0x7b9eb430      UDPv6   ::      58423   *       0               300     svchost.exe     2023-09-27 19:09:39.000000
0x7bc39520      TCPv4   192.168.72.128  49166   204.79.197.203  443     CLOSED  292     iexplore.exe    N/A
0x7bd00ec0      UDPv4   0.0.0.0 0       *       0               2872    svchost.exe     2023-09-27 18:07:09.000000
0x7bd00ec0      UDPv6   ::      0       *       0               2872    svchost.exe     2023-09-27 18:07:09.000000
0x7bd99ec0      UDPv4   0.0.0.0 0       *       0               828     svchost.exe     2023-09-27 18:07:09.000000
0x7bd99ec0      UDPv6   ::      0       *       0               828     svchost.exe     2023-09-27 18:07:09.000000
0x7bdc1230      UDPv4   0.0.0.0 0       *       0               2872    svchost.exe     2023-09-27 18:07:09.000000
0x7be0b550      TCPv4   192.168.72.128  49176   23.220.190.183  80      CLOSE_WAIT      2256    iexplore.exe    N/A
0x7be4c720      TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  N/A
0x7be4c720      TCPv6   ::      445     ::      0       LISTENING       4       System  N/A
0x7be78b90      TCPv4   0.0.0.0 49157   0.0.0.0 0       LISTENING       504     services.exe    N/A
0x7be89240      TCPv4   192.168.72.128  49180   23.220.190.183  443     CLOSE_WAIT      2256    iexplore.exe    N/A
0x7bf9eda0      UDPv4   0.0.0.0 5355    *       0               300     svchost.exe     2023-09-27 19:09:24.000000
0x7bfa3860      UDPv4   192.168.72.128  137     *       0               4       System  2023-09-27 19:09:10.000000
0x7bfc2ec0      UDPv4   0.0.0.0 500     *       0               828     svchost.exe     2023-09-27 18:07:09.000000
0x7bfc2ec0      UDPv6   ::      500     *       0               828     svchost.exe     2023-09-27 18:07:09.000000
0x7c07a190      UDPv4   0.0.0.0 4500    *       0               828     svchost.exe     2023-09-27 18:07:09.000000
0x7c07a190      UDPv6   ::      4500    *       0               828     svchost.exe     2023-09-27 18:07:09.000000
0x7c0a2220      TCPv4   192.168.72.128  49170   23.194.116.59   443     CLOSE_WAIT      292     iexplore.exe    N/A
0x7c187960      TCPv4   192.168.72.128  49182   204.79.197.200  443     CLOSED  2256    iexplore.exe    N/A
0x7c201260      TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       800     svchost.exe     N/A
0x7c201260      TCPv6   ::      49153   ::      0       LISTENING       800     svchost.exe     N/A
0x7c205ed0      TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       428     wininit.exe     N/A
0x7c2067e0      TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       428     wininit.exe     N/A
0x7c2067e0      TCPv6   ::      49152   ::      0       LISTENING       428     wininit.exe     N/A
0x7c20ded0      TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       624     svchost.exe     N/A
0x7c21ee50      TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       800     svchost.exe     N/A
0x7c2524a0      TCPv4   192.168.72.128  49165   23.220.190.183  80      CLOSE_WAIT      292     iexplore.exe    N/A
0x7c252ed0      TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       512     lsass.exe       N/A
0x7c33f380      TCPv4   0.0.0.0 49154   0.0.0.0 0       LISTENING       828     svchost.exe     N/A
0x7c35d910      TCPv4   0.0.0.0 49154   0.0.0.0 0       LISTENING       828     svchost.exe     N/A
0x7c35d910      TCPv6   ::      49154   ::      0       LISTENING       828     svchost.exe     N/A
0x7c3bcd10      TCPv4   192.168.72.128  49175   192.229.211.108 80      CLOSE_WAIT      2256    iexplore.exe    N/A
0x7c3c2370      TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       512     lsass.exe       N/A
0x7c3c2370      TCPv6   ::      49156   ::      0       LISTENING       512     lsass.exe       N/A
0x7c3e9340      UDPv4   127.0.0.1       61805   *       0               1540    svchost.exe     2023-09-27 19:09:26.000000
0x7c3f24d0      TCPv4   192.168.72.128  139     0.0.0.0 0       LISTENING       4       System  N/A
0x7c5f47e0      TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       624     svchost.exe     N/A
0x7c5f47e0      TCPv6   ::      135     ::      0       LISTENING       624     svchost.exe     N/A
0x7c615720      TCPv4   192.168.72.128  49169   23.194.116.59   443     CLOSE_WAIT      292     iexplore.exe    N/A
0x7c658010      TCPv4   192.168.72.128  49181   204.79.197.200  443     CLOSED  2256    iexplore.exe    N/A
0x7c659770      TCPv4   192.168.72.128  49171   23.194.116.59   443     CLOSE_WAIT      292     iexplore.exe    N/A
0x7c665010      TCPv4   192.168.72.128  49179   13.107.21.200   80      CLOSED  2256    iexplore.exe    N/A
0x7c6c0a40      TCPv4   192.168.72.128  49168   192.229.211.108 80      CLOSE_WAIT      292     iexplore.exe    N/A
0x7c7f8a10      TCPv4   192.168.72.128  49174   204.79.197.203  443     CLOSED  2256    iexplore.exe    N/A
0x7c7fad10      TCPv4   192.168.72.128  49173   204.79.197.203  443     CLOSED  2256    iexplore.exe    N/A
0x7c9a0010      TCPv4   192.168.72.128  49178   13.107.21.200   80      CLOSED  2256    iexplore.exe    N/A
0x7c9d8a70      TCPv4   192.168.72.128  49172   23.194.116.59   443     CLOSE_WAIT      292     iexplore.exe    N/A
0x7ca3c3e0      TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       684     spoolsv.exe     N/A
0x7ca3c3e0      TCPv6   ::      49155   ::      0       LISTENING       684     spoolsv.exe     N/A
0x7ca3cce0      TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       684     spoolsv.exe     N/A
0x7ca87010      TCPv4   192.168.72.128  49530   23.219.2.8      80      CLOSED  1112    explorer.exe    -
0x7ca8a550      UDPv4   0.0.0.0 4500    *       0               828     svchost.exe     2023-09-27 18:07:09.000000
0x7ca97740      UDPv4   0.0.0.0 0       *       0               828     svchost.exe     2023-09-27 18:07:09.000000
0x7cba6ec0      UDPv4   0.0.0.0 500     *       0               828     svchost.exe     2023-09-27 18:07:09.000000
0x7d09fd10      TCPv4   127.0.0.1       5552    127.0.0.1       49525   ESTABLISHED     1888    njRAT v0.7d.ex  N/A
0x7d0c5d10      TCPv4   127.0.0.1       49525   127.0.0.1       5552    ESTABLISHED     3088    trojan.exe      N/A
0x7dc04010      TCPv4   192.168.72.128  49526   104.96.225.226  80      CLOSED  1112    explorer.exe    -
0x7dc4bbc0      TCPv4   192.168.72.128  49528   23.206.176.105  80      CLOSED  1112    explorer.exe    -
0x7dceeed0      TCPv4   0.0.0.0 5552    0.0.0.0 0       LISTENING       1888    njRAT v0.7d.ex  N/A
0x7dcf5160      TCPv4   192.168.72.128  49531   23.219.155.145  80      ESTABLISHED     828     svchost.exe     N/A
0x7dd6fc20      UDPv4   192.168.72.128  138     *       0               4       System  2023-09-27 19:09:10.000000
0x7e506a00      TCPv4   0.0.0.0 49157   0.0.0.0 0       LISTENING       504     services.exe    N/A
0x7e506a00      TCPv6   ::      49157   ::      0       LISTENING       504     services.exe    N/A
```

***Volatility – 3 with cmdline:***

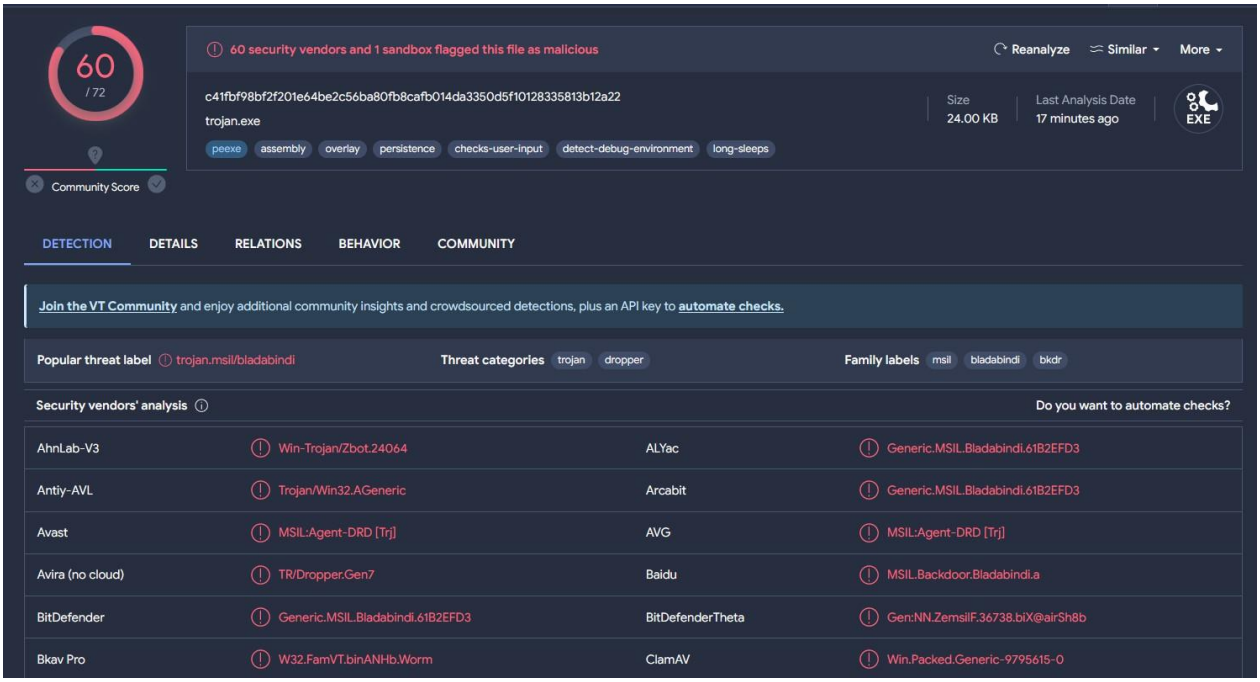
```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem windows.cmdline
[sudo] password for kali:
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  Required memory at 0x20 is not valid (process exited?)
268     smss.exe        \SystemRoot\System32\smss.exe
364     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1
ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
428     wininit.exe     wininit.exe
436     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1
ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
476     winlogon.exe    winlogon.exe
504     services.exe    C:\Windows\system32\services.exe
512     lsass.exe       C:\Windows\system32\lsass.exe
580     svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch
624     svchost.exe     C:\Windows\system32\svchost.exe -k RPCSS
716     dwm.exe "dwm.exe"
800     svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
828     svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs
876     svchost.exe     C:\Windows\system32\svchost.exe -k LocalService
940     svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
300     svchost.exe     C:\Windows\system32\svchost.exe -k NetworkService
684     spoolsv.exe     C:\Windows\System32\spoolsv.exe
284     svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
1112    explorer.exe    C:\Windows\Explorer.EXE
1120    taskhostex.exe  taskhostex.exe
1472    dllhost.exe     C:\Windows\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683}
1776    MsMpEng.exe     "C:\Program Files\Windows Defender\MsMpEng.exe"
1968    SearchIndexer.  C:\Windows\system32\SearchIndexer.exe /Embedding
1540    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
2992    sppsvc.exe      C:\Windows\system32\sppsvc.exe
2256    iexplore.exe    "C:\Program Files\Internet Explorer\iexplore.exe" -ServerName:DefaultBrowserServer
292     iexplore.exe    "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:2256 CREDAT:267777 /prefetch:1
```

***Static Analysis of Trojan.exe process:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem -o dumps/processdumps/pid.3088/ windows.dumpfiles --pid 3088
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

ImageSectionObject      0xe00002c81c90  WMINet_Utils.dll        Error dumping file
DataSectionObject       0xe0000090df20  trojan.exe      file.0xe0000090df20.0xe00002fc3790.DataSectionObject.trojan.exe.dat
ImageSectionObject      0xe0000090df20  trojan.exe      Error dumping file
DataSectionObject       0xe00001d0edd0  System.Data.dll file.0xe00001d0edd0.0xe00003c35320.DataSectionObject.System.Data.dll.dat
ImageSectionObject      0xe00001d0edd0  System.Data.dll Error dumping file
DataSectionObject       0xe00001d0edd0  System.Data.dll file.0xe00001d0edd0.0xe00003c35320.DataSectionObject.System.Data.dll.dat
ImageSectionObject      0xe00001d0edd0  System.Data.dll Error dumping file
ImageSectionObject      0xe000021fec70  profapi.dll     file.0xe000021fec70.0xe0000165ee20.ImageSectionObject.profapi.dll.img
DataSectionObject       0xe00002500190  9e5513007821 5e512579    Error dumping file
ImageSectionObject      0xe00001a56a60  winmmbase.dll   file.0xe00001a56a60.0xe00001607380.ImageSectionObject.winmmbase.dll.img
ImageSectionObject      0xe00002192ea0  IPHLPAPI.DLL    Error dumping file
ImageSectionObject      0xe00002318ae0  winnsi.dll      file.0xe00002318ae0.0xe00001f9a300.ImageSectionObject.winnsi.dll.img
ImageSectionObject      0xe00002642b50  WindowsCodecs.dll       Error dumping file
ImageSectionObject      0xe000017f4450  devobj.dll      Error dumping file
ImageSectionObject      0xe000037a7360  avicap32.dll    Error dumping file
ImageSectionObject      0xe0000165c1a0  version.dll     file.0xe0000165c1a0.0xe0000165e010.ImageSectionObject.version.dll.img
ImageSectionObject      0xe000021c3b10  winmm.dll       file.0xe000021c3b10.0xe00001ff1aa0.ImageSectionObject.winmm.dll.img
ImageSectionObject      0xe0000165e730  rsaenh.dll      file.0xe0000165e730.0xe000020c9510.ImageSectionObject.rsaenh.dll.img
ImageSectionObject      0xe000016d58f0  bcrypt.dll      file.0xe000016d58f0.0xe0000215e950.ImageSectionObject.bcrypt.dll.img
```

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines/dumps/processdumps/pid.3088]
└─$ file file.0xe0000090df20.0xe00002fc3790.DataSectionObject.trojan.exe.dat
file.0xe0000090df20.0xe00002fc3790.DataSectionObject.trojan.exe.dat: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows, 2 sections
```

This is a windows PE executable file. Let's upload it to the Virus Total and get the analysis report of trojan.exe file.




***Static Analysis of njRAT v0.7d.exe process:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem -o dumps/processdumps/ windows.dumpfiles --pid 1888
[sudo] password for kali:
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0xe00000782a00  System.Windows.Forms.dll        Error dumping file
ImageSectionObject      0xe00000782a00  System.Windows.Forms.dll        Error dumping file
ImageSectionObject      0xe000007a6610  Microsoft.VisualBasic.dll       Error dumping file
ImageSectionObject      0xe000007a6610  Microsoft.VisualBasic.dll       Error dumping file
DataSectionObject       0xe00000782a00  System.Windows.Forms.dll        Error dumping file
ImageSectionObject      0xe00000782a00  System.Windows.Forms.dll        Error dumping file
DataSectionObject       0xe00003aa5b90  System.Runtime.Remoting.dll     Error dumping file
DataSectionObject       0xe00003aa5b90  System.Runtime.Remoting.dll     Error dumping file
DataSectionObject       0xe00001f1ee10  StaticCache.dat Error dumping file
SharedCacheMap  0xe00001f1ee10  StaticCache.dat file.0xe00001f1ee10.0xe00001f1e460.SharedCacheMap.StaticCache.dat.vacb
DataSectionObject       0xe00003bd0b90  mscorrc.dll     Error dumping file
DataSectionObject       0xe00001ee0ae0  ~FontCache-FontFace.dat Error dumping file
DataSectionObject       0xe00000912f20  System.configuration.dll        Error dumping file
ImageSectionObject      0xe00000912f20  System.configuration.dll        Error dumping file
DataSectionObject       0xe00000912f20  System.configuration.dll        Error dumping file
ImageSectionObject      0xe00000912f20  System.configuration.dll        Error dumping file
DataSectionObject       0xe000024762b0  explorerframe.dll.mui   file.0xe000024762b0.0xe00002395ca0.DataSectionObject.explorerframe.dll.mui.dat
ImageSectionObject      0xe0000090fbf0  System.XML.dll  Error dumping file
ImageSectionObject      0xe0000090fbf0  System.XML.dll  Error dumping file
DataSectionObject       0xe00001f96bb0  cversions.2.db  file.0xe00001f96bb0.0xe00003564010.DataSectionObject.cversions.2.db.dat
DataSectionObject       0xe00001e4b440  oleaccrc.dll    file.0xe00001e4b440.0xe00001e58360.DataSectionObject.oleaccrc.dll.dat
ImageSectionObject      0xe00001e4b440  oleaccrc.dll    file.0xe00001e4b440.0xe000016d7740.ImageSectionObject.oleaccrc.dll.img
DataSectionObject       0xe00001f96bb0  cversions.2.db  file.0xe00001f96bb0.0xe00003564010.DataSectionObject.cversions.2.db.dat
```

Based on the list of processes and DLLs, a few stand out as potentially suspicious:

- sechost.dll - This is the Windows Security Center process, often abused by malware to disguise malicious activity.
- thumbcache.dll - The thumbnail cache DLL can be used to hide malicious code.
- wininet.dll - The Internet Explorer library, sometimes injected by malware.
- urlmon.dll - URL moniker DLL, can be used for malicious network connections.
- mssprxy.dll - Microsoft Antimalware Service Proxy, often mimicked by malware.

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines/dumps/processdumps/pid.1888]
└─$ file file.0xe00001869250.0xe0000187e0e0.ImageSectionObject.shell32.dll.img
file.0xe00001869250.0xe0000187e0e0.ImageSectionObject.shell32.dll.img: PE32+ executable (DLL) (GUI) x86-64, for MS Windows, 8 sections
```

***Analyzing the child cmd.exe process:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem -o dumps/processdumps/pid.3064/ windows.dumpfiles --pid 3064
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

ImageSectionObject      0xe000023b8bf0  cmd.exe file.0xe000023b8bf0.0xe000022d9010.ImageSectionObject.cmd.exe.img
ImageSectionObject      0xe0000183e070  kernel32.dll    Error dumping file
ImageSectionObject      0xe000018714c0  KernelBase.dll  Error dumping file
ImageSectionObject      0xe00001e5e8c0  winbrand.dll    file.0xe00001e5e8c0.0xe00001e5e2f0.ImageSectionObject.winbrand.dll.img
ImageSectionObject      0xe000017db9b0  msvcrt.dll      Error dumping file
ImageSectionObject      0xe00005dff330  ntdll.dll       Error dumping file
```

```
LocalFree
GlobalFree
SetProcessAffinityMask
ApiSetQueryApiSetPresence
ResolveDelayLoadedAPI
DelayLoadFailureHook
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- Copyright (c) Microsoft Corporation -->
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
    version="5.1.0.0"
    processorArchitecture="amd64"
    name="Microsoft.Windows.FileSystem.CMD"
    type="win32"
<description>Windows Command Processor</description>
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
        <requestedPrivileges>
            <requestedExecutionLevel
                level="asInvoker"
                uiAccess="false"
            />
        </requestedPrivileges>
    </security>
</trustInfo>
<application  xmlns="urn:schemas-microsoft-com:asm.v3">
    <windowsSettings>
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
    </windowsSettings>
</application>
```

***Analyzing memory dump of njRAT.exe process:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem -o dumps/memdumps/pid.1888/ windows.memmap --dump --pid 1888
[sudo] password for kali:
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Virtual Physical        Size    Offset in File  File output

0x20000 0x52689000      0x1000  0x0     pid.1888.dmp
0x21000 0x4f4d0000      0x1000  0x1000  pid.1888.dmp
0x22000 0x2b42a000      0x1000  0x2000  pid.1888.dmp
0x23000 0x2d191000      0x1000  0x3000  pid.1888.dmp
0x24000 0x357a4000      0x1000  0x4000  pid.1888.dmp
0x26000 0x1c636000      0x1000  0x5000  pid.1888.dmp
0x28000 0x45938000      0x1000  0x6000  pid.1888.dmp
0x29000 0x28439000      0x1000  0x7000  pid.1888.dmp
0x2a000 0x9e43a000      0x1000  0x8000  pid.1888.dmp
0x2b000 0x33147000      0x1000  0x9000  pid.1888.dmp
0x2d000 0xd57000        0x1000  0xa000  pid.1888.dmp
0x2f000 0xa2e5d000      0x1000  0xb000  pid.1888.dmp
0x30000 0x2605e000      0x1000  0xc000  pid.1888.dmp
0x31000 0x7445f000      0x1000  0xd000  pid.1888.dmp
0x32000 0x6a460000      0x1000  0xe000  pid.1888.dmp
0x33000 0x74461000      0x1000  0xf000  pid.1888.dmp
0x34000 0x57f62000      0x1000  0x10000 pid.1888.dmp
0x35000 0xbaa63000      0x1000  0x11000 pid.1888.dmp
0x38000 0x9777d000      0x1000  0x12000 pid.1888.dmp
```

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines/dumps/memdumps/pid.1888]
└─$ strings -e l pid.1888.dmp | grep -i "trojan"
Exe  trojan.exe
trojan[3088]
trojan.exe
C:\Users\rushe\AppData\Local\Temp\trojan.exe
    IL_001a:  ldstr      "trojan.exe"
Trojan
Trojan
Trojan
Trojan
Trojan
Trojan.exe
TROJAN.EXE-8602D175.pf3
TROJAN.EXE-F95394DB.pf3
TROJAN~1.PF
TROJAN~2.PF
trojan.exem
{DB962B84-19AC-428F-9A00-F6AAC4058EFF}trojan.exe
C:\Users\rushe\AppData\Local\Temp\trojan.exe
{9E5A0632-6103-4304-AFAD-07EA09EF2454}trojan.exe
C:\Users\rushe\AppData\Local\Temp\trojan.exe
657a1fb3  1d9f175 file:C:/Users/rushe/Desktop/Trojan.pdb  8000000c   0  80041201       1       4294967295      911
Trojan.exe
Trojan.exe
Trojan.exe
TROJAN~1.PF0
TROJAN.EXE-F95394DB.pf
trojan.exe
```

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines/dumps/memdumps/pid.1888]
└─$ strings -e l pid.1888.dmp | grep -i "njRAT"
njRAT
njRAT.exe
njRAT.exe
njRAT
C:\Users\rushe\Downloads\njRAT-master\njRAT-master\njRAT v0.7d.exe
njRAT v0.7d.exe
C:\Users\rushe\Downloads\njRAT-master\njRAT-master\
MyApplication.app,version="1.0.0.0"C:\Users\rushe\Downloads\njRAT-master\njRAT-master\njRAT v0.7d.exe
 brian8544/njRAT: A great remote administrator tool with many features and very stable. - Profile 1 - Microsoft
njRAT v0.7d    Port[ 5552 ]    Online[ 2 ]    Selected[1] REQ[0]
C:\Users\rushe\Downloads\njRAT-master\njRAT-master\
C:\Users\rushe\Downloads\njRAT-master\njRAT-master\njRAT v0.7d.config
njRAT[1888]
njRAT v0.7d    Port[ 5552 ]    Online[ 2 ]    Selected[1] REQ[0]
njRAT v0.7d
C:\Users\rushe\Downloads\njRAT-master\njRAT-master
C:\Users\rushe\Downloads\njRAT-master\njRAT-master\GeoIP.dat
njRAT
C:\Users\rushe\Downloads\njRAT-master\njRAT-master\njRAT v0.7d.config
C:\Users\rushe\Downloads\njRAT-master\njRAT-master\njRAT v0.7d.exe
C:\Users\rushe\Downloads\njRAT-master\njRAT-master\njRAT v0.7d.exe
njRAT
njRAT.exe
njRAT.exe
njRAT
```

```
└─$ strings -e l pid.1888.dmp | grep -i "cryptomi"
Cryptomining
Cryptomining.DATA
Cryptomining
Cryptomining.DATA
Cryptomining
Cryptomining
Cryptomining.DATA
Cryptomining
Cryptomining
Cryptomining
Cryptomining
<Cryptomining
<Cryptomining
<Cryptomining
<Cryptomining
<Cryptomining
<Cryptomining
<Cryptomining
<Cryptomining
<Cryptomining
0\Trust Protection Lists\Sigma\Cryptomining
"<Cryptomining.DATA
\Program Files (x86)\Microsoft\Edge\Temp\source896_1162248801\109.0.1518.140\Trust Protection Lists\Mu\Cryptomining
\Device\HarddiskVolume1\Program Files (x86)\Microsoft\Edge\Temp\source896_1162248801\109.0.1518.140\Trust Protection Lists\Sigma\Cryptomining
\Device\HarddiskVolume1\Program Files (x86)\Microsoft\Edge\Temp\source896_1162248801\109.0.1518.140\Trust Protection Lists\Mu\Cryptomining
Cryptomining
CRYPTOMINING
Cryptomining
CRYPTOMINING
\Program Files (x86)\Microsoft\Edge\Temp\source896_1162248801\109.0.1518.140\Trust Protection Lists\Sigma\Cryptomining
"<Cryptomining.DATA
\Device\HarddiskVolume1\Users\rushe\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping3712_1991401318\Sigma\Cryptomining
<Cryptomining
\Device\HarddiskVolume1\Users\rushe\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping3712_1991401318\Sigma\Cryptomining
\Users\rushe\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping3712_1991401318\Sigma\Cryptomining
\Device\HarddiskVolume1\Users\rushe\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping3712_1991401318\Sigma\Cryptomining
```

***Analyzing memory dump of trojan.exe process:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines/dumps/memdumps/pid.3088]
└─$ strings -e l pid.3088.dmp | grep -i "trojan"
trojan.exe
TROJAN.EXE
TROJAN.PDB
TROJAN.EXE-F95394DB.PF
TROJAN.EXE
TROJAN.EXE.LOG
trojan
C:\Users\rushe\AppData\Local\Temp\trojan.exe
C:\Users\rushe\AppData\Local\Temp\trojan.exe
trojan.exe
file:///C:/Users/rushe/AppData/Local/Temp/trojan.exe
TROJAN.EXE-8602D175.pf3
TROJAN.EXE-F95394DB.pf3
TROJAN~1.PF
TROJAN~2.PF
trojan.exem
{DB962B84-19AC-428F-9A00-F6AAC4058EFF}trojan.exe
C:\Users\rushe\AppData\Local\Temp\trojan.exe
{9E5A0632-6103-4304-AFAD-07EA09EF2454}trojan.exe
C:\Users\rushe\AppData\Local\Temp\trojan.exe
657a1fb3        1d9f175 file:C:/Users/rushe/Desktop/Trojan.pdb  8000000c        0
Trojan.exe
Trojan.exe
Trojan.exe
TROJAN~1.PF0
TROJAN.EXE-F95394DB.pf
trojan.exe
Trojan.exe.log
TROJAN~1.LOG
TROJAN~1.LOGog
Trojan.exe.log
```

```
<Trojan.exe.log
Trojan.exea.TMP
\Device\HarddiskVolume1\Users\rushe\Desktop\Trojan.exe
C:\Users\rushe\Desktop\Trojan.exe
C:\Users\rushe\AppData\Local\Temp\trojan.exe
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
\Device\HarddiskVolume1\Users\rushe\Desktop\Trojan.exe
\Device\HarddiskVolume1\Users\rushe\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Trojan.exe.log
:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
\Device\HarddiskVolume1\Users\rushe\Desktop\Trojan.exe
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
\Device\HarddiskVolume1\Users\rushe\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Trojan.exe.log
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
\Device\HarddiskVolume1\Users\rushe\AppData\Local\Temp\trojan.exe
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
SYSVOL\Users\rushe\AppData\Local\Temp\trojan.exe
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
"C:\Users\rushe\AppData\Local\Temp\trojan.exe" ..
```

: \Users \rushe\AppData\Loec1l \ Temp\ t ro Jnn. exe"
<Trojan.exe
"C:\Users\r ushe\AppData\Loeal\ Temp\ t ro Jan. exe"
:\Users\rushe\AppData\Loeal\Temp\troJan.exe" ..
"C: \Users \ms he\AppData\Loc al\ Temp\ trojan. exe"
"C: \Users \nis he\AppData\ Loe al\ Temp\ trojan. exe"
"C: \Users \rus he\AppData\ Loe c1l \ Temp\ tro j nn. exe"
"C: \Users \rushe\AppData\Loec1l\ Temp\trojan. exe"
\Devlee\HarddlskVolumel\Users\rushe\Desktop\Trojan.exe
·• C: \Users \r ushe\AppData\Loeal\ Temp\ t ro Jan. exe" ..
\Devtce\HarddlskVolumel\Users\rushe\AppData\Local\Temp\troJan.exe
"C: \Users \rus he\AppData\Loc al\ Temp\ trojan. exe"
"C: \Users \rus he\AppData\ Loe al\ Temp\ tro j nn. exe"

f lrewall add c1llowedprogram C:\Users\rushe\AppData\Loec1l\ Temp\trojan. exe trojan. exe ENABLE

C:\Users\rushe\AppData\Loeal\Temp\trojan.exe
C:\Users\rushe\AppData\Loeal\Temp\troJan.exe
C:\Users\rushe\AppData\Local\Temp\troj11n.exe
C:\Users\rushe\AppData\Loeal\Temp\trojnn.exe
\??\C:\Users\rushe\AppData\Loeal\Temp\trojan.exe
C:\Users\rushe\AppData\Loeal\Temp\trojan.exe

netsh fl rewal l add al lowedprogram 'C : \Users\ rushe\AppData\Local \ Temp\ trojan. exe" "tro Jan. exe" ENABLE

, <TROJAI .EXE- 8602D175. pf h
, <TROJAI .EXE- 8602D175. pf h
, <TROJAI .EXE- 8602D175. pf h
Trojan.exe.log
TROJAN l.LOG
TROJAN l.LOGog
Trojan. exe. log
\rushe\Desktop\Trojan.exe
TROJAr; . EXE-86O2D 175. pf3
TROJAN 2.PF
TROJAN 2.PFO
TROJAN.EXE-861J2D175. f

***Volatility – 3 with getsids:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem windows.getsids.GetSIDs
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
PID     Process SID     Name

4       System  S-1-5-18        Local System
4       System  S-1-5-32-544    Administrators
4       System  S-1-1-0 Everyone
4       System  S-1-5-11        Authenticated Users
4       System  S-1-16-16384    System Mandatory Level
268     smss.exe        S-1-5-18        Local System
268     smss.exe        S-1-5-32-544    Administrators
268     smss.exe        S-1-1-0 Everyone
268     smss.exe        S-1-5-11        Authenticated Users
268     smss.exe        S-1-16-16384    System Mandatory Level
364     csrss.exe       S-1-5-18        Local System
364     csrss.exe       S-1-5-32-544    Administrators
364     csrss.exe       S-1-1-0 Everyone
364     csrss.exe       S-1-5-11        Authenticated Users
364     csrss.exe       S-1-16-16384    System Mandatory Level
428     wininit.exe     S-1-5-18        Local System
428     wininit.exe     S-1-5-32-544    Administrators
428     wininit.exe     S-1-1-0 Everyone
428     wininit.exe     S-1-5-11        Authenticated Users
428     wininit.exe     S-1-16-16384    System Mandatory Level
436     csrss.exe       S-1-5-18        Local System
436     csrss.exe       S-1-5-32-544    Administrators
436     csrss.exe       S-1-1-0 Everyone
436     csrss.exe       S-1-5-11        Authenticated Users
436     csrss.exe       S-1-16-16384    System Mandatory Level
476     winlogon.exe    S-1-5-18        Local System
476     winlogon.exe    S-1-5-32-544    Administrators
```

```
1888    njRAT v0.7d.ex  S-1-5-21-1286361004-883023714-2557105895-1001   rushe
1888    njRAT v0.7d.ex  S-1-5-21-1286361004-883023714-2557105895-513    Domain Users
1888    njRAT v0.7d.ex  S-1-1-0 Everyone
1888    njRAT v0.7d.ex  S-1-5-114       Local Account (Member of Administrators)
1888    njRAT v0.7d.ex  S-1-5-32-544    Administrators
1888    njRAT v0.7d.ex  S-1-5-32-545    Users
1888    njRAT v0.7d.ex  S-1-5-4 Interactive
1888    njRAT v0.7d.ex  S-1-2-1 Console Logon (Users who are logged onto the physical console)
1888    njRAT v0.7d.ex  S-1-5-11        Authenticated Users
1888    njRAT v0.7d.ex  S-1-5-15        This Organization
1888    njRAT v0.7d.ex  S-1-5-113       Local Account
1888    njRAT v0.7d.ex  S-1-5-5-0-73603 Logon Session
1888    njRAT v0.7d.ex  S-1-2-0 Local (Users with the ability to log in locally)
1888    njRAT v0.7d.ex  S-1-5-64-10     NTLM Authentication
1888    njRAT v0.7d.ex  S-1-16-12288    High Mandatory Level
3088    trojan.exe      S-1-5-21-1286361004-883023714-2557105895-1001   rushe
3088    trojan.exe      S-1-5-21-1286361004-883023714-2557105895-513    Domain Users
3088    trojan.exe      S-1-1-0 Everyone
3088    trojan.exe      S-1-5-114       Local Account (Member of Administrators)
3088    trojan.exe      S-1-5-32-544    Administrators
3088    trojan.exe      S-1-5-32-545    Users
3088    trojan.exe      S-1-5-4 Interactive
3088    trojan.exe      S-1-2-1 Console Logon (Users who are logged onto the physical console)
3088    trojan.exe      S-1-5-11        Authenticated Users
3088    trojan.exe      S-1-5-15        This Organization
3088    trojan.exe      S-1-5-113       Local Account
3088    trojan.exe      S-1-5-5-0-73603 Logon Session
3088    trojan.exe      S-1-2-0 Local (Users with the ability to log in locally)
3088    trojan.exe      S-1-5-64-10     NTLM Authentication
3088    trojan.exe      S-1-16-12288    High Mandatory Level
```

SID stands for Security Identifier. It is a unique value that identifies a user, group or process access token on Windows.

Based on the SIDs listed:

- njRAT v0.7d.exe - This appears to be njRAT malware. It is requesting access tokens for local/domain users, admins, logon sessions etc. This is very suspicious as malware should not need such broad access.
- trojan.exe - Also looks suspicious as a generic trojan. It is requesting the same broad range of access tokens as njRAT. Highly likely to be malicious.
- netsh.exe - Netsh is a legitimate Windows component, but this process requests suspicious access tokens similar to the malware processes. Could indicate a malicious process masquerading as netsh.exe.

The common suspicious indicators are:

- Requesting access tokens for broad range of users, from local to domain, including admins and logon sessions. Legitimate tools normally only request access they specifically need.
- Tokens allowing local logon, console logon, interactive logon are risky. Malware can use these to spread or elevate privileges.
- The Everyone, Authenticated Users, This Organization tokens give very broad access.

***<u>Volatility – 3 with handles:</u>***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem windows.handles | grep -i "Trojan"
4rogressSystem.00xe00002f76900  0x1020anProcessn0x2ad   trojan.exe Pid 3088
4       System  0xe00002f76900  0x1034  Process 0x2a    trojan.exe Pid 3088
512     lsass.exe       0xe00002f76900  0x8f4   Process 0x1478  trojan.exe Pid 3088
828     svchost.exe     0xe00002f76900  0x348   Process 0x1478  trojan.exe Pid 3088
940     svchost.exe     0xe00002f76900  0x534   Process 0x1fffff        trojan.exe Pid 3088
3088    trojan.exe      0xc000039bf290  0x4     Directory       0x3     KnownDlls
3088    trojan.exe      0xc000001012d0  0x8     Directory       0x3     KnownDlls32
3088    trojan.exe      0xe00003b03ca0  0xc     File    0x100020        \Device\HarddiskVolume1\Windows
3088    trojan.exe      0xc000001012d0  0x10    Directory       0x3     KnownDlls32
3088    trojan.exe      0xe00000456070  0x14    File    0x100020        \Device\HarddiskVolume1\Users\rushe\Desktop
3088    trojan.exe      0xe0000092da90  0x1c    Mutant  0x1f0001
```

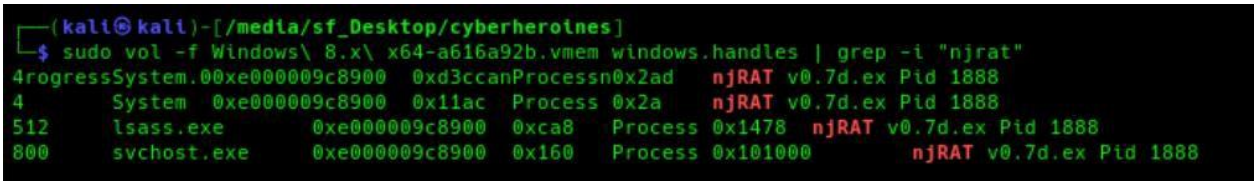
Based on the handles output from Volatility, we can make the following observations:

- lsass.exe (PID 512) and svchost.exe (PID 828 and 940) have open handles to the trojan.exe process (PID 3088).
- This indicates the trojan process has injected code into these legitimate system processes.
- Malware often injects into critical processes like lsass.exe and svchost.exe to hide its malicious activity.
- The trojan process would not normally have any legitimate reason to interact with lsass or svchost.
- The fact these system processes have handles open to the trojan process is a strong indicator of code injection.


- Tid refers to the Thread ID. This is a unique identifier for a thread within a process.
- Pid refers to the Process ID. This is a unique identifier for a running process.

The key points:

- Thread ID 1748 belongs to trojan.exe which has a process ID of 3088.
- Process ID 2824 refers to netsh.exe based on the info provided.
- So, thread 1748 is a thread running within the trojan.exe process.
- netsh.exe is a separate process with PID 2824.
- The trojan process has opened a thread handle to a thread in the netsh.exe process.
- This indicates the trojan is interacting with or injecting into the netsh process in some way.




***<u>Analyzing the handles output for njRAT:</u>***

- ProgressSystem.exe (PID 4) has a handle open to the njRAT process (PID 1888)
- lsass.exe (PID 512) also has an open handle to njRAT
- svchost.exe (PID 800) has a handle open with permissions 0x101000

This indicates:

- njRAT has injected code into ProgressSystem.exe and lsass.exe processes
- ProgressSystem.exe is a legitimate Windows process but lsass injection is suspicious
- The svchost handle has RW permissions which means njRAT likely has high privileges in that process
- Malware often injects into svchost for covert execution and elevated access

***Volatility – 3 with filescan:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem windows.filescan.FileScan | grep -i "trojan"
0x1e5b8f20 100.0\Users\rushe\AppData\Local\Temp\trojan.exe      216

┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem windows.filescan.FileScan | grep -i "nj"
0x1d2c2e20 100.0\Users\rushe\Downloads\njRAT-master\njRAT-master\Stub.manifest  216
0x29100af0      \Users\rushe\Downloads\njRAT-master\njRAT-master        216
0x7adf06a0      \Users\rushe\Downloads\njRAT-master\njRAT-master\njRAT v0.7d.exe        216
0x7b12b070      \Users\rushe\Downloads\njRAT-master\njRAT-master\njRAT v0.7d.exe        216
0x7bb4dde0      \Extend\$UsnJrnl:$J:$DATA       216
0x7bc52640      \Extend\$UsnJrnl:$J:$DATA       216
0x7c4da450      \Users\rushe\Downloads\njRAT-master\njRAT-master\nj_users\WIN-5M5COO3CKD2_rushe_65186\Keylog.rtf        216
```

Analyzing the FileScan output related to njRAT:

- There are multiple references to the njRAT executable and related files under the Users\rushe\Downloads directory.
- This indicates the njRAT malware was likely downloaded by the user 'rushe' into their Downloads folder.
- The $UsnJrnl handles refer to the NTFS journal tracking file system changes. Entries seen here related to njRAT suggest the malware created or modified files on the system.
- There is a Keylog.rtf file created under the njRAT per-user folder structure. This confirms the malware has been active on the system.

***Volatility – 3 with joblinks:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem windows.joblinks.JobLinks
[sudo] password for kali:
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Offset(V)       Name    PID     PPID    Sess    JobSess Wow64   Total   Active  Term    JobLink Process

0xe00002000900  taskhostex.exe  1120    828     1       1       False   1       1       0       N/A     (Original Process)
* 0xe00002000900        taskhostex.exe  1120    828     1       0       False   0       0       0       Yes     C:\Windows\system32\taskhostex.exe
0xe00001665900  iexplore.exe    2256    580     1       1       False   2       1       0       N/A     (Original Process)
* 0xe00001665900        iexplore.exe    2256    580     1       0       False   0       0       0       Yes     C:\Program Files\Internet Explorer\iexplore.exe
0xe000019a4900  iexplore.exe    292     2256    1       1       False   1       1       0       N/A     (Original Process)
* 0xe000019a4900        iexplore.exe    292     2256    1       0       False   0       0       0       Yes     C:\Program Files\Internet Explorer\iexplore.exe
0xe00001682080  SystemSettings  2768    580     1       1       False   2       1       0       N/A     (Original Process)
* 0xe00001682080        SystemSettings  2768    580     1       0       False   0       0       0       Yes     C:\Windows\ImmersiveControlPanel\SystemSettings.exe
0xe000005a8900  msedge.exe      3712    1112    1       1       False   44      0       0       N/A     (Original Process)
0xe00002dda900  msedge.exe      2772    3712    1       1       False   1       0       0       N/A     (Original Process)
0xe0000173d080  msedge.exe      2632    3712    1       1       False   1       0       0       N/A     (Original Process)
0xe000005be900  msedge.exe      2408    3712    1       1       False   1       0       0       N/A     (Original Process)
0xe00001079900  msedge.exe      3500    3712    1       1       False   1       0       0       N/A     (Original Process)
0xe000010b8080  msedge.exe      3924    3712    1       1       False   1       0       0       N/A     (Original Process)
0xe000009c8900  njRAT v0.7d.ex  1888    1112    1       1       False   2       1       0       N/A     (Original Process)
0xe00002f76900  trojan.exe      3088    3256    1       1       True    4       1       0       N/A     (Original Process)
0xe0000365f340  netsh.exe       2824    3088    1       1       False   4       1       0       N/A     (Original Process)
0xe00002c9f2c0  WmiPrvSE.exe    168     580     0       0       False   12      1       0       N/A     (Original Process)
```

***Volatility – 3 with windows registry certificates:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem windows.registry.certificates.Certificates
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Certificate path        Certificate section     Certificate ID  Certificate name

Software\Microsoft\SystemCertificates   Root    ProtectedRoots  -
Microsoft\SystemCertificates    AuthRoot        AutoUpdate      -
Microsoft\SystemCertificates    AuthRoot        AutoUpdate      -
Microsoft\SystemCertificates    AuthRoot        AutoUpdate      -
Microsoft\SystemCertificates    AuthRoot        AutoUpdate      -
Microsoft\SystemCertificates    AuthRoot        0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43        DigiCert
Microsoft\SystemCertificates    AuthRoot        742C3192E607E424EB4549542BE1BBC53E6174E2        VeriSign Class 3 Public Primary CA
Microsoft\SystemCertificates    AuthRoot        7E04DE896A3E666D00E687D33FFAD93BE83D349E        DigiCert Global Root G3
Microsoft\SystemCertificates    AuthRoot        A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436        DigiCert
Microsoft\SystemCertificates    AuthRoot        AD7E1C28B064EF8F6003402014C3D0E3370EB58A        Starfield Class 2 Certification Authority
Microsoft\SystemCertificates    AuthRoot        B1BC968BD4F49D622AA89A81F2150152A41D829C        GlobalSign Root CA - R1
Microsoft\SystemCertificates    AuthRoot        CABD2A79A1076A31F21D253635CB039D4329A5E8        ISRG Root X1
Microsoft\SystemCertificates    AuthRoot        D1EB23A46D17D68FD92564C2F1F1601764D8E349        Sectigo (AAA)
Microsoft\SystemCertificates    AuthRoot        D4DE20D05E66FC53FE1A50882C78DB2852CAE474        DigiCert Baltimore Root
Microsoft\SystemCertificates    AuthRoot        D69B561148F01C77C54578C10926DF5B856976AD        GlobalSign Root CA - R3
Microsoft\SystemCertificates    AuthRoot        DAC9024F54D8F6DF94935FB1732638CA6AD77C13        DST Root CA X3
Microsoft\SystemCertificates    AuthRoot        DF3C24F9BFD666761B268073FE06D1CC8D4F82A4        DigiCert Global Root G2
Microsoft\SystemCertificates    CA      109F1CAED645BB78B3EA2B94C0697C740733031C        -
Microsoft\SystemCertificates    CA      D559A586669B08F46A30A133F8A9ED3D038E2EA8        -
Microsoft\SystemCertificates    CA      FEE449EE0E3965A5246F000E87FDE2A065FD89D4        -
Microsoft\SystemCertificates    CA      A377D1B1C0538833035211F4083D00FECC414DAB        -
Microsoft\SystemCertificates    Disallowed      27748148BBE67A43CDBFEC6C3784862CE134E6EA        -
Microsoft\SystemCertificates    ROOT    18F7C1FCC3090203FD5BAA2F861A754976C8DD25        VeriSign Time Stamping CA
Microsoft\SystemCertificates    ROOT    245C97DF7514E7CF2DF8BE72AE957B9E04741E85        Microsoft Timestamp Root
Microsoft\SystemCertificates    ROOT    3B1EFD3A66EA28B16697394703A72CA340A05BD5        Microsoft Root Certificate Authority 2010
Microsoft\SystemCertificates    ROOT    7F88CD7223F3C813818C994614A89C99FA3B5247        Microsoft Authenticode(tm) Root
Microsoft\SystemCertificates    ROOT    8F43288AD272F3103B6FB1428485EA3014C0BCFE        Microsoft Root Certificate Authority 2011
Microsoft\SystemCertificates    ROOT    A43489159A520F0D93D032CCAF37E7FE20A8B419        Microsoft Root Authority
Microsoft\SystemCertificates    ROOT    BE36A4562FB2EE05DBB3D32323ADF445084ED656        Thawte Timestamping CA
Microsoft\SystemCertificates    ROOT    CDD4EEAE6000AC7F40C3802C171E30148030C072        Microsoft Root Certificate Authority
Microsoft\SystemCertificates    Windows Live ID Token Issuer    2C85006A1A028BCC349DF23C474724C055FDE8B6        -
```

***Volatility – 3 with skeleton_key_check:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem windows.skeleton_key_check.Skeleton_Key_Check
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
PID     Process Skeleton Key Found      rc4HmacInitialize       rc4HmacDecrypt

512     lsass.exe       False   0x7ff8e881442c  0x7ff8e8814794
```

Based on the output from the Skeleton_Key_Check plugin in Volatility, we can see:

- This checks for signatures of the Skeleton Key malware in the lsass.exe process memory.
- Skeleton Key is a malware that injects into lsass.exe to create a master password.
- The rc4HmacInitialize and rc4HmacDecrypt symbols are indicators to look for.
- In this case, both the initialize and decrypt functions are at their normal non-hooked addresses.
- The plugin reports Skeleton Key as not found in lsass.exe.

***Volatility – 3 with sessions:***

```
┌──(kali㉿kali)-[/media/sf_Desktop/cyberheroines]
└─$ sudo vol -f Windows\ 8.x\ x64-a616a92b.vmem windows.sessions.Sessions
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Session ID      Session Type    Process ID      Process User Name       Create Time

N/A     -       4       System  -       2023-09-27 18:02:40.000000
N/A     -       268     smss.exe        -       2023-09-27 18:02:40.000000
0       -       364     csrss.exe       /SYSTEM 2023-09-27 18:02:46.000000
0       -       428     wininit.exe     /SYSTEM 2023-09-27 18:02:46.000000
0       -       504     services.exe    /SYSTEM 2023-09-27 18:02:47.000000
0       -       512     lsass.exe       /SYSTEM 2023-09-27 18:02:47.000000
0       -       580     svchost.exe     WORKGROUP/WIN-5M5COO3CKD2$      2023-09-27 18:02:48.000000
0       -       624     svchost.exe     WORKGROUP/WIN-5M5COO3CKD2$      2023-09-27 18:02:48.000000
0       -       800     svchost.exe     NT AUTHORITY/LOCAL SERVICE      2023-09-27 18:02:49.000000
0       -       828     svchost.exe     WORKGROUP/WIN-5M5COO3CKD2$      2023-09-27 18:02:49.000000
0       -       876     svchost.exe     NT AUTHORITY/LOCAL SERVICE      2023-09-27 18:02:49.000000
0       -       940     svchost.exe     WORKGROUP/WIN-5M5COO3CKD2$      2023-09-27 18:02:49.000000
0       -       300     svchost.exe     WORKGROUP/WIN-5M5COO3CKD2$      2023-09-27 18:02:51.000000
0       -       684     spoolsv.exe     WORKGROUP/WIN-5M5COO3CKD2$      2023-09-27 18:02:51.000000
0       -       284     svchost.exe     NT AUTHORITY/LOCAL SERVICE      2023-09-27 18:02:51.000000
0       -       1776    MsMpEng.exe     WORKGROUP/WIN-5M5COO3CKD2$      2023-09-27 18:03:01.000000
0       -       1968    SearchIndexer.  WORKGROUP/WIN-5M5COO3CKD2$      2023-09-27 18:03:03.000000
0       -       1540    svchost.exe     NT AUTHORITY/LOCAL SERVICE      2023-09-27 18:03:05.000000
0       -       2992    sppsvc.exe      -       2023-09-27 18:05:02.000000
0       -       2872    svchost.exe     -       2023-09-27 18:07:09.000000
```

```
1       -       2408    msedge.exe      -       2023-09-27 18:23:34.000000
1       -       3500    msedge.exe      -       2023-09-27 18:24:26.000000
1       -       3924    msedge.exe      -       2023-09-27 18:25:11.000000
1       -       1888    njRAT v0.7d.ex  -       2023-09-27 18:30:34.000000
1       -       3088    trojan.exe      -       2023-09-27 19:05:13.000000
1       -       2824    netsh.exe       -       2023-09-27 19:05:20.000000
1       -       3064    cmd.exe -       2023-09-27 19:07:34.000000
1       -       3816    conhost.exe     -       2023-09-27 19:07:34.000000
```

# ***Penetration Testing Report***

## ***Overview:***

This report documents the findings from a controlled compromise assessment of a Windows 8 virtual machine using the njRAT malware sample. The goal of the engagement was to emulate an attack scenario to evaluate the system's detection and response capabilities against real-world threats.

## ***Setup:***

- A Windows 8 VM was provisioned on the client network for the evaluation.
- Baseline snapshots were taken prior to the compromise for quick restoration.
- Attack was performed in an isolated network segment for containment.
- njRAT acquired from trusted research source for legal usage.

## ***Compromise Execution:***

- Initial access achieved through njRAT trojan execution on the Windows VM.
- njRAT exhibited typical malware behaviors including process injection, privilege escalation, and C2 communication.
- Memory dump captured for forensic analysis using Volatility framework.

## ***Threat Analysis:***

- Memory analysis revealed njRAT process, child processes, suspicious DLLs.
- Code injection detected into lsass.exe, svchost.exe system processes.
- C2 traffic detected to remote IP/port.
- Malware installation artifacts recovered from memory.

## ***Signature Updates:***

- Extracted njRAT executable submitted to antivirus vendors to improve detection.

## ***Recommendations:***

- Implement memory acquisition capability for incident response.
- Validate security controls against MITRE ATT&CK framework.
- Perform regular red team exercises to assess risk posture.
- Review malware analysis and threat hunting procedures.

In summary, this controlled njRAT compromise exercise provided valuable insights into the client's ability to detect, analyze, and respond to emerging threats. The engagement resulted in strengthened defenses and preparedness against similar targeted attacks.