University of Victoria

University of Victoria

ECE 570 - Digital Forensics Methodologies

PROJECT PART 1

Investigating an Infected Machine

Somayeh Roshandel V00942553
Behnaz Saropourian V00857804

June 2020

University of Victoria

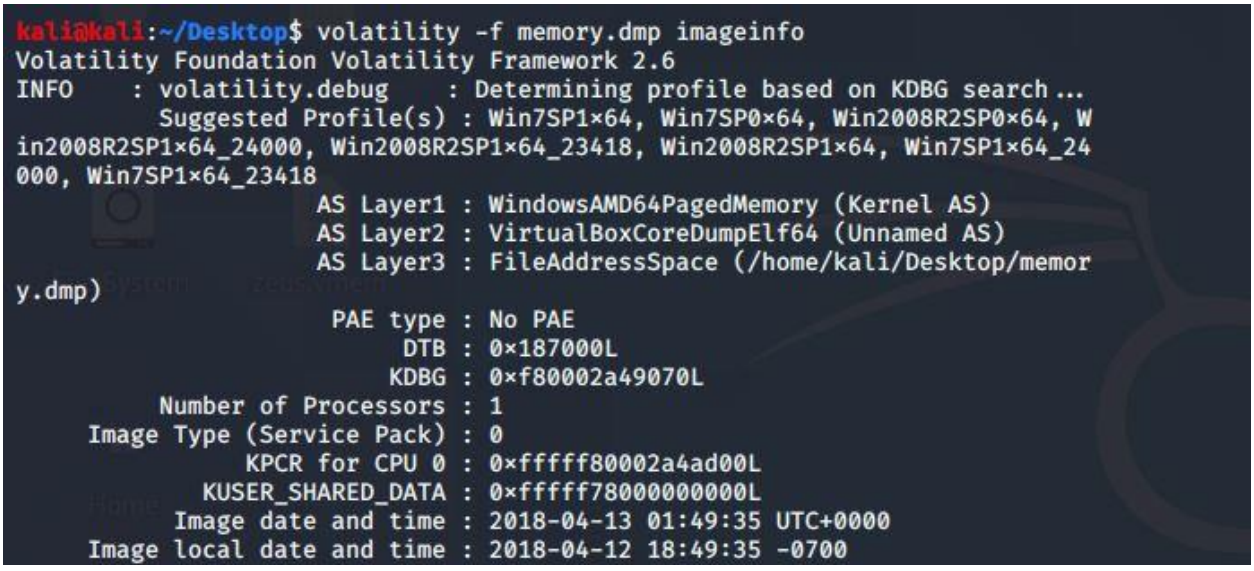
Contents

University of Victoria

1- Identify running processes, and determine which ones look suspicious and justify why?

At very first step to find what operating system this memory image belongs to and find memory profile on suspected memory we run volatility and use the command:

volatility -f memory.dmp imageinfo



From the result of this command we have service pack 0 so our suggested profile is Win7SP0x64 .

We now have the computer OS from which this memory dump comes from (Win7SP0x64). The investigation can now begin, we can specify to volatility the OS profile (--profile=Win7SP0x64) and try to find what happened on the victim's computer

To determine the processes were running on the system at the time of capturing the memory image we use pslist, and pstree command as follow:

University of Victoria

volatility -f memory.dmp --profile=Win7SP0x64 pstree

volatility -f memory.dmp --profile=Win7SP0x64 pslist

```
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Ses
s  Wow64 Start                         Exit
------------------ -------------------- ------ ------ ------ -------- -----
- ------ ------------------------------ ------------------------------
0xfffffa8000cb8040 System                    4      0     84      528 -----
-      0 2018-04-06 23:12:36 UTC+0000
0xfffffa8001d185f0 smss.exe                276      4      2       29 -----
-      0 2018-04-06 23:12:36 UTC+0000
0xfffffa80024e2800 csrss.exe               360    352      9      402
0      0 2018-04-06 23:12:43 UTC+0000
0xfffffa8002340060 wininit.exe             392    352      3       75
0      0 2018-04-06 23:12:43 UTC+0000
0xfffffa8001c9a4e0 csrss.exe               404    384      8      259
1      0 2018-04-06 23:12:43 UTC+0000
0xfffffa8002519060 winlogon.exe            444    384      3      108
1      0 2018-04-06 23:12:43 UTC+0000
0xfffffa800252c460 services.exe            488    392     11      207
0      0 2018-04-06 23:12:43 UTC+0000
0xfffffa800255ab30 lsass.exe               496    392      7      553
0      0 2018-04-06 23:12:43 UTC+0000
0xfffffa8002541b30 lsm.exe                 504    392     10      144
0      0 2018-04-06 23:12:43 UTC+0000
0xfffffa80025ae600 svchost.exe             612    488     10      345
0      0 2018-04-06 23:12:43 UTC+0000
0xfffffa80025d96b0 VBoxService.ex          672    488     12      114
0      0 2018-04-06 23:12:43 UTC+0000
0xfffffa80025ef060 svchost.exe             736    488      9      264
0      0 2018-04-06 23:12:44 UTC+0000
0xfffffa8002570b30 svchost.exe             824    488     18      457
0      0 2018-04-06 23:12:44 UTC+0000
0xfffffa80027d2740 svchost.exe             872    488     19      478
0      0 2018-04-06 23:12:44 UTC+0000
```

```
0xfffffa8002644b30 svchost.exe            904    488     39     1238
0      0 2018-04-06 23:12:44 UTC+0000
0xfffffa800285d4a0 svchost.exe            332    488     12      325
0      0 2018-04-06 23:12:45 UTC+0000
0xfffffa800288e920 svchost.exe            900    488     15      395
0      0 2018-04-06 23:12:46 UTC+0000
0xfffffa8002897b30 spoolsv.exe           1120    488     12      279
0      0 2018-04-06 23:12:47 UTC+0000
0xfffffa8002930060 svchost.exe           1152    488     17      319
0      0 2018-04-06 23:12:47 UTC+0000
0xfffffa80029c5b30 svchost.exe           1296    488     13      220
0      0 2018-04-06 23:12:48 UTC+0000
0xfffffa80029eab30 dwm.exe               1588    872      3       70
1      0 2018-04-06 23:12:50 UTC+0000
0xfffffa8002aa4b30 taskhost.exe          1596    488      7      141
1      0 2018-04-06 23:12:50 UTC+0000
0xfffffa8002ab6b30 explorer.exe          1652   1580     23      817
1      0 2018-04-06 23:12:51 UTC+0000
0xfffffa8002b53b30 svchost.exe           1948    488      5       96
0      0 2018-04-06 23:12:53 UTC+0000
0xfffffa8002afeb30 VBoxTray.exe          1376   1652     10      103      1      0 2018-04-06 23:12:56 UTC+0000
0xfffffa8002618060 python.exe            1208   1652      1       92      1      0 2018-04-06 23:12:59 UTC+0000
0xfffffa800288a5e0 conhost.exe           1916    404      2       53      1      0 2018-04-06 23:12:59 UTC+0000
0xfffffa8002cd3b30 acrotray.exe          2144   1484      2       60      1      1 2018-04-06 23:13:08 UTC+0000
0xfffffa80015e1b30 SearchIndexer.        2180    488     12      765      0      0 2018-04-06 23:13:10 UTC+0000
0xfffffa8002daab30 wmpnetwk.exe          2540    488     10      214      0      0 2018-04-06 23:13:22 UTC+0000
0xfffffa8002e82520 SndVol.exe            2568   1652      0 --------      1      0 2018-04-06 23:13:23 UTC+0000   2018-04-06 23:13:25 UTC+0000
0xfffffa8002a83950 python.exe            2176   1208     16      233      1      0 2018-04-13 01:28:34 UTC+0000
0xfffffa8000e9f060 7004af389d633b         512   2156      0 --------      1      0 2018-04-13 01:28:25 UTC+0000   2018-04-13 01:29:09 UTC+0000
0xfffffa8000e70060 mscorsvw.exe          2740    488      8      124      0      1 2018-04-13 01:28:34 UTC+0000
0xfffffa8000e2fb30 mscorsvw.exe          3056    488      7       86      0      0 2018-04-13 01:28:40 UTC+0000
0xfffffa8000eb4b30 svchost.exe           1404    488     13      355      0      0 2018-04-13 01:28:45 UTC+0000
0xfffffa8000e26790 7004af389d633b        1400    512      0 --------      1      0 2018-04-13 01:29:07 UTC+0000   2018-04-13 01:29:15 UTC+0000
```

```
0xfffffa8002afeb30 VBoxTray.exe          1376   1652     10      103      1      0 2018-04-06 23:12:56 UTC+0000
0xfffffa8002618060 python.exe            1208   1652      1       92      1      0 2018-04-06 23:12:59 UTC+0000
0xfffffa800288a5e0 conhost.exe           1916    404      2       53      1      0 2018-04-06 23:12:59 UTC+0000
0xfffffa8002cd3b30 acrotray.exe          2144   1484      2       60      1      1 2018-04-06 23:13:08 UTC+0000
0xfffffa80015e1b30 SearchIndexer.        2180    488     12      765      0      0 2018-04-06 23:13:10 UTC+0000
0xfffffa8002daab30 wmpnetwk.exe          2540    488     10      214      0      0 2018-04-06 23:13:22 UTC+0000
0xfffffa8002e82520 SndVol.exe            2568   1652      0 --------      1      0 2018-04-06 23:13:23 UTC+0000   2018-04-06 23:13:25 UTC+0000
0xfffffa8002a83950 python.exe            2176   1208     16      233      1      0 2018-04-13 01:28:34 UTC+0000
0xfffffa8000e9f060 7004af389d633b         512   2156      0 --------      1      0 2018-04-13 01:28:25 UTC+0000   2018-04-13 01:29:09 UTC+0000
0xfffffa8000e70060 mscorsvw.exe          2740    488      8      124      0      1 2018-04-13 01:28:34 UTC+0000
0xfffffa8000e2fb30 mscorsvw.exe          3056    488      7       86      0      0 2018-04-13 01:28:40 UTC+0000
0xfffffa8000eb4b30 svchost.exe           1404    488     13      355      0      0 2018-04-13 01:28:45 UTC+0000
0xfffffa8000e26790 7004af389d633b        1400    512      0 --------      1      0 2018-04-13 01:29:07 UTC+0000   2018-04-13 01:29:15 UTC+0000
0xfffffa8000e2cb30 aifkydk.exe           2652   1400      0 --------      1      0 2018-04-13 01:29:11 UTC+0000   2018-04-13 01:29:58 UTC+0000
0xfffffa8000efa480 cmd.exe               2920   1400      0 --------      1      0 2018-04-13 01:29:15 UTC+0000   2018-04-13 01:29:18 UTC+0000
0xfffffa8000edeb30 aifkydk.exe           1728   2652      0 --------      1      0 2018-04-13 01:29:54 UTC+0000   2018-04-13 01:37:58 UTC+0000
0xfffffa8002551550 bcdedit.exe            812   1728      0 --------      1      0 2018-04-13 01:30:08 UTC+0000   2018-04-13 01:30:09 UTC+0000
0xfffffa8002afe060 vssadmin.exe           580   1728      0 --------      1      0 2018-04-13 01:30:09 UTC+0000   2018-04-13 01:30:18 UTC+0000
0xfffffa8000e2bb30 bcdedit.exe           1752   1728      0 --------      1      0 2018-04-13 01:30:10 UTC+0000   2018-04-13 01:30:10 UTC+0000
0xfffffa8000dbfb30 bcdedit.exe           2208   1728      0 --------      1      0 2018-04-13 01:30:11 UTC+0000   2018-04-13 01:30:12 UTC+0000
0xfffffa8000f22920 bcdedit.exe           2768   1728      0 --------      1      0 2018-04-13 01:30:13 UTC+0000   2018-04-13 01:30:13 UTC+0000
0xfffffa8000f5c6a0 bcdedit.exe           2852   1728      0 --------      1      0 2018-04-13 01:30:14 UTC+0000   2018-04-13 01:30:14 UTC+0000
0xfffffa8000fe8930 notepad.exe            364   1728      1       68      1      1 2018-04-13 01:37:40 UTC+0000
0xfffffa800124e920 iexplore.exe          2800   1728     13      547      1      1 2018-04-13 01:37:41 UTC+0000
0xfffffa8000dbd250 dllhost.exe           1932    612      7      205      1      1 2018-04-13 01:37:46 UTC+0000
0xfffffa80011c9060 vssadmin.exe           400   1728      0 --------      1      0 2018-04-13 01:37:46 UTC+0000   2018-04-13 01:37:57 UTC+0000
0xfffffa8001153240 iexplore.exe          2120   2800      6      351      1      1 2018-04-13 01:37:47 UTC+0000
0xfffffa8000f22060 cmd.exe               1080   1728      0 --------      1      0 2018-04-13 01:37:57 UTC+0000   2018-04-13 01:38:02 UTC+0000
0xfffffa8002de6b30 VSSVC.exe             1564    488      9      184      0      0 2018-04-13 01:44:43 UTC+0000
0xfffffa8001050650 svchost.exe           2312    488      4       78      0      0 2018-04-13 01:44:47 UTC+0000
0xfffffa8000e39b30 mscorsvw.exe          2728   2740      8      145      0      1 2018-04-13 01:49:17 UTC+0000
```

An alternative to the pslist plugin, we used to display the processes and their parent processes is **pstree.**

University of Victoria

```
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                 Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa8002340060:wininit.exe                       392    352      3     75 2018-04-06 23:12:43 UTC+0000
. 0xfffffa800252c460:services.exe                     488    392     11    207 2018-04-06 23:12:43 UTC+0000
.. 0xfffffa8002930060:svchost.exe                    1152    488     17    319 2018-04-06 23:12:47 UTC+0000
.. 0xfffffa80029c5b30:svchost.exe                    1296    488     13    220 2018-04-06 23:12:48 UTC+0000
.. 0xfffffa800288e920:svchost.exe                     900    488     15    395 2018-04-06 23:12:46 UTC+0000
.. 0xfffffa8002b53b30:svchost.exe                    1948    488      5     96 2018-04-06 23:12:53 UTC+0000
.. 0xfffffa8000eb4b30:svchost.exe                    1404    488     13    355 2018-04-13 01:28:45 UTC+0000
.. 0xfffffa80025d96b0:VBoxService.ex                  672    488     12    114 2018-04-06 23:12:43 UTC+0000
.. 0xfffffa8000e2fb30:mscorsvw.exe                   3056    488      7     86 2018-04-13 01:28:40 UTC+0000
.. 0xfffffa8002de6b30:VSSVC.exe                      1564    488      9    184 2018-04-13 01:44:43 UTC+0000
.. 0xfffffa8002644b30:svchost.exe                     904    488     39   1238 2018-04-06 23:12:44 UTC+0000
.. 0xfffffa8002570b30:svchost.exe                     824    488     18    457 2018-04-06 23:12:44 UTC+0000
.. 0xfffffa8000e70060:mscorsvw.exe                   2740    488      8    124 2018-04-13 01:28:34 UTC+0000
... 0xfffffa8000e39b30:mscorsvw.exe                  2728   2740      8    145 2018-04-13 01:49:17 UTC+0000
.. 0xfffffa8001050650:svchost.exe                    2312    488      4     78 2018-04-13 01:44:47 UTC+0000
.. 0xfffffa8002897b30:spoolsv.exe                    1120    488     12    279 2018-04-06 23:12:47 UTC+0000
.. 0xfffffa80015e1b30:SearchIndexer.                 2180    488     12    765 2018-04-06 23:13:10 UTC+0000
.. 0xfffffa800285d4a0:svchost.exe                     332    488     12    325 2018-04-06 23:12:45 UTC+0000
.. 0xfffffa80027d2740:svchost.exe                     872    488     19    478 2018-04-06 23:12:44 UTC+0000
... 0xfffffa80029eab30:dwm.exe                       1588    872      3     70 2018-04-06 23:12:50 UTC+0000
.. 0xfffffa80025ef060:svchost.exe                     736    488      9    264 2018-04-06 23:12:44 UTC+0000
.. 0xfffffa80025ae600:svchost.exe                     612    488     10    345 2018-04-06 23:12:43 UTC+0000
... 0xfffffa8000dbd250:dllhost.exe                   1932    612      7    205 2018-04-13 01:37:46 UTC+0000
.. 0xfffffa8002aa4b30:taskhost.exe                   1596    488      7    141 2018-04-06 23:12:50 UTC+0000
.. 0xfffffa8002daab30:wmpnetwk.exe                   2540    488     10    214 2018-04-06 23:13:22 UTC+0000
. 0xfffffa800255ab30:lsass.exe                        496    392      7    553 2018-04-06 23:12:43 UTC+0000
. 0xfffffa8002541b30:lsm.exe                          504    392     10    144 2018-04-06 23:12:43 UTC+0000
 0xfffffa80024e2800:csrss.exe                         360    352      9    402 2018-04-06 23:12:43 UTC+0000
 0xfffffa8002ab6b30:explorer.exe                     1652   1580     23    817 2018-04-06 23:12:51 UTC+0000
. 0xfffffa8002afeb30:VBoxTray.exe                    1376   1652     10    103 2018-04-06 23:12:56 UTC+0000
. 0xfffffa8002618060:python.exe                      1208   1652      1     92 2018-04-06 23:12:59 UTC+0000
. 0xfffffa8002618060:python.exe                      1208   1652      1     92 2018-04-06 23:12:59 UTC+0000
.. 0xfffffa8002a83950:python.exe                     2176   1208     16    233 2018-04-13 01:28:34 UTC+0000
. 0xfffffa8002e82520:SndVol.exe                      2568   1652      0 ------ 2018-04-06 23:13:23 UTC+0000
 0xfffffa8000cb8040:System                              4      0     84    528 2018-04-06 23:12:36 UTC+0000
. 0xfffffa8001d185f0:smss.exe                        276      4      2     29 2018-04-06 23:12:36 UTC+0000
 0xfffffa8002cd3b30:acrotray.exe                     2144   1484      2     60 2018-04-06 23:13:08 UTC+0000
 0xfffffa8000e9f060:7004af389d633b                    512   2156      0 ------ 2018-04-13 01:28:25 UTC+0000
. 0xfffffa8000e26790:7004af389d633b                  1400    512      0 ------ 2018-04-13 01:29:07 UTC+0000
.. 0xfffffa8000efa480:cmd.exe                        2920   1400      0 ------ 2018-04-13 01:29:15 UTC+0000
.. 0xfffffa8000e2cb30:aifkydk.exe                    2652   1400      0 ------ 2018-04-13 01:29:11 UTC+0000
... 0xfffffa8000edeb30:aifkydk.exe                   1728   2652      0 ------ 2018-04-13 01:29:54 UTC+0000
.... 0xfffffa8000dbfb30:bcdedit.exe                  2208   1728      0 ------ 2018-04-13 01:30:11 UTC+0000
.... 0xfffffa8000f22060:cmd.exe                      1080   1728      0 ------ 2018-04-13 01:37:57 UTC+0000
.... 0xfffffa8000fe8930:notepad.exe                   364   1728      1     68 2018-04-13 01:37:40 UTC+0000
.... 0xfffffa8000f5c6a0:bcdedit.exe                  2852   1728      0 ------ 2018-04-13 01:30:14 UTC+0000
.... 0xfffffa8002551550:bcdedit.exe                   812   1728      0 ------ 2018-04-13 01:30:08 UTC+0000
.... 0xfffffa8002afe060:vssadmin.exe                  580   1728      0 ------ 2018-04-13 01:30:09 UTC+0000
.... 0xfffffa8000f22920:bcdedit.exe                  2768   1728      0 ------ 2018-04-13 01:30:13 UTC+0000
.... 0xfffffa8000e2bb30:bcdedit.exe                  1752   1728      0 ------ 2018-04-13 01:30:10 UTC+0000
.... 0xfffffa80011c9060:vssadmin.exe                  400   1728      0 ------ 2018-04-13 01:37:46 UTC+0000
.... 0xfffffa800124e920:iexplore.exe                 2800   1728     13    547 2018-04-13 01:37:41 UTC+0000
..... 0xfffffa8001153240:iexplore.exe                2120   2800      6    351 2018-04-13 01:37:47 UTC+0000
 0xfffffa8002519060:winlogon.exe                      444    384      3    108 2018-04-06 23:12:43 UTC+0000
 0xfffffa8001c9a4e0:csrss.exe                         404    384      8    259 2018-04-06 23:12:43 UTC+0000
. 0xfffffa800288a5e0:conhost.exe                     1916    404      2     53 2018-04-06 23:12:59 UTC+0000
```

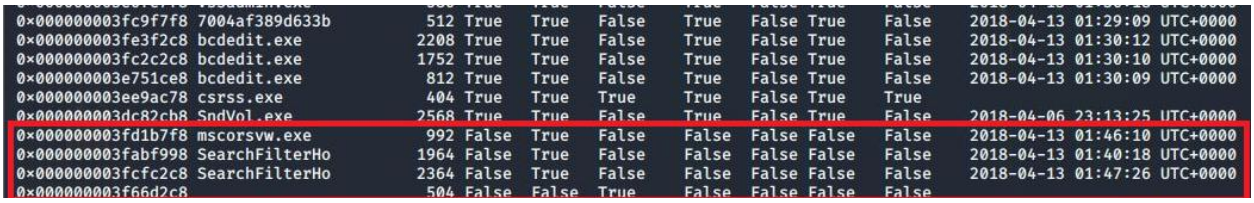
So, based on results of pstree we can find more details and a lot of information about the behavior of processes.

By running **psscan** and **psxview** , we do more investigation.**psxview** will list processes that are trying to hide themselves while running on the computer, if we see “False” in the first two columns (**pslist** and **psscan**).

Volatility -f memory.dmp --profile=Win7SP0x64 psxview

```
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
------------------ -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x000000003e28ad78 conhost.exe            1916 True   True   True     True   True  True    True
0x000000003fe3c9e8 dllhost.exe            1932 True   True   True     True   True  True    True
0x000000003e4187f8 python.exe             1208 True   True   True     True   True  True    True
0x000000003fc302c8 mscorsvw.exe           3056 True   True   True     True   True  True    True
0x000000003e1542c8 svchost.exe            1948 True   True   True     True   True  True    True
0x000000003e7197f8 winlogon.exe            444 True   True   True     True   True  True    True
0x000000003fcb52c8 svchost.exe            1404 True   True   True     True   True  True    True
0x000000003e7aed98 svchost.exe             612 True   True   True     True   True  True    True
0x000000003e0b72c8 explorer.exe           1652 True   True   True     True   True  True    True
0x000000003e28f0b8 svchost.exe             900 True   True   True     True   True  True    True
0x000000003ded42c8 acrotray.exe           2144 True   True   True     True   True  True    True
0x000000003e2982c8 spoolsv.exe            1120 True   True   True     True   True  True    True
0x000000003e4452c8 svchost.exe             904 True   True   True     True   True  True    True
0x000000003fb539d8 iexplore.exe           2120 True   True   True     True   True  True    True
0x000000003fc3a2c8 mscorsvw.exe           2728 True   True   True     True   True  True    True
0x000000003e3eb2c8 dwm.exe                1588 True   True   True     True   True  True    True
0x000000003e0a52c8 taskhost.exe           1596 True   True   True     True   True  True    True
0x000000003e9407f8 wininit.exe             392 True   True   True     True   True  True    True
0x000000003e75b2c8 lsass.exe               496 True   True   True     True   True  True    False
0x000000003e25dc38 svchost.exe             332 True   True   True     True   True  True    True
0x000000003e0ff2c8 VBoxTray.exe           1376 True   True   True     True   True  True    True
0x000000003f84f0b8 iexplore.exe           2800 True   True   True     True   True  True    True
0x000000003e7422c8 lsm.exe                 504 True   True   True     True   True  True    False
0x000000003e7712c8 svchost.exe             824 True   True   True     True   True  True    False
0x000000003e3307f8 svchost.exe            1152 True   True   True     True   True  True    True
0x000000003e3c62c8 svchost.exe            1296 True   True   True     True   True  True    False
0x000000003f7e22c8 SearchIndexer.         2180 True   True   True     True   True  True    True
0x000000003e5d2ed8 svchost.exe             872 True   True   True     True   True  True    True
0x000000003dfe72c8 VSSVC.exe              1564 True   True   True     True   True  True    True
0x000000003e7ef7f8 svchost.exe             736 True   True   True     True   True  True    True
```

```
0x000000003e7ef7f8 svchost.exe             736 True   True   True     True   True  True    True
0x000000003fa50de8 svchost.exe            2312 True   True   True     True   True  True    True
0x000000003dfab2c8 wmpnetwk.exe           2540 True   True   True     True   True  True    True
0x000000003e7d9e48 VBoxService.ex          672 True   True   True     True   True  True    False
0x000000003e0840e8 python.exe             2176 True   True   True     True   True  True    True
0x000000003e72cbf8 services.exe            488 True   True   True     True   True  True    False
0x000000003fc707f8 mscorsvw.exe           2740 True   True   True     True   True  True    True
0x000000003fde90c8 notepad.exe             364 True   True   True     True   True  True    True
0x000000003fd5ce38 bcdedit.exe            2852 True   True   False    True   False True    False   2018-04-13 01:30:14 UTC+0000
0x000000003ef18d88 smss.exe                276 True   True   True     True   False False   False
0x000000003fd230b8 bcdedit.exe            2768 True   True   False    True   False True    False   2018-04-13 01:30:13 UTC+0000
0x000000003e6e2f98 csrss.exe               360 True   True   True     True   False True    True
0x000000003ff377d8 System                    4 True   True   True     True   False False   False
0x000000003fcdf2c8 aifkydk.exe            1728 True   True   False    True   False True    False   2018-04-13 01:37:58 UTC+0000
0x000000003fc26f28 7004af389d633b         1400 True   True   False    True   False True    False   2018-04-13 01:29:15 UTC+0000
0x000000003fd227f8 cmd.exe                1080 True   True   False    True   False True    False   2018-04-13 01:38:02 UTC+0000
0x000000003fcfac18 cmd.exe                2920 True   True   False    True   False True    False   2018-04-13 01:29:18 UTC+0000
0x000000003fc2d2c8 aifkydk.exe            2652 True   True   False    True   False True    False   2018-04-13 01:29:58 UTC+0000
0x000000003fbc97f8 vssadmin.exe            400 True   True   False    True   False True    False   2018-04-13 01:37:57 UTC+0000
0x000000003e0fe7f8 vssadmin.exe            580 True   True   False    True   False True    False   2018-04-13 01:30:18 UTC+0000
0x000000003fc9f7f8 7004af389d633b          512 True   True   False    True   False True    False   2018-04-13 01:29:09 UTC+0000
0x000000003fe3f2c8 bcdedit.exe            2208 True   True   False    True   False True    False   2018-04-13 01:30:12 UTC+0000
0x000000003fc2c2c8 bcdedit.exe            1752 True   True   False    True   False True    False   2018-04-13 01:30:10 UTC+0000
0x000000003e751ce8 bcdedit.exe             812 True   True   False    True   False True    False   2018-04-13 01:30:09 UTC+0000
0x000000003ee9ac78 csrss.exe               404 True   True   True     True   False True    True
0x000000003dc82cb8 SndVol.exe             2568 True   True   False    True   False True    False   2018-04-06 23:13:25 UTC+0000
0x000000003fd1b7f8 mscorsvw.exe            992 False  True   False    False  False False   False   2018-04-13 01:46:10 UTC+0000
0x000000003fabf998 SearchFilterHo         1964 False  True   False    False  False False   False   2018-04-13 01:40:18 UTC+0000
0x000000003fcfc2c8 SearchFilterHo         2364 False  True   False    False  False False   False   2018-04-13 01:47:26 UTC+0000
0x000000003f66d2c8                         504 False  False  True     False  False False   False
```



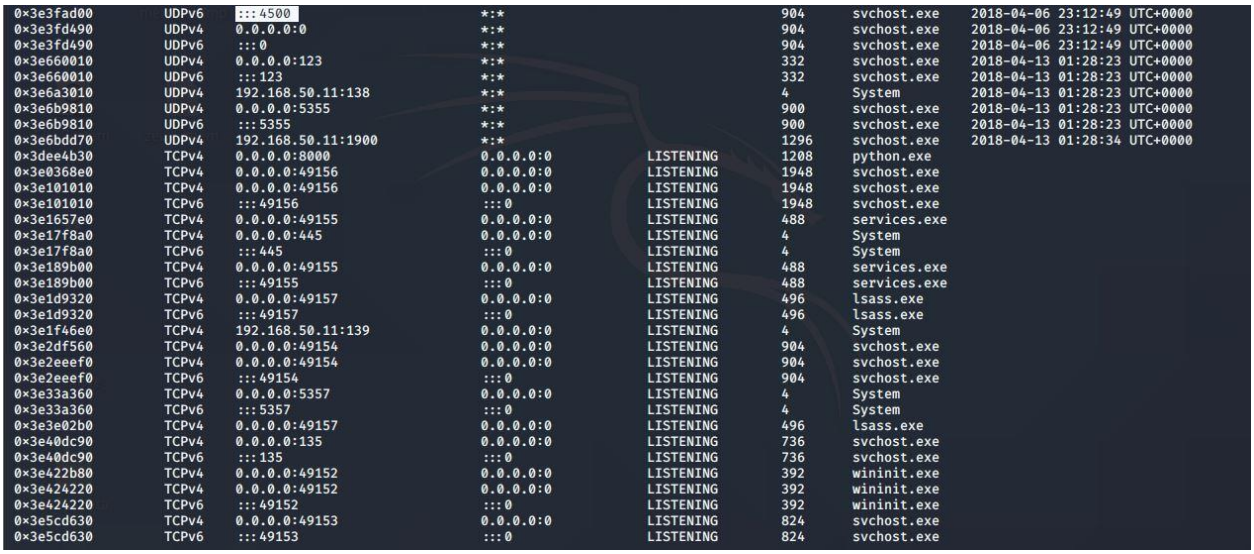
```
0×000000003fc9f7f8 7004af389d633b          512 True   True   False   True   False True   False   2018-04-13 01:29:09 UTC+0000
0×000000003fe3f2c8 bcdedit.exe            2208 True   True   False   True   False True   False   2018-04-13 01:30:12 UTC+0000
0×000000003fc2c2c8 bcdedit.exe            1752 True   True   False   True   False True   False   2018-04-13 01:30:10 UTC+0000
0×000000003e751ce8 bcdedit.exe             812 True   True   False   True   False True   False   2018-04-13 01:30:09 UTC+0000
0×000000003ee9ac78 csrss.exe               404 True   True   True    True   False True   True
0×000000003dc82cb8 SndVol.exe             2568 True   True   False   True   False True   False   2018-04-06 23:13:25 UTC+0000
0×000000003fd1b7f8 mscorsvw.exe            992 False  True   False   False  False False  False   2018-04-13 01:46:10 UTC+0000
0×000000003fabf998 SearchFilterHo         1964 False  True   False   False  False False  False   2018-04-13 01:40:18 UTC+0000
0×000000003fcfc2c8 SearchFilterHo         2364 False  True   False   False  False False  False   2018-04-13 01:47:26 UTC+0000
0×000000003f66d2c8                         504 False  False  True    False  False False  False
```

In our scenario, the last four processes of psxview are a little complicatable. **Psxview** shows that there is some unlinked process which is listed in psscan but not in pslist like PID992,PID1964,PID2364.

By running **netscan** we have found more information to see possibilility of open ports and network connections.

Volatility -f memory.dmp --profile=Win7SP0x64 netscan

```
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State          Pid      Owner          Created
0x3dc4e230         UDPv6    fe80::c0c9:aa19:31b7:43c6:1900 *:*                                  1296     svchost.exe    2018-04-13 01:28:34 UTC+0000
0x3dc9b8e0         TCPv4    192.168.50.11:49598            192.168.50.1:2042    CLOSED         2176     python.exe
0x3de08da0         UDPv4    0.0.0.0:0                      *:*                                 332      svchost.exe    2018-04-13 01:28:31 UTC+0000
0x3de1c9c0         UDPv6    fe80::c0c9:aa19:31b7:43c6:64671 *:*                                 1296     svchost.exe    2018-04-13 01:28:34 UTC+0000
0x3de22730         UDPv6    ::1:1900                       *:*                                 1296     svchost.exe    2018-04-13 01:28:34 UTC+0000
0x3e0358b0         UDPv4    0.0.0.0:0                      *:*                                 1948     svchost.exe    2018-04-06 23:12:54 UTC+0000
0x3e091340         UDPv4    0.0.0.0:3702                   *:*                                 1296     svchost.exe    2018-04-13 01:28:26 UTC+0000
0x3e0972f0         UDPv4    0.0.0.0:60992                  *:*                                 1296     svchost.exe    2018-04-06 23:12:50 UTC+0000
0x3e097ec0         UDPv4    0.0.0.0:3702                   *:*                                 1296     svchost.exe    2018-04-13 01:28:26 UTC+0000
0x3e097ec0         UDPv6    :::3702                        *:*                                 1296     svchost.exe    2018-04-13 01:28:26 UTC+0000
0x3e098a10         UDPv4    0.0.0.0:60993                  *:*                                 1296     svchost.exe    2018-04-06 23:12:50 UTC+0000
0x3e098a10         UDPv6    :::60993                       *:*                                 1296     svchost.exe    2018-04-06 23:12:50 UTC+0000
0x3e0a6160         UDPv4    0.0.0.0:3702                   *:*                                 1296     svchost.exe    2018-04-13 01:28:26 UTC+0000
0x3e0a6160         UDPv6    :::3702                        *:*                                 1296     svchost.exe    2018-04-13 01:28:26 UTC+0000
0x3e0a6660         UDPv4    0.0.0.0:3702                   *:*                                 1296     svchost.exe    2018-04-13 01:28:26 UTC+0000
0x3e0f69c0         UDPv4    0.0.0.0:0                      *:*                                 1948     svchost.exe    2018-04-06 23:12:54 UTC+0000
0x3e0f69c0         UDPv6    :::0                           *:*                                 1948     svchost.exe    2018-04-06 23:12:54 UTC+0000
0x3e10c0e0         UDPv4    0.0.0.0:0                      *:*                                 332      svchost.exe    2018-04-13 01:28:31 UTC+0000
0x3e10c0e0         UDPv6    :::0                           *:*                                 332      svchost.exe    2018-04-13 01:28:31 UTC+0000
0x3e15cec0         UDPv4    127.0.0.1:1900                 *:*                                 1296     svchost.exe    2018-04-13 01:28:34 UTC+0000
0x3e1bb9b0         UDPv4    127.0.0.1:64674                *:*                                 1296     svchost.exe    2018-04-13 01:28:34 UTC+0000
0x3e2a2a00         UDPv4    192.168.50.11:64673            *:*                                 1296     svchost.exe    2018-04-13 01:28:34 UTC+0000
0x3e2be920         UDPv4    0.0.0.0:0                      *:*                                 900      svchost.exe    2018-04-13 01:28:23 UTC+0000
0x3e2be920         UDPv6    :::0                           *:*                                 900      svchost.exe    2018-04-13 01:28:23 UTC+0000
0x3e356bc0         UDPv4    127.0.0.1:58141                *:*                                 2800     iexplore.exe   2018-04-13 01:38:18 UTC+0000
0x3e3f0500         UDPv4    0.0.0.0:500                    *:*                                 904      svchost.exe    2018-04-06 23:12:49 UTC+0000
0x3e3f0500         UDPv6    :::500                         *:*                                 904      svchost.exe    2018-04-06 23:12:49 UTC+0000
0x3e3f0980         UDPv4    0.0.0.0:4500                   *:*                                 904      svchost.exe    2018-04-06 23:12:49 UTC+0000
0x3e3f0c20         UDPv4    0.0.0.0:500                    *:*                                 904      svchost.exe    2018-04-06 23:12:49 UTC+0000
0x3e3f8ec0         UDPv4    0.0.0.0:0                      *:*                                 904      svchost.exe    2018-04-06 23:12:49 UTC+0000
0x3e3fad00         UDPv4    0.0.0.0:4500                   *:*                                 904      svchost.exe    2018-04-06 23:12:49 UTC+0000
0x3e3fad00         UDPv6    :::4500                        *:*                                 904      svchost.exe    2018-04-06 23:12:49 UTC+0000
```



0×3e3fad00	UDPv6	:::4500	*:*		904	svchost.exe	2018-04-06 23:12:49 UTC+0000
0×3e3fd490	UDPv4	0.0.0.0:0	*:*		904	svchost.exe	2018-04-06 23:12:49 UTC+0000
0×3e3fd490	UDPv6	:::0	*:*		904	svchost.exe	2018-04-06 23:12:49 UTC+0000
0×3e660010	UDPv4	0.0.0.0:123	*:*		332	svchost.exe	2018-04-13 01:28:23 UTC+0000
0×3e660010	UDPv6	:::123	*:*		332	svchost.exe	2018-04-13 01:28:23 UTC+0000
0×3e6a3010	UDPv4	192.168.50.11:138	*:*		4	System	2018-04-13 01:28:23 UTC+0000
0×3e6b9810	UDPv4	0.0.0.0:5355	*:*		900	svchost.exe	2018-04-13 01:28:23 UTC+0000
0×3e6b9810	UDPv6	:::5355	*:*		900	svchost.exe	2018-04-13 01:28:23 UTC+0000
0×3e6bdd70	UDPv4	192.168.50.11:1900	*:*		1296	svchost.exe	2018-04-13 01:28:34 UTC+0000
0×3dee4b30	TCPv4	0.0.0.0:8000	0.0.0.0:0	LISTENING	1208	python.exe	
0×3e0368e0	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	1948	svchost.exe	
0×3e101010	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	1948	svchost.exe	
0×3e101010	TCPv6	:::49156	:::0	LISTENING	1948	svchost.exe	
0×3e1657e0	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	488	services.exe	
0×3e17f8a0	TCPv4	0.0.0.0:445	0.0.0.0:0	LISTENING	4	System	
0×3e17f8a0	TCPv6	:::445	:::0	LISTENING	4	System	
0×3e189b00	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	488	services.exe	
0×3e189b00	TCPv6	:::49155	:::0	LISTENING	488	services.exe	
0×3e1d9320	TCPv4	0.0.0.0:49157	0.0.0.0:0	LISTENING	496	lsass.exe	
0×3e1d9320	TCPv6	:::49157	:::0	LISTENING	496	lsass.exe	
0×3e1f46e0	TCPv4	192.168.50.11:139	0.0.0.0:0	LISTENING	4	System	
0×3e2df560	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	904	svchost.exe	
0×3e2eeef0	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	904	svchost.exe	
0×3e2eeef0	TCPv6	:::49154	:::0	LISTENING	904	svchost.exe	
0×3e33a360	TCPv4	0.0.0.0:5357	0.0.0.0:0	LISTENING	4	System	
0×3e33a360	TCPv6	:::5357	:::0	LISTENING	4	System	
0×3e3e02b0	TCPv4	0.0.0.0:49157	0.0.0.0:0	LISTENING	496	lsass.exe	
0×3e40dc90	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	736	svchost.exe	
0×3e40dc90	TCPv6	:::135	:::0	LISTENING	736	svchost.exe	
0×3e422b80	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	392	wininit.exe	
0×3e424220	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	392	wininit.exe	
0×3e424220	TCPv6	:::49152	:::0	LISTENING	392	wininit.exe	
0×3e5cd630	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	824	svchost.exe	
0×3e5cd630	TCPv6	:::49153	:::0	LISTENING	824	svchost.exe	

Result from netscan is a good thing to do is to check the running sockets and open connections on the computer.

Then we used the command **cmdline** plugin which displays process command-line arguments.this gave us interesting information about the directory of executed processes on the system.

Volatility -f memory.dmp --profile=Win7SP0x64 cmdline

```
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 cmdline
Volatility Foundation Volatility Framework 2.6
************************************************************************
System pid:      4
************************************************************************
smss.exe pid:    276
Command line : \SystemRoot\System32\smss.exe
************************************************************************
csrss.exe pid:    360
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=wi
nsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
************************************************************************
wininit.exe pid:    392
Command line : wininit.exe
************************************************************************
csrss.exe pid:    404
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=wi
nsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
************************************************************************
winlogon.exe pid:    444
Command line : winlogon.exe
************************************************************************
services.exe pid:    488
Command line : C:\Windows\system32\services.exe
************************************************************************
lsass.exe pid:    496
Command line : C:\Windows\system32\lsass.exe
************************************************************************
lsm.exe pid:    504
Command line : C:\Windows\system32\lsm.exe
************************************************************************
svchost.exe pid:    612
Command line : C:\Windows\system32\svchost.exe -k DcomLaunch
```

```
VBoxService.ex pid:    672
Command line : system32\VBoxService.exe
************************************************************************
svchost.exe pid:    736
Command line : C:\Windows\system32\svchost.exe -k RPCSS
************************************************************************
svchost.exe pid:    824
Command line : C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
************************************************************************
svchost.exe pid:    872
Command line : C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
************************************************************************
svchost.exe pid:    904
Command line : C:\Windows\system32\svchost.exe -k netsvcs
************************************************************************
svchost.exe pid:    332
Command line : C:\Windows\system32\svchost.exe -k LocalService
************************************************************************
svchost.exe pid:    900
Command line : C:\Windows\system32\svchost.exe -k NetworkService
************************************************************************
spoolsv.exe pid:   1120
Command line : C:\Windows\System32\spoolsv.exe
************************************************************************
svchost.exe pid:   1152
Command line : C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
************************************************************************
svchost.exe pid:   1296
Command line : C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
************************************************************************
dwm.exe pid:   1588
Command line : "C:\Windows\system32\Dwm.exe"
************************************************************************
taskhost.exe pid:   1596
Command line : "taskhost.exe"
```

```
**********************************************************************
explorer.exe pid:   1652
Command line : C:\Windows\Explorer.EXE
**********************************************************************
svchost.exe pid:   1948
Command line : C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted
**********************************************************************
VBoxTray.exe pid:   1376
Command line : "C:\Windows\System32\VBoxTray.exe"
**********************************************************************
python.exe pid:   1208
Command line : "C:\Python27\python.exe" "C:\Users\Win7\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\agent.py"
**********************************************************************
conhost.exe pid:   1916
Command line : \??\C:\Windows\system32\conhost.exe
**********************************************************************
acrotray.exe pid:   2144
Command line : "C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\acrotray.exe"
**********************************************************************
SearchIndexer. pid:   2180
Command line : C:\Windows\system32\SearchIndexer.exe /Embedding
**********************************************************************
wmpnetwk.exe pid:   2540
Command line : "C:\Program Files\Windows Media Player\wmpnetwk.exe"
**********************************************************************
SndVol.exe pid:   2568
**********************************************************************
python.exe pid:   2176
Command line : C:\Python27\python.exe C:/tmpifsbua/analyzer.py
**********************************************************************
7004af389d633b pid:    512
**********************************************************************
mscorsvw.exe pid:   2740
Command line : C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
**********************************************************************
```

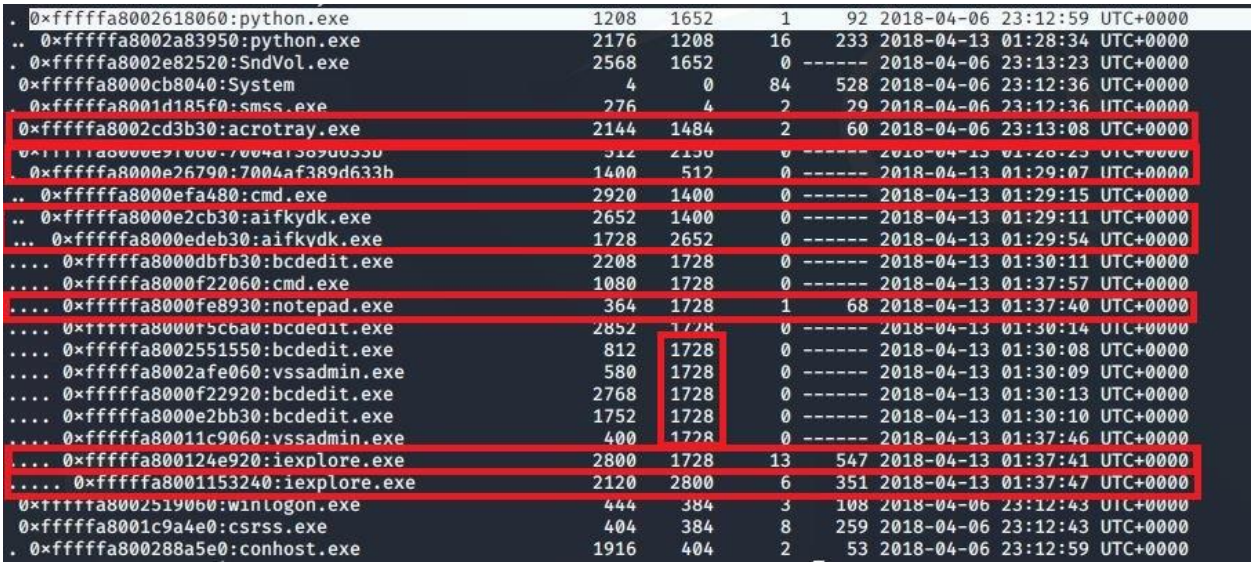
```
**********************************************************************
mscorsvw.exe pid:   3056
Command line : C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe
**********************************************************************
svchost.exe pid:   1404
Command line : C:\Windows\System32\svchost.exe -k secsvcs
**********************************************************************
7004af389d633b pid:   1400
**********************************************************************
aifkydk.exe pid:   2652
**********************************************************************
cmd.exe pid:   2920
**********************************************************************
aifkydk.exe pid:   1728
**********************************************************************
bcdedit.exe pid:    812
**********************************************************************
vssadmin.exe pid:    580
**********************************************************************
bcdedit.exe pid:   1752
**********************************************************************
bcdedit.exe pid:   2208
**********************************************************************
bcdedit.exe pid:   2768
**********************************************************************
bcdedit.exe pid:   2852
**********************************************************************
notepad.exe pid:    364
Command line : "C:\Windows\system32\NOTEPAD.EXE" C:\Users\Win7\Desktop\help_recover_instructions.TXT
**********************************************************************
iexplore.exe pid:   2800
Command line : "C:\Program Files (x86)\Internet Explorer\iexplore.exe" -nohome
**********************************************************************
dllhost.exe pid:   1932
Command line : C:\Windows\SysWOW64\DllHost.exe /Processid:{76D0CB12-7604-4048-B83C-1005C7DDC503}
```

```
**********************************************************************
vssadmin.exe pid:    400
**********************************************************************
iexplore.exe pid:   2120
Command line : "C:\Program Files (x86)\Internet Explorer\iexplore.exe" SCODEF:2800 CREDAT:14337
**********************************************************************
cmd.exe pid:   1080
**********************************************************************
VSSVC.exe pid:   1564
Command line : C:\Windows\system32\vssvc.exe
**********************************************************************
svchost.exe pid:   2312
Command line : C:\Windows\System32\svchost.exe -k swprv
**********************************************************************
mscorsvw.exe pid:   2728
Command line : C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe -UseCLSID {170EFAC6-D812-4C86-B1B5-9BC8570FD482} -Comment "Compile worker for ehiVidCtl, Ver
sion=6.1.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"
```

After doing more analysis on above results we found some of these process seem to be legitimate but some of them look more malicious as follow :

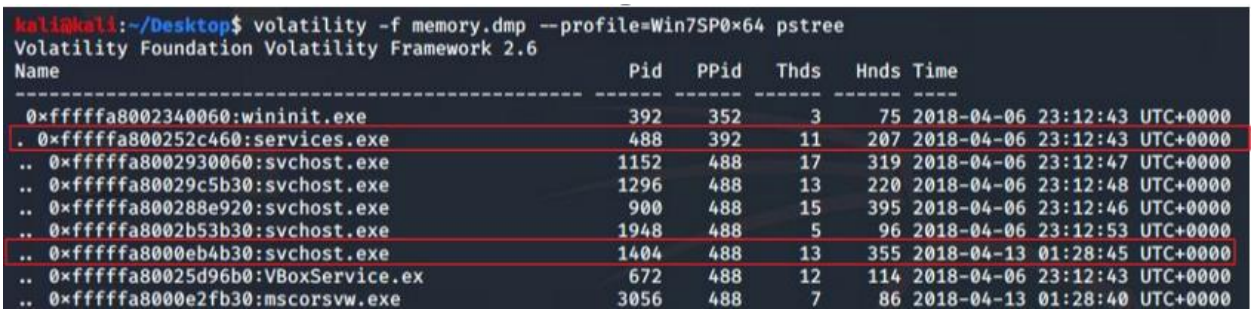
By Comparison between cmdline (Display process command-line arguments) and pstree (Print process list as a tree) we can see that:

```
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa8002340060:wininit.exe                       392    352      3     75 2018-04-06 23:12:43 UTC+0000
. 0xfffffa800252c460:services.exe                     488    392     11    207 2018-04-06 23:12:43 UTC+0000
.. 0xfffffa8002930060:svchost.exe                    1152    488     17    319 2018-04-06 23:12:47 UTC+0000
.. 0xfffffa80029c5b30:svchost.exe                    1296    488     13    220 2018-04-06 23:12:48 UTC+0000
.. 0xfffffa800288e920:svchost.exe                     900    488     15    395 2018-04-06 23:12:46 UTC+0000
.. 0xfffffa8002b53b30:svchost.exe                    1948    488      5     96 2018-04-06 23:12:53 UTC+0000
.. 0xfffffa8000eb4b30:svchost.exe                    1404    488     13    355 2018-04-13 01:28:45 UTC+0000
.. 0xfffffa80025d96b0:VBoxService.ex                  672    488     12    114 2018-04-06 23:12:43 UTC+0000
.. 0xfffffa8000e2fb30:mscorsvw.exe                   3056    488      7     86 2018-04-13 01:28:40 UTC+0000
.. 0xfffffa8002de6b30:VSSVC.exe                      1564    488      9    184 2018-04-13 01:44:43 UTC+0000
.. 0xfffffa8002644b30:svchost.exe                     904    488     39   1238 2018-04-06 23:12:44 UTC+0000
.. 0xfffffa8002570b30:svchost.exe                     824    488     18    457 2018-04-06 23:12:44 UTC+0000
.. 0xfffffa8000e70060:mscorsvw.exe                   2740    488      8    124 2018-04-13 01:28:34 UTC+0000
... 0xfffffa8000e39b30:mscorsvw.exe                  2728   2740      8    145 2018-04-13 01:49:17 UTC+0000
.. 0xfffffa8001050650:svchost.exe                    2312    488      4     78 2018-04-13 01:44:47 UTC+0000
.. 0xfffffa8002897b30:spoolsv.exe                    1120    488     12    279 2018-04-06 23:12:47 UTC+0000
.. 0xfffffa80015e1b30:SearchIndexer.                 2180    488     12    765 2018-04-06 23:13:10 UTC+0000
.. 0xfffffa800285d4a0:svchost.exe                     332    488     12    325 2018-04-06 23:12:45 UTC+0000
.. 0xfffffa80027d2740:svchost.exe                     872    488     19    478 2018-04-06 23:12:44 UTC+0000
... 0xfffffa80029eab30:dwm.exe                       1588    872      3     70 2018-04-06 23:12:50 UTC+0000
.. 0xfffffa80025ef060:svchost.exe                     736    488      9    264 2018-04-06 23:12:44 UTC+0000
.. 0xfffffa80025ae600:svchost.exe                     612    488     10    345 2018-04-06 23:12:43 UTC+0000
... 0xfffffa8000dbd250:dllhost.exe                   1932    612      7    205 2018-04-13 01:37:46 UTC+0000
.. 0xfffffa8002aa4b30:taskhost.exe                   1596    488      7    141 2018-04-06 23:12:50 UTC+0000
.. 0xfffffa8002daab30:wmpnetwk.exe                   2540    488     10    214 2018-04-06 23:13:22 UTC+0000
. 0xfffffa800255ab30:lsass.exe                        496    392      7    553 2018-04-06 23:12:43 UTC+0000
. 0xfffffa8002541b30:lsm.exe                          504    392     10    144 2018-04-06 23:12:43 UTC+0000
 0xfffffa80024e2800:csrss.exe                         360    352      9    402 2018-04-06 23:12:43 UTC+0000
 0xfffffa8002ab6b30:explorer.exe                     1652   1580     23    817 2018-04-06 23:12:51 UTC+0000
. 0xfffffa8002afeb30:VBoxTray.exe                    1376   1652     10    103 2018-04-06 23:12:56 UTC+0000
. 0xfffffa8002618060:python.exe                      1208   1652      1     92 2018-04-06 23:12:59 UTC+0000
```



. 0×fffffa8002618060:python.exe	1208	1652	1	92	2018-04-06 23:12:59 UTC+0000
.. 0×fffffa8002a83950:python.exe	2176	1208	16	233	2018-04-13 01:28:34 UTC+0000
. 0×fffffa8002e82520:SndVol.exe	2568	1652	0	------	2018-04-06 23:13:23 UTC+0000
0×fffffa8000cb8040:System	4	0	84	528	2018-04-06 23:12:36 UTC+0000
. 0×fffffa8001d185f0:smss.exe	276	4	2	29	2018-04-06 23:12:36 UTC+0000
0×fffffa8002cd3b30:acrotray.exe	2144	1484	2	60	2018-04-06 23:13:08 UTC+0000
. 0×fffffa8000e26790:7004af389d633b	1400	512	0	------	2018-04-13 01:29:07 UTC+0000
.. 0×fffffa8000efa480:cmd.exe	2920	1400	0	------	2018-04-13 01:29:15 UTC+0000
.. 0×fffffa8000e2cb30:aifkydk.exe	2652	1400	0	------	2018-04-13 01:29:11 UTC+0000
... 0×fffffa8000edeb30:aifkydk.exe	1728	2652	0	------	2018-04-13 01:29:54 UTC+0000
.... 0×fffffa8000dbfb30:bcdedit.exe	2208	1728	0	------	2018-04-13 01:30:11 UTC+0000
.... 0×fffffa8000f22060:cmd.exe	1080	1728	0	------	2018-04-13 01:37:57 UTC+0000
.... 0×fffffa8000fe8930:notepad.exe	364	1728	1	68	2018-04-13 01:37:40 UTC+0000
.... 0×fffffa8000f5c6a0:bcdedit.exe	2852	1728	0	------	2018-04-13 01:30:14 UTC+0000
.... 0×fffffa8002551550:bcdedit.exe	812	1728	0	------	2018-04-13 01:30:08 UTC+0000
.... 0×fffffa8002afe060:vssadmin.exe	580	1728	0	------	2018-04-13 01:30:09 UTC+0000
.... 0×fffffa8000f22920:bcdedit.exe	2768	1728	0	------	2018-04-13 01:30:13 UTC+0000
.... 0×fffffa8000e2bb30:bcdedit.exe	1752	1728	0	------	2018-04-13 01:30:10 UTC+0000
.... 0×fffffa80011c9060:vssadmin.exe	400	1728	0	------	2018-04-13 01:37:46 UTC+0000
.... 0×fffffa800124e920:iexplore.exe	2800	1728	13	547	2018-04-13 01:37:41 UTC+0000
..... 0×fffffa8001153240:iexplore.exe	2120	2800	6	351	2018-04-13 01:37:47 UTC+0000
0×fffffa80025190b0:winlogon.exe	444	384	3	108	2018-04-06 23:12:43 UTC+0000
0×fffffa8001c9a4e0:csrss.exe	404	384	8	259	2018-04-06 23:12:43 UTC+0000
. 0×fffffa800288a5e0:conhost.exe	1916	404	2	53	2018-04-06 23:12:59 UTC+0000

Examining at the above listing, several issues have been highlighted (in red) as they represent potentially suspicious processes.



```
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 pstree
Volatility Foundation Volatility Framework 2.6
```

Name	Pid	PPid	Thds	Hnds	Time
0×fffffa8002340060:wininit.exe	392	352	3	75	2018-04-06 23:12:43 UTC+0000
. 0×fffffa800252c460:services.exe	488	392	11	207	2018-04-06 23:12:43 UTC+0000
.. 0×fffffa8002930060:svchost.exe	1152	488	17	319	2018-04-06 23:12:47 UTC+0000
.. 0×fffffa80029c5b30:svchost.exe	1296	488	13	220	2018-04-06 23:12:48 UTC+0000
.. 0×fffffa800288e920:svchost.exe	900	488	15	395	2018-04-06 23:12:46 UTC+0000
.. 0×fffffa8002b53b30:svchost.exe	1948	488	5	96	2018-04-06 23:12:53 UTC+0000
.. 0×fffffa8000eb4b30:svchost.exe	1404	488	13	355	2018-04-13 01:28:45 UTC+0000
.. 0×fffffa80025d96b0:VBoxService.ex	672	488	12	114	2018-04-06 23:12:43 UTC+0000
.. 0×fffffa8000e2fb30:mscorsvw.exe	3056	488	7	86	2018-04-13 01:28:40 UTC+0000

. In this case **svchost.exe** with **PID is 1404** created by **PPID 448**

As we can see that **448** is the **PID of services.exe.** However**, services.exe** is a child of **wininit.exe.**

Our machine in this project is **WIN7SP0x64** and we know that in windows vista and later all windows have this process. So, it seems that it is OK

But we know that **Svchost.exe** is a process on the computer that hosts, or contains, other individual services that Windows uses to perform various functions. For example, **Windows Defender** and **Windows Update** use a service that is hosted by a svchost.exe process. The file often connects to www.windowsupdate.microsoft.com by either visiting the **Microsoft Update website**, **Microsoft Windows Update website**, or through automatic updating without a browser. "svchost.exe" is the host processor that manages the group of update service DLLs in the database from the Windows User Automatic Updates Server (WUAUSERV).

When we check **svcscan,** we use this command to scan for Windows services. All process that run on windows services are shown with this command. So based on this result, the PID 1404 is windows services.

Volatility -f memory.dmp --profile=Win7SP0x64 svcscan

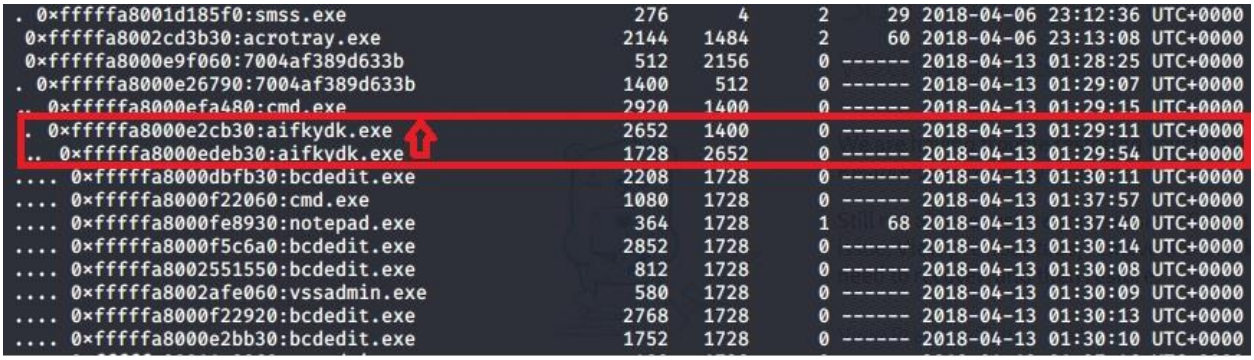
```
kali@kali:~/Desktop$
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 svcscan
```

```
Offset: 0x98cb10
Order: 368
Start: SERVICE_AUTO_START
Process ID: 1404
Service Name: WinDefend
Display Name: Windows Defender
Service Type: SERVICE_WIN32_SHARE_PROCESS
Service State: SERVICE_RUNNING
Binary Path: C:\Windows\System32\svchost.exe -k secsvcs
```

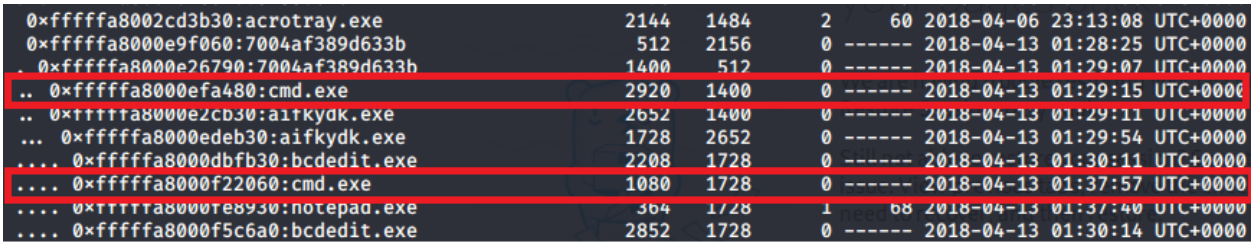
With malfind command we prove that 1404 is suspicious.

```
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 malfind -p 1404
Volatility Foundation Volatility Framework 2.6
Process: svchost.exe Pid: 1404 Address: 0x69c0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 128, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x069c0000  20 00 00 00 e0 ff 07 00 0c 00 00 00 01 00 07 00   ................
0x069c0010  00 42 00 30 00 70 00 60 00 50 00 c0 00 d0 00 00   .B.0.p.`.P......
0x069c0020  08 00 42 00 00 00 00 05 48 8b 45 20 48 89 c2 48   ..B.....H.E.H..H
0x069c0030  8b 45 18 48 8b 00 48 89 02 48 8b 45 20 81 00 b8   .E.H..H..H.E....

0x069c0000 2000            AND [EAX], AL
0x069c0002 0000            ADD [EAX], AL
0x069c0004 e0ff            LOOPNZ 0x69c0005
0x069c0006 07              POP ES
```

Another process **aifkydk.exe**

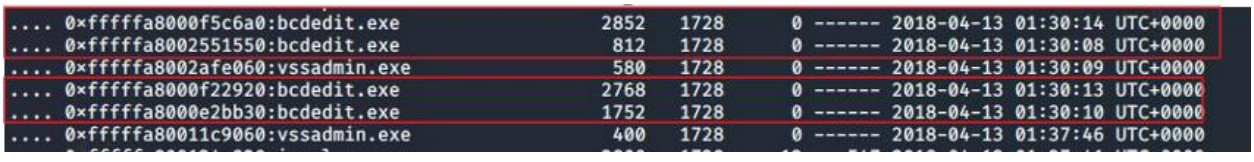


This is suspicious because the parent of **aifkydk.exe** with 2652 as a process ID, the parent's ID of this process is 1728. As highlighted with the red box in the above picture we can see that both processes have the same process name but different process ID and different parents ID. Second one was not started by winlogon.exe or wininit.exe but these processes were started by unknown aifkydk.exe .



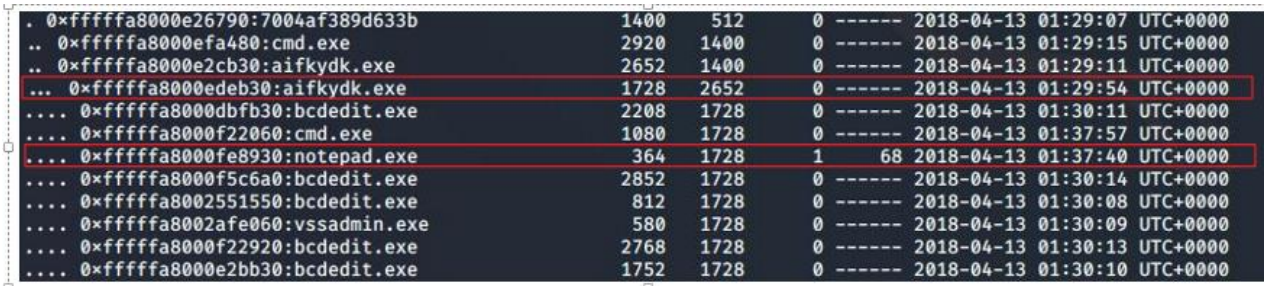
In the above screen shot **cmd.exe** the process id is 2920 with parents ID of 1400.
1400 is the PID of a process that is unknown. This process parent ID is 512. and again 512 is an unknown process. So, cmd.exe in this case is suspicious.

In the second red highlighted box, **cmd.exe** with process ID of 1080 seems suspicious.
Because of the PPID of this process in 1728.
According to the above description, the process with this ID is suspicious.



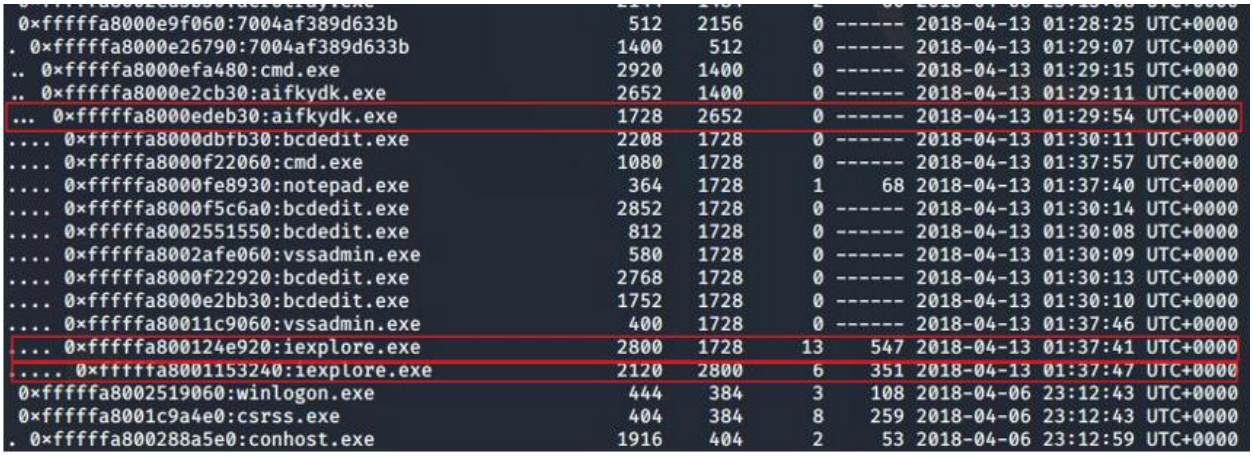
bcdedit.exe is an executable file that is part of **Windows 10 Operating System** developed by **Microsoft Corporation**. In some cases, executable files can damage the computer.

Four process IDs for **bcdedit.exe** have the same PPID including ; 2852, 812, 2768, and 1752. and it is another suspicious. All processes come from the same PPID and these are suspicious.



. 0×fffffa8000e26790:7004af389d633b	1400	512	0	------	2018-04-13 01:29:07	UTC+0000
.. 0×fffffa8000efa480:cmd.exe	2920	1400	0	------	2018-04-13 01:29:15	UTC+0000
.. 0×fffffa8000e2cb30:aifkydk.exe	2652	1400	0	------	2018-04-13 01:29:11	UTC+0000
... 0×fffffa8000edeb30:aifkydk.exe	1728	2652	0	------	2018-04-13 01:29:54	UTC+0000
.... 0×fffffa8000dbfb30:bcdedit.exe	2208	1728	0	------	2018-04-13 01:30:11	UTC+0000
.... 0×fffffa8000f22060:cmd.exe	1080	1728	0	------	2018-04-13 01:37:57	UTC+0000
.... 0×fffffa8000fe8930:notepad.exe	364	1728	1	68	2018-04-13 01:37:40	UTC+0000
.... 0×fffffa8000f5c6a0:bcdedit.exe	2852	1728	0	------	2018-04-13 01:30:14	UTC+0000
.... 0×fffffa8002551550:bcdedit.exe	812	1728	0	------	2018-04-13 01:30:08	UTC+0000
.... 0×fffffa8002afe060:vssadmin.exe	580	1728	0	------	2018-04-13 01:30:09	UTC+0000
.... 0×fffffa8000f22920:bcdedit.exe	2768	1728	0	------	2018-04-13 01:30:13	UTC+0000
.... 0×fffffa8000e2bb30:bcdedit.exe	1752	1728	0	------	2018-04-13 01:30:10	UTC+0000

Notepad.exe with PID 364. In this case 364 is the PPID of 1728. And also 1728 is the PID of aifkydk.exe .it seems suspicious and in the previous page IN AIFKYDK part explain in detail.



0×fffffa8000e9f060:7004af389d633b	512	2156	0	------	2018-04-13 01:28:25	UTC+0000
. 0×fffffa8000e26790:7004af389d633b	1400	512	0	------	2018-04-13 01:29:07	UTC+0000
.. 0×fffffa8000efa480:cmd.exe	2920	1400	0	------	2018-04-13 01:29:15	UTC+0000
.. 0×fffffa8000e2cb30:aifkydk.exe	2652	1400	0	------	2018-04-13 01:29:11	UTC+0000
... 0×fffffa8000edeb30:aifkydk.exe	1728	2652	0	------	2018-04-13 01:29:54	UTC+0000
.... 0×fffffa8000dbfb30:bcdedit.exe	2208	1728	0	------	2018-04-13 01:30:11	UTC+0000
.... 0×fffffa8000f22060:cmd.exe	1080	1728	0	------	2018-04-13 01:37:57	UTC+0000
.... 0×fffffa8000fe8930:notepad.exe	364	1728	1	68	2018-04-13 01:37:40	UTC+0000
.... 0×fffffa8000f5c6a0:bcdedit.exe	2852	1728	0	------	2018-04-13 01:30:14	UTC+0000
.... 0×fffffa8002551550:bcdedit.exe	812	1728	0	------	2018-04-13 01:30:08	UTC+0000
.... 0×fffffa8002afe060:vssadmin.exe	580	1728	0	------	2018-04-13 01:30:09	UTC+0000
.... 0×fffffa8000f22920:bcdedit.exe	2768	1728	0	------	2018-04-13 01:30:13	UTC+0000
.... 0×fffffa8000e2bb30:bcdedit.exe	1752	1728	0	------	2018-04-13 01:30:10	UTC+0000
.... 0×fffffa80011c9060:vssadmin.exe	400	1728	0	------	2018-04-13 01:37:46	UTC+0000
... 0×fffffa800124e920:iexplore.exe	2800	1728	13	547	2018-04-13 01:37:41	UTC+0000
.... 0×fffffa8001153240:iexplore.exe	2120	2800	6	351	2018-04-13 01:37:47	UTC+0000
0×fffffa8002519060:winlogon.exe	444	384	3	108	2018-04-06 23:12:43	UTC+0000
0×fffffa8001c9a4e0:csrss.exe	404	384	8	259	2018-04-06 23:12:43	UTC+0000
. 0×fffffa800288a5e0:conhost.exe	1916	404	2	53	2018-04-06 23:12:59	UTC+0000

According to comparison between cmdline and pstree command result

Iexplorer.exe with a PID of 2800 . It is clear that PPID=1728 of this process is aifkydk.exe. And we know that this process PPID of an unknown process. So. it seems this process is suspicious, too.

IExplore.exe with PID 2120 has a PPID of 2800. 2800 is the same process name with different PPID. And also, when we use **svcscan** command. we can
Scan for Windows services. However, we cannot find Iexplore.exe with PPID 2120 in **svcscan** logs. So the information proves that this process is suspicious.

The Malfind for iexplore.exe on PID of 2120 we can find useful information.

```
Process: iexplore.exe Pid: 2120 Address: 0×120000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

Malifind for iexoplore.exe on PID 2800

```
Process: iexplore.exe Pid: 2800 Address: 0×2820000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 2, MemCommit: 1, PrivateMemory: 1, Protection: 6

0×02820000  b0 00 eb 70 b0 01 eb 6c b0 02 eb 68 b0 03 eb 64    ...p...l...h...d
0×02820010  b0 04 eb 60 b0 05 eb 5c b0 06 eb 58 b0 07 eb 54    ...`...\...X...T
0×02820020  b0 08 eb 50 b0 09 eb 4c b0 0a eb 48 b0 0b eb 44    ...P...L...H...D
0×02820030  b0 0c eb 40 b0 0d eb 3c b0 0e eb 38 b0 0f eb 34    ...@...<...8...4
```

Those screenshots lead to determining more specifically. In this case, 2120 is malicious. The explorer.exe is executing protection which indicates the process is malicious. In the process of checking the malfind log.

According to pstree logs and more information in pslist and cmdline. It shows that:

```
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0×64 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0×fffffa8002340060:wininit.exe                       392    352      3     75 2018-04-06 23:12:43 UTC+0000
. 0×fffffa800252c460:services.exe                     488    392     11    207 2018-04-06 23:12:43 UTC+0000
.. 0×fffffa8002930060:svchost.exe                    1152    488     17    319 2018-04-06 23:12:47 UTC+0000
.. 0×fffffa80029c5b30:svchost.exe                    1296    488     13    220 2018-04-06 23:12:48 UTC+0000
.. 0×fffffa800288e920:svchost.exe                     900    488     15    395 2018-04-06 23:12:46 UTC+0000
.. 0×fffffa8002b53b30:svchost.exe                    1948    488      5     96 2018-04-06 23:12:53 UTC+0000
.. 0×fffffa8000eb4b30:svchost.exe                    1404    488     13    355 2018-04-13 01:28:45 UTC+0000
.. 0×fffffa8000e2fb30:mscorsvw.exe                   3056    488      7     86 2018-04-13 01:28:40 UTC+0000
.. 0×fffffa8002de6b30:VSSVC.exe                      1564    488      9    184 2018-04-13 01:44:43 UTC+0000
.. 0×fffffa8002644b30:svchost.exe                     904    488     39   1238 2018-04-06 23:12:44 UTC+0000
. 0×fffffa8000e70060:mscorsvw.exe                    2740    488      8    124 2018-04-13 01:28:34 UTC+0000
... 0×fffffa8000e39b30:mscorsvw.exe                  2728   2740      8    145 2018-04-13 01:49:17 UTC+0000
.. 0×fffffa8001050650:svchost.exe                    2312    488      4     78 2018-04-13 01:44:47 UTC+0000
.. 0×fffffa8002897b30:spoolsv.exe                    1120    488     12    279 2018-04-06 23:12:47 UTC+0000
```

mscorsvw.exe is a legitimate file from Microsoft Corporation that is used for running .NET programs. It precompiled .NET assemblies in the background. It is commonly located in c:\windows\microsoft.NET\framework.
But in this case when we use **cmdline** we can find another folder as a location of mscorsvw.exe

```
**************************************************************************
mscorsvw.exe pid:   2740
Command line : C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
**************************************************************************
mscorsvw.exe pid:   3056
Command line : C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe
**************************************************************************
```

```
**********************************************************************
mscorsvw.exe pid:   2728
Command line : C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe -UseCLSID {170EFAC6-D812-4C86-B1B5-9BC8570FD482} -Comment "Compile worker for ehiVidCtl, Version=6.1.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"
```

Both PID 2740 and 3056 in the first picture are the same PPID. Their PPID is 448. But in **cmdline** result it's obviously that both processes are located in different directories. Although they have the same PPID and same process name.

Surprisingly, mscorsw.exe with PPID of 2728 is malicious. It does not have a weird directory in **cmdline.** It can be shown in the above picture. PPID of 2728 is 2740. It can be seen that two different PID for the same PPID = 448 with the same name show that this process is suspicious.

In another browsing malicious process we can find **vssadmin.exe**

```
.... 0×fffffa80011c9060:vssadmin.exe          400   1728      0 ------ 2018-04-13 01:37:46 UTC+0000
..... 0×fffffa8001153240:iexplore.exe        2120   2800      6    351 2018-04-13 01:37:47 UTC+0000
```

This file is a command-line tool made available to interface with the “Volume Shadow Copy Service”. But many times all ransomware will use **vssadmin.exe** to delete “shadow copies” of files, which we probably didn’t even know we had, before encrypting the files we do know about. So, it seems that this file is suspicious.

According to the pstree result, **python.exe** is suspicious.

```
 0×fffffa8002ab6b30:explorer.exe              1652   1580     23    817 2018-04-06 23:12:51 UTC+0000
. 0×fffffa8002618060:python.exe               1208   1652      1     92 2018-04-06 23:12:59 UTC+0000
.. 0×fffffa8002a83950:python.exe              2176   1208     16    233 2018-04-13 01:28:34 UTC+0000
. 0×fffffa8002e82520:SndVol.exe               2568   1652      0 ------ 2018-04-06 23:13:23 UTC+0000
```

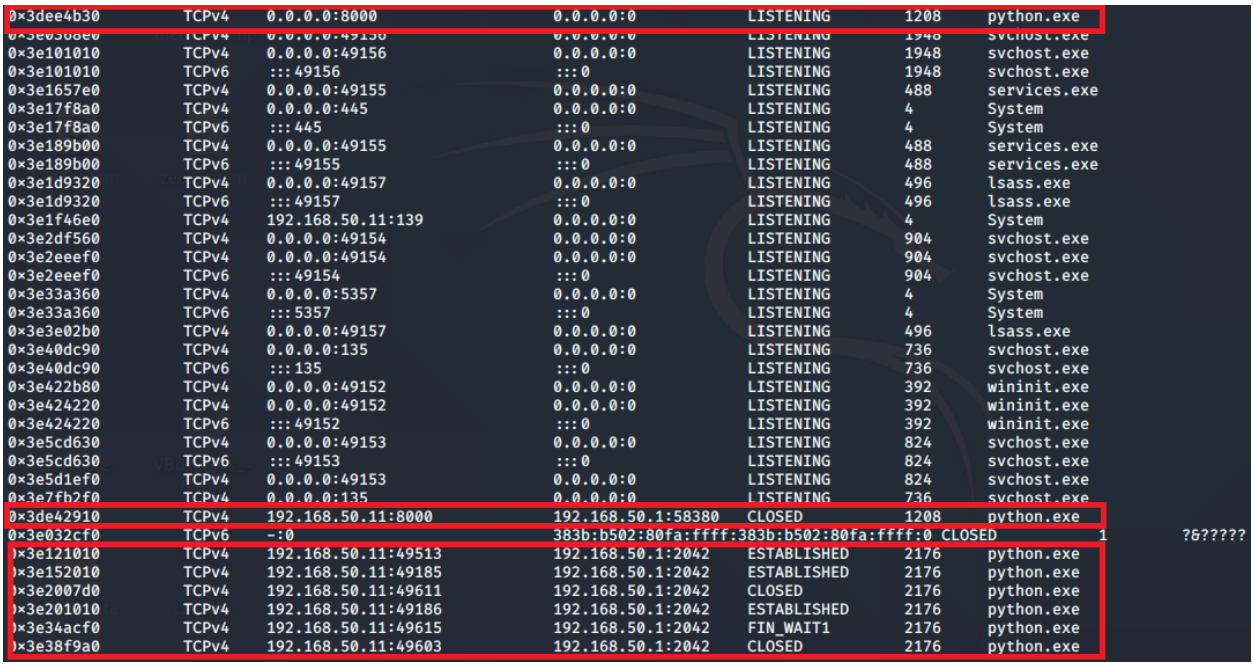
Python.exe with process ID 1208 that parents ID of another Python.exe process.
1652 is the PPID of python.exe and also, the PID of explorer.exe
It seems that this is suspicious.

According to **cmdline** information and also **netscan** information we can find that:

```
**********************************************************************
python.exe pid:   1208
Command line : "C:\Python27\python.exe" "C:\Users\Win7\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\agent.py"
**********************************************************************
```

But

When we look for python.exe in **netscan** we find a lot of information.



0×3dee4b30	TCPv4	0.0.0.0:8000	0.0.0.0:0	LISTENING	1208	python.exe
0×3e101010	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	1948	svchost.exe
0×3e101010	TCPv6	:::49156	:::0	LISTENING	1948	svchost.exe
0×3e1657e0	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	488	services.exe
0×3e17f8a0	TCPv4	0.0.0.0:445	0.0.0.0:0	LISTENING	4	System
0×3e17f8a0	TCPv6	:::445	:::0	LISTENING	4	System
0×3e189b00	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	488	services.exe
0×3e189b00	TCPv6	:::49155	:::0	LISTENING	488	services.exe
0×3e1d9320	TCPv4	0.0.0.0:49157	0.0.0.0:0	LISTENING	496	lsass.exe
0×3e1d9320	TCPv6	:::49157	:::0	LISTENING	496	lsass.exe
0×3e1f46e0	TCPv4	192.168.50.11:139	0.0.0.0:0	LISTENING	4	System
0×3e2df560	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	904	svchost.exe
0×3e2eeef0	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	904	svchost.exe
0×3e2eeef0	TCPv6	:::49154	:::0	LISTENING	904	svchost.exe
0×3e33a360	TCPv4	0.0.0.0:5357	0.0.0.0:0	LISTENING	4	System
0×3e33a360	TCPv6	:::5357	:::0	LISTENING	4	System
0×3e3e02b0	TCPv4	0.0.0.0:49157	0.0.0.0:0	LISTENING	496	lsass.exe
0×3e40dc90	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	736	svchost.exe
0×3e40dc90	TCPv6	:::135	:::0	LISTENING	736	svchost.exe
0×3e422b80	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	392	wininit.exe
0×3e424220	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	392	wininit.exe
0×3e424220	TCPv6	:::49152	:::0	LISTENING	392	wininit.exe
0×3e5cd630	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	824	svchost.exe
0×3e5cd630	TCPv6	:::49153	:::0	LISTENING	824	svchost.exe
0×3e5d1ef0	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	824	svchost.exe
0×3e7fb2f0	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	736	svchost.exe
0×3de42910	TCPv4	192.168.50.11:8000	192.168.50.1:58380	CLOSED	1208	python.exe
0×3e032cf0	TCPv6	-:0	383b:b502:80fa:ffff:383b:b502:80fa:ffff:0	CLOSED	1	?&?????
0×3e121010	TCPv4	192.168.50.11:49513	192.168.50.1:2042	ESTABLISHED	2176	python.exe
0×3e152010	TCPv4	192.168.50.11:49185	192.168.50.1:2042	ESTABLISHED	2176	python.exe
0×3e2007d0	TCPv4	192.168.50.11:49611	192.168.50.1:2042	CLOSED	2176	python.exe
0×3e201010	TCPv4	192.168.50.11:49186	192.168.50.1:2042	ESTABLISHED	2176	python.exe
0×3e34acf0	TCPv4	192.168.50.11:49615	192.168.50.1:2042	FIN_WAIT1	2176	python.exe
0×3e38f9a0	TCPv4	192.168.50.11:49603	192.168.50.1:2042	CLOSED	2176	python.exe

Note: Like TCP (Transmission Control **Protocol**), UDP is used with IP (the Internet **Protocol**) but unlike TCP on Port 8000, UDP Port 8000 is connectionless and does not guarantee reliable communication; it's up to the application that received the message on Port 8000 to process any errors and verify correct delivery.

After **python.exe** is closed on port 8000 on TCP, another **python.exe** with different PID that is 2176 is coming to Established. Two processes with the same name and different PID and also different treatment in **netscan** show that this process is malicious.

Moreover, **FIN_WAIT_2** in **netscan** seems to occur when the server has an active connection with a client and wants to shut down the TCP connection. The server sends the client a packet with a "FIN" bit set. At this point, the server is in FIN_WAIT_1 state. The client gets the FIN packet and goes into CLOSE_WAIT state, and sends an acknowledgment packet back to the server. When the server gets that packet, it goes into FIN_WAIT_2 state. From the server's perspective, the connection is now closed, and the server can't send any more data. However, under the TCP protocol, the client needs to shut down also by sending a FIN packet, which the server TCP implementation should ACK. The server should close after a period of time defined by the Maximum Segment Lifetime.

```
... 0xfffffa80029eab30:dwm.exe                1588    872      3     70 2018-04-06 23:12:50 UTC+0000
.. 0xfffffa80025ef060:svchost.exe              736    488      9    264 2018-04-06 23:12:44 UTC+0000
.. 0xfffffa80025ae600:svchost.exe              612    488     10    345 2018-04-06 23:12:43 UTC+0000
... 0xfffffa8000dbd250:dllhost.exe            1932    612      7    205 2018-04-13 01:37:46 UTC+0000
.. 0xfffffa8002aa4b30:taskhost.exe            1596    488      7    141 2018-04-06 23:12:50 UTC+0000
.. 0xfffffa8002daab30:wmpnetwk.exe            2540    488     10    214 2018-04-06 23:13:22 UTC+0000
. 0xfffffa800255ab30:lsass.exe                 496    392      7    553 2018-04-06 23:12:43 UTC+0000
. 0xfffffa8002541b30:lsm.exe                   504    392     10    144 2018-04-06 23:12:43 UTC+0000
 0xfffffa80024e2800:csrss.exe                  360    352      9    402 2018-04-06 23:12:43 UTC+0000
 0xfffffa8002ab6b30:explorer.exe              1652   1580     23    817 2018-04-06 23:12:51 UTC+0000
. 0xfffffa8002afeb30:VBoxTray.exe             1376   1652     10    103 2018-04-06 23:12:56 UTC+0000
. 0xfffffa8002618060:python.exe               1208   1652      1     92 2018-04-06 23:12:59 UTC+0000
.. 0xfffffa8002a83950:python.exe              2176   1208     16    233 2018-04-13 01:28:34 UTC+0000
. 0xfffffa8002e82520:SndVol.exe               2568   1652      0 ------ 2018-04-06 23:13:23 UTC+0000
 0xfffffa8000cb8040:System                       4      0     84    528 2018-04-06 23:12:36 UTC+0000
. 0xfffffa8001d185f0:smss.exe                  276      4      2     29 2018-04-06 23:12:36 UTC+0000
 0xfffffa8002cd3b30:acrotray.exe              2144   1484      2     60 2018-04-06 23:13:08 UTC+0000
```

Another information that we can find from the above screenshots are:

The process **acrotray.exe** with PID 2144 and parent ID 1484 is associated with Adobe Acrobat. If it has another word after the name acrotray.exe it seems that suspicious.
According to **cmdline** logs, this process location is OK.

```
acrotray.exe pid:   2144
Command line : "C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\acrotray.exe"
```

The process with the PID 1932 is **dllhost.exe** under parent ID 612 needs more investigation. This PID 1932 started 7 days after its parent starting time, svchost.exe.
According to **cmdline** logs, we can find a little abnormal thing in the description of this file.

```
dllhost.exe pid:   1932
Command line : C:\Windows\SysWOW64\DllHost.exe /Processid:{76D0CB12-7604-4048-B83C-1005C7DDC503}
```

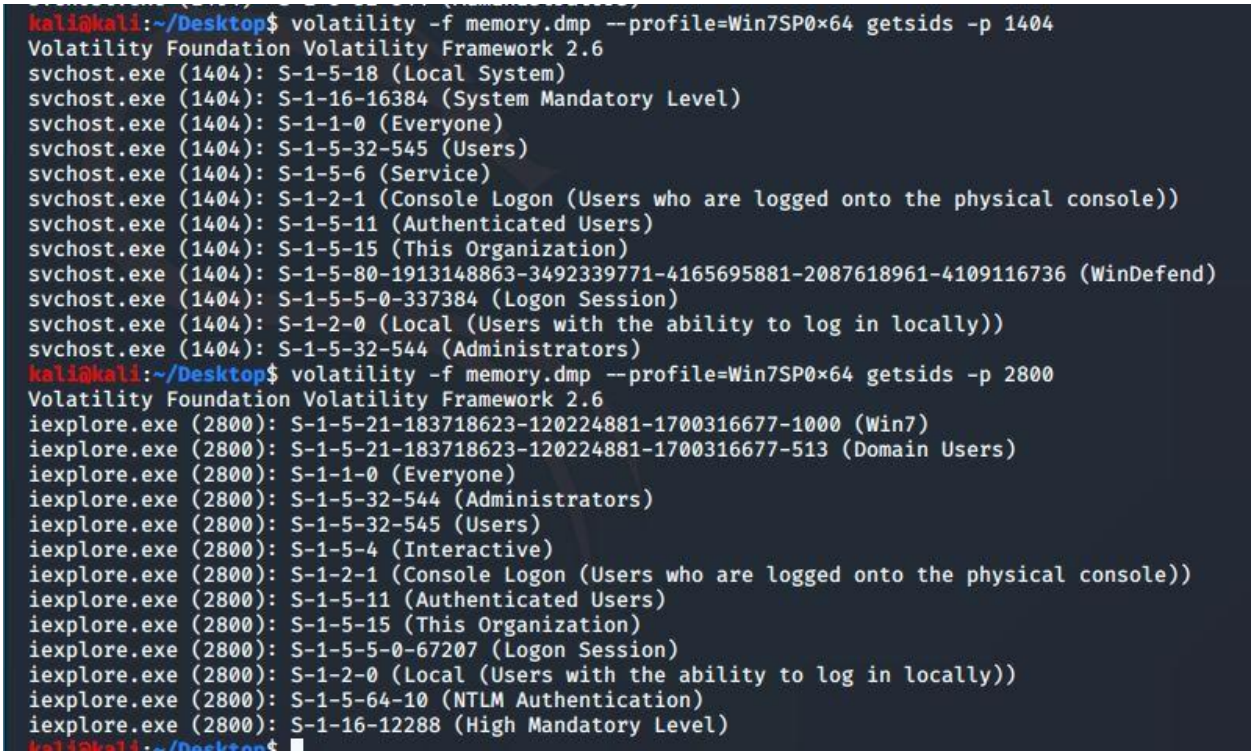
The process with the PID 352 is **winit.exe** and PID 360 **cress.exe** have same PPID 352 with no more information about this ID, we know that for some process like **Winint .exe**, **cress.exe** and **explorer exe** which are created by an instance of **smss.exe** and sometimes analysis tools not show their parent ID.

```
.... 0xfffffa80011c9060:vssadmin.exe           400   1728      0 ------ 2018-04-13 01:37:46 UTC+0000
.... 0xfffffa800124e920:iexplore.exe          2800   1728     13    547 2018-04-13 01:37:41 UTC+0000
..... 0xfffffa8001153240:iexplore.exe         2120   2800      6    351 2018-04-13 01:37:47 UTC+0000
 0xfffffa8002519060:winlogon.exe               444    384      3    108 2018-04-06 23:12:43 UTC+0000
 0xfffffa8001c9a4e0:csrss.exe                  404    384      8    259 2018-04-06 23:12:43 UTC+0000
. 0xfffffa800288a5e0:conhost.exe              1916    404      2     53 2018-04-06 23:12:59 UTC+0000
```

The process with the PID 360 is **csrss.exe** with PPID 352 and then we PID 404 **csrss.exe** same name but with different parent ID 384, and for both these PPID there is no more information.

The process with the PID 276 with parent ID 4 is **smss.exe** started exactly at the same time as its parent 4,**system.exe**. Maybe we can do more consideration about this process too.

We tried command **getsids** for some of our suspicious processes such as PID 1404,2120,280,512. **Getsids** give us ideas about malicious escalated privileges.



```
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 getsids -p 2120
Volatility Foundation Volatility Framework 2.6
iexplore.exe (2120): S-1-5-21-183718623-120224881-1700316677-1000 (Win7)
iexplore.exe (2120): S-1-5-21-183718623-120224881-1700316677-513 (Domain Users)
iexplore.exe (2120): S-1-1-0 (Everyone)
iexplore.exe (2120): S-1-5-32-544 (Administrators)
iexplore.exe (2120): S-1-5-32-545 (Users)
iexplore.exe (2120): S-1-5-4 (Interactive)
iexplore.exe (2120): S-1-2-1 (Console Logon (Users who are logged onto the physical console))
iexplore.exe (2120): S-1-5-11 (Authenticated Users)
iexplore.exe (2120): S-1-5-15 (This Organization)
iexplore.exe (2120): S-1-5-5-0-67207 (Logon Session)
iexplore.exe (2120): S-1-2-0 (Local (Users with the ability to log in locally))
iexplore.exe (2120): S-1-5-64-10 (NTLM Authentication)
iexplore.exe (2120): S-1-16-12288 (High Mandatory Level)
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 getsids -p 512
Volatility Foundation Volatility Framework 2.6
7004af389d633b (512): S-1-5-21-183718623-120224881-1700316677-1000 (Win7)
7004af389d633b (512): S-1-5-21-183718623-120224881-1700316677-513 (Domain Users)
7004af389d633b (512): S-1-1-0 (Everyone)
7004af389d633b (512): S-1-5-32-544 (Administrators)
7004af389d633b (512): S-1-5-32-545 (Users)
7004af389d633b (512): S-1-5-4 (Interactive)
7004af389d633b (512): S-1-2-1 (Console Logon (Users who are logged onto the physical console))
7004af389d633b (512): S-1-5-11 (Authenticated Users)
7004af389d633b (512): S-1-5-15 (This Organization)
7004af389d633b (512): S-1-5-5-0-67207 (Logon Session)
7004af389d633b (512): S-1-2-0 (Local (Users with the ability to log in locally))
7004af389d633b (512): S-1-5-64-10 (NTLM Authentication)
7004af389d633b (512): S-1-16-12288 (High Mandatory Level)
```

.Also we examine the command **PRIVIS** --silet to see processes which were not enabled as default but gave them privilege to be enabled.

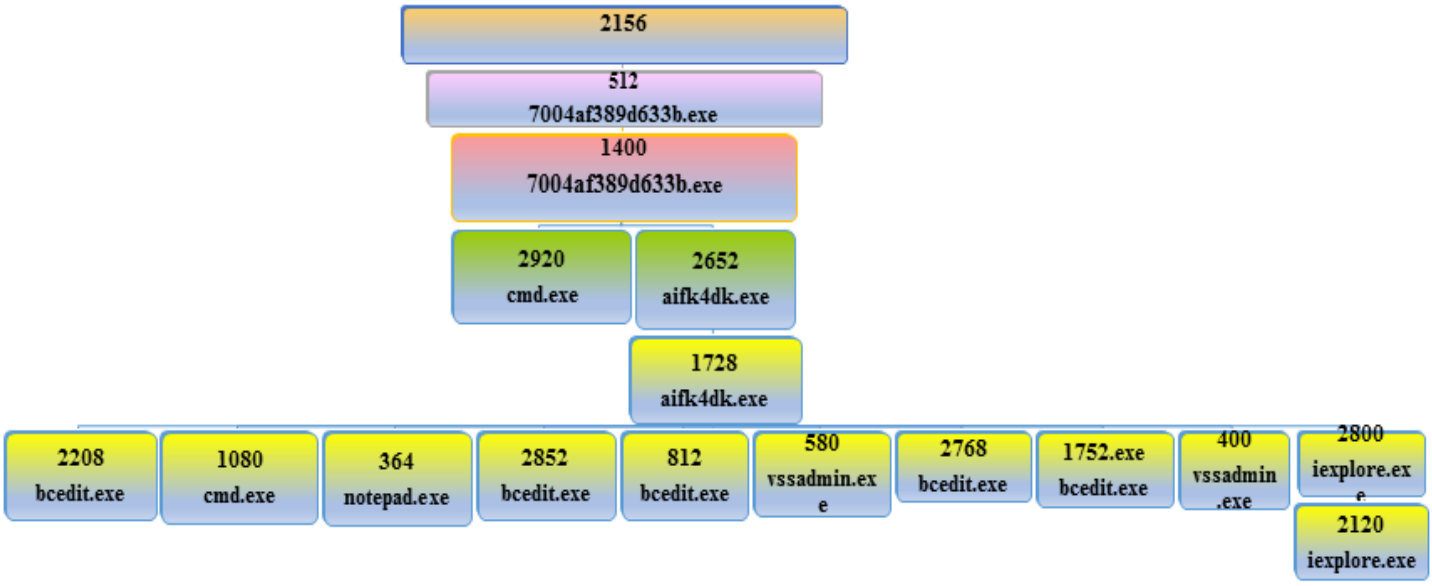
```
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 privs --silent
Volatility Foundation Volatility Framework 2.6
Pid      Process          Value  Privilege                       Attributes             Description
-------- ---------------- ------ ------------------------------- ---------------------- -----------
     496 lsass.exe             2 SeCreateTokenPrivilege          Present,Enabled        Create a token object
     672 VBoxService.ex       12 SeSystemtimePrivilege           Present,Enabled        Change the system time
     332 svchost.exe          12 SeSystemtimePrivilege           Present,Enabled        Change the system time
     900 svchost.exe          21 SeAuditPrivilege                Present,Enabled        Generate security audits
    1152 svchost.exe          21 SeAuditPrivilege                Present,Enabled        Generate security audits
    1948 svchost.exe          21 SeAuditPrivilege                Present,Enabled        Generate security audits
    2176 python.exe           10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
    2176 python.exe           20 SeDebugPrivilege                Present,Enabled        Debug programs
     512 7004af389d633b       10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
     512 7004af389d633b       20 SeDebugPrivilege                Present,Enabled        Debug programs
    1404 svchost.exe           3 SeAssignPrimaryTokenPrivilege   Present,Enabled        Replace a process-level token
    1404 svchost.exe           5 SeIncreaseQuotaPrivilege        Present,Enabled        Increase quotas
    1404 svchost.exe           8 SeSecurityPrivilege             Present,Enabled        Manage auditing and security log
    1404 svchost.exe          17 SeBackupPrivilege               Present,Enabled        Backup files and directories
    1404 svchost.exe          18 SeRestorePrivilege              Present,Enabled        Restore files and directories
    1404 svchost.exe          19 SeShutdownPrivilege             Present,Enabled        Shut down the system
    1400 7004af389d633b       10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
    1400 7004af389d633b       20 SeDebugPrivilege                Present,Enabled        Debug programs
    2652 aifkydk.exe          10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
    2652 aifkydk.exe          20 SeDebugPrivilege                Present,Enabled        Debug programs
    2920 cmd.exe              10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
    2920 cmd.exe              20 SeDebugPrivilege                Present,Enabled        Debug programs
    1728 aifkydk.exe          10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
    1728 aifkydk.exe          20 SeDebugPrivilege                Present,Enabled        Debug programs
     812 bcdedit.exe          10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
     812 bcdedit.exe          20 SeDebugPrivilege                Present,Enabled        Debug programs
     580 vssadmin.exe         10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
     580 vssadmin.exe         17 SeBackupPrivilege               Present,Enabled        Backup files and directories
     580 vssadmin.exe         20 SeDebugPrivilege                Present,Enabled        Debug programs
    1752 bcdedit.exe          10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
    1752 bcdedit.exe          20 SeDebugPrivilege                Present,Enabled        Debug programs
    2208 bcdedit.exe          10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
    2208 bcdedit.exe          20 SeDebugPrivilege                Present,Enabled        Debug programs
    2768 bcdedit.exe          10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
    2768 bcdedit.exe          20 SeDebugPrivilege                Present,Enabled        Debug programs
    2852 bcdedit.exe          10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
    2852 bcdedit.exe          20 SeDebugPrivilege                Present,Enabled        Debug programs
     364 notepad.exe          10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
     364 notepad.exe          20 SeDebugPrivilege                Present,Enabled        Debug programs
    2800 iexplore.exe         10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
    2800 iexplore.exe         20 SeDebugPrivilege                Present,Enabled        Debug programs
     400 vssadmin.exe         10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
     400 vssadmin.exe         17 SeBackupPrivilege               Present,Enabled        Backup files and directories
     400 vssadmin.exe         20 SeDebugPrivilege                Present,Enabled        Debug programs
    2120 iexplore.exe         10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
    2120 iexplore.exe         20 SeDebugPrivilege                Present,Enabled        Debug programs
    1080 cmd.exe              10 SeLoadDriverPrivilege           Present,Enabled        Load and unload device drivers
    1080 cmd.exe              20 SeDebugPrivilege                Present,Enabled        Debug programs
    1564 VSSVC.exe            17 SeBackupPrivilege               Present,Enabled        Backup files and directories
    1564 VSSVC.exe            18 SeRestorePrivilege              Present,Enabled        Restore files and directories
```

2. Determine and explain the relationships (i.e., parent-child) between the suspicious processes identified above. Identify which process is most likely responsible for the initial exploit.

For this part we have two analyses. One of them is based on pstree, pslist, and cmdline and the other one focuses on **netscan** log.

Based on malicious processes and suspected processes which have been found above. And by considering **pslist** and **pstree** we see hierarchical of these processes under **winit.exe** and the system looks fine. But as we see we have PID 512, 7004af389d633b, which is an unknown process and it is a child of process ID 2156, which is unknown without any more information about its initial baseline. following hierarchical diagram shows that PID 2120, iexplore.exe is child of PID 2800, iexplore.exe. and then all PIDs 2800,400,1752,2768,580, 812,2852,364,1080,2208 are child of parent process ID 1728, **aifkydk.exe** which is unknown process. Then PID 1728 is child of process ID 2652, **aifkydk**. Both these child and parent processes have the same name with different starting time about 43seconds. Then process 2652 with process 2920 both are child of parent process 1400, 7004af389d633b. process ID 1400 is a child of process 512, 7004af389d633b which have the same name and unknown name. at the end PID 512 is a child of parent process 2152 which is completely unknown without any more information about its initial baseline. So looks these processes 2156 and its child PID 512 are most likely responsible for initial and their child's are suspected.

And if we look at the starting time of other suspected processes which we notified in question 1, like PID 1404 SVChost.exe and PID 2176 started a few seconds after initial PID 512.



Hierarchical diagram

Also, according to the incident overview, and the whole information above in the first question, First of all, **svchost.exe is always** using **port** 53. According to information from **netscan**, **pstree** and **cmdine**.
Specifically, in **netscan** the svchost.exe tries to login to the machine several times with different ports. But it cannot. Surprisingly, svchost.exe with PID 1296 is malicious.
In **pstree**, **pslist, svcscan, cmdline, malfind** we cannot find any information about 1296.

0×3e0368e0	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	1948	svchost.exe
0×3e101010	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	1948	svchost.exe
0×3e101010	TCPv6	:::49156	:::0	LISTENING	1948	svchost.exe
0×3e1657e0	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	488	services.exe
0×3e17f8a0	TCPv4	0.0.0.0:445	0.0.0.0:0	LISTENING	4	System
0×3e17f8a0	TCPv6	:::445	:::0	LISTENING	4	System
0×3e189b00	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	488	services.exe
0×3e189b00	TCPv6	:::49155	:::0	LISTENING	488	services.exe
0×3e1d9320	TCPv4	0.0.0.0:49157	0.0.0.0:0	LISTENING	496	lsass.exe
0×3e1d9320	TCPv6	:::49157	:::0	LISTENING	496	lsass.exe
0×3e1f46e0	TCPv4	192.168.50.11:139	0.0.0.0:0	LISTENING	4	System
0×3e2df560	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	904	svchost.exe
0×3e2eeef0	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	904	svchost.exe
0×3e2eeef0	TCPv6	:::49154	:::0	LISTENING	904	svchost.exe
0×3e33a360	TCPv4	0.0.0.0:5357	0.0.0.0:0	LISTENING	4	System
0×3e33a360	TCPv6	:::5357	:::0	LISTENING	4	System
0×3e3e02b0	TCPv4	0.0.0.0:49157	0.0.0.0:0	LISTENING	496	lsass.exe
0×3e40dc90	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	736	svchost.exe
0×3e40dc90	TCPv6	:::135	:::0	LISTENING	736	svchost.exe
0×3e422b80	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	392	wininit.exe
0×3e424220	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	392	wininit.exe
0×3e424220	TCPv6	:::49152	:::0	LISTENING	392	wininit.exe
0×3e5cd630	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	824	svchost.exe
0×3e5cd630	TCPv6	:::49153	:::0	LISTENING	824	svchost.exe
0×3e5d1ef0	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	824	svchost.exe
0×3e7fb2f0	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	736	svchost.exe
0×3de42910	TCPv4	192.168.50.11:8000	192.168.50.1:58380	CLOSED	1208	python.exe

Svchost.exe in this scenario is listening to the port and then closes when python.exe will come.

Volatility Foundation Volatility Framework 2.6

Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner	Created
0×3dc4e230	UDPv6	fe80::c0c9:aa19:31b7:43c6:1900	*:*		1296	svchost.exe	2018-04-13 01:28:34 UTC+0000
0×3dc9b8e0	TCPv4	192.168.50.11:49598	192.168.50.1:2042	CLOSED	2176	python.exe	
0×3de08da0	UDPv4	0.0.0.0:0	*:*		332	svchost.exe	2018-04-13 01:28:31 UTC+0000
0×3de1c9c0	UDPv6	fe80::c0c9:aa19:31b7:43c6:64671	*:*		1296	svchost.exe	2018-04-13 01:28:34 UTC+0000
0×3de22730	UDPv6	::1:1900	*:*		1296	svchost.exe	2018-04-13 01:28:34 UTC+0000

Svshost.exe with PID of 1296 is **local service (no impersonation).** "To exploit these vulnerabilities, the attacker would first need to identify systems running vulnerable UPnP services. UPnP makes this easy by providing a discovery service over **UDP port 1900. In Netscan svchost.exe with PID 1296 is on port UDP 1900.**

Python.exe's port number is 49598 on TCP . Whenever the system changes the process ID of python.exe to 2176. It is obvious that attackers use python in several ports. It is worth noting that python 1276 has a Parent PID 1208 (python.exe). And again the parent ID of this python is 1652. 1652 is PPID of two different processes and also unknown. So, python.exe with process ID 2176 can be one of the initial.

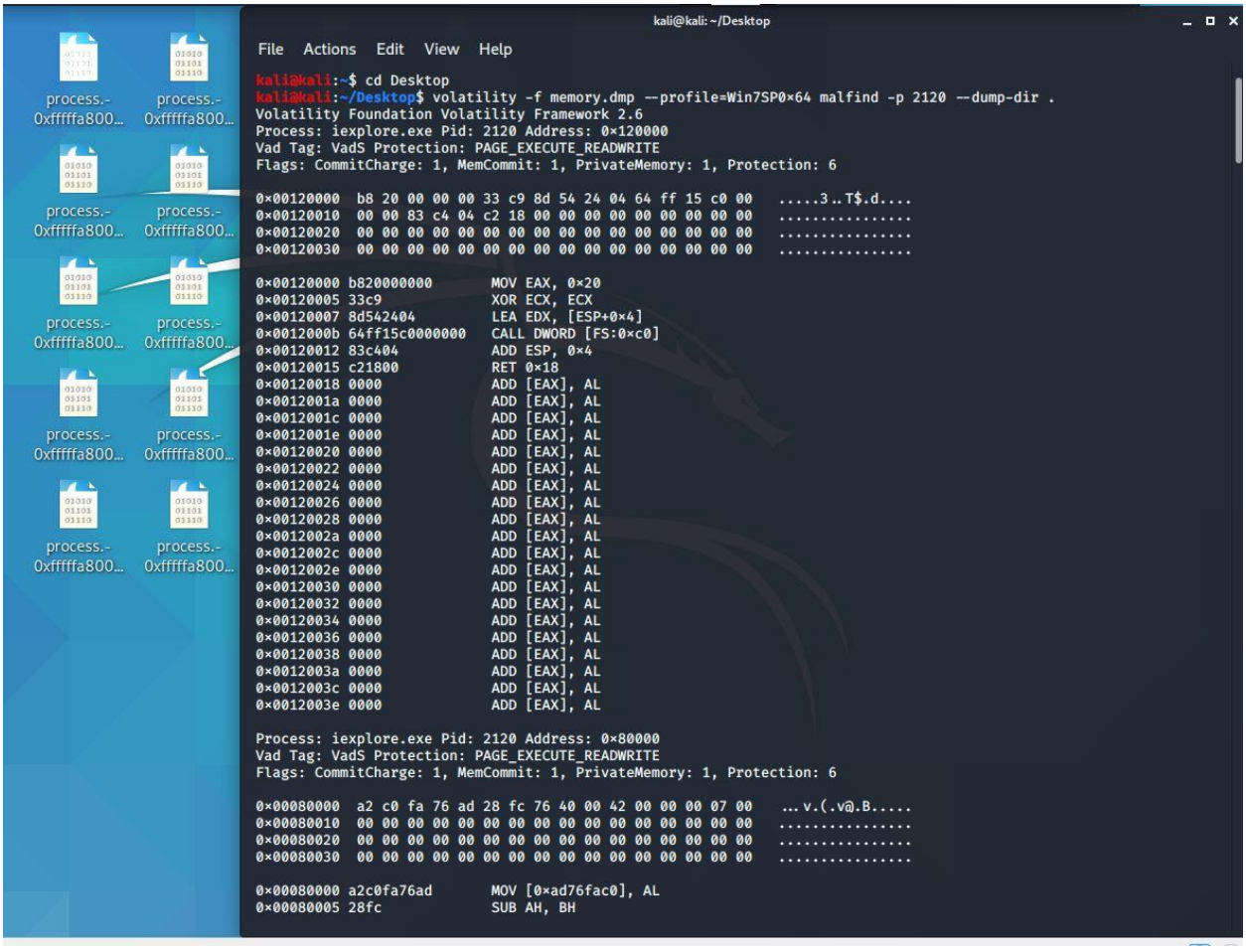
University of Victoria

3.From the above list of suspicious processes, identify at least one process with hidden or injected code/DLLs, and identify corresponding hidden DLLs

We select PID 1404 , PID 2120 From suspicious processes which discussed above. By using command malfind as follow:

For PID 2120:

volatility -f memory.dmp --profile=Win7SP0x64 malfind -p 2120



```
0x00080000 a2c0fa76ad       MOV [0xad76fac0], AL
0x00080005 28fc             SUB AH, BH
0x00080007 7640             JBE 0x80049
0x00080009 004200           ADD [EDX+0x0], AL
0x0008000c 0000             ADD [EAX], AL
0x0008000e 07               POP ES
0x0008000f 0000             ADD [EAX], AL
0x00080011 0000             ADD [EAX], AL
0x00080013 0000             ADD [EAX], AL
0x00080015 0000             ADD [EAX], AL
0x00080017 0000             ADD [EAX], AL
0x00080019 0000             ADD [EAX], AL
0x0008001b 0000             ADD [EAX], AL
0x0008001d 0000             ADD [EAX], AL
0x0008001f 0000             ADD [EAX], AL
0x00080021 0000             ADD [EAX], AL
0x00080023 0000             ADD [EAX], AL
0x00080025 0000             ADD [EAX], AL
0x00080027 0000             ADD [EAX], AL
0x00080029 0000             ADD [EAX], AL
0x0008002b 0000             ADD [EAX], AL
0x0008002d 0000             ADD [EAX], AL
0x0008002f 0000             ADD [EAX], AL
0x00080031 0000             ADD [EAX], AL
0x00080033 0000             ADD [EAX], AL
0x00080035 0000             ADD [EAX], AL
0x00080037 0000             ADD [EAX], AL
0x00080039 0000             ADD [EAX], AL
0x0008003b 0000             ADD [EAX], AL
0x0008003d 0000             ADD [EAX], AL
0x0008003f 00               DB 0x0

Process: iexplore.exe Pid: 2120 Address: 0x70000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00070000  43 00 3a 00 5c 00 74 00 6d 00 70 00 69 00 66 00   C.:.\.t.m.p.i.f.
0x00070010  73 00 62 00 75 00 61 00 5c 00 62 00 69 00 6e 00   s.b.u.a.\.b.i.n.
0x00070020  5c 00 6d 00 6f 00 6e 00 69 00 74 00 6f 00 72 00   \.m.o.n.i.t.o.r.
0x00070030  2d 00 78 00 38 00 36 00 2e 00 64 00 6c 00 6c 00   -.x.8.6.....d.l.l.

0x00070000 43               INC EBX
0x00070001 003a             ADD [EDX], BH
0x00070003 005c0074         ADD [EAX+EAX+0x74], BL
0x00070007 006d00           ADD [EBP+0x0], CH
0x0007000a 7000             JO 0x7000c
0x0007000c 690066007300     IMUL EAX, [EAX], 0x730066
0x00070012 6200             BOUND EAX, [EAX]
0x00070014 7500             JNZ 0x70016
0x00070016 61               POPA
```

Fro PID 2120 ten memory segments were detected which start at 0x00120000,0x00080000, 0x00070000,0x00090000,0x001e0000,0x00210000 ,0x00230000,0x02510000, 0x029b0000 ,0x5fff0000. All of them are executable. It has Vad Tag (memory protection) as PAGE_EXECUTE_READAWRITE, and based on disassembly in the data in the address looks there is some injection and suspicious

here. Also by using dump-dir we could dump the binary that was injected into this process. As above image.

Also for the detection of injected and hidden dlls we compare the PEB(process environment block) and the VAD(Virtual address descriptor) structure by using the command ldrmodules as follow:

volatility -f memory.dmp --profile=Win7SP0x64 ldrmodules -p 2120

```
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 ldrmodules -p 2120
Volatility Foundation Volatility Framework 2.6
Pid      Process            Base               InLoad InInit InMem MappedPath
-------- ------------------ ------------------ ------ ------ ----- ----------
    2120 iexplore.exe       0x0000000000d70000 True   False  True  \Program Files (x86)\Internet Explorer\iexplo
re.exe
    2120 iexplore.exe       0x0000000000020000 False  False  False \Program Files (x86)\Internet Explorer\en-US\
iexplore.exe.mui
    2120 iexplore.exe       0x00000000745c0000 True   True   True  \Windows\SysWOW64\ntmarta.dll
    2120 iexplore.exe       0x00000000024f0000 False  False  False \Windows\SysWOW64\en-US\setupapi.dll.mui
    2120 iexplore.exe       0x0000000074570000 True   True   True  \Windows\SysWOW64\dnsapi.dll
    2120 iexplore.exe       0x000000006bdb0000 True   True   True  \PROGRA~2\MICROS~1\Office15\GROOVEEX.DLL
    2120 iexplore.exe       0x0000000075fe0000 True   True   True  \Windows\SysWOW64\clbcatq.dll
    2120 iexplore.exe       0x00000000745f0000 True   True   True  \Windows\SysWOW64\rsaenh.dll
    2120 iexplore.exe       0x0000000073780000 True   True   True  \Program Files (x86)\Internet Explorer\ieprox
y.dll
    2120 iexplore.exe       0x000000006c670000 True   True   True  \Program Files (x86)\Internet Explorer\IEShim
s.dll
    2120 iexplore.exe       0x0000000073eb0000 True   True   True  \Program Files (x86)\Microsoft Office\Office1
5\OCHelper.dll
    2120 iexplore.exe       0x0000000074ad0000 True   True   True  \Windows\SysWOW64\cryptbase.dll
    2120 iexplore.exe       0x000000006b0e0000 True   True   True  \Windows\SysWOW64\mshtml.dll
    2120 iexplore.exe       0x0000000076670000 True   True   True  \Windows\SysWOW64\ws2_32.dll
    2120 iexplore.exe       0x0000000073f30000 True   True   True  \Windows\SysWOW64\uxtheme.dll
    2120 iexplore.exe       0x0000000074540000 True   True   True  \Windows\SysWOW64\winnsi.dll
    2120 iexplore.exe       0x0000000075390000 True   True   True  \Windows\SysWOW64\shell32.dll
    2120 iexplore.exe       0x00000000769a0000 True   True   True  \Windows\SysWOW64\kernel32.dll
    2120 iexplore.exe       0x00000000761e0000 True   True   True  \Windows\SysWOW64\iertutil.dll
    2120 iexplore.exe       0x0000000075290000 True   True   True  \Windows\SysWOW64\user32.dll
    2120 iexplore.exe       0x000000006c640000 True   True   True  \Windows\SysWOW64\msls31.dll
    2120 iexplore.exe       0x0000000074c50000 True   True   True  \Windows\SysWOW64\crypt32.dll
    2120 iexplore.exe       0x0000000002870000 False  False  False \Windows\SysWOW64\stdole2.tlb
    2120 iexplore.exe       0x0000000073e80000 True   True   True  \Windows\SysWOW64\dwmapi.dll
    2120 iexplore.exe       0x0000000076aa0000 True   True   True  \Windows\SysWOW64\comdlg32.dll
    2120 iexplore.exe       0x000000006c6c0000 True   True   True  \Windows\SysWOW64\mlang.dll
    2120 iexplore.exe       0x0000000073f00000 True   True   True  \Windows\SysWOW64\msimtf.dll
    2120 iexplore.exe       0x0000000076b20000 True   True   True  \Windows\SysWOW64\KernelBase.dll
    2120 iexplore.exe       0x00000000743f0000 True   True   True  \Windows\SysWOW64\version.dll
    2120 iexplore.exe       0x0000000003360000 False  False  False \Windows\SysWOW64\en-US\propsys.dll.mui
    2120 iexplore.exe       0x00000000763e0000 True   True   True  \Windows\SysWOW64\psapi.dll
    2120 iexplore.exe       0x0000000076120000 True   True   True  \Windows\SysWOW64\oleaut32.dll
    2120 iexplore.exe       0x0000000074ed0000 True   True   True  \Windows\SysWOW64\advapi32.dll
    2120 iexplore.exe       0x00000000734e0000 True   True   True  \Windows\System32\wow64cpu.dll
    2120 iexplore.exe       0x0000000076100000 True   True   True  \Windows\SysWOW64\sechost.dll
    2120 iexplore.exe       0x0000000076940000 True   True   True  \Windows\SysWOW64\shlwapi.dll
    2120 iexplore.exe       0x000000006bb70000 True   True   True  \Windows\SysWOW64\msi.dll
    2120 iexplore.exe       0x0000000074180000 True   True   True  \Program Files (x86)\Common Files\Adobe\Acrob
```

University of Victoria

```
    2120 iexplore.exe         0x000000000734e0000 True   True   True  \Windows\System32\wow64cpu.dll
    2120 iexplore.exe         0x0000000076100000 True   True   True  \Windows\SysWOW64\sechost.dll
    2120 iexplore.exe         0x0000000076940000 True   True   True  \Windows\SysWOW64\shlwapi.dll
    2120 iexplore.exe         0x000000006bb70000 True   True   True  \Windows\SysWOW64\msi.dll
    2120 iexplore.exe         0x0000000074180000 True   True   True  \Program Files (x86)\Common Files\Adobe\Acrob
at\ActiveX\AcroIEHelper.dll
    2120 iexplore.exe         0x0000000073550000 True   True   True  \Windows\System32\wow64.dll
    2120 iexplore.exe         0x000000073bf0000 True   True   True  \Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll
    2120 iexplore.exe         0x000000006c200000 True   True   True  \Windows\SysWOW64\ieapfltr.dll
    2120 iexplore.exe         0x0000000003630000 False  False  False \Windows\SysWOW64\en-US\shell32.dll.mui
    2120 iexplore.exe         0x0000000075050000 True   True   True  \Windows\SysWOW64\wininet.dll
    2120 iexplore.exe         0x0000000074660000 True   True   True  \Program Files (x86)\Common Files\Adobe\Acrob
at\ActiveX\AcroIEHelperShim.dll
    2120 iexplore.exe         0x0000000000280000 False  False  False \Windows\SysWOW64\oleaccrc.dll
    2120 iexplore.exe         0x000000000744b0000 True   True   True  \Windows\SysWOW64\oleacc.dll
    2120 iexplore.exe         0x0000000003520000 False  False  False \Windows\SysWOW64\en-US\mshtml.dll.mui
    2120 iexplore.exe         0x00000000766e0000 True   True   True  \Windows\SysWOW64\rpcrt4.dll
    2120 iexplore.exe         0x0000000003910000 False  False  False \Windows\SysWOW64\en-US\ieframe.dll.mui
    2120 iexplore.exe         0x0000000075150000 True   True   True  \Windows\SysWOW64\urlmon.dll
    2120 iexplore.exe         0x0000000074d70000 True   True   True  \Windows\SysWOW64\ole32.dll
    2120 iexplore.exe         0x000000006c5b0000 True   True   True  \Program Files (x86)\Common Files\Adobe\Acrob
at\ActiveX\AcroIEFavClient.dll
    2120 iexplore.exe         0x00000000767e0000 True   True   True  \Windows\SysWOW64\msctf.dll
    2120 iexplore.exe         0x0000000074b40000 True   True   True  \Windows\SysWOW64\nsi.dll
    2120 iexplore.exe         0x0000000074630000 True   True   True  \Windows\SysWOW64\cryptsp.dll
    2120 iexplore.exe         0x0000000073e70000 True   True   True  \Windows\SysWOW64\RpcRtRemote.dll
    2120 iexplore.exe         0x00000000766b0000 True   True   True  \Windows\SysWOW64\devobj.dll
    2120 iexplore.exe         0x0000000076f70000 True   True   True  \Windows\SysWOW64\ntdll.dll
    2120 iexplore.exe         0x0000000074650000 True   True   True  \Windows\SysWOW64\profapi.dll
    2120 iexplore.exe         0x0000000072a60000 True   True   True  \Windows\SysWOW64\ieframe.dll
    2120 iexplore.exe         0x0000000076070000 True   True   True  \Windows\SysWOW64\gdi32.dll
    2120 iexplore.exe         0x00000000768b0000 True   True   True  \Windows\SysWOW64\imm32.dll
    2120 iexplore.exe         0x00000000764d0000 True   True   True  \Windows\SysWOW64\setupapi.dll
    2120 iexplore.exe         0x0000000074ae0000 True   True   True  \Windows\SysWOW64\sspicli.dll
    2120 iexplore.exe         0x0000000072700000 True   True   True  \Windows\SysWOW64\sxs.dll
    2120 iexplore.exe         0x0000000076f40000 True   True   True  \Windows\SysWOW64\normaliz.dll
    2120 iexplore.exe         0x0000000074550000 True   True   True  \Windows\SysWOW64\IPHLPAPI.DLL
    2120 iexplore.exe         0x0000000074170000 True   True   True  \Program Files (x86)\Microsoft Office\Office1
5\1033\OcHelperResource.dll
    2120 iexplore.exe         0x0000000076d90000 True   True   True  \Windows\System32\ntdll.dll
    2120 iexplore.exe         0x0000000074fc0000 True   True   True  \Windows\SysWOW64\comctl32.dll
    2120 iexplore.exe         0x0000000072760000 True   True   True  \Windows\SysWOW64\msvcp100.dll
    2120 iexplore.exe         0x0000000076420000 True   True   True  \Windows\SysWOW64\msvcrt.dll
    2120 iexplore.exe         0x000000006c270000 True   True   True  \Windows\SysWOW64\msvcr100.dll
    2120 iexplore.exe         0x00000000726d0000 True   True   True  \Windows\SysWOW64\atl100.dll
    2120 iexplore.exe         0x00000000742f0000 True   True   True  \Windows\SysWOW64\apphelp.dll
    2120 iexplore.exe         0x0000000073f10000 True   True   True  \PROGRA~2\MICROS~1\Office15\MSOHEV.DLL
    2120 iexplore.exe         0x000000006c520000 True   True   True  \Windows\winsxs\x86_microsoft.vc90.crt_1fc8b3
b9a1e18e3b_9.0.30729.4926_none_508ed732bcbc0e5a\msvcp90.dll
```

```
b9a1e18e3b_9.0.30729.4926_none_508ed732bcbc0e5a\msvcp90.dll
    2120 iexplore.exe         0x000000006cb30000 True   True   True  \Windows\SysWOW64\propsys.dll
    2120 iexplore.exe         0x0000000074bb0000 True   True   True  \Windows\SysWOW64\usp10.dll
    2120 iexplore.exe         0x00000000767d0000 True   True   True  \Windows\SysWOW64\msasn1.dll
    2120 iexplore.exe         0x00000000763f0000 True   True   True  \Windows\SysWOW64\cfgmgr32.dll
    2120 iexplore.exe         0x0000000074010000 True   True   True  \Windows\SysWOW64\secur32.dll
    2120 iexplore.exe         0x0000000074f70000 True   True   True  \Windows\SysWOW64\Wldap32.dll
    2120 iexplore.exe         0x000000006c470000 True   True   True  \Windows\winsxs\x86_microsoft.vc90.crt_1fc8b3
b9a1e18e3b_9.0.30729.4926_none_508ed732bcbc0e5a\msvcr90.dll
    2120 iexplore.exe         0x000000006b6a0000 False  False  False \Program Files (x86)\Common Files\microsoft s
hared\OFFICE15\Cultures\OFFICE.ODF
    2120 iexplore.exe         0x00000000766d0000 True   True   True  \Windows\SysWOW64\lpk.dll
    2120 iexplore.exe         0x00000000734f0000 True   True   True  \Windows\System32\wow64win.dll
    2120 iexplore.exe         0x0000000002b00000 False  False  False \Windows\SysWOW64\en-US\urlmon.dll.mui
    2120 iexplore.exe         0x000000006c110000 True   True   True  \PROGRA~2\MICROS~1\Office15\URLREDIR.DLL
kali@kali:~/Desktop$
```

University of Victoria

For PID 1404

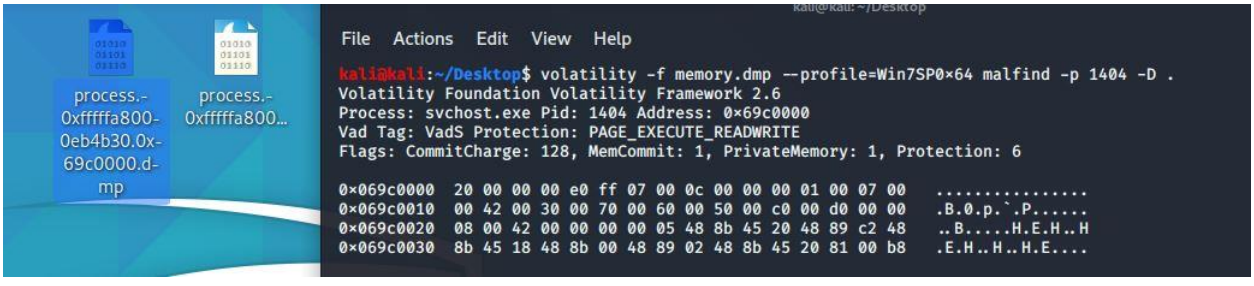
volatility -f memory.dmp –profile=Win7SP0x64 malfind -p1404

```
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 malfind -p 1404
Volatility Foundation Volatility Framework 2.6
Process: svchost.exe Pid: 1404 Address: 0x69c0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 128, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x069c0000  20 00 00 00 e0 ff 07 00 0c 00 00 00 01 00 07 00   ................
0x069c0010  00 42 00 30 00 70 00 60 00 50 00 c0 00 d0 00 00   .B.0.p.`.P......
0x069c0020  08 00 42 00 00 00 00 05 48 8b 45 20 48 89 c2 48   ..B.....H.E.H..H
0x069c0030  8b 45 18 48 8b 00 48 89 02 48 8b 45 20 81 00 b8   .E.H..H..H.E....

0x069c0000 2000            AND [EAX], AL
0x069c0002 0000            ADD [EAX], AL
0x069c0004 e0ff            LOOPNZ 0x69c0005
0x069c0006 07              POP ES
0x069c0007 000c00          ADD [EAX+EAX], CL
0x069c000a 0000            ADD [EAX], AL
0x069c000c 0100            ADD [EAX], EAX
0x069c000e 07              POP ES
0x069c000f 0000            ADD [EAX], AL
0x069c0011 42              INC EDX
0x069c0012 0030            ADD [EAX], DH
0x069c0014 007000          ADD [EAX+0x0], DH
0x069c0017 60              PUSHA
0x069c0018 005000          ADD [EAX+0x0], DL
0x069c001b c000d0          ROL BYTE [EAX], 0xd0
0x069c001e 0000            ADD [EAX], AL
0x069c0020 0800            OR [EAX], AL
0x069c0022 42              INC EDX
0x069c0023 0000            ADD [EAX], AL
0x069c0025 0000            ADD [EAX], AL
0x069c0027 05488b4520      ADD EAX, 0x20458b48
0x069c002c 48              DEC EAX
0x069c002d 89c2            MOV EDX, EAX
0x069c002f 48              DEC EAX
0x069c0030 8b4518          MOV EAX, [EBP+0x18]
0x069c0033 48              DEC EAX
0x069c0034 8b00            MOV EAX, [EAX]
0x069c0036 48              DEC EAX
0x069c0037 8902            MOV [EDX], EAX
0x069c0039 48              DEC EAX
0x069c003a 8b4520          MOV EAX, [EBP+0x20]
0x069c003d 81              DB 0x81
0x069c003e 00              DB 0x0
0x069c003f b8              DB 0xb8

Process: svchost.exe Pid: 1404 Address: 0x6a40000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 256, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

University of Victoria

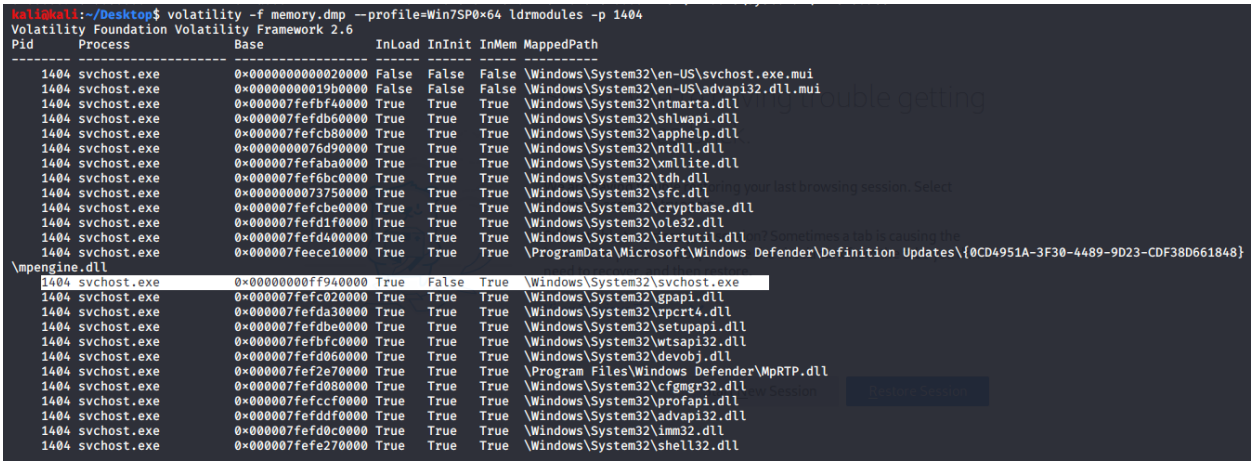
```
0x06a40000  20 00 00 00 e0 ff 0f 00 0c 00 00 00 01 00 07 00   ................
0x06a40010  00 42 00 30 00 70 00 60 00 50 00 c0 00 d0 00 00   .B.0.p.`.P......
0x06a40020  0c 00 4e 00 0c 00 01 05 48 8b 55 28 48 8b 8d c0   ..N.....H.U(H...
0x06a40030  00 00 00 48 8d 54 0a 10 48 89 d7 b9 08 00 1a 00   ...H.T..H.......

0x06a40000 2000            AND [EAX], AL
0x06a40002 0000            ADD [EAX], AL
0x06a40004 e0ff            LOOPNZ 0x6a40005
0x06a40006 0f000c00        STR WORD [EAX+EAX]
0x06a4000a 0000            ADD [EAX], AL
0x06a4000c 0100            ADD [EAX], EAX
0x06a4000e 07              POP ES
0x06a4000f 0000            ADD [EAX], AL
0x06a40011 42              INC EDX
0x06a40012 0030            ADD [EAX], DH
0x06a40014 007000          ADD [EAX+0x0], DH
0x06a40017 60              PUSHA
0x06a40018 005000          ADD [EAX+0x0], DL
0x06a4001b c000d0          ROL BYTE [EAX], 0xd0
0x06a4001e 0000            ADD [EAX], AL
0x06a40020 0c00            OR AL, 0x0
0x06a40022 4e              DEC ESI
0x06a40023 000c00          ADD [EAX+EAX], CL
0x06a40026 0105488b5528    ADD [0x28558b48], EAX
0x06a4002c 48              DEC EAX
0x06a4002d 8b8dc0000000    MOV ECX, [EBP+0xc0]
0x06a40033 48              DEC EAX
0x06a40034 8d540a10        LEA EDX, [EDX+ECX+0x10]
0x06a40038 48              DEC EAX
0x06a40039 89d7            MOV EDI, EDX
0x06a4003b b908001a00      MOV ECX, 0x1a0008
```

For PID 1404 two memory segments were detected, first memory segment starts at 0x069c000 and second at 0x06a4000. Both are executable. It has Vad Tag (memory protection) as PAGE_EXECUTE_READWRITE, and based on disassembly in the data in the address looks there is some injection and suspicious here. Also by using dump-dir as follow we could dump the binary that was injected into this process.



Also for the detection of injected and hidden dlls we compare the PEB(process environment block) and the VAD(Virtual address descriptor) structure by using the command **ldrmodules** as follow:

volatility -f memory.dmp --profile=Win7SP0x64 ldrmodules -p 1404



```
1404 svchost.exe          0x0000000001900000 False  False  False \Windows\System32\en-US\setupapi.dll.mui
1404 svchost.exe          0x000007fefd1d0000 True   True   True  \Windows\System32\sechost.dll
1404 svchost.exe          0x000007fefe0f0000 True   True   True  \Windows\System32\urlmon.dll
1404 svchost.exe          0x0000000076f50000 True   True   True  \Windows\System32\psapi.dll
1404 svchost.exe          0x000007fefc720000 True   True   True  \Windows\System32\ncrypt.dll
1404 svchost.exe          0x000007fefd770000 True   True   True  \Windows\System32\Wldap32.dll
1404 svchost.exe          0x000007fefcb20000 True   True   True  \Windows\System32\secur32.dll
1404 svchost.exe          0x000007fefd1c0000 True   True   True  \Windows\System32\lpk.dll
1404 svchost.exe          0x000007fefc5a0000 True   True   True  \Windows\System32\cryptsp.dll
1404 svchost.exe          0x000007fefcb50000 True   True   True  \Windows\System32\sspicli.dll
1404 svchost.exe          0x000007fefbfb0000 True   True   True  \Windows\System32\version.dll
1404 svchost.exe          0x000007fefc1c0000 True   True   True  \Windows\System32\bcryptprimitives.dll
1404 svchost.exe          0x000007fefc150000 True   True   True  \Windows\System32\credssp.dll
1404 svchost.exe          0x000007fefcde0000 True   True   True  \Windows\System32\KernelBase.dll
1404 svchost.exe          0x000007fefcda0000 True   True   True  \Windows\System32\wintrust.dll
1404 svchost.exe          0x0000000076b70000 True   True   True  \Windows\System32\user32.dll
1404 svchost.exe          0x000007fef1220000 True   True   True  \Program Files\Windows Defender\MpClient.dll
1404 svchost.exe          0x000007fefcd90000 True   True   True  \Windows\System32\msasn1.dll
1404 svchost.exe          0x000007fefe050000 True   True   True  \Windows\System32\clbcatq.dll
1404 svchost.exe          0x000007fefd660000 True   True   True  \Windows\System32\msctf.dll
1404 svchost.exe          0x0000000076c70000 True   True   True  \Windows\System32\kernel32.dll
1404 svchost.exe          0x000007fefc280000 True   True   True  \Windows\System32\rsaenh.dll
1404 svchost.exe          0x000007fefb490000 True   True   True  \Windows\System32\powrprof.dll
1404 svchost.exe          0x000007fefcef0000 True   True   True  \Windows\System32\crypt32.dll
1404 svchost.exe          0x000007fef10b0000 True   True   True  \Program Files\Windows Defender\MpSvc.dll
1404 svchost.exe          0x000007fefc040000 True   True   True  \Windows\System32\userenv.dll
1404 svchost.exe          0x000007fefccd0000 True   True   True  \Windows\System32\RpcRtRemote.dll
1404 svchost.exe          0x000007fef2ee0000 True   True   True  \Windows\System32\wscapi.dll
1404 svchost.exe          0x000007fef9cf0000 True   True   True  \Windows\System32\sfc_os.dll
1404 svchost.exe          0x000007fefddd0000 True   True   True  \Windows\System32\imagehlp.dll
1404 svchost.exe          0x000007feff000000 True   True   True  \Windows\System32\msvcrt.dll
1404 svchost.exe          0x000007fefd9c0000 True   True   True  \Windows\System32\gdi32.dll
```

And use **dlllist** command:

volatility -f memory.dmp --profile=Win7SP0x64 dlllist -p 1404

```
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 dlllist -p 1404
Volatility Foundation Volatility Framework 2.6
************************************************************************
svchost.exe pid:   1404
Command line : C:\Windows\System32\svchost.exe -k secsvcs

Base                             Size          LoadCount LoadTime                       Path
-------------------- ---------------- ---------- ------------------------------ ----
0x00000000ff940000           0xb000             0xffff 1970-01-01 00:00:00 UTC+0000   C:\Windows\System32\svchost.exe
0x0000000076d90000         0x1ab000             0xffff 1970-01-01 00:00:00 UTC+0000   C:\Windows\SYSTEM32\ntdll.dll
0x0000000076c70000         0x11f000             0xffff 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\kernel32.dll
0x000007fefcde0000          0x6b000             0xffff 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\KERNELBASE.dll
0x000007feff000000          0x9f000             0xffff 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\msvcrt.dll
0x000007fefd1d0000          0x1f000             0xffff 2018-04-13 01:28:45 UTC+0000   C:\Windows\SYSTEM32\sechost.dll
0x000007fefda30000         0x12e000             0xffff 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\RPCRT4.dll
0x000007fef10b0000          0xfb000                0x1 2018-04-13 01:28:45 UTC+0000   c:\program files\windows defender\mpsvc.dll
0x000007fefddf0000          0xdb000               0x14 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\ADVAPI32.dll
0x000007fefd1f0000         0x201000                0xe 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\ole32.dll
0x000007fefd9c0000          0x67000               0x39 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\GDI32.dll
0x0000000076b70000          0xfa000               0x3d 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\USER32.dll
0x000007fefd1c0000           0xe000                0xb 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\LPK.dll
0x000007fefd8f0000          0xca000                0xb 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\USP10.dll
0x000007fefbfc0000          0x11000                0x1 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\WTSAPI32.dll
0x0000000073750000           0x3000                0x1 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\sfc.dll
0x000007fef9cf0000          0x10000                0x1 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\sfc_os.DLL
0x000007fef1220000          0x90000                0x2 2018-04-13 01:28:45 UTC+0000   c:\program files\windows defender\MpClient.dll
0x000007fefded0000          0xd7000                0x8 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\OLEAUT32.dll
0x000007fefc040000          0x1e000                0x3 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\USERENV.dll
0x000007fefccf0000           0xf000                0x4 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\profapi.dll
0x000007fefcda0000          0x39000                0x2 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\WINTRUST.dll
0x000007fefcef0000         0x166000                0x6 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\CRYPT32.dll
0x000007fefcd90000           0xf000                0x7 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\MSASN1.dll
0x000007fefbfb0000           0xc000                0x5 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\VERSION.dll
0x000007fefe270000          0xd86000                0x2 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\SHELL32.dll
```

```
0x000007fefdb60000          0x71000                0x4 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\SHLWAPI.dll
0x000007fefd0c0000           0x2e000               0x2 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\IMM32.DLL
0x000007fefd660000         0x109000                0x1 2018-04-13 01:28:45 UTC+0000   C:\Windows\system32\MSCTF.dll
0x000007fefc020000          0x1b000                0x4 2018-04-13 01:28:46 UTC+0000   C:\Windows\System32\GPAPI.dll
0x000007fefc5a0000          0x17000                0x4 2018-04-13 01:28:46 UTC+0000   C:\Windows\System32\CRYPTSP.dll
0x000007fefc280000          0x47000                0x1 2018-04-13 01:28:46 UTC+0000   C:\Windows\system32\rsaenh.dll
0x000007fefcbe0000           0xf000                0x2 2018-04-13 01:28:46 UTC+0000   C:\Windows\System32\CRYPTBASE.dll
0x000007fefddd0000          0x17000                0x1 2018-04-13 01:28:49 UTC+0000   C:\Windows\system32\imagehlp.dll
0x000007fefc6f0000          0x22000                0xa 2018-04-13 01:28:49 UTC+0000   C:\Windows\System32\bcrypt.dll
0x000007fefc1c0000          0x4c000                0x1 2018-04-13 01:28:49 UTC+0000   C:\Windows\system32\bcryptprimitives.dll
0x000007fefc720000          0x4e000                0x1 2018-04-13 01:28:57 UTC+0000   C:\Windows\System32\ncrypt.dll
0x000007fef2e70000          0x35000                0x1 2018-04-13 01:28:57 UTC+0000   c:\program files\windows defender\mprtp.dll
0x0000000076f50000           0x7000                0x1 2018-04-13 01:28:57 UTC+0000   C:\Windows\system32\PSAPI.DLL
0x000007fef6bc0000          0xd3000                0x1 2018-04-13 01:28:57 UTC+0000   C:\Windows\System32\tdh.dll
0x000007fefcb20000           0xb000                0x1 2018-04-13 01:28:57 UTC+0000   C:\Windows\System32\secur32.dll
0x000007fefcb50000          0x25000                0x6 2018-04-13 01:28:57 UTC+0000   C:\Windows\System32\SSPICLI.DLL
0x000007fefc150000           0x9000                0x1 2018-04-13 01:28:57 UTC+0000   C:\Windows\System32\credssp.dll
0x000007fefccd0000          0x14000                0x1 2018-04-13 01:28:57 UTC+0000   C:\Windows\System32\RpcRtRemote.dll
0x000007fef2ee0000          0x12000                0x1 2018-04-13 01:28:57 UTC+0000   C:\Windows\System32\wscapi.dll
0x000007fefe0f0000         0x178000                0x1 2018-04-13 01:28:57 UTC+0000   C:\Windows\system32\urlmon.dll
0x000007fefd400000         0x258000                0x1 2018-04-13 01:28:57 UTC+0000   C:\Windows\system32\iertutil.dll
0x000007fefbf40000          0x2d000                0x1 2018-04-13 01:28:57 UTC+0000   C:\Windows\System32\ntmarta.dll
0x000007fefd770000          0x50000                0x1 2018-04-13 01:28:57 UTC+0000   C:\Windows\system32\WLDAP32.dll
0x000007fefe050000          0x99000                0x1 2018-04-13 01:28:57 UTC+0000   C:\Windows\system32\CLBCatQ.DLL
0x000007fefaba0000          0x35000                0x2 2018-04-13 01:34:11 UTC+0000   C:\Windows\System32\XmlLite.dll
0x000007fefcb80000          0x57000            0xffff 2018-04-13 01:44:06 UTC+0000   C:\Windows\system32\apphelp.dll
0x000007feece10000          0xdbe000                0x1 2018-04-13 01:46:34 UTC+0000   C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0CD4951A-3F30-4489-9D23-CDF38D661848}\mpengine.dll
0x000007fefb490000          0x2c000                0x1 2018-04-13 01:46:40 UTC+0000   C:\Windows\system32\powrprof.dll
0x000007fefdbe0000          0x1d7000               0x1 2018-04-13 01:46:40 UTC+0000   C:\Windows\system32\SETUPAPI.dll
0x000007fefd080000          0x36000                0x3 2018-04-13 01:46:40 UTC+0000   C:\Windows\system32\CFGMGR32.dll
0x000007fefd060000          0x1a000                0x1 2018-04-13 01:46:40 UTC+0000   C:\Windows\system32\DEVOBJ.dll
```

The PEB structure resides in the process memory and keeps tracks of the full path to the executable and its base address, whereas VAD structure resides in the kernel memory.Comparing these two structures for discrepancy can tell if a process is hollowed out. In the below screenshot running the dlllist plugin shows the full path to **svchosts.exe (pid 1404)** and the base address (**0x00000000ff940000**) where it is loaded. The dlllist plugin gets this information from the PEB.So, svchost.exe is malicious.

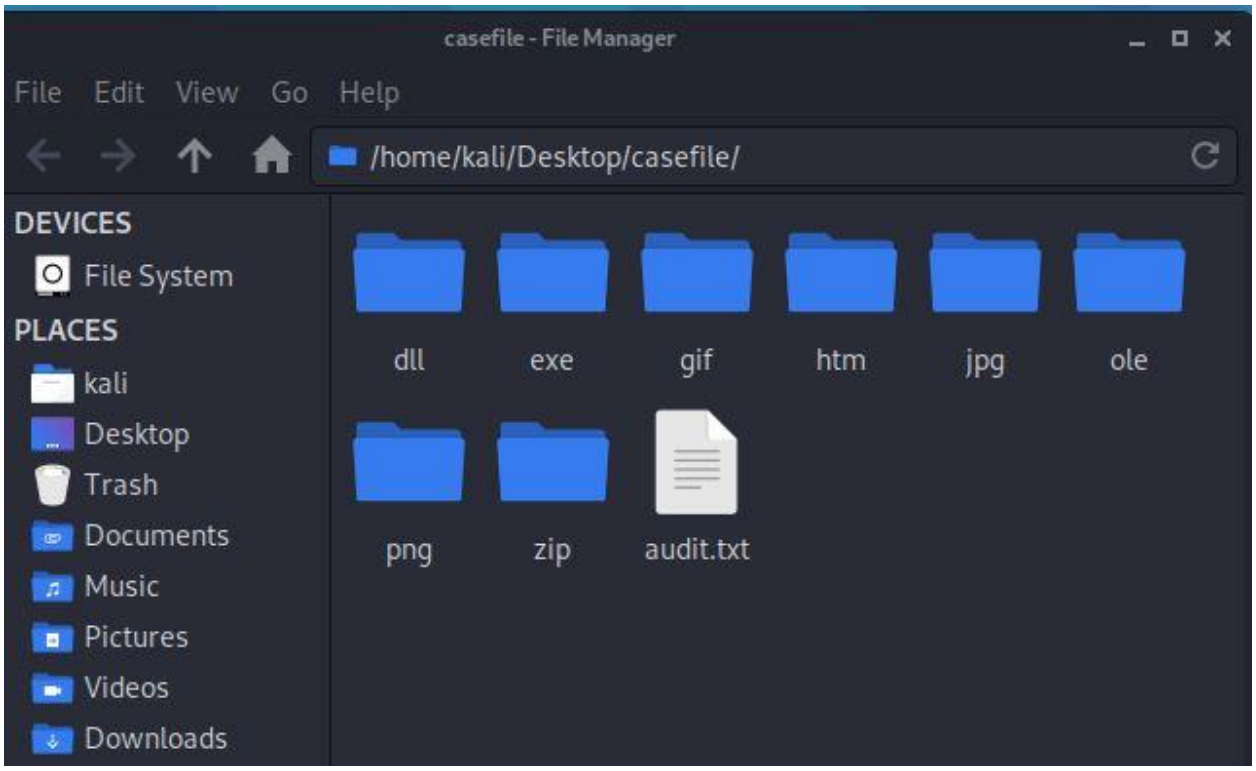
University of Victoria

4.Extract the executables for one of the suspicious processes identified above, and check whether at least one of these files is malicious using an online virus scanner [1%].

For this question we chose PID 2120 for analysis. In the first step we have dumped memory of that process by using command as:

volatility -f memory.dmp –profile=Win7SP0x64 memdump -p 2120–dump-dir .

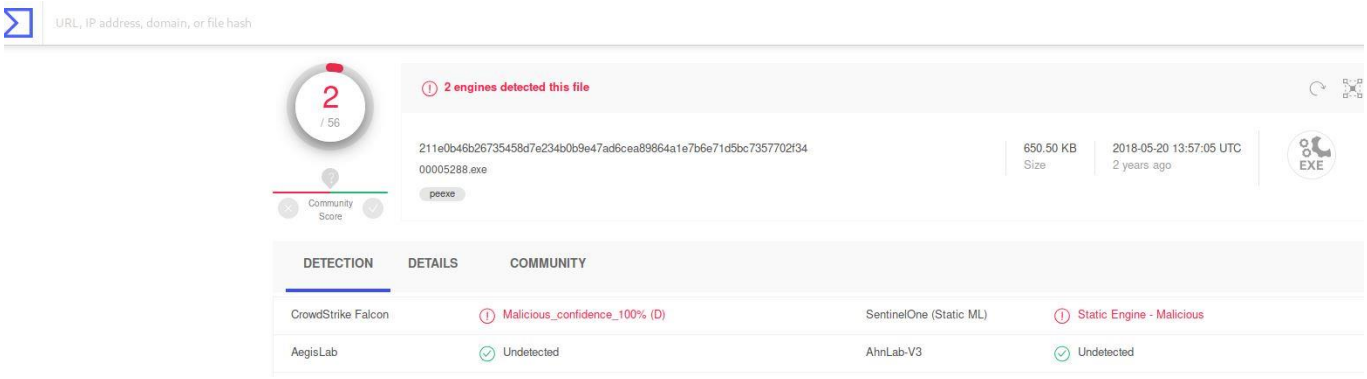
By using foremost command exe files for scanning have been separated as follow:



When we open audit.text file we see content of this dump.

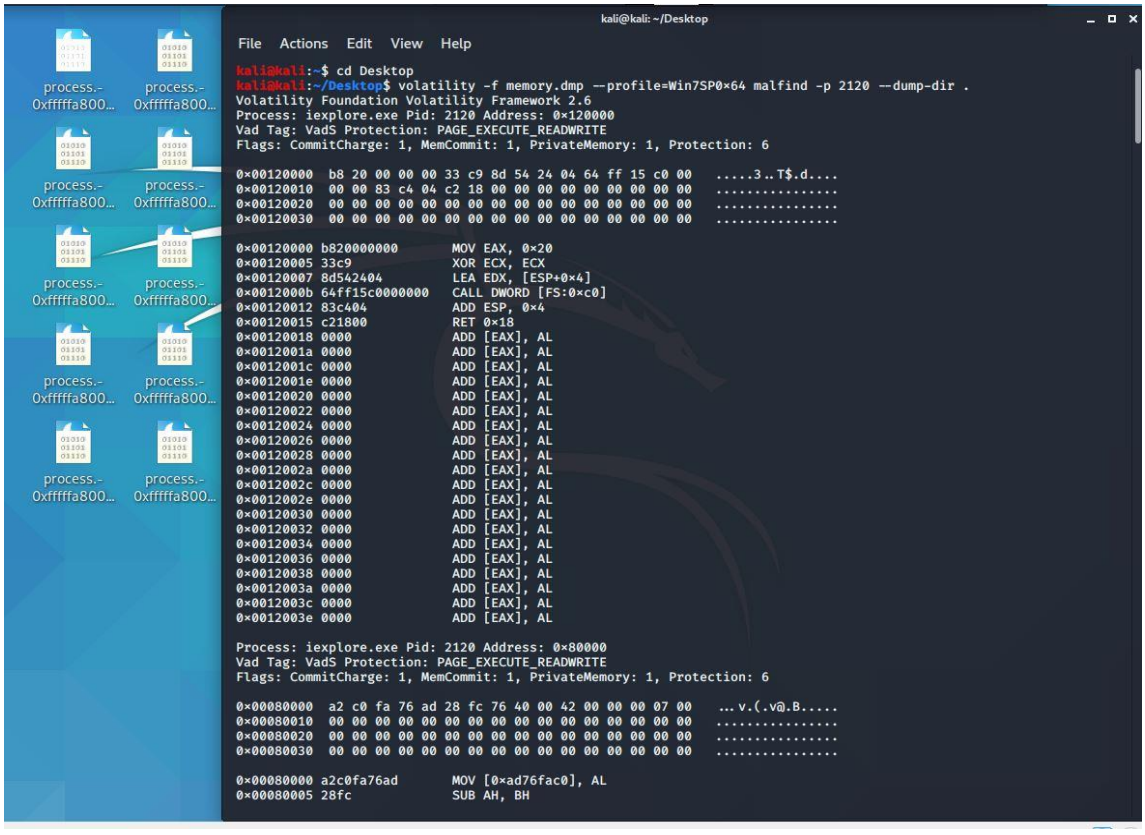
```
127 FILES EXTRACTED

jpg:= 1
gif:= 6
htm:= 69
ole:= 1
zip:= 1
exe:= 34
png:= 15
------------------------------------------------------------------
```

By checking these files in Virus scanner, we see this process is malicious. We see that different information about kind of suspicious is provided too.



Also we used malfind command for PID 2120 and dump memory of this process as follow too :

Volatility -f memory.dmp –profile=Win7SP0x64 malfind 2120 –dump-dir .



As a result, we have 8 files that we create their hashes and gave it to virus scanner.

```
kali@kali:~/Desktop$ ls
 casefile   memdump   memory.dmp  'New Folder'   process.0×fffffa8000eb4b30.0×69c0000.dmp   process.0×fffffa8000eb4b30.0×6a40000.dmp
kali@kali:~/Desktop$ md5sum process.0×fffffa8000eb4b30.0×69c0000.dmp
890b36c3147d039dc64a66b988fc6a97  process.0×fffffa8000eb4b30.0×69c0000.dmp
kali@kali:~/Desktop$ md5sum  process.0×fffffa8000eb4b30.0×6a40000.dmp
23ad17ebb87c07135e196fe67213471f  process.0×fffffa8000eb4b30.0×6a40000.dmp
kali@kali:~/Desktop$
```

5.Identify the URLs (and a corresponding IP address) for one of the possible remote command and control servers visited by the malware. Confirm that the selected URL is malicious using an online scanner. Note: You can limit the search to the initial (suspicious) process that triggered the exploit, or any other relevant process

One samples are as a follows for **Iexplore.exe process ID 2120** is selected based on the question. As you can see that based on question 1 and 2, we found a lot of suspicious process.
We use this command for finding url:
First we create dmp file and then strings to find a url

volatility -f memory.dmp --profile=Win7SP0x64 -p 2120 memdump –dump-dir=dump

```
kali@kali:~/Desktop$ volatility -f  memory.dmp --profile=Win7SP0x64 -p 2120 memdump --dump-dir=dump
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing iexplore.exe [  2120] to 2120.dmp
```

Strings /home/kali/Desktop/dump/2120.dmp | grep “http://”

```
kali@kali:~/Desktop$ strings /home/kali/Desktop/dump/2120.dmp | grep "http://"
```

URLs list

List of any suspicious URLs that may be in the suspected process’s memory are as follows. All 8 pages that contain URLs of process ID 2120 are show as a follows:

```
kali@kali:~/Desktop$ strings /home/kali/Desktop/dump/2120.dmp | grep "http://"
<!------111-111-111-1111-1111-111-111-111  —><b>1.<a href="http://pot98bza3sgfjr35t.fausttime.com/4497C53C81B91BAB"   target="_blank">http://pot98bza3sgfjr35t.faustt
ime.com/449v8
<!------111-111-111-1111-1111-111-111-111  —><b>2.<a href="http://h5534bvnrnkj345.maniupulp.com/4497C53C81B91BAB"   target="_blank">http://h5534bvnrnkj345.maniupulp.
com/4497i8
<!------111-111-111-1111-1111-111-111-111  —><b>3.<a href="http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB"   target="_blank">http://i4sdmjn4fsdsdqfhu12l.
orbyscabz@8
<a href="http://www.torproject.org/projects/torbrowser.html.en" target="_blank">http://www.torproject.org/projects/torbrowser.html.en</a><br>
<b><br> <a href="http://pot98bza3sgfjr35t.fausttime.
3C81B91BAB" target="_blank">http://pot98bza3sgfjr35t.fausttime.com/4497C53C81B91BAB</a> <br><a href="http://h5534bvnrnkj345.maniupulp.com/4497C53C81B91BAB" target="_b
lank">http://h5534bvnrnkc;
<!-----111-111-111-1111-1111-111-111-111  —><a href="http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB" target="_blank">http://i4sdmjn4fsdsdqfhu1Z;
za3sgfjr35t.fausttime.com/4497C53C81B91BAB"   target="_blank">http://pot98bza3sgfjr35t.fausttime.com/4497C53C81B91BAB</a></b><br>
<!------111-111-111-1111-1111-111-111-111  —><b>2.<a href="http://h5534bvnrnkj345.maniupulp.com/4497C53C81B91BAB"   target="_blank">http://h5534bvnrnkj345.maniupulp.
com/4497C53C81B91BAB</a></b><br>
.orbyscabz.com/4497C53C81B91BAB"   target="_blank">http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB</a></b><br>
found here: <a href="http://en.wikipedia.org/wiki/RSA_(cryptosystem)" target="_blank">http://en.wikipedia.org/wiki/RSA_(cryptosystem)</a><br></font>
<!------111-111-111-1111-1111-111-111-111  —><b>1.<a href="http://pot98bza3sgfjr35t.fausttime.com/4497C53C81B91BAB"   target="_blank">http://pot98bza3sgfjr35t.faustt
ime.com/4497C53C81B91BAB</a></b><br>
<!------111-111-111-1111-1111-111-111-111  —><b>2.<a href="http://h5534bvnrnkj345.maniupulp.com/4497C53C81B91BAB"   target="_blank">http://h5534bvnrnkj345.maniupulp.
com/4497C53C81B91BAB</a></b><br>
<!------111-111-111-1111-1111-111-111-111  —><b>3.<a href="http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB"   target="_blank">http://i4sdmjn4fsdsdqfhu12l.
orbyscabz.com/4497C53C81B91BAB</a></b><br>
<a href="http://www.torproject.org/projects/torbrowser.html.en" target="_blank">http://www.torproject.org/projects/torbrowser.html.en</a><br>
<b><br> <a href="http://pot98bza3sgfjr35t.fausttime.com/4497C53C81B91BAB" target="_blank">http://pot98bza3sgfjr35t.fausttime.com/4497C53C81B91BAB</a> <br><a href="htt
p://h5534bvnrnkj345.maniupulp.com/4497C53C81B91BAB" target="_blank">http://h5534bvnrnkj345.maniupulp.com/4497C53C81B91BAB</a> <br>
<!-----111-111-111-1111-1111-111-111-111  —><a href="http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB" target="_blank">http://i4sdmjn4fsdsdqfhu12l.orbyscab
z.com/4497C53C81B91BAB</a>  <br>
    <asmv3:windowsSettings xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">
feedplat:http://go.microsoft.com/fwlink/?LinkId=68928
feedplat:http://go.microsoft.com/fwlink/?LinkId=68929
feedplat:http://go.microsoft.com/fwlink/?LinkId=44406
feedplat:http://go.microsoft.com/fwlink/?LinkId=121315
feedplat:http://go.microsoft.com/fwlink/?LinkId=129793
```

```
feedplat:http://go.microsoft.com/fwlink/?LinkId=129794
<a style="font: 8pt Tahoma, MS Shell Dlg" href="http://go.microsoft.com/fwlink/?LinkId=54758" id="copyright">
<a style="font: 8pt Tahoma, MS Shell Dlg" href="http://go.microsoft.com/fwlink/?LinkId=54758" id="copyright">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
                        <p id="errorExplanation"><a href="http://go.microsoft.com/fwlink/?LinkId=124983">Go online to learn about the Data Execution Prevention (DEP)
security feature</a></p>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
http://Microsoft.STS.STSWeb/
http://Microsoft.Live.URSTelemetry/
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
    <asmv3:windowsSettings xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
<ie8tldlistdescription xmlns="http://www.microsoft.com/schemas/ie8tldlistdescription/1.0">
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
        <dpiAware  xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
```

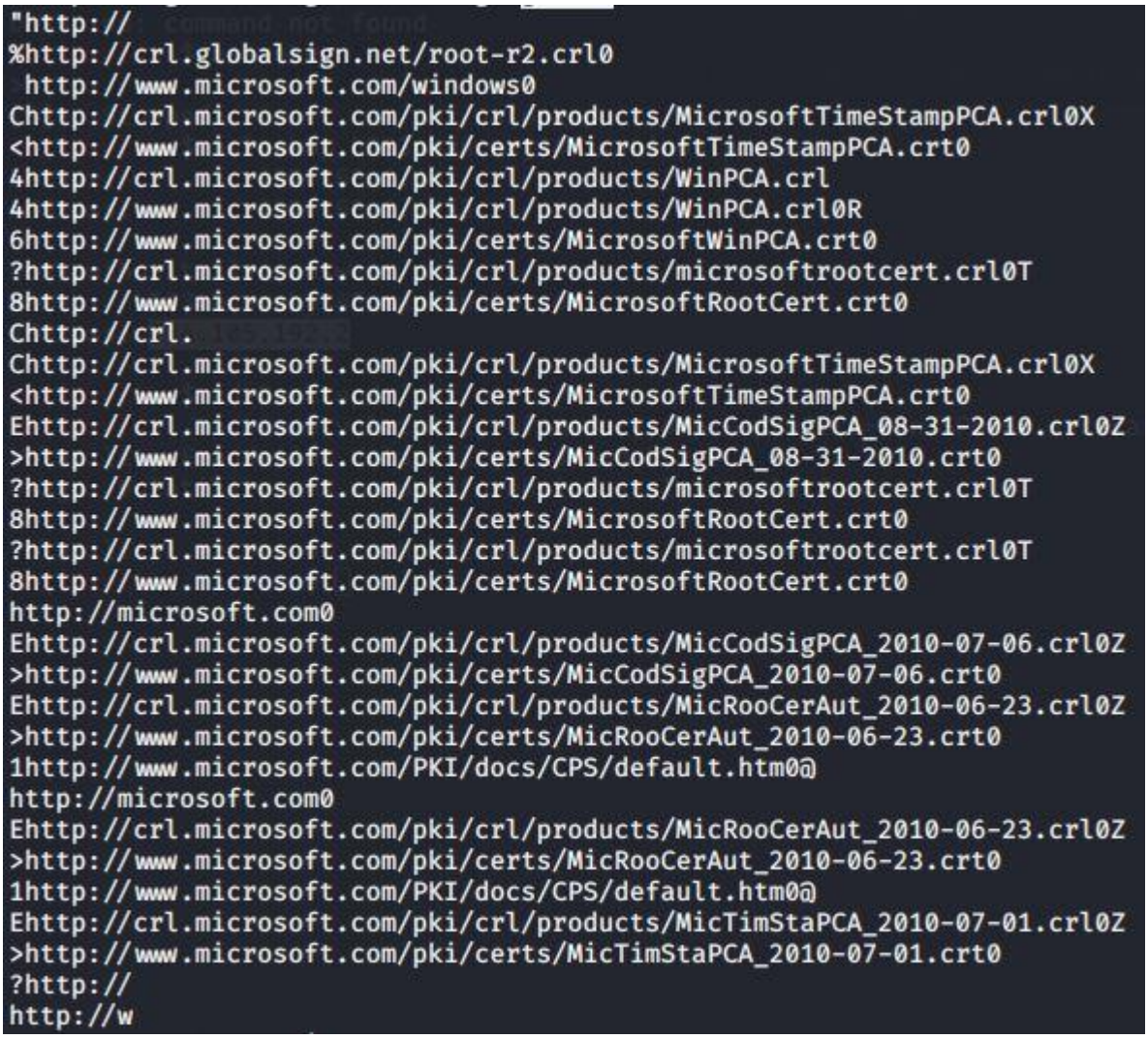
```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
^http://dmd-ca-beta2/CertEnroll/dmd-ca-beta2_Microsoft%20Digital%20Media%20Authority%202005.crt0d
Qhttp://dmd-ca-beta2/CertEnroll/Microsoft%20Digital%20Media%20Authority%202005.crl
^http://dmd-ca-beta2/CertEnroll/dmd-ca-beta2_Microsoft%20Digital%20Media%20Authority%202005.crt0d
Qhttp://dmd-ca-beta2/CertEnroll/Microsoft%20Digital%20Media%20Authority%202005.crl
Monitor Lizards Mating - 030708 - http://www.archive.org/details/Carmen-NyalaMonitorLizardsMating-030708
license: http://creativecommons.org/licenses/publicdomain/
^http://dmd-ca-beta2/CertEnroll/dmd-ca-beta2_Microsoft%20Digital%20Media%20Authority%202005.crt0d
Qhttp://dmd-ca-beta2/CertEnroll/Microsoft%20Digital%20Media%20Authority%202005.crl
^http://dmd-ca-beta2/CertEnroll/dmd-ca-beta2_Microsoft%20Digital%20Media%20Authority%202005.crt0d
Qhttp://dmd-ca-beta2/CertEnroll/Microsoft%20Digital%20Media%20Authority%202005.crl
http://www.microsoft.com/provisioning/eaptlsuserpropertiesv1
http://www.microsoft.com/provisioning/mschapv2userpropertiesv1
http://www.microsoft.com/provisioning/mspeapuserpropertiesv1
Khttp://mscrl.microsoft.com/pki/mscorp/crl/Microsoft%20IT%20TLS%20CA%205.crl
Ihttp://crl.microsoft.com/pki/mscorp/crl/Microsoft%20IT%20TLS%20CA%205.crl0
Ehttp://www.microsoft.com/pki/mscorp/Microsoft%20IT%20TLS%20CA%205.crt0"
http://ocsp.msocsp.com0>
'http://www.microsoft.com/pki/mscorp/cps0'
1. http://pot98bza3sgfjr35t.fausttime.com/4497C53C81B91BAB
2. http://h5534bvnrnkj345.maniupulp.com/4497C53C81B91BAB
3. http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB
1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
http://pot98bza3sgfjr35t.fausttime.com/4497C53C81B91BAB
http://h5534bvnrnkj345.maniupulp.com/4497C53C81B91BAB
```

```
http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB
More information about the encryption keys using RSA-4096 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://www.microsoft.com/provisioning/eaptlsconnectionpropertiesv1
http://www.microsoft.com/provisioning/mschapv2connectionpropertiesv1
http://www.microsoft.com/provisioning/mspeapconnectionpropertiesv1
http://www.microsoft.com/provisioning/eaptlsuserpropertiesv1
http://www.microsoft.com/provisioning/mschapv2userpropertiesv1
http://www.microsoft.com/provisioning/mspeapuserpropertiesv1
http://+:80/116B50EB-ECE2-41ac-8429-9F9E963361B7/
http://+:80/Temporary_Listen_Addresses/
]Jhttp://+:10243/WMPNSSv4/
http://*:2869/
http://+:47001/wsman/
http://+:5985/wsman/
http://*:5357/
http://+:80/Temporary_Listen_Addresses/
]Jhttp://+:10243/WMPNSSv4/
http://+:47001/wsman/
http://+:5985/wsman/
http://+:80/116B50EB-ECE2-41ac-8429-9F9E963361B7/
http://*:2869/
http://*:5357/
http://www.microsoft.com/provisioning/mspeapuserpropertiesv1
http://www.microsoft.com/provisioning/eaptlsconnectionpropertiesv1
http://www.microsoft.com/provisioning/eaptlsuserpropertiesv1
http://www.microsoft.com/provisioning/mschapv2connectionpropertiesv1
http://www.microsoft.com/provisioning/mschapv2userpropertiesv1
http://www.microsoft.com/provisioning/mspeapconnectionpropertiesv1
 http://crl.verisign.com/pca3.crl0
http://schemas.microsoft.com/winfx/2006/xaml/presentation
khttp://drmlicense.one.microsoft.com
http://preview.services.wmdrm.windowsmedia.com
http://schemas.microsoft.com/winfx/2006/xaml/presentation
http://schemas.microsoft.com/office/smartdocuments/2003
#http://logo.verisign.com/vslogo.gif0
```

```
%http://crl.globalsign.net/root-r2.crl0
# This file is part of Cuckoo Sandbox - http://www.cuckoosandbox.org
# This file is part of Cuckoo Sandbox - http://www.cuckoosandbox.org
# This file is part of Cuckoo Sandbox - http://www.cuckoosandbox.org
# This file is part of Cuckoo Sandbox - http://www.cuckoosandbox.org
# This file is part of Cuckoo Sandbox - http://www.cuckoosandbox.org
# This file is part of Cuckoo Sandbox - http://www.cuckoosandbox.org
# This file is part of Cuckoo Sandbox - http://www.cuckoosandbox.org
# This file is part of Cuckoo Sandbox - http://www.cuckoosandbox.org
2018-04-12      18:44:22:746     904    694     DnldMgr   * Downloading from http://download.windowsupdate.com/d/msdownload/update/software/defu/2018/04/mpas-fe_01533
846d0aafefd2fa68a25155008d7ec364039.exe to C:\Windows\SoftwareDistribution\Download\52e6783f08f8df0daf7ad9d56af352b6\01533846d0aafefd2fa68a25155008d7ec364039 (full fi
le).
URL=http://go.microsoft.com/fwlink/?LinkId=121315
FeedUrl=http://go.microsoft.com/fwlink/?LinkId=121315
URL=http://go.microsoft.com/fwlink/?LinkId=129791
URL=http://go.microsoft.com/fwlink/?LinkId=129792
    url = "http://www.google.com/search?q=%s" % s
http://ocsp.verisign.com0
"http://crl.verisign.com/tss-ca.crl0
http://ocsp.verisign.com0
0http://crl.verisign.com/ThawteTimestampingCA.crl0
#http://logo.verisign.com/vslogo.gif0
http://ocsp.verisign.com01
 http://crl.verisign.com/pca3.crl0)
3http://csc3-2009-2-crl.verisign.com/CSC3-2009-2.crl0D
http://ocsp.verisign.com0?
3http://csc3-2009-2-aia.verisign.com/CSC3-2009-2.cer0
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
http://ocsp.verisign.com0
"http://crl.verisign.com/tss-ca.crl0
http://ocsp.verisign.com0
0http://crl.verisign.com/ThawteTimestampingCA.crl0
#http://logo.verisign.com/vslogo.gif0
http://ocsp.verisign.com01
```

```
 http://crl.verisign.com/pca3.crl0)
3http://csc3-2009-2-crl.verisign.com/CSC3-2009-2.crl0D
http://ocsp.verisign.com0?
3http://csc3-2009-2-aia.verisign.com/CSC3-2009-2.cer0
<frame  title='Content'  src="http://waysandmeans.house.gov/legacy/trade/105cong/3-31-98/3-31thie.htm">
More information about the encryption keys using RSA-4096 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)
1. http://pot98bza3sgfjr35t.fausttime.com/4497C53C81B91BAB
2. http://h5534bvnrnkj345.maniupulp.com/4497C53C81B91BAB
3. http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB
1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
http://pot98bza3sgfjr35t.fausttime.com/4497C53C81B91BAB
http://h5534bvnrnkj345.maniupulp.com/4497C53C81B91BAB
http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB
 xmlns:c="http://schemas.microsoft.com/Contact" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
URL=http://go.microsoft.com/fwlink/?LinkId=54729
URL=http://go.microsoft.com/fwlink/?LinkId=68925
More information about the encryption keys using RSA-4096 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)
1. http://pot98bza3sgfjr35t.fausttime.com/4497C53C81B91BAB
2. http://h5534bvnrnkj345.maniupulp.com/4497C53C81B91BAB
3. http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB
1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
http://pot98bza3sgfjr35t.fausttime.com/4497C53C81B91BAB
http://h5534bvnrnkj345.maniupulp.com/4497C53C81B91BAB
http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB
FMsl http://
 http://
?http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl0T
8http://www.microsoft.com/pki/certs/MicrosoftRootCert.crt0!
ReTa http://
http://www-physics.lbl.gov/~gilg/SCTWeeklyMeetings/Jan212003/
found here: <a href="http://en.wikipedia.org/wiki/RSA_(cryptosystem)" target="_blank">http://en.wikipedia.org/wiki/RSA_(cryptosystem)</a><br></font>
 http://
3. http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB
```

```
1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
http://pot98bza3sgfjr35t.fausttime.com/4497C53C81B91BAB
http://h5534bvnrnkj345.maniupulp.com/4497C53C81B91BAB
http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB
NpFR http://
MmCa http://
http://ocsp.digicert.com0:
)http://crl3.digicert.com/Omniroot2025.crl0=
ere: http://
http://i4
 http://[
1. http://pot98bza3sgfjr35t.fa
http://www.bing.com/favicon.ico
        http://technology.jsc.nasa.gov/habconference
 http://
MmCa http://`
ere: http://
 http://
MmSi http://
<link rel="profile" href="http://gmpg.org/xfn/11">
<link rel="pingback" href="http://www.pedagogiablanca.net/xmlrpc.php" />
a Blanca &raquo; Feed" href="http://www.pedagogiablanca.net/feed/" />
a Blanca &raquo; RSS de los comentarios" href="http://www.pedagogiablanca.net/comments/feed/" />
<link rel='stylesheet' id='cnss_font_awesome_css-css'  href='http://www.pedagogiablanca.net/wp-content/plugins/easy-social-icons/css/font-awesome/css/font-awesome.min
.css?ver=4.7' type='text/css' media='all' />
<link rel='stylesheet' id='cnss_css-css'  href='http://www.pedagogiablanca.net/wp-content/plugins/easy-social-icons/css/cnss.css?ver=1.0' type='text/css' media='all'
/>
<link rel='stylesheet' id='contact-form-7-css'  href='http://www.pedagogiablanca.net/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=4.4' type='text/c
MmCa http://
MmCa http://
 http://
URL=http://go.microsoft.com/fwlink/?LinkId=129791
#http://logo.verisign.com/vslogo.gif0
```



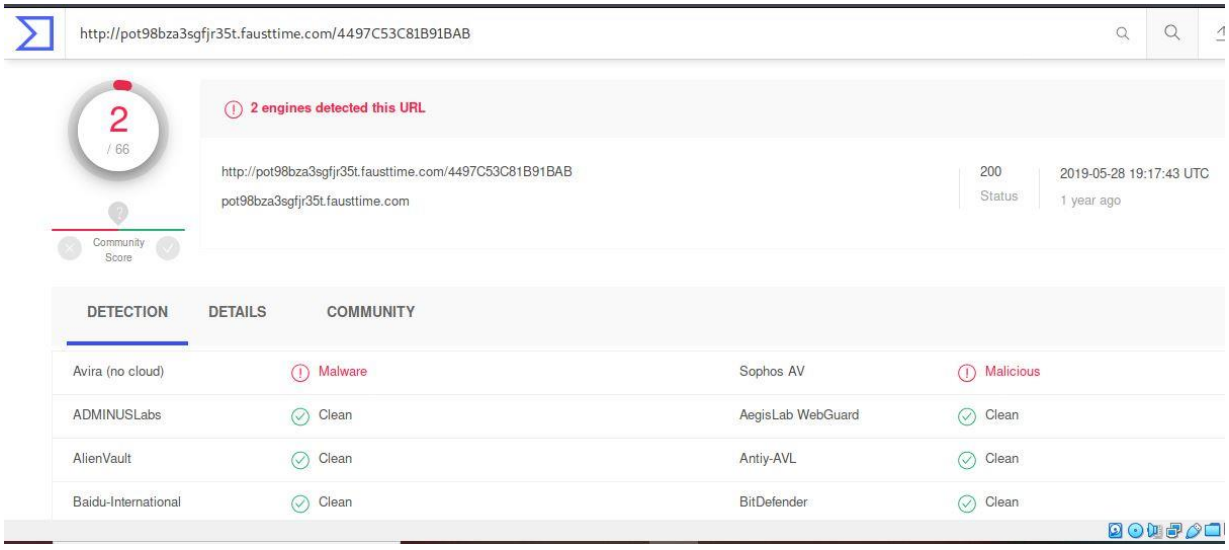
The URL, we found related IP addresses. When we test URLs wit Virus scanner,virustotal.com and test to find an IP address based on URLs in IPvoid.com. We found some of these URLs are suspicious with different percentages. It means that different process with different result from different virus scanners.

We use nslookup to find an IP address of each URLs. Three URLs of process ID 2120 are as follows.

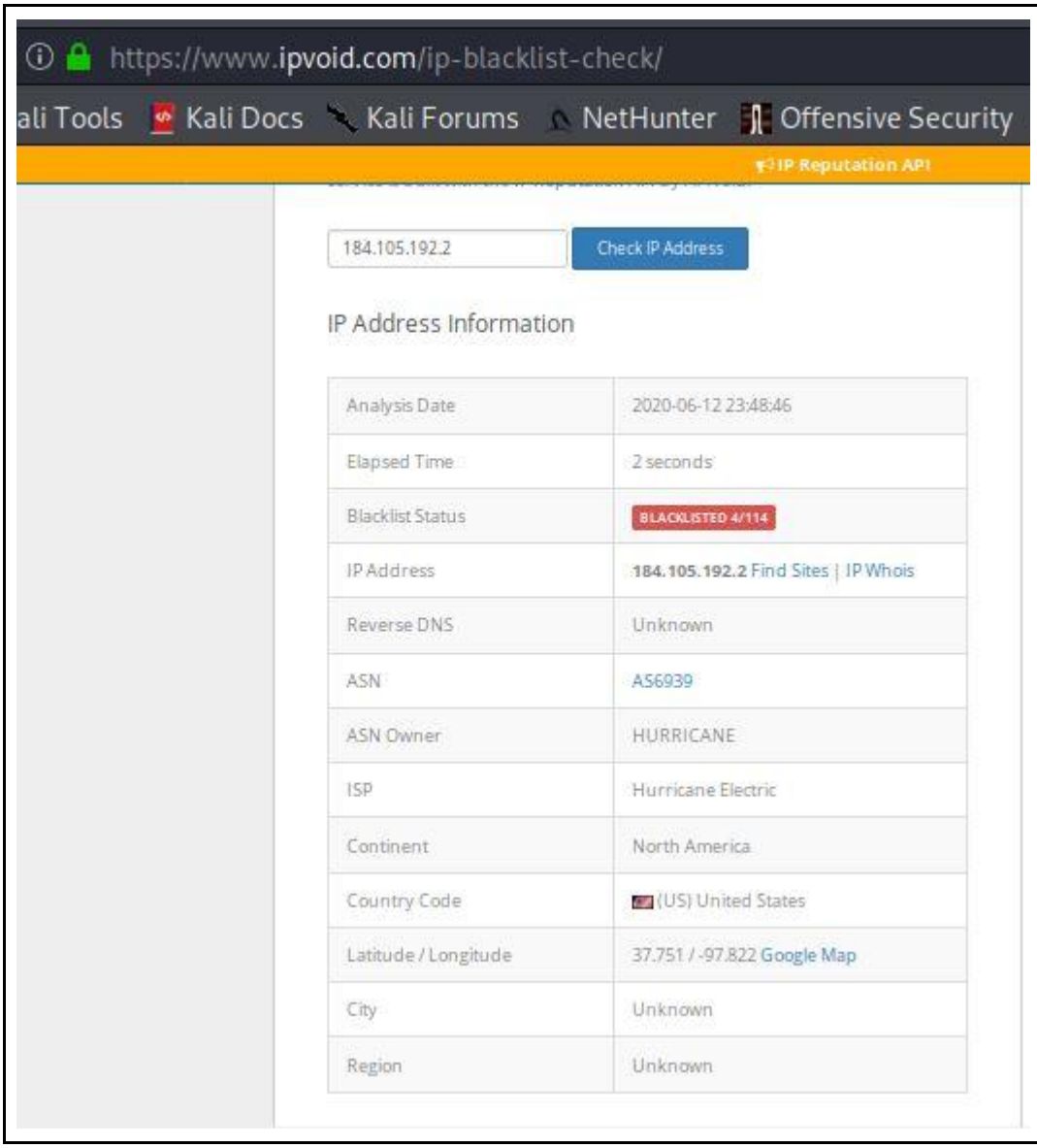
University of Victoria

1-

```
kali@kali:~/Desktop$ strings /home/kali/Desktop/dump/2120.dmp | grep "http://"
<!------111-111-111-1111-1111-111-111-111  ⟶<b>1.<a href="http://pot98bza3sgfjr35t.fausttime.com/4497C53C81B91BAB"
ime.com/449v8
<!------111-111-111-1111-1111-111-111-111  ⟶<b>2.<a href="http://h5534bvnrnkj345.maniupulp.com/4497C53C81B91BAB"   ta
com/4497i8
<!------111-111-111-1111-1111-111-111-111  ⟶<b>3.<a href="http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB"
```



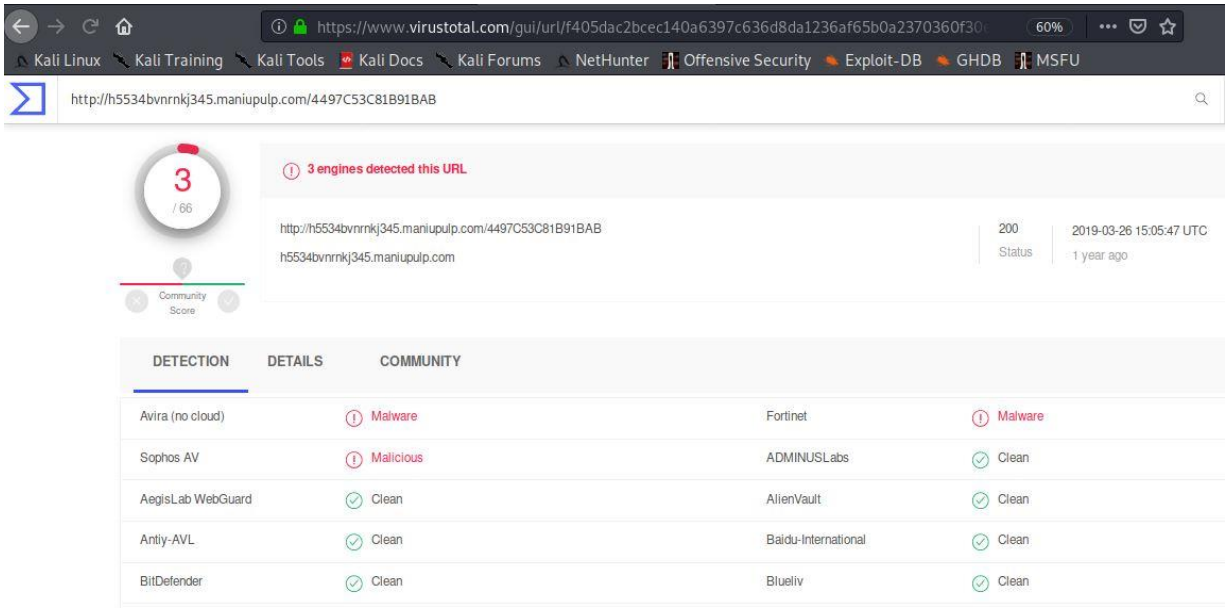

```
kali@kali:~$ nslookup pot98bza3sgfjr35t.fausttime.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   pot98bza3sgfjr35t.fausttime.com
Address: 184.105.192.2
```


https://www.ipvoid.com/ip-blacklist-check/
ali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
IP Reputation API
184.105.192.2
Check IP Address
IP Address Information
Analysis Date
2020-06-12 23:48:46
Elapsed Time
2 seconds
Blacklist Status
BLACKLISTED 4/114
IP Address
184.105.192.2 Find Sites | IP Whois
Reverse DNS
Unknown
ASN
AS6939
ASN Owner
HURRICANE
ISP
Hurricane Electric
Continent
North America
Country Code
(US) United States
Latitude / Longitude
37.751 / -97.822 Google Map
City
Unknown
Region
Unknown

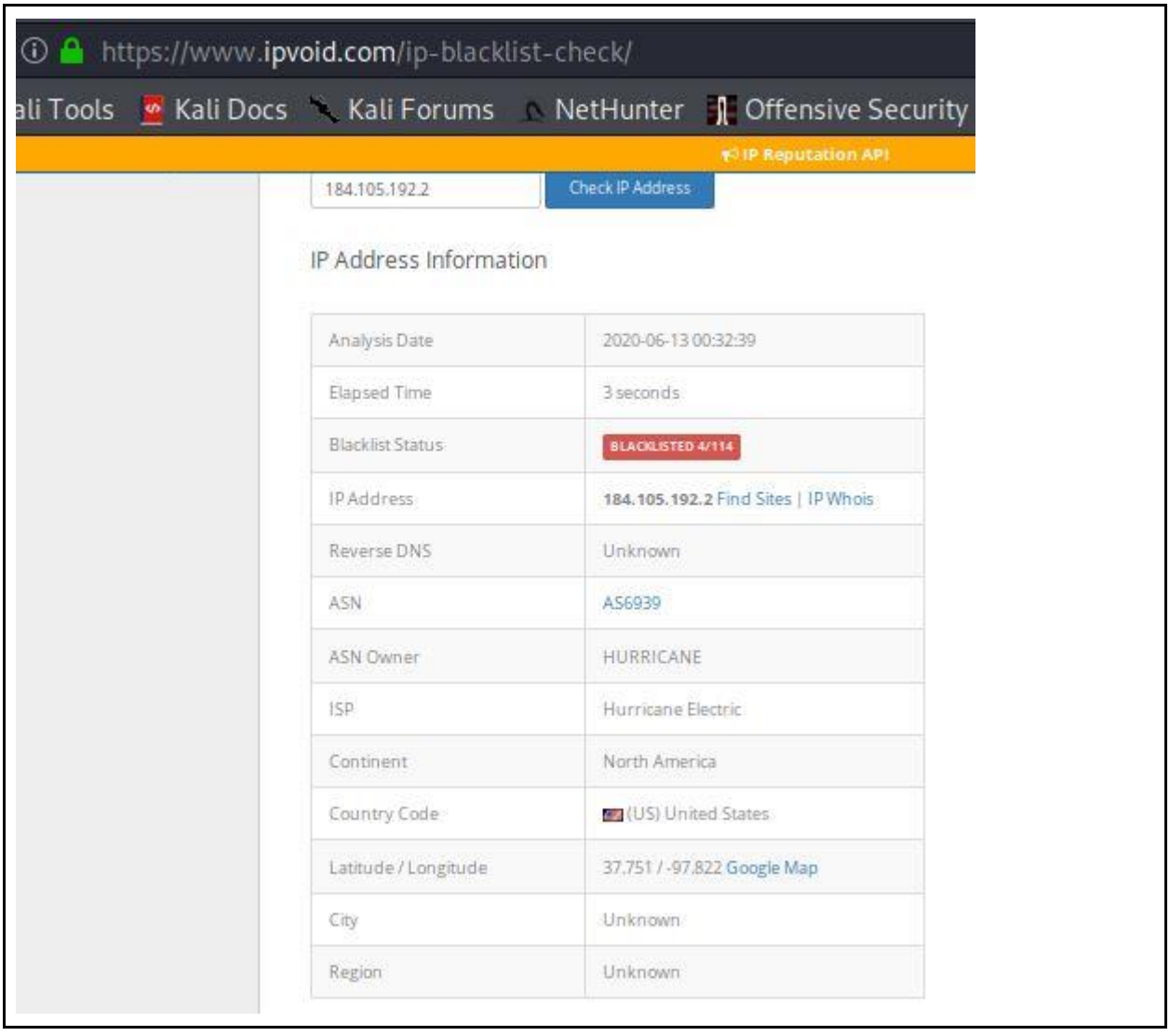
University of Victoria

2-

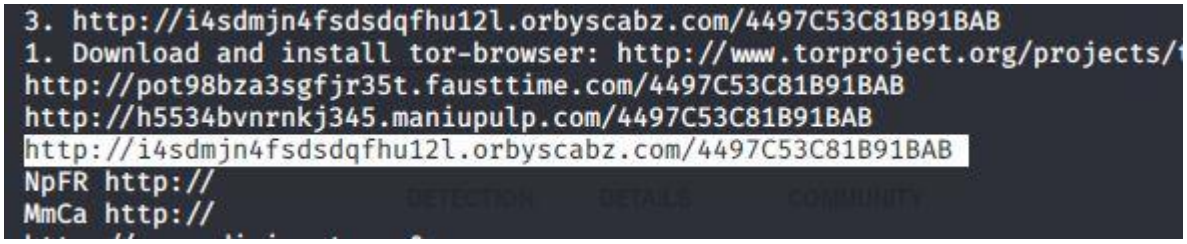
```
found here: <a href="http://en.wikipedia.org/wiki/RSA_(cryptosystem)" target="_blank">http:
 http://
3. http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB
1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
http://pot98bza3sgfjr35t.fausttime.com/4497C53C81B91BAB
http://h5534bvnrnkj345.maniupulp.com/4497C53C81B91BAB
http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB
NpFR http://
MmCa http://
http://ocsp.digicert.com0:
```

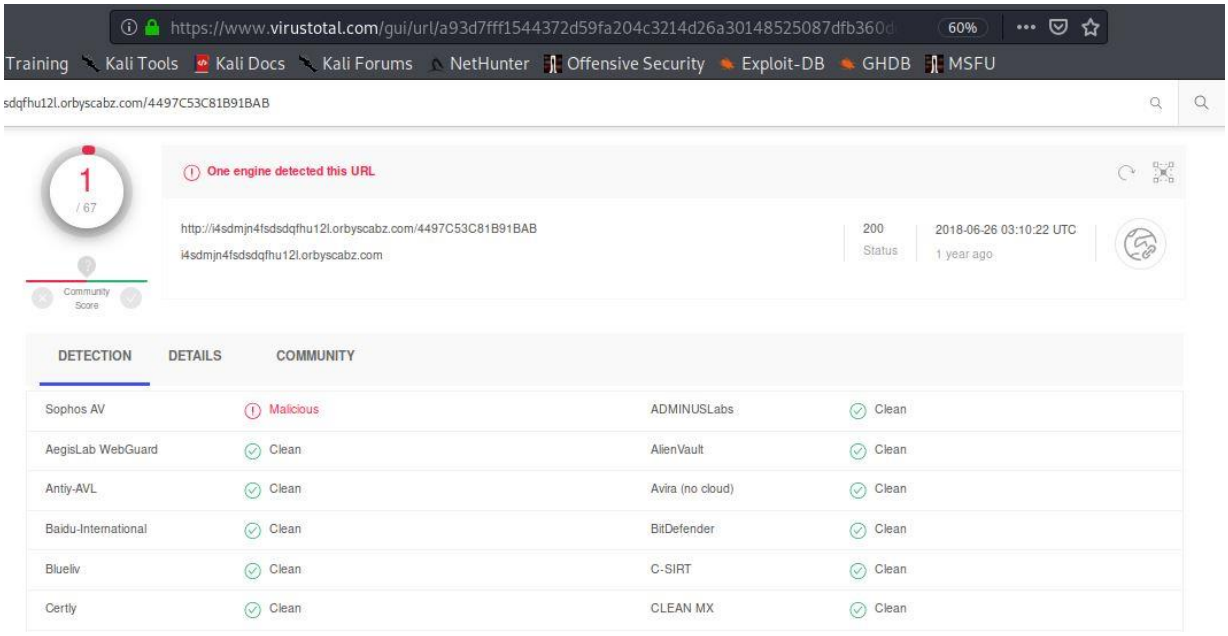


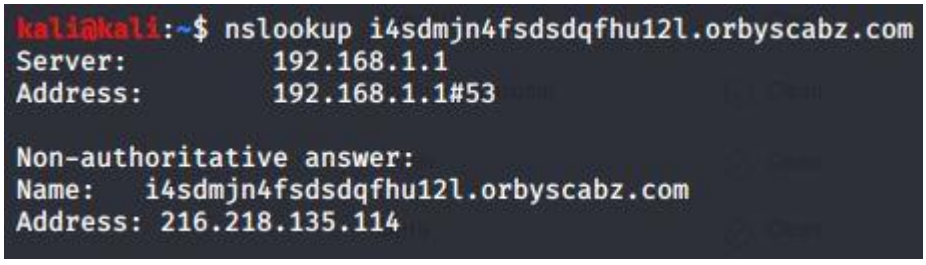

```
kali@kali:~$ nslookup h5534bvnrnkj345.maniupulp.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   h5534bvnrnkj345.maniupulp.com
Address: 184.105.192.2
```

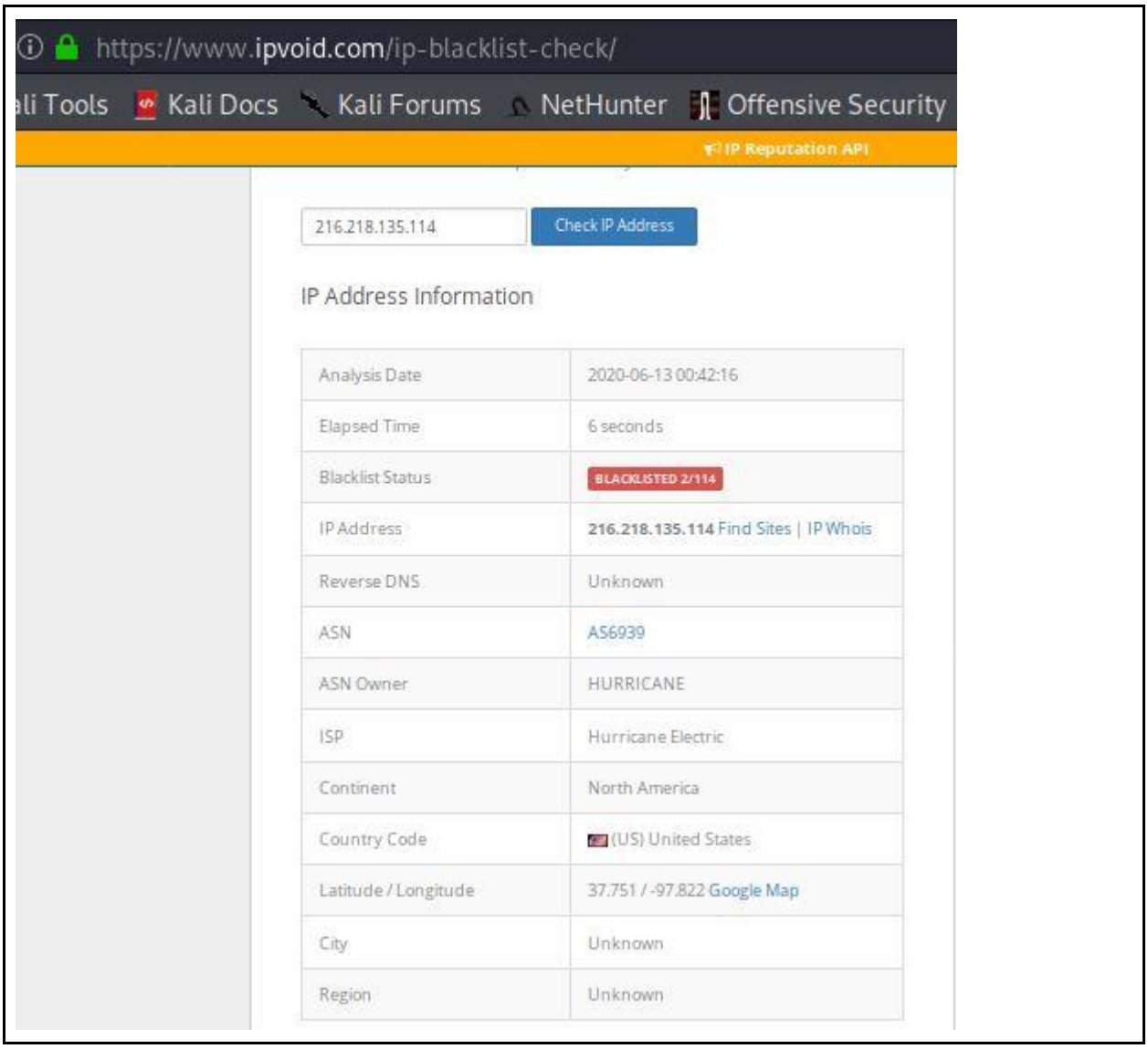

https://www.ipvoid.com/ip-blacklist-check/
ali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
IP Reputation API
184.105.192.2
Check IP Address
IP Address Information
Analysis Date
2020-06-13 00:32:39
Elapsed Time
3 seconds
Blacklist Status
BLACKLISTED 4/114
IP Address
184.105.192.2 Find Sites | IP Whois
Reverse DNS
Unknown
ASN
AS6939
ASN Owner
HURRICANE
ISP
Hurricane Electric
Continent
North America
Country Code
(US) United States
Latitude / Longitude
37.751 / -97.822 Google Map
City
Unknown
Region
Unknown

3-


3. http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB
1. Download and install tor-browser: http://www.torproject.org/projects/
http://pot98bza3sgfjr35t.fausttime.com/4497C53C81B91BAB
http://h5534bvnrnkj345.maniupulp.com/4497C53C81B91BAB
http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB
NpFR http://
MmCa http://


https://www.virustotal.com/gui/url/a93d7fff1544372d59fa204c3214d26a30148525087dfb360d
60%
Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
sdqfhu12l.orbyscabz.com/4497C53C81B91BAB
1
/ 67
Community Score
One engine detected this URL
http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com/4497C53C81B91BAB
i4sdmjn4fsdsdqfhu12l.orbyscabz.com
200
Status
2018-06-26 03:10:22 UTC
1 year ago
DETECTION
DETAILS
COMMUNITY
Sophos AV
Malicious
ADMINUSLabs
Clean
AegisLab WebGuard
Clean
AlienVault
Clean
Antiy-AVL
Clean
Avira (no cloud)
Clean
Baidu-International
Clean
BitDefender
Clean
Blueliv
Clean
C-SIRT
Clean
Certly
Clean
CLEAN MX
Clean


kali@kali:~$ nslookup i4sdmjn4fsdsdqfhu12l.orbyscabz.com
Server: 192.168.1.1
Address: 192.168.1.1#53
Non-authoritative answer:
Name: i4sdmjn4fsdsdqfhu12l.orbyscabz.com
Address: 216.218.135.114



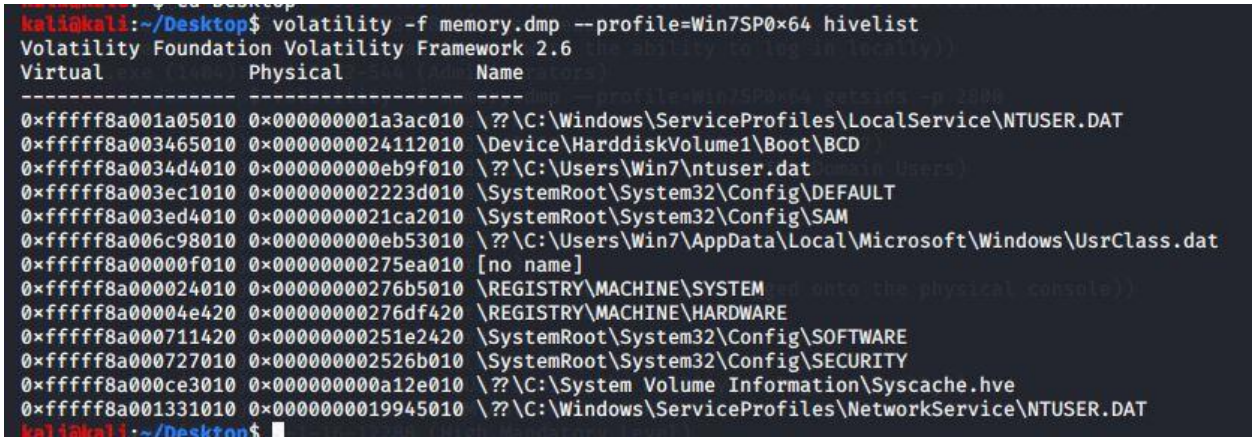
All sample URLs and IP address are shown in bellow table:

URL	IP address
http://h5534bvnrnkj345.maniupulp.com	184.105.192.2
http://i4sdmjn4fsdsdqfhu12l.orbyscabz.com	216.218.135.114
http://pot98bza3sgfjr35t.fausttime.com/	184.105.192.2

6.List available registry hives and identify a potentially malicious hive from the list. Explain and justify why such hive could potentially be malicious

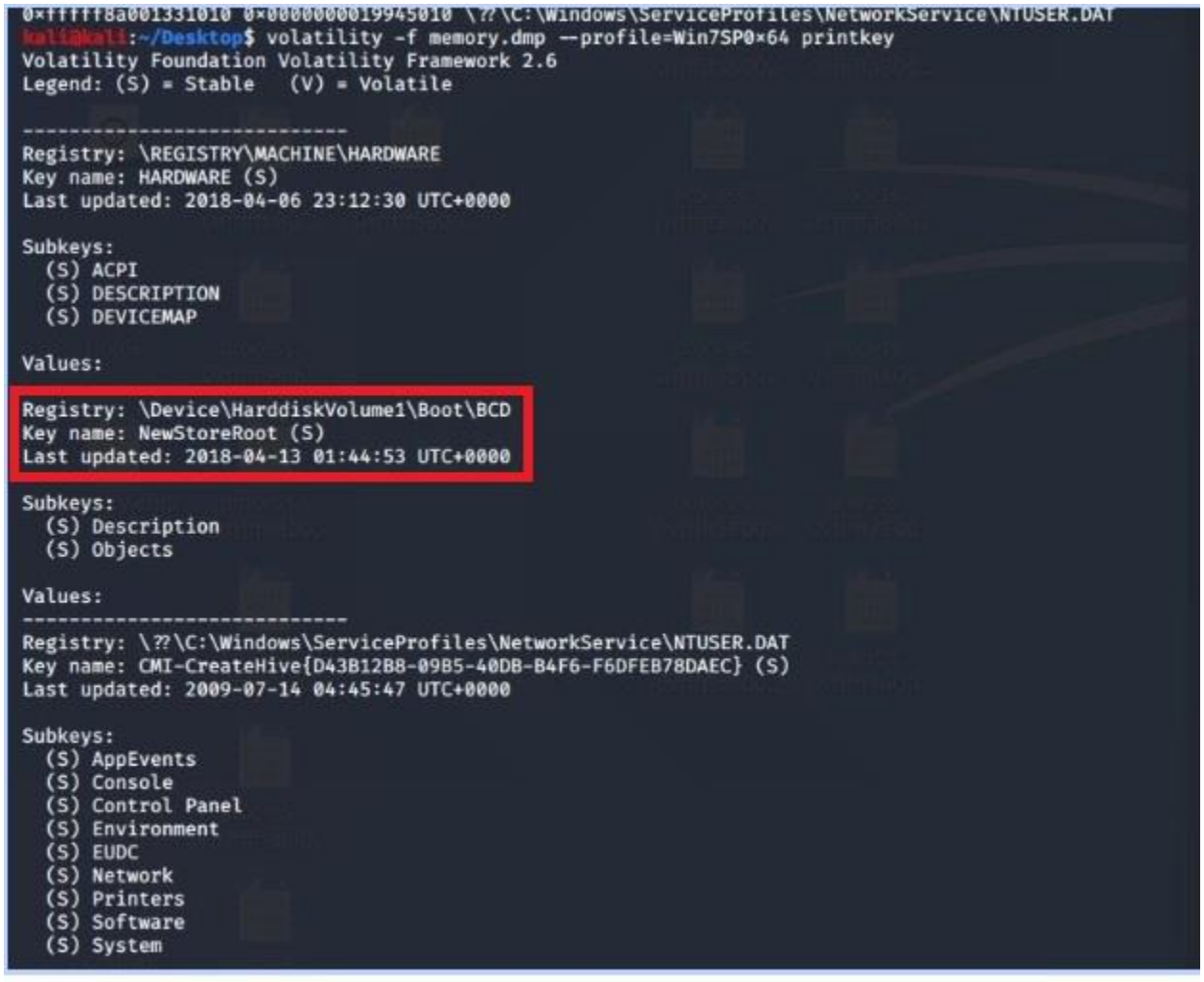
By using command as follow we see all registry hives:

Volatility -f memory.dmp –profile=Win7SP0x64 hivelist



For selecting which registry use to do more investigation we need more information about the time and keys,

Volatility -f memory.dmp –profile=Win7SP0x64 printkey


0×fffff8a001331010 0×0000000019945010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 printkey
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile
Registry: \REGISTRY\MACHINE\HARDWARE
Key name: HARDWARE (S)
Last updated: 2018-04-06 23:12:30 UTC+0000
Subkeys:
(S) ACPI
(S) DESCRIPTION
(S) DEVICEMAP
Values:
Registry: \Device\HarddiskVolume1\Boot\BCD
Key name: NewStoreRoot (S)
Last updated: 2018-04-13 01:44:53 UTC+0000
Subkeys:
(S) Description
(S) Objects
Values:
Registry: \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
Key name: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC} (S)
Last updated: 2009-07-14 04:45:47 UTC+0000
Subkeys:
(S) AppEvents
(S) Console
(S) Control Panel
(S) Environment
(S) EUDC
(S) Network
(S) Printers
(S) Software
(S) System

```
Values:
---------------------------
Registry: \SystemRoot\System32\Config\DEFAULT
Key name: CMI-CreateHive{BD6FA63F-599C-4F99-99DE-A05742AA2377} (S)
Last updated: 2009-07-14 04:57:10 UTC+0000

Subkeys:
  (S) Control Panel
  (S) Environment
  (S) EUDC
  (S) Keyboard Layout
  (S) Printers
  (S) Software
  (S) SYSTEM

Values:
---------------------------
Registry: \SystemRoot\System32\Config\SOFTWARE
Key name: CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902} (S)
Last updated: 2018-01-17 05:29:04 UTC+0000

Subkeys:
  (S) ATI Technologies
  (S) Classes
  (S) Clients
  (S) IM Providers
  (S) Microsoft
  (S) ODBC
  (S) Oracle
  (S) Policies
  (S) Python
  (S) RegisteredApplications
  (S) Sonic
  (S) Wow6432Node

Values:

Registry: \??\C:\System Volume Information\Syscache.hve
Key name: {f3f9f3c5-fb40-11e7-8e97-8cd02931979a} (S)
Last updated: 2018-04-06 23:12:58 UTC+0000

Subkeys:
  (S) DefaultObjectStore
```

```
Values:

Registry: \SystemRoot\System32\Config\SECURITY
Key name: CMI-CreateHive{0297523D-E529-4E42-8BE7-E1AABC063C84} (S)
Last updated: 2018-04-06 23:12:37 UTC+0000

Subkeys:
  (S) Policy
  (S) RXACT

Values:
---------------------------
Registry: \??\C:\Users\Win7\ntuser.dat
Key name: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC} (S)
Last updated: 2018-04-06 23:12:50 UTC+0000

Subkeys:
  (S) AppEvents
  (S) Console
  (S) Control Panel
  (S) Environment
  (S) EUDC
  (S) Identities
  (S) Keyboard Layout
  (S) Network
  (S) Printers
  (S) Software
  (S) System
  (V) Volatile Environment

Values:
---------------------------
Registry: \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
Key name: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC} (S)
Last updated: 2009-07-14 04:45:48 UTC+0000

Subkeys:
  (S) AppEvents
  (S) Console
  (S) Control Panel
  (S) Environment
  (S) EUDC
  (S) Network
  (S) Printers
  (S) Software
  (S) System
```

```
Values:
---------------------------
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: CMI-CreateHive{2A7FB991-7BBE-4F9D-B91E-7CB51D4737F5} (S)
Last updated: 2018-04-06 23:12:30 UTC+0000

Subkeys:
  (S) ControlSet001
  (S) ControlSet002
  (S) MountedDevices
  (S) RNG
  (S) Select
  (S) Setup
  (S) WPA
  (V) CurrentControlSet

Values:
---------------------------
Registry: [no name]
Key name: REGISTRY (S)
Last updated: 2018-04-06 23:12:30 UTC+0000

Subkeys:
  (S) A
  (S) MACHINE
  (S) USER

Values:
---------------------------
Registry: \SystemRoot\System32\Config\SAM
Key name: CMI-CreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7} (S)
Last updated: 2009-07-14 04:45:46 UTC+0000

Subkeys:
  (S) SAM

Values:
---------------------------
Registry: \??\C:\Users\Win7\AppData\Local\Microsoft\Windows\UsrClass.dat
Key name: S-1-5-21-183718623-120224881-1700316677-1000_Classes (S)
Last updated: 2018-01-17 04:49:09 UTC+0000

Subkeys:
  (S) Local Settings
```

When we reviewed these registries we see that \Device\HarddiskVolume1\Boot\BCD

Updated after start time of all of our suspicious process and also \SystemRoot\System32\Config\SECURITY updated after suspicious process 276,smss.exe and ??\C:\System Volume Information\Syscache.hve updated after suspicious process 1208 python.exe

To do more investigation related to subkeys and analysis in detail we are going under Software\Microsoft\Windows\Currentversio as follow:

University of Victoria

Volatility -f memory.dmp –profile=Win7SP0x64 printkey –K "Software\Microsoft\Windows\Currentversion"

```
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 printkey -K "Software\Microsoft\Windows\Current
Version"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
Key name: CurrentVersion (S)
Last updated: 2009-07-14 04:45:47 UTC+0000

Subkeys:
  (S) Explorer
  (S) Internet Settings
  (S) RADAR
  (S) Run
  (S) RunOnce
  (S) Screensavers
  (S) Sidebar
  (S) Telephony
  (S) WinTrust

Values:
----------------------------
Registry: \SystemRoot\System32\Config\DEFAULT
Key name: CurrentVersion (S)
Last updated: 2018-01-17 05:07:29 UTC+0000

Subkeys:
  (S) Explorer
  (S) Internet Settings
  (S) Media Center
  (S) Run
  (S) Shell Extensions
  (S) Telephony
  (S) ThemeManager
  (S) WinTrust

Values:
----------------------------
Registry: \??\C:\Users\Win7\ntuser.dat
Key name: CurrentVersion (S)
Last updated: 2018-04-06 23:13:37 UTC+0000
```

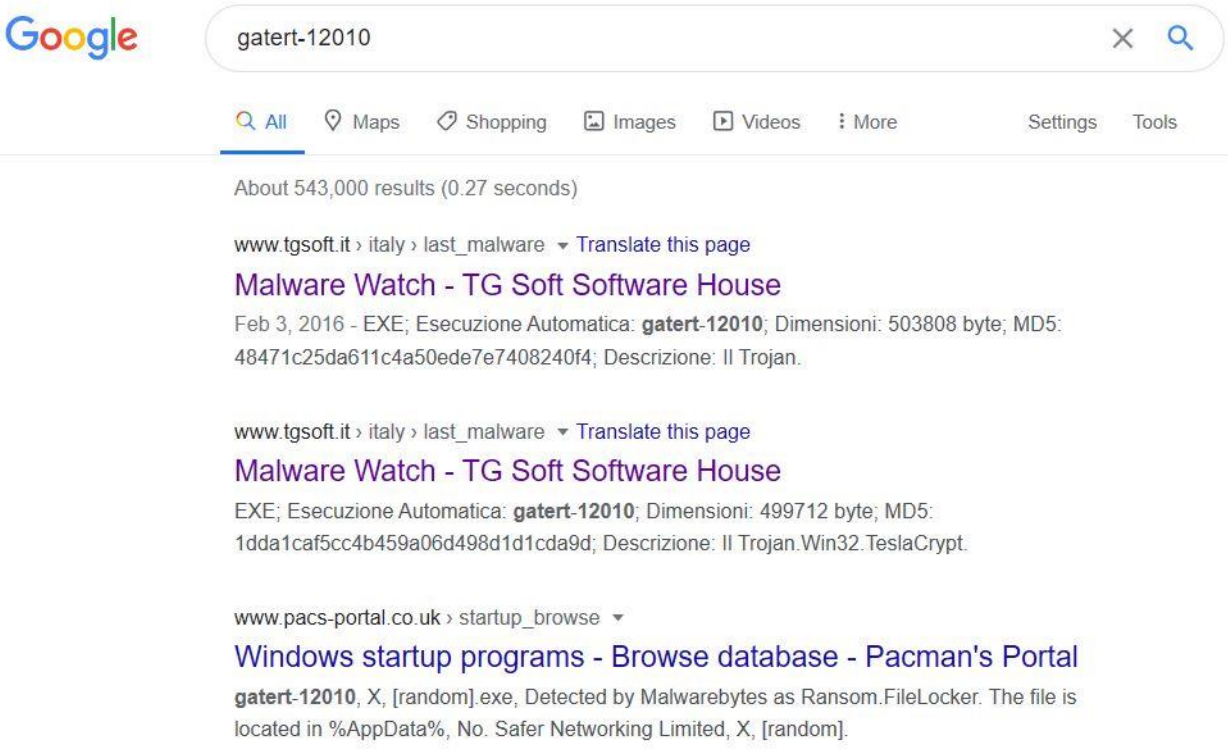
```
---------------------------
Registry: \??\C:\Users\Win7\ntuser.dat
Key name: CurrentVersion (S)
Last updated: 2018-04-06 23:13:37 UTC+0000

Subkeys:
  (S) Action Center
  (S) Applets
  (S) Controls Folder
  (S) Explorer
  (S) Ext
  (S) Group Policy
  (S) HomeGroup
  (S) ime
  (S) Internet Settings
  (S) MCT
  (S) NetCache
  (S) Policies
  (S) RADAR
  (S) Run
  (S) RunOnce
  (S) Screensavers
  (S) Shell Extensions
  (S) Sidebar
  (S) Telephony
  (S) ThemeManager
  (S) Themes
  (S) WinTrust
  (V) WindowsUpdate

Values:
---------------------------
Registry: \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
Key name: CurrentVersion (S)
Last updated: 2018-04-05 00:39:10 UTC+0000

Subkeys:
  (S) Explorer
  (S) ime
  (S) Internet Settings
  (S) RADAR
  (S) Run
  (S) RunOnce
  (S) Screensavers
  (S) Shell Extensions
  (S) Sidebar
  (S) Telephony
  (S) Themes
```

Software\Microsoft\Windows\CurrentVersion\Run, we see updated REG_SZ running exactly after suspicious processed at 2018-04-13 01:30:08, **aifkydk.exe**

```
REG_DWORD     EnableNegotiate : (S) 1
kali@kali:~/Desktop$ volatility -f memory.dmp --profile=Win7SP0x64 printkey -K "Software\Microsoft\Windows\Current
Version\Run"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
Key name: Run (S)
Last updated: 2009-07-14 04:45:47 UTC+0000

Subkeys:

Values:
REG_EXPAND_SZ Sidebar         : (S) %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun
----------------------------
Registry: \SystemRoot\System32\Config\DEFAULT
Key name: Run (S)
Last updated: 2018-01-17 04:46:32 UTC+0000

Subkeys:

Values:
----------------------------
Registry: \??\C:\Users\Win7\ntuser.dat
Key name: Run (S)
Last updated: 2018-04-13 01:30:08 UTC+0000

Subkeys:

Values:
REG_SZ        gatert-12010    : (S) C:\Users\Win7\AppData\Roaming\aifkydk.exe
Registry: \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
Key name: Run (S)
Last updated: 2009-07-14 04:45:48 UTC+0000

Subkeys:

Values:
REG_EXPAND_SZ Sidebar         : (S) %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun
```

and when we google gatertt- 12010 we see its malicious as follow.

University of Victoria



University of Victoria

Scheda malware: Trojan.Win32.TeslaCrypt.AT

Nome: Trojan.Win32.TeslaCrypt.AT
Tipologia: Trojan

Data: 03/02/2016
Nome file: COMBFNF.EXE
Esecuzione Automatica: gatert-12010
Dimensioni: 499712 byte
MD5: 1dda1caf5cc4b459a06d498d1d1cda9d
Descrizione:
Il Trojan.Win32.TeslaCrypt.AT si copia in %USERPROFILE%\DATI APPLICAZIONI\COMBFNF.EXE
Modifica la seguente chiave di registro:
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
[gatert-12010] = %USERPROFILE%\DATI APPLICAZIONI\COMBFNF.EXE
Note aggiuntive: Rimosso da **VirIT 8.1.3** e successivi.

Data: 03/02/2016
Nome file: BDJOSSG.EXE
Esecuzione Automatica: gatert-12010
Dimensioni: 491520 byte
MD5: a5e2a27e2b3c8956d28c82e5421a2a70
Descrizione:
Il Trojan.Win32.TeslaCrypt.AT si copia in %USERPROFILE%\APPDATA\ROAMING\BDJOSSG.EXE
Modifica la seguente chiave di registro:
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
[gatert-12010] = %USERPROFILE%\APPDATA\ROAMING\BDJOSSG.EXE
Note aggiuntive: Rimosso da **VirIT 8.1.3** e successivi.

Data: 03/02/2016
Nome file: EDXDDFC.EXE
Esecuzione Automatica: gatert-12010
Dimensioni: 778240 byte
MD5: 5a5f609caa38746f47a0790fb9ca3aec
Descrizione:
Il Trojan.Win32.TeslaCrypt.AT si copia in %USERPROFILE%\APPDATA\ROAMING\EDXDDFC.EXE
Modifica la seguente chiave di registro:
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
[gatert-12010] = %USERPROFILE%\APPDATA\ROAMING\EDXDDFC.EXE
Note aggiuntive: Rimosso da **VirIT 8.1.3** e successivi.
