CSEC 730 ADVANCED FORENSICS

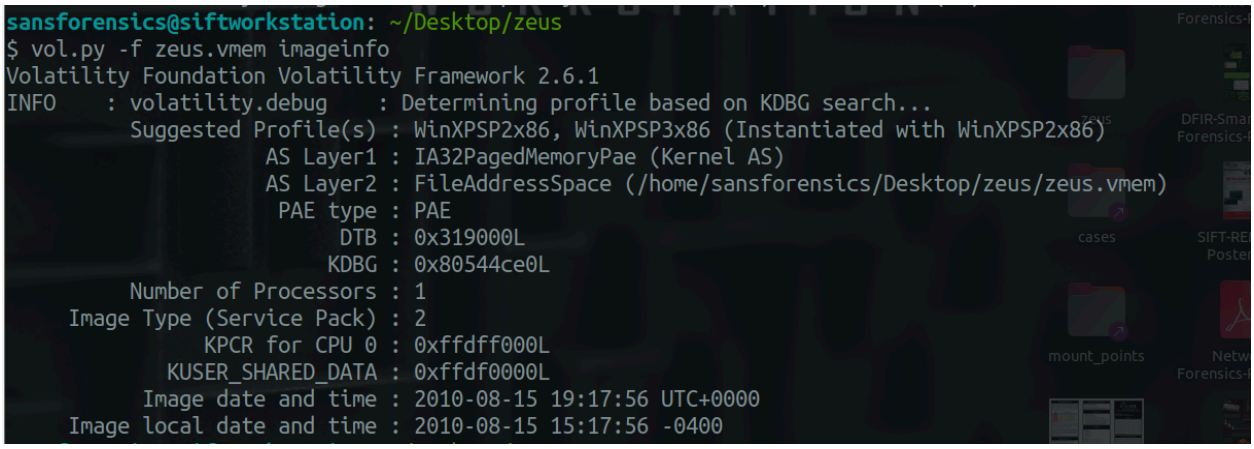
Name : Shriram Karpoora Sundara Pandian (KP)

Title : Homework 2

Part 1 : Windows Analysis with Volatility 2

1. What is the suggested type of OS and when was the sample collected ?

The OS type it suggested is WindXPSP2x86 (32 bit), WinXPSP3x86
It is created on 2019-08-15 19:17:56



2. Comparing *pslist* with *psscan*, which plugin walks through the doubly-linked list of EPROCESS pointed by PsActiveProcessHead? Which one does not rely on the doubly-list of EPROCESS and can detect unlinked (hidden) processes?

Pslist walks through the doubly linked list of EPROCESS and Rootkit can unlink the hidden process.

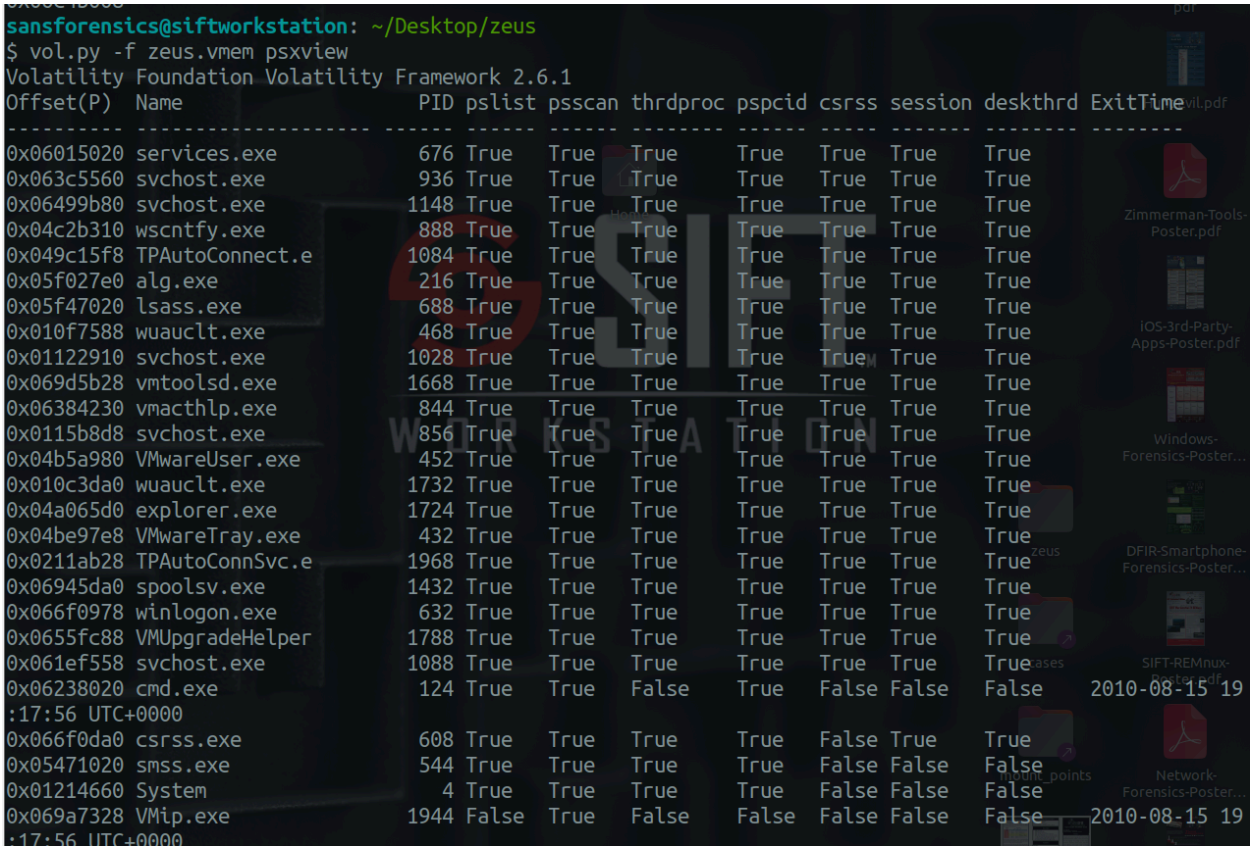
```
sansforensics@siftworkstation: ~/Desktop/zeus
$ vol.py -f zeus.vmem pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
  Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ----------
- ------------------------------
0x810b1660 System                    4      0     58      379 ------      0
0xff2ab020 smss.exe                544      4      3       21 ------      0 2010-08-11 06:06:21 UTC+0000
0xff1ecda0 csrss.exe               608    544     10      410      0      0 2010-08-11 06:06:23 UTC+0000
0xff1ec978 winlogon.exe            632    544     24      536      0      0 2010-08-11 06:06:23 UTC+0000
0xff247020 services.exe            676    632     16      288      0      0 2010-08-11 06:06:24 UTC+0000
0xff255020 lsass.exe               688    632     21      405      0      0 2010-08-11 06:06:24 UTC+0000
0xff218230 vmacthlp.exe            844    676      1       37      0      0 2010-08-11 06:06:24 UTC+0000
0x80ff88d8 svchost.exe             856    676     29      336      0      0 2010-08-11 06:06:24 UTC+0000
0xff217560 svchost.exe             936    676     11      288      0      0 2010-08-11 06:06:24 UTC+0000
0x80fbf910 svchost.exe            1028    676     88     1424      0      0 2010-08-11 06:06:24 UTC+0000
0xff22d558 svchost.exe            1088    676      7       93      0      0 2010-08-11 06:06:25 UTC+0000
0xff203b80 svchost.exe            1148    676     15      217      0      0 2010-08-11 06:06:26 UTC+0000
0xff1d7da0 spoolsv.exe            1432    676     14      145      0      0 2010-08-11 06:06:26 UTC+0000
0xff1b8b28 vmtoolsd.exe           1668    676      5      225      0      0 2010-08-11 06:06:35 UTC+0000
0xff1fdc88 VMUpgradeHelper        1788    676      5      112      0      0 2010-08-11 06:06:38 UTC+0000
0xff143b28 TPAutoConnSvc.e        1968    676      5      106      0      0 2010-08-11 06:06:39 UTC+0000
0xff25a7e0 alg.exe                 216    676      8      120      0      0 2010-08-11 06:06:39 UTC+0000
0xff364310 wscntfy.exe             888   1028      1       40      0      0 2010-08-11 06:06:49 UTC+0000
```

We can see the Process, no hidden link found

Psscan does not rely on DLL of EPROCESS.

```
sansforensics@siftworkstation: ~/Desktop/zeus
$ vol.py -f zeus.vmem psscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Name                PID   PPID PDB        Time created                   Time exited
------------------ ---------------- ------ ------ ---------- ------------------------------ ------------------
0x00000000010c3da0 wuauclt.exe        1732   1028 0x06cc02c0 2010-08-11 06:07:44 UTC+0000

0x00000000010f7588 wuauclt.exe         468   1028 0x06cc0180 2010-08-11 06:09:37 UTC+0000

0x0000000001122910 svchost.exe        1028    676 0x06cc0120 2010-08-11 06:06:24 UTC+0000

0x000000000115b8d8 svchost.exe         856    676 0x06cc00e0 2010-08-11 06:06:24 UTC+0000

0x0000000001214660 System                4      0 0x00319000

0x000000000211ab28 TPAutoConnSvc.e    1968    676 0x06cc0260 2010-08-11 06:06:39 UTC+0000

0x00000000049c15f8 TPAutoConnect.e    1084   1968 0x06cc0220 2010-08-11 06:06:52 UTC+0000

0x0000000004a065d0 explorer.exe       1724   1708 0x06cc0280 2010-08-11 06:09:29 UTC+0000

0x0000000004b5a980 VMwareUser.exe      452   1724 0x06cc0300 2010-08-11 06:09:32 UTC+0000

0x0000000004be97e8 VMwareTray.exe      432   1724 0x06cc02e0 2010-08-11 06:09:31 UTC+0000

0x0000000004c2b310 wscntfy.exe         888   1028 0x06cc0200 2010-08-11 06:06:49 UTC+0000

0x0000000005471020 smss.exe            544      4 0x06cc0020 2010-08-11 06:06:21 UTC+0000

0x0000000005f027e0 alg.exe             216    676 0x06cc0240 2010-08-11 06:06:39 UTC+0000

0x0000000005f47020 lsass.exe           688    632 0x06cc00a0 2010-08-11 06:06:24 UTC+0000

0x0000000006015020 services.exe        676    632 0x06cc0080 2010-08-11 06:06:24 UTC+0000

0x00000000061ef558 svchost.exe        1088    676 0x06cc0140 2010-08-11 06:06:25 UTC+0000

0x0000000006238020 cmd.exe             124   1668 0x06cc02a0 2010-08-15 19:17:55 UTC+0000   2010-08-15 19
:17:56 UTC+0000
0x0000000006384230 vmacthlp.exe        844    676 0x06cc00c0 2010-08-11 06:06:24 UTC+0000

0x00000000063c5560 svchost.exe         936    676 0x06cc0100 2010-08-11 06:06:24 UTC+0000

0x0000000006499b80 svchost.exe        1148    676 0x06cc0160 2010-08-11 06:06:26 UTC+0000
```

```
0x00000000069a7328 VMip.exe           1944    124 0x06cc0320 2010-08-15 19:17:55 UTC+0000   2010-08-15 19
:17:56 UTC+0000
0x00000000069d5b28 vmtoolsd.exe       1668    676 0x06cc01c0 2010-08-11 06:06:35 UTC+0000
```



```
sansforensics@siftworkstation: ~/Desktop/zeus
$ vol.py -f zeus.vmem psxview
Volatility Foundation Volatility Framework 2.6.1
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x06015020 services.exe            676 True   True   True     True   True  True    True
0x063c5560 svchost.exe             936 True   True   True     True   True  True    True
0x06499b80 svchost.exe            1148 True   True   True     True   True  True    True
0x04c2b310 wscntfy.exe             888 True   True   True     True   True  True    True
0x049c15f8 TPAutoConnect.e        1084 True   True   True     True   True  True    True
0x05f027e0 alg.exe                 216 True   True   True     True   True  True    True
0x05f47020 lsass.exe               688 True   True   True     True   True  True    True
0x010f7588 wuauclt.exe             468 True   True   True     True   True  True    True
0x01122910 svchost.exe            1028 True   True   True     True   True  True    True
0x069d5b28 vmtoolsd.exe           1668 True   True   True     True   True  True    True
0x06384230 vmacthlp.exe            844 True   True   True     True   True  True    True
0x0115b8d8 svchost.exe             856 True   True   True     True   True  True    True
0x04b5a980 VMwareUser.exe          452 True   True   True     True   True  True    True
0x010c3da0 wuauclt.exe            1732 True   True   True     True   True  True    True
0x04a065d0 explorer.exe           1724 True   True   True     True   True  True    True
0x04be97e8 VMwareTray.exe          432 True   True   True     True   True  True    True
0x0211ab28 TPAutoConnSvc.e        1968 True   True   True     True   True  True    True
0x06945da0 spoolsv.exe            1432 True   True   True     True   True  True    True
0x066f0978 winlogon.exe            632 True   True   True     True   True  True    True
0x0655fc88 VMUpgradeHelper        1788 True   True   True     True   True  True    True
0x061ef558 svchost.exe            1088 True   True   True     True   True  True    True
0x06238020 cmd.exe                 124 True   True   False    True   False False   False    2010-08-15 19
:17:56 UTC+0000
0x066f0da0 csrss.exe               608 True   True   True     True   False True    True
0x05471020 smss.exe                544 True   True   True     True   False False   False
0x01214660 System                    4 True   True   True     True   False False   False
0x069a7328 VMip.exe               1944 False  True   False    False  False False   False    2010-08-15 19
:17:56 UTC+0000
```

Here VMip.exe is a hidden link.

3. **Run *vol.py* using both *connections* and *connscan*. (Note: both *connections* and *connscan* do not work for Windows Vista and later version memory image. You will use plugin *netscan* instead)**

Do you see any active TCP connections or previous connections? Provide screenshots as your supporting data.

Which process made these TCP connections?

Using "whois RemoteAddress" to find out where the IP is located. Provide screenshots as your supporting data.

```
sansforensics@siftworkstation: ~/Desktop/zeus
$ vol.py -f zeus.vmem connections
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
sansforensics@siftworkstation: ~/Desktop/zeus
$ vol.py -f zeus.vmem connscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x02214988 172.16.176.143:1054       193.104.41.75:80          856
0x06015ab0 0.0.0.0:1056              193.104.41.75:80          856
```

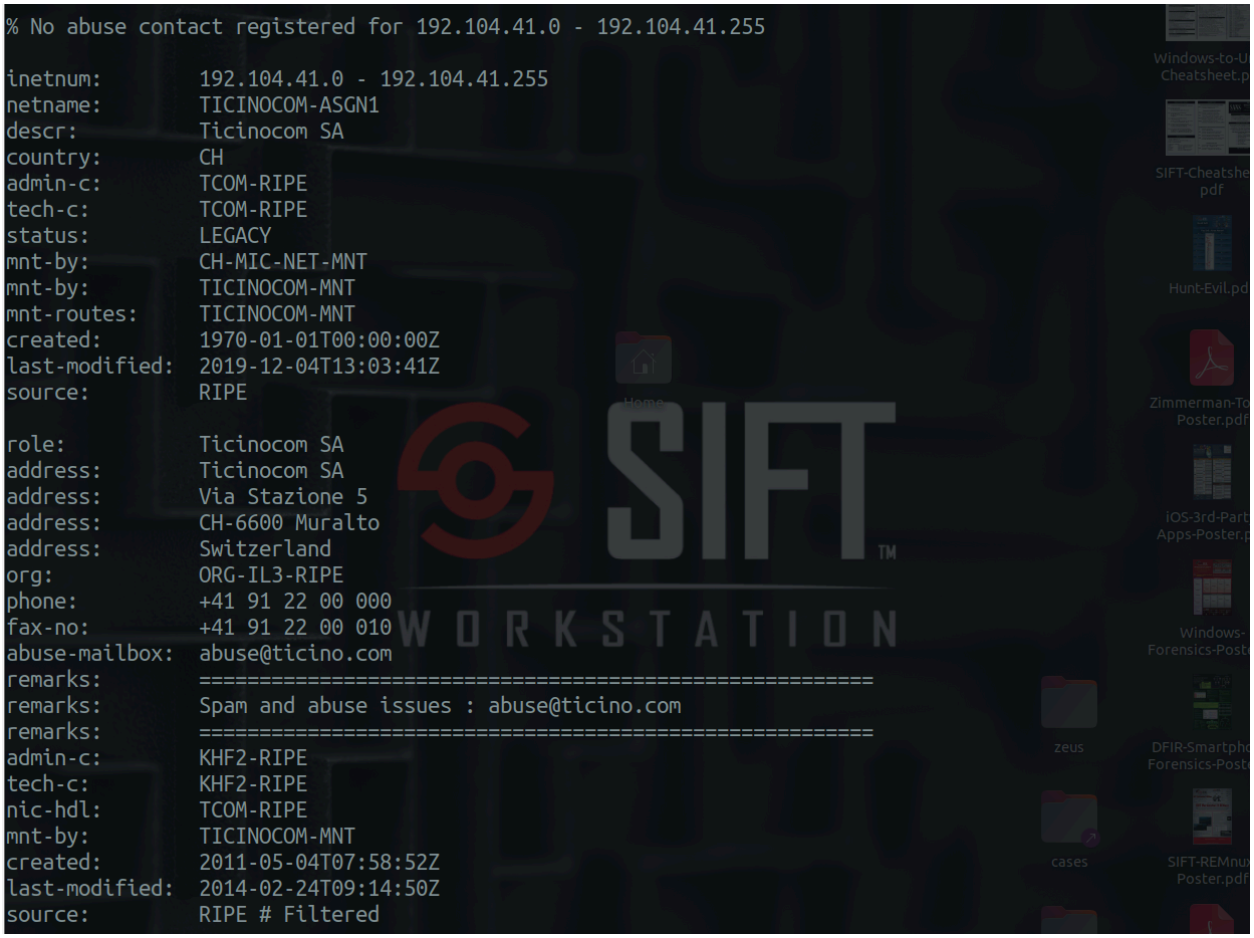
For connections, I didn't find any, but for the connscan we got one local and remote address.

```
0xff218230 vmacthlp.exe          844    676      1       37      0      0 2010-08-11 06:06:24 UTC+0000
0x80ff88d8 svchost.exe           856    676     29      336      0      0 2010-08-11 06:06:24 UTC+0000
0xff217560 svchost.exe           936    676     11      288      0      0 2010-08-11 06:06:24 UTC+0000
0x80fbf910 svchost.exe          1028    676     88     1424      0      0 2010-08-11 06:06:24 UTC+0000
```

856 PID belongs to svchost.exe began this connection.

Below is the location and details of the IP address

```
$ whois 192.104.41.75

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#


NetRange:       192.104.41.0 - 192.104.41.255
CIDR:           192.104.41.0/24
NetName:        RIPE-ERX-192-104-41-0
NetHandle:      NET-192-104-41-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        Early Registrations, Transferred to RIPE NCC
OriginAS:
Organization:   RIPE Network Coordination Centre (RIPE)
RegDate:        2005-02-28
Updated:        2005-02-28
Comment:        These addresses have been further assigned to users in
Comment:        the RIPE NCC region.  Contact information can be found in
Comment:        the RIPE database at http://www.ripe.net/whois
Ref:            https://rdap.arin.net/registry/ip/192.104.41.0

ResourceLink:  https://apps.db.ripe.net/search/query.html
ResourceLink:  whois.ripe.net


OrgName:        RIPE Network Coordination Centre
OrgId:          RIPE
Address:        P.O. Box 10096
City:           Amsterdam
StateProv:
PostalCode:     1001EB
Country:        NL
RegDate:
Updated:        2013-07-29
Ref:            https://rdap.arin.net/registry/entity/RIPE

ReferralServer:  whois://whois.ripe.net
ResourceLink:  https://apps.db.ripe.net/search/query.html
```


% No abuse contact registered for 192.104.41.0 - 192.104.41.255
inetnum: 192.104.41.0 - 192.104.41.255
netname: TICINOCOM-ASGN1
descr: Ticinocom SA
country: CH
admin-c: TCOM-RIPE
tech-c: TCOM-RIPE
status: LEGACY
mnt-by: CH-MIC-NET-MNT
mnt-by: TICINOCOM-MNT
mnt-routes: TICINOCOM-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2019-12-04T13:03:41Z
source: RIPE
role: Ticinocom SA
address: Ticinocom SA
address: Via Stazione 5
address: CH-6600 Muralto
address: Switzerland
org: ORG-IL3-RIPE
phone: +41 91 22 00 000
fax-no: +41 91 22 00 010
abuse-mailbox: abuse@ticino.com
remarks: ==========
remarks: Spam and abuse issues : abuse@ticino.com
remarks: ==========
admin-c: KHF2-RIPE
tech-c: KHF2-RIPE
nic-hdl: TCOM-RIPE
mnt-by: TICINOCOM-MNT
created: 2011-05-04T07:58:52Z
last-modified: 2014-02-24T09:14:50Z
source: RIPE # Filtered
SIFT
WORKSTATION
Home
zeus
cases

4.

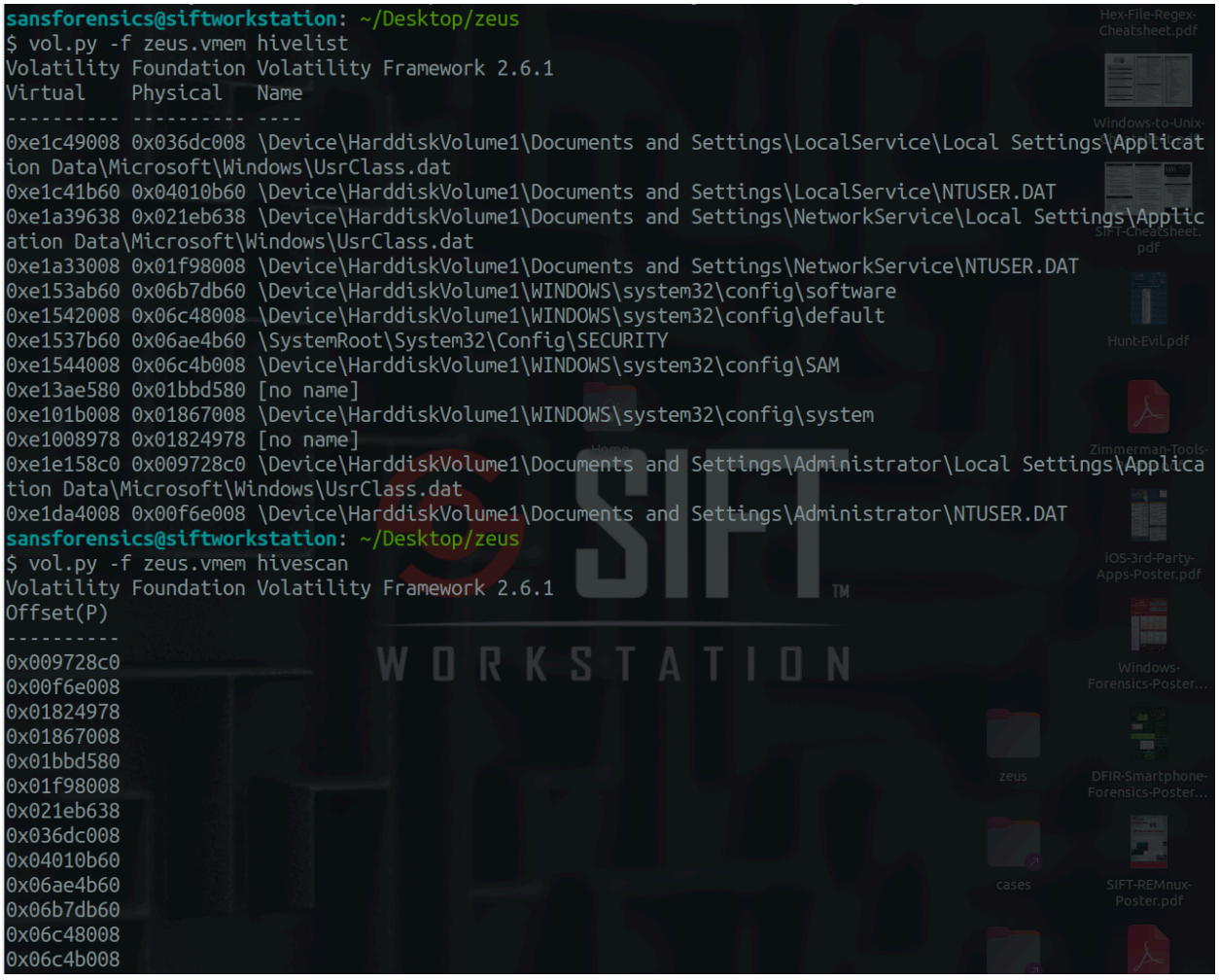
Run *vol.py –f zeus.vmem hivelist*, *vol.py –f zeus.vmem hivescan*, and *vol.py -f zeus.vmem printkey -K "Microsoft\Windows NT\CurrentVersion\Winlogon"*.

Which plugin shows the virtual addresses of registry hives in memory along with the full paths to the corresponding hive on disk? Provide screenshots as your supporting data.

The string '*Userinit*' specifies the executables that Winlogon runs after a user logs into Windows. The default executable is C:\windows\system32\userinit.exe which restores your profile, fonts, colors, etc. for your username. **It is possible to add additional executables to '*Userinit*' by separating the executables with a comma. It's a common place for trojans.** The *Userinit* entry is resided in *"Microsoft\Windows NT\CurrentVersion\Winlogon"*.

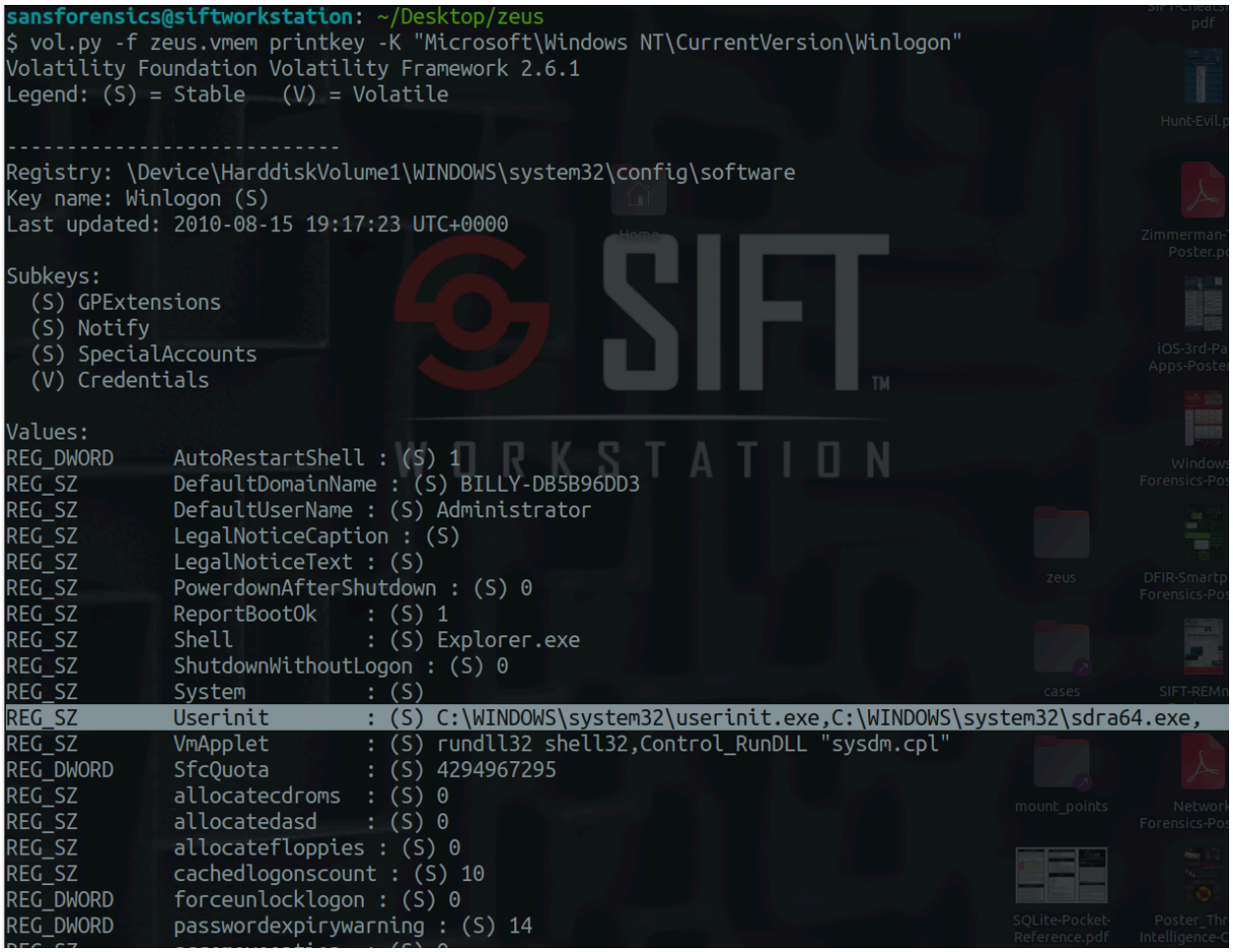
After you run *vol.py -f zeus.vmem printkey -K "Microsoft\Windows NT\CurrentVersion\Winlogon",* **Which** suspicious executable(s) do you see in *Userinit*? Provide screenshots as your supporting data.

We can see belo that **hivelist** shows the virtual address along with full paths corresponding hive on disk.


sansforensics@siftworkstation: ~/Desktop/zeus
$ vol.py -f zeus.vmem hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual Physical Name
---------- ---------- ----
0xe1c49008 0x036dc008 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1c41b60 0x04010b60 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe1a39638 0x021eb638 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1a33008 0x01f98008 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe153ab60 0x06b7db60 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1542008 0x06c48008 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe1537b60 0x06ae4b60 \SystemRoot\System32\Config\SECURITY
0xe1544008 0x06c4b008 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe13ae580 0x01bbd580 [no name]
0xe101b008 0x01867008 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe1008978 0x01824978 [no name]
0xe1e158c0 0x009728c0 \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1da4008 0x00f6e008 \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
sansforensics@siftworkstation: ~/Desktop/zeus
$ vol.py -f zeus.vmem hivescan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)

0x009728c0
0x00f6e008
0x01824978
0x01867008
0x01bbd580
0x01f98008
0x021eb638
0x036dc008
0x04010b60
0x06ae4b60
0x06b7db60
0x06c48008
0x06c4b008
SIFT
WORKSTATION
Hex-File-Regex-Cheatsheet.pdf
Windows-to-Unix-
SIFT-Cheatsheet.pdf
Hunt-Evil.pdf
Zimmerman-Tools-
iOS-3rd-Party-Apps-Poster.pdf
Windows-Forensics-Poster...
zeus
DFIR-Smartphone-Forensics-Poster...
cases
SIFT-REMnux-Poster.pdf

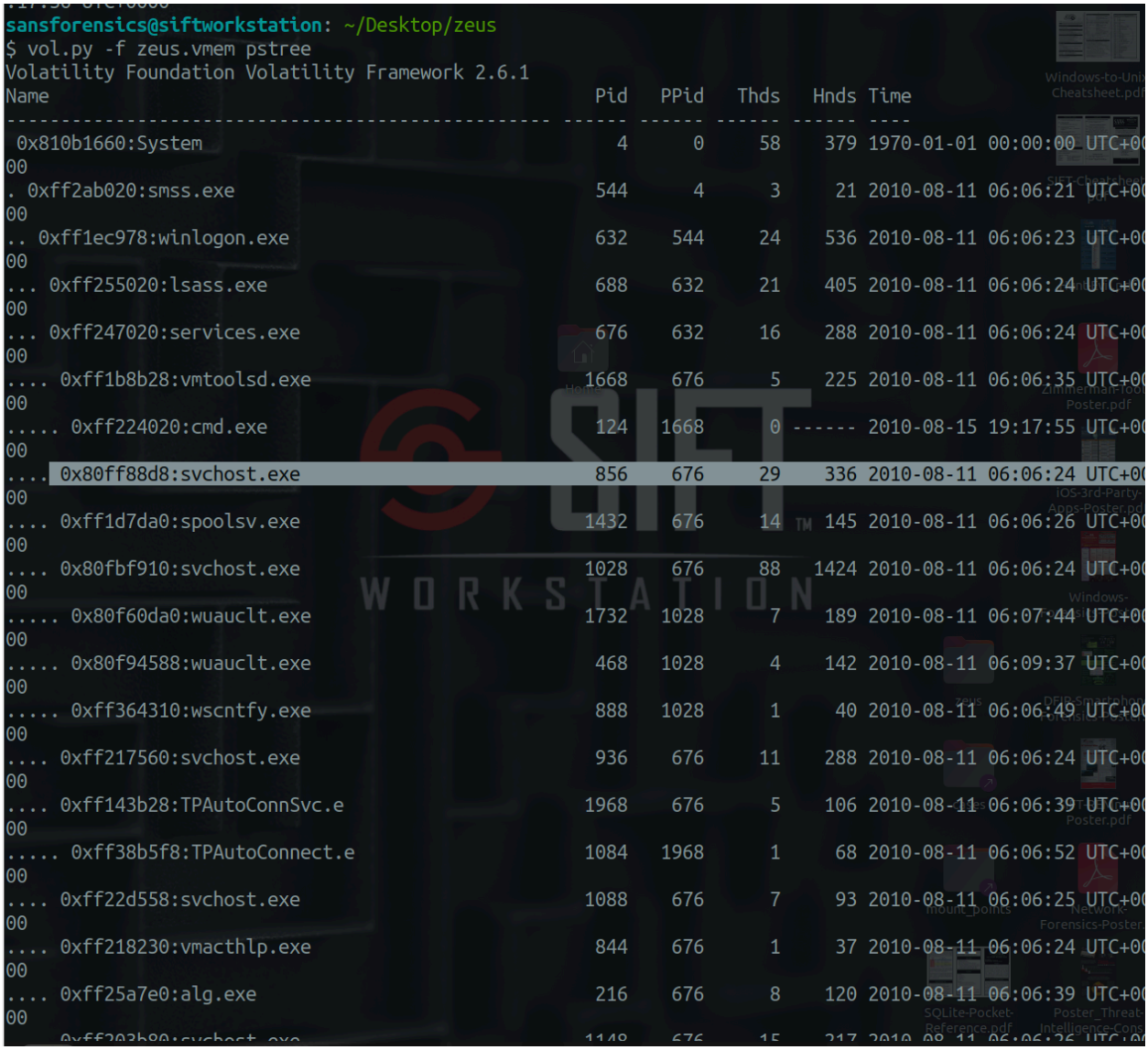
Also the suspicious executable is sdra64.exe



5. Run *vol.py* using the plugin, *pstree,* to view the process listing in tree form.

   Based on the results from Q3 and Q4 above, **what** can you conclude by analyzing Pid and PPid in the process tree list? (hint: which program launched the process that made the internet connection in Q3?). Provide screenshots as your supporting data.

From the Q3 and Q4 the process that made internet is svchost.exe executable :

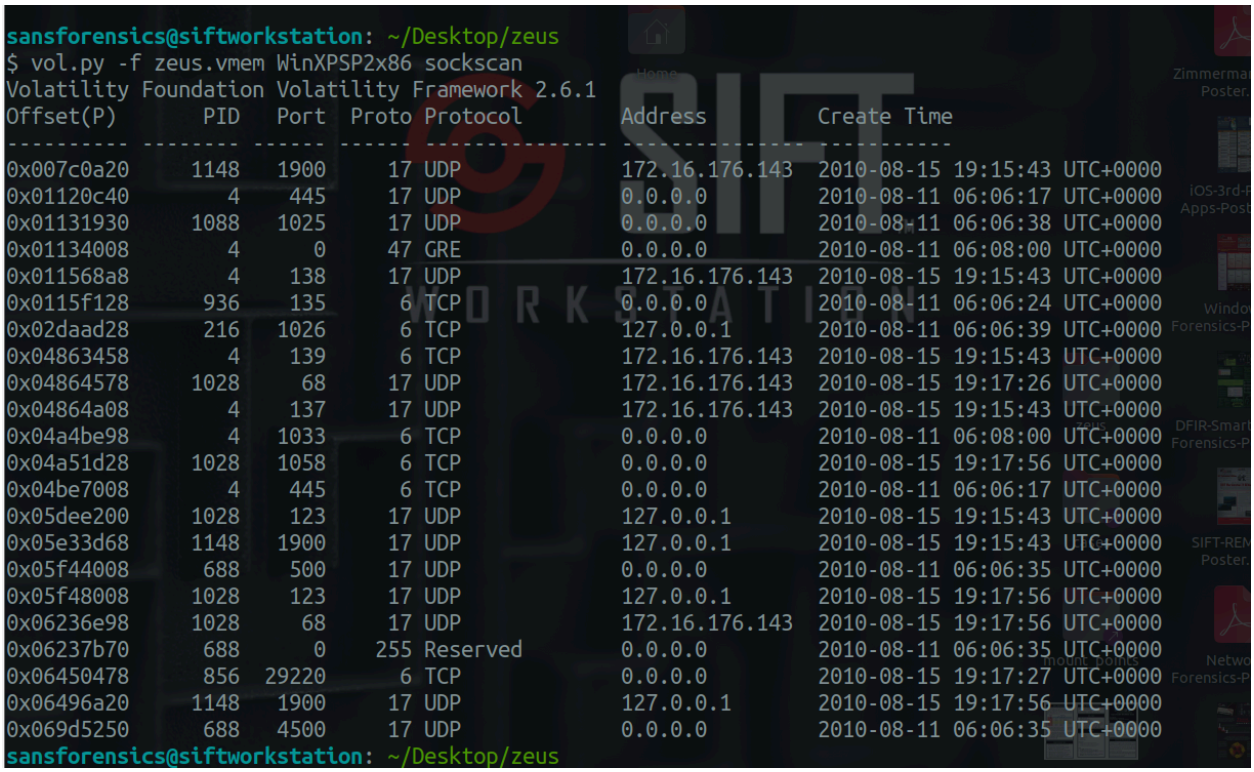


```
sansforensics@siftworkstation: ~/Desktop/zeus
$ vol.py -f zeus.vmem pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x810b1660:System                                      4      0     58    379 1970-01-01 00:00:00 UTC+00
00
. 0xff2ab020:smss.exe                                 544      4      3     21 2010-08-11 06:06:21 UTC+00
00
.. 0xff1ec978:winlogon.exe                            632    544     24    536 2010-08-11 06:06:23 UTC+00
00
... 0xff255020:lsass.exe                              688    632     21    405 2010-08-11 06:06:24 UTC+00
00
... 0xff247020:services.exe                           676    632     16    288 2010-08-11 06:06:24 UTC+00
00
.... 0xff1b8b28:vmtoolsd.exe                         1668    676      5    225 2010-08-11 06:06:35 UTC+00
00
..... 0xff224020:cmd.exe                              124   1668      0 ------ 2010-08-15 19:17:55 UTC+00
00
.... 0x80ff88d8:svchost.exe                           856    676     29    336 2010-08-11 06:06:24 UTC+00
00
.... 0xff1d7da0:spoolsv.exe                          1432    676     14    145 2010-08-11 06:06:26 UTC+00
00
.... 0x80fbf910:svchost.exe                          1028    676     88   1424 2010-08-11 06:06:24 UTC+00
00
..... 0x80f60da0:wuauclt.exe                         1732   1028      7    189 2010-08-11 06:07:44 UTC+00
00
..... 0x80f94588:wuauclt.exe                          468   1028      4    142 2010-08-11 06:09:37 UTC+00
00
..... 0xff364310:wscntfy.exe                          888   1028      1     40 2010-08-11 06:06:49 UTC+00
00
.... 0xff217560:svchost.exe                           936    676     11    288 2010-08-11 06:06:24 UTC+00
00
.... 0xff143b28:TPAutoConnSvc.e                      1968    676      5    106 2010-08-11 06:06:39 UTC+00
00
..... 0xff38b5f8:TPAutoConnect.e                     1084   1968      1     68 2010-08-11 06:06:52 UTC+00
00
.... 0xff22d558:svchost.exe                          1088    676      7     93 2010-08-11 06:06:25 UTC+00
00
.... 0xff218230:vmacthlp.exe                          844    676      1     37 2010-08-11 06:06:24 UTC+00
00
.... 0xff25a7e0:alg.exe                               216    676      8    120 2010-08-11 06:06:39 UTC+00
00
```

6. Try other plugins from the Windows volatility2 plugins at https://github.com/volatilityfoundation/volatility/wiki/Command-Reference or

https://github.com/volatilityfoundation/volatility/wiki/Command-Reference-Mal. show me at least two other plugins that provide you interesting results.

We can see the active TCP connection from this plugin “sockscan”



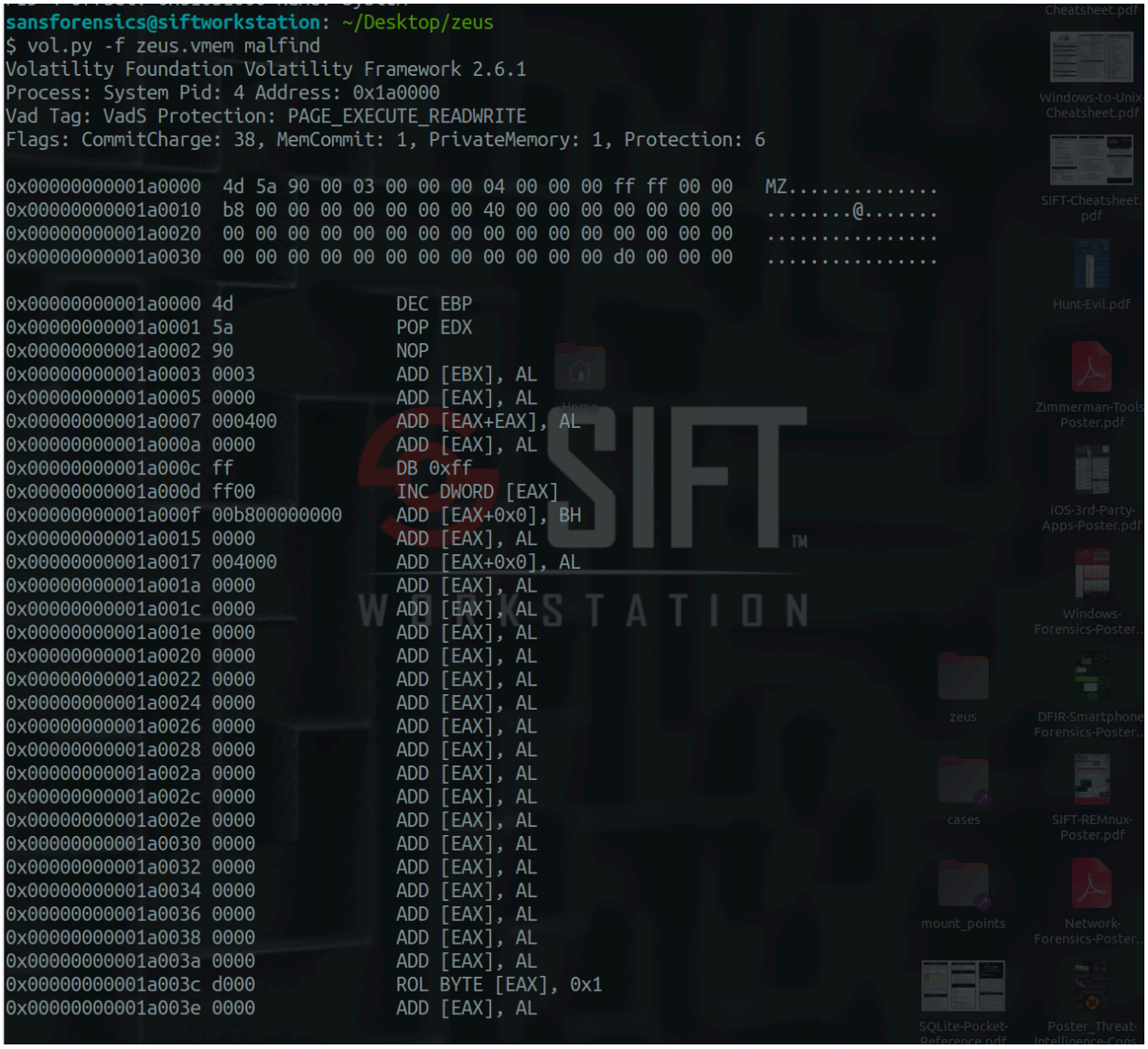
```
sansforensics@siftworkstation: ~/Desktop/zeus
$ vol.py -f zeus.vmem WinXPSP2x86 sockscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ -------------- --------------- -----------
0x007c0a20     1148   1900     17 UDP            172.16.176.143  2010-08-15 19:15:43 UTC+0000
0x01120c40        4    445     17 UDP            0.0.0.0         2010-08-11 06:06:17 UTC+0000
0x01131930     1088   1025     17 UDP            0.0.0.0         2010-08-11 06:06:38 UTC+0000
0x01134008        4      0     47 GRE            0.0.0.0         2010-08-11 06:08:00 UTC+0000
0x011568a8        4    138     17 UDP            172.16.176.143  2010-08-15 19:15:43 UTC+0000
0x0115f128      936    135      6 TCP            0.0.0.0         2010-08-11 06:06:24 UTC+0000
0x02daad28      216   1026      6 TCP            127.0.0.1       2010-08-11 06:06:39 UTC+0000
0x04863458        4    139      6 TCP            172.16.176.143  2010-08-15 19:15:43 UTC+0000
0x04864578     1028     68     17 UDP            172.16.176.143  2010-08-15 19:17:26 UTC+0000
0x04864a08        4    137     17 UDP            172.16.176.143  2010-08-15 19:15:43 UTC+0000
0x04a4be98        4   1033      6 TCP            0.0.0.0         2010-08-11 06:08:00 UTC+0000
0x04a51d28     1028   1058      6 TCP            0.0.0.0         2010-08-15 19:17:56 UTC+0000
0x04be7008        4    445      6 TCP            0.0.0.0         2010-08-11 06:06:17 UTC+0000
0x05dee200     1028    123     17 UDP            127.0.0.1       2010-08-15 19:15:43 UTC+0000
0x05e33d68     1148   1900     17 UDP            127.0.0.1       2010-08-15 19:15:43 UTC+0000
0x05f44008      688    500     17 UDP            0.0.0.0         2010-08-11 06:06:35 UTC+0000
0x05f48008     1028    123     17 UDP            127.0.0.1       2010-08-15 19:17:56 UTC+0000
0x06236e98     1028     68     17 UDP            172.16.176.143  2010-08-15 19:17:56 UTC+0000
0x06237b70      688      0    255 Reserved       0.0.0.0         2010-08-11 06:06:35 UTC+0000
0x06450478      856  29220      6 TCP            0.0.0.0         2010-08-15 19:17:27 UTC+0000
0x06496a20     1148   1900     17 UDP            127.0.0.1       2010-08-15 19:17:56 UTC+0000
0x069d5250      688   4500     17 UDP            0.0.0.0         2010-08-11 06:06:35 UTC+0000
sansforensics@siftworkstation: ~/Desktop/zeus
```

And PID 856 is one of the connection through TCP handshake.

Second one is “malprocfind” and surprisingly the first process has PID 856

```
sansforensics@siftworkstation: ~/Desktop/zeus
$ vol.py -f zeus.vmem WinXPSP2x86 malprocfind
Volatility Foundation Volatility Framework 2.6.1
Offset     ProcessName     PID   PPID  Name  Path  Priority  Cmdline User  Sess  Time  CMD   PHollow SPat
h
---------- -------------- ----- ----- ----- ----- --------- ------- ----- ----- ----- ----- ------- ----
-
0x80ff88d8 svchost.exe       856 True  True  True  True      True    True  True  True  True  True    True

0xff1d7da0 spoolsv.exe      1432 True  True  True  True      True    True  True  True  True  True    True

0x810b1660 system              4 True  True  True  True      True    True  None  True  True  True    True

0x80fbf910 svchost.exe      1028 True  True  True  True      True    True  True  True  True  True    True

0xff2ab020 smss.exe          544 True  True  True  True      True    True  None  True  True  False   True

0xff255020 lsass.exe         688 True  True  True  True      True    True  True  True  True  True    True

0xff247020 services.exe      676 True  True  True  True      True    True  True  True  True  True    True

0xff217560 svchost.exe       936 True  True  True  True      True    True  True  True  True  True    True

0xff22d558 svchost.exe      1088 True  True  True  True      True    True  True  True  True  True    True

0xff3865d0 explorer.exe     1724 True  True  True  True      True    True  True  True  True  True    True

0xff1ec978 winlogon.exe      632 True  True  True  True      True    True  True  True  True  True    True

0xff1ecda0 csrss.exe         608 True  True  True  True      True    True  True  True  True  False   True

0xff203b80 svchost.exe      1148 True  True  True  True      True    True  True  True  True  True    True


Unusual process counts:
-----------------------

Processes without running parent process:
-----------------------------------------
PID 1724 Offset: 0xff3865d0 Name: explorer.exe
PID 4 Offset: 0x810b1660 Name: System
```

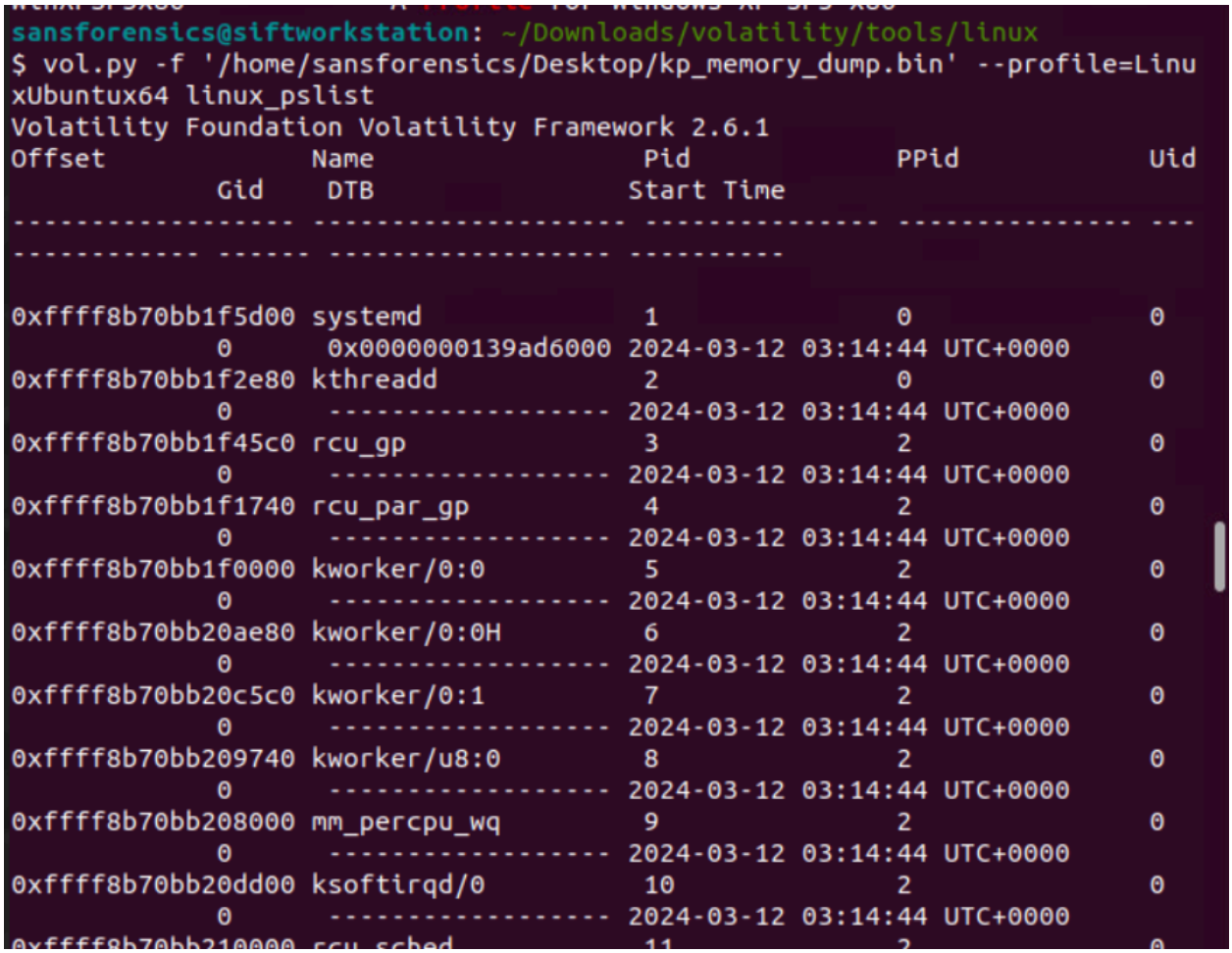
7.


sansforensics@siftworkstation: ~/Desktop/zeus
$ vol.py -f zeus.vmem malfind
Volatility Foundation Volatility Framework 2.6.1
Process: System Pid: 4 Address: 0x1a0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 38, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x00000000001a0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
0x00000000001a0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@.......
0x00000000001a0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000000001a0030 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 ....
0x00000000001a0000 4d DEC EBP
0x00000000001a0001 5a POP EDX
0x00000000001a0002 90 NOP
0x00000000001a0003 0003 ADD [EBX], AL
0x00000000001a0005 0000 ADD [EAX], AL
0x00000000001a0007 000400 ADD [EAX+EAX], AL
0x00000000001a000a 0000 ADD [EAX], AL
0x00000000001a000c ff DB 0xff
0x00000000001a000d ff00 INC DWORD [EAX]
0x00000000001a000f 00b800000000 ADD [EAX+0x0], BH
0x00000000001a0015 0000 ADD [EAX], AL
0x00000000001a0017 004000 ADD [EAX+0x0], AL
0x00000000001a001a 0000 ADD [EAX], AL
0x00000000001a001c 0000 ADD [EAX], AL
0x00000000001a001e 0000 ADD [EAX], AL
0x00000000001a0020 0000 ADD [EAX], AL
0x00000000001a0022 0000 ADD [EAX], AL
0x00000000001a0024 0000 ADD [EAX], AL
0x00000000001a0026 0000 ADD [EAX], AL
0x00000000001a0028 0000 ADD [EAX], AL
0x00000000001a002a 0000 ADD [EAX], AL
0x00000000001a002c 0000 ADD [EAX], AL
0x00000000001a002e 0000 ADD [EAX], AL
0x00000000001a0030 0000 ADD [EAX], AL
0x00000000001a0032 0000 ADD [EAX], AL
0x00000000001a0034 0000 ADD [EAX], AL
0x00000000001a0036 0000 ADD [EAX], AL
0x00000000001a0038 0000 ADD [EAX], AL
0x00000000001a003a 0000 ADD [EAX], AL
0x00000000001a003c d000 ROL BYTE [EAX], 0x1
0x00000000001a003e 0000 ADD [EAX], AL
Cheatsheet.pdf
Windows-to-Unix-Cheatsheet.pdf
SIFT-Cheatsheet.pdf
Hunt-Evil.pdf
Zimmerman-Tools-Poster.pdf
iOS-3rd-Party-Apps-Poster.pdf
Windows-Forensics-Poster..
DFIR-Smartphone-Forensics-Poster..
SIFT-REMnux-Poster.pdf
Network-Forensics-Poster..
Poster_Threat-Intelligence-Cons..
SQLite-Pocket-Reference.pdf
Home
zeus
cases
mount_points
SIFT
WORKSTATION

```
Process: lsass.exe Pid: 688 Address: 0xad0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000000ad0000  b8 35 00 00 00 e9 cd d7 e3 7b b8 91 00 00 00 e9   .5.......{......
0x0000000000ad0010  4f df e3 7b 8b ff 55 8b ec e9 ef 17 74 76 8b ff   O..{..U.....tv..
0x0000000000ad0020  55 8b ec e9 95 76 6f 76 8b ff 55 8b ec e9 be 53   U....vov..U....S
0x0000000000ad0030  70 76 8b ff 55 8b ec e9 d6 18 74 76 8b ff 55 8b   pv..U.....tv..U.

0x0000000000ad0000 b835000000       MOV EAX, 0x35
0x0000000000ad0005 e9cdd7e37b       JMP 0x7c90d7d7
0x0000000000ad000a b891000000       MOV EAX, 0x91
0x0000000000ad000f e94fdfe37b       JMP 0x7c90df63
0x0000000000ad0014 8bff             MOV EDI, EDI
0x0000000000ad0016 55               PUSH EBP
0x0000000000ad0017 8bec             MOV EBP, ESP
0x0000000000ad0019 e9ef177476       JMP 0x7721180d
0x0000000000ad001e 8bff             MOV EDI, EDI
0x0000000000ad0020 55               PUSH EBP
0x0000000000ad0021 8bec             MOV EBP, ESP
0x0000000000ad0023 e995766f76       JMP 0x771c76bd
0x0000000000ad0028 8bff             MOV EDI, EDI
0x0000000000ad002a 55               PUSH EBP
0x0000000000ad002b 8bec             MOV EBP, ESP
0x0000000000ad002d e9be537076       JMP 0x771d53f0
0x0000000000ad0032 8bff             MOV EDI, EDI
0x0000000000ad0034 55               PUSH EBP
0x0000000000ad0035 8bec             MOV EBP, ESP
0x0000000000ad0037 e9d6187476       JMP 0x77211912
0x0000000000ad003c 8bff             MOV EDI, EDI
0x0000000000ad003e 55               PUSH EBP
0x0000000000ad003f 8b               DB 0x8b
```

Part 2 : Linux Memory Analysis using Volatility 2

linux_pslist



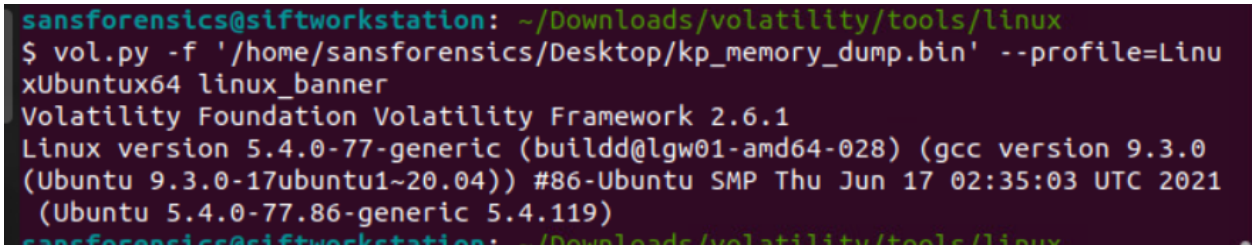
Linux_bash : Previous Commands

```
$ vol.py -f '/home/sansforensics/Desktop/kp_memory_dump.bin' --profile=Linu
xUbuntux64 linux_bash
Volatility Foundation Volatility Framework 2.6.1
Pid      Name                 Command Time                   Command
-------- -------------------- ------------------------------ -------
    2222 bash                 2024-03-12 03:19:01 UTC+0000   cat /etc/sift-
version
    2222 bash                 2024-03-12 03:19:01 UTC+0000   @????U
    2222 bash                 2024-03-12 03:19:01 UTC+0000   cd Desktop/
    2222 bash                 2024-03-12 03:19:01 UTC+0000   exit
    2222 bash                 2024-03-12 03:19:01 UTC+0000   mkdir SIFT Ima
ges
    2222 bash                 2024-03-12 03:19:01 UTC+0000   ls
    2222 bash                 2024-03-12 03:19:01 UTC+0000   ls
    2222 bash                 2024-03-12 03:19:01 UTC+0000   rmdir Images
    2222 bash                 2024-03-12 03:19:01 UTC+0000   scp student@19
2.168.201.100:~/SIFT\ Images/* .
    2222 bash                 2024-03-12 03:19:01 UTC+0000   cd SIFT-Images
/
    2222 bash                 2024-03-12 03:19:01 UTC+0000   scp student@19
2.168.201.100:/home/student/SIFT-Images/* .
    2222 bash                 2024-03-12 03:19:01 UTC+0000   mv SIFT SIFT-I
mages
    2222 bash                 2024-03-12 03:19:01 UTC+0000   scp student@19
2.168.201.100:~/'SIFT Images'/* .
    2222 bash                 2024-03-12 03:19:45 UTC+0000   cd Desktop
    2222 bash                 2024-03-12 03:20:03 UTC+0000   git clone http
s://github.com/504ensicsLabs/LiME.git
    2222 bash                 2024-03-12 03:20:11 UTC+0000   cd LiME/src
    2222 bash                 2024-03-12 03:20:14 UTC+0000   make
    2222 bash                 2024-03-12 03:21:18 UTC+0000   sudo insmod li
```

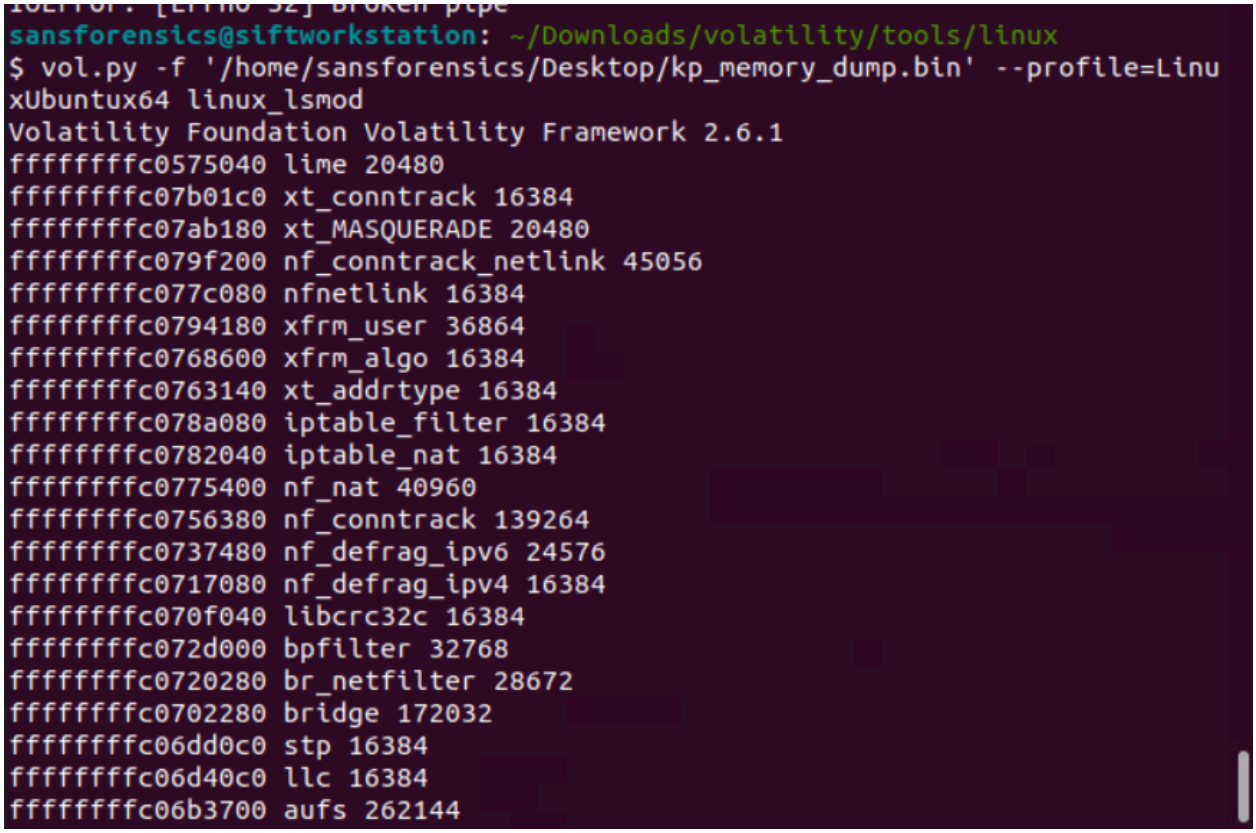
Linux_netstat : Statistics about the network.

```
sansforensics@siftworkstation: ~/Downloads/volatility/tools/linux
$ vol.py -f '/home/sansforensics/Desktop/kp_memory_dump.bin' --profile=Linu
xUbuntux64 linux_netstat | head
Volatility Foundation Volatility Framework 2.6.1
UNIX 32565              systemd/1     /run/systemd/journal/stdout
UNIX 16723              systemd/1     /run/systemd/notify
UNIX 16724              systemd/1
UNIX 16725              systemd/1
UNIX 16726              systemd/1     /run/systemd/private
UNIX 16728              systemd/1     /run/systemd/userdb/io.systemd.Dynami
cUser
UNIX 32566              systemd/1     /run/systemd/journal/stdout
UNIX 41423              systemd/1     /run/systemd/journal/stdout
UNIX 40520              systemd/1     /run/systemd/journal/stdout
UNIX 16737              systemd/1     /run/systemd/journal/syslog
```

Linux_Banner : Shows about the linux version.

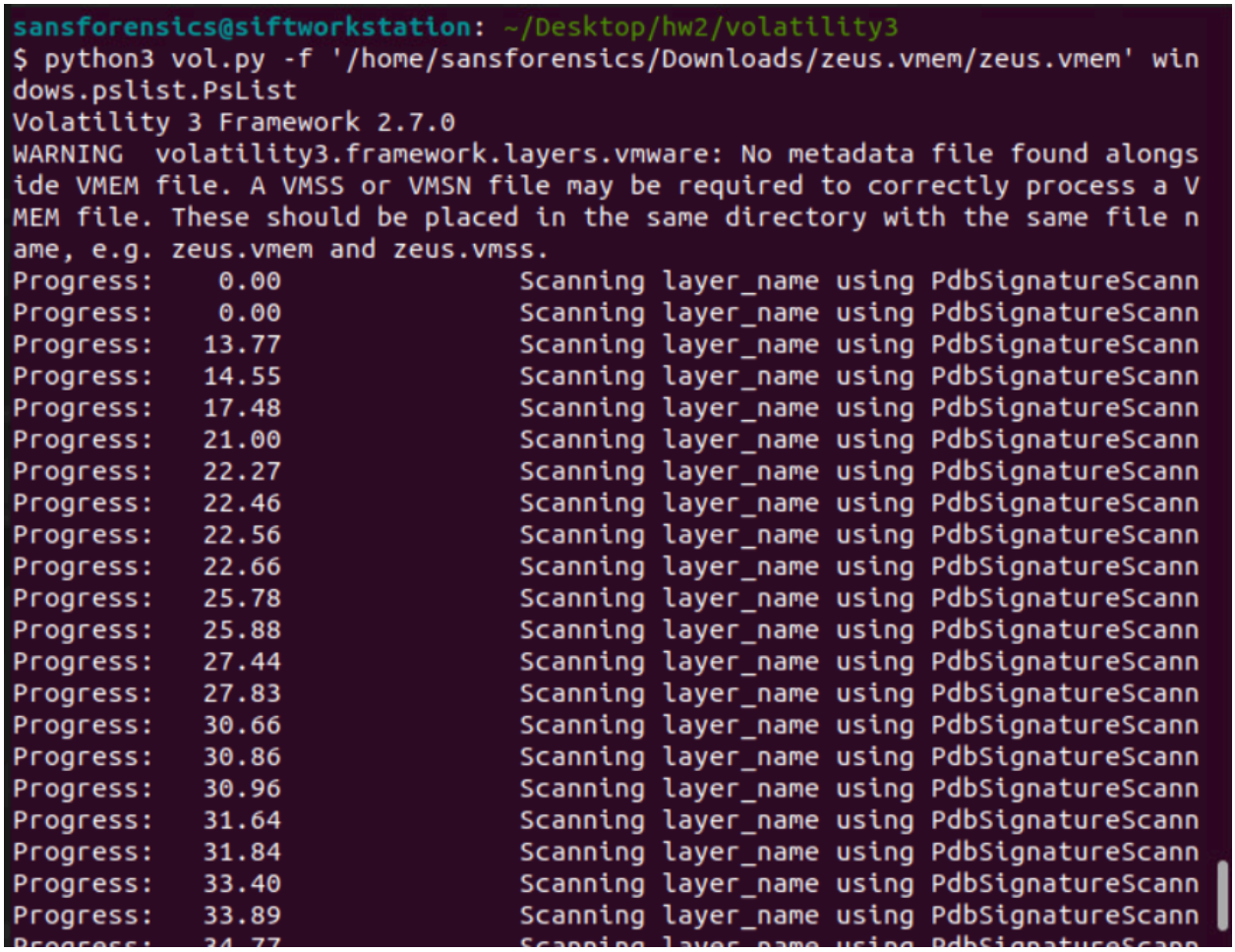


Linux_lsmod :



Part 3 : Volatility 3 and windows Plugins

windows.pslist.PsList



```
sansforensics@siftworkstation: ~/Desktop/hw2/volatility3
$ python3 vol.py -f '/home/sansforensics/Downloads/zeus.vmem/zeus.vmem' win
dows.pslist.PsList
Volatility 3 Framework 2.7.0
WARNING  volatility3.framework.layers.vmware: No metadata file found alongs
ide VMEM file. A VMSS or VMSN file may be required to correctly process a V
MEM file. These should be placed in the same directory with the same file n
ame, e.g. zeus.vmem and zeus.vmss.
Progress:    0.00               Scanning layer_name using PdbSignatureScann
Progress:    0.00               Scanning layer_name using PdbSignatureScann
Progress:   13.77               Scanning layer_name using PdbSignatureScann
Progress:   14.55               Scanning layer_name using PdbSignatureScann
Progress:   17.48               Scanning layer_name using PdbSignatureScann
Progress:   21.00               Scanning layer_name using PdbSignatureScann
Progress:   22.27               Scanning layer_name using PdbSignatureScann
Progress:   22.46               Scanning layer_name using PdbSignatureScann
Progress:   22.56               Scanning layer_name using PdbSignatureScann
Progress:   22.66               Scanning layer_name using PdbSignatureScann
Progress:   25.78               Scanning layer_name using PdbSignatureScann
Progress:   25.88               Scanning layer_name using PdbSignatureScann
Progress:   27.44               Scanning layer_name using PdbSignatureScann
Progress:   27.83               Scanning layer_name using PdbSignatureScann
Progress:   30.66               Scanning layer_name using PdbSignatureScann
Progress:   30.86               Scanning layer_name using PdbSignatureScann
Progress:   30.96               Scanning layer_name using PdbSignatureScann
Progress:   31.64               Scanning layer_name using PdbSignatureScann
Progress:   31.84               Scanning layer_name using PdbSignatureScann
Progress:   33.40               Scanning layer_name using PdbSignatureScann
Progress:   33.89               Scanning layer_name using PdbSignatureScann
```

```
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId W
ow64    CreateTime      ExitTime        File output

4       0       System  0x810b1660      58      379     N/A     False   N/A
N/A     Disabled
544     4       smss.exe        0xff2ab020      3       21      N/A     Fal
se      2010-08-11 06:06:21.000000      N/A     Disabled
608     544     csrss.exe       0xff1ecda0      10      410     0       Fal
se      2010-08-11 06:06:23.000000      N/A     Disabled
632     544     winlogon.exe    0xff1ec978      24      536     0       Fal
se      2010-08-11 06:06:23.000000      N/A     Disabled
676     632     services.exe    0xff247020      16      288     0       Fal
se      2010-08-11 06:06:24.000000      N/A     Disabled
688     632     lsass.exe       0xff255020      21      405     0       Fal
se      2010-08-11 06:06:24.000000      N/A     Disabled
844     676     vmacthlp.exe    0xff218230      1       37      0       Fal
se      2010-08-11 06:06:24.000000      N/A     Disabled
856     676     svchost.exe     0x80ff88d8      29      336     0       Fal
se      2010-08-11 06:06:24.000000      N/A     Disabled
936     676     svchost.exe     0xff217560      11      288     0       Fal
se      2010-08-11 06:06:24.000000      N/A     Disabled
1028    676     svchost.exe     0x80fbf910      88      1424    0       Fal
se      2010-08-11 06:06:24.000000      N/A     Disabled
1088    676     svchost.exe     0xff22d558      7       93      0       Fal
se      2010-08-11 06:06:25.000000      N/A     Disabled
```

windows.psscan.PsScan

```
sansforensics@siftworkstation: ~/Desktop/hw2/volatility3
$ python3 vol.py -f '/home/sansforensics/Downloads/zeus.vmem/zeus.vmem' win
dows.psscan.PsScan
Volatility 3 Framework 2.7.0
WARNING  volatility3.framework.layers.vmware: No metadata file found alongs
ide VMEM file. A VMSS or VMSN file may be required to correctly process a V
MEM file. These should be placed in the same directory with the same file n
ame, e.g. zeus.vmem and zeus.vmss.
```

```
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId W
ow64    CreateTime      ExitTime        File output

1732    1028    wuauclt.exe     0x10c3da0       7       189     0       Fal
se      2010-08-11 06:07:44.000000      N/A     Disabled
468     1028    wuauclt.exe     0x10f7588       4       142     0       Fal
se      2010-08-11 06:09:37.000000      N/A     Disabled
1028    676     svchost.exe     0x1122910       88      1424    0       Fal
se      2010-08-11 06:06:24.000000      N/A     Disabled
856     676     svchost.exe     0x115b8d8       29      336     0       Fal
se      2010-08-11 06:06:24.000000      N/A     Disabled
4       0       System  0x1214660       58      379     N/A     False   N/A
N/A     Disabled
1968    676     TPAutoConnSvc.e 0x211ab28       5       106     0       Fal
se      2010-08-11 06:06:39.000000      N/A     Disabled
1084    1968    TPAutoConnect.e 0x49c15f8       1       68      0       Fal
se      2010-08-11 06:06:52.000000      N/A     Disabled
1724    1708    explorer.exe    0x4a065d0       13      326     0       Fal
se      2010-08-11 06:09:29.000000      N/A     Disabled
452     1724    VMwareUser.exe  0x4b5a980       8       207     0       Fal
se      2010-08-11 06:09:32.000000      N/A     Disabled
432     1724    VMwareTray.exe  0x4be97e8       1       60      0       Fal
se      2010-08-11 06:09:31.000000      N/A     Disabled
888     1028    wscntfy.exe     0x4c2b310       1       40      0       Fal
se      2010-08-11 06:06:49.000000      N/A     Disabled
544     4       smss.exe        0x5471020       3       21      N/A     Fal
se      2010-08-11 06:06:21.000000      N/A     Disabled
1699873240      1182038117      tCharacterPlacem        0x55b47fc       195
```

windows.registry.userassist.UserAssist

```
$ python3 vol.py -f '/home/sansforensics/Downloads/zeus.vmem/zeus.vmem' win
dows.registry.userassist.UserAssist
Volatility 3 Framework 2.7.0
WARNING  volatility3.framework.layers.vmware: No metadata file found alongs
ide VMEM file. A VMSS or VMSN file may be required to correctly process a V
MEM file. These should be placed in the same directory with the same file n
ame, e.g. zeus.vmem and zeus.vmss.
```

```
Hive Offset     Hive Name       Path    Last Write Time Type    Name    IDC
ount    Focus Count     Time Focused    Last Updated    Raw Data

0xe1da4008      \Device\HarddiskVolume1\Documents and Settings\Administrato
r\NTUSER.DAT    NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explor
er\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count      2010-06-10
16:11:44.000000         Key     N/A     N/A     N/A     N/A     N/A     N/A
N/A
* 0xe1da4008    \Device\HarddiskVolume1\Documents and Settings\Administrato
r\NTUSER.DAT    NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explor
er\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count      2010-06-10
16:11:44.000000         Value   UEME_CTLSESSION -       -       -       - -
00 00 00 00 00 00 00 00 ........
0xe1da4008      \Device\HarddiskVolume1\Documents and Settings\Administrato
r\NTUSER.DAT    NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explor
er\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count      2010-08-15
19:17:23.000000         Key     N/A     N/A     N/A     N/A     N/A     N/A
N/A
* 0xe1da4008    \Device\HarddiskVolume1\Documents and Settings\Administrato
r\NTUSER.DAT    NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explor
er\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count      2010-08-15
19:17:23.000000         Value   UEME_CTLSESSION -       -       -       - -
d7 c8 59 0e 02 00 00 00 ..Y.....
* 0xe1da4008    \Device\HarddiskVolume1\Documents and Settings\Administrato
r\NTUSER.DAT    NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explor
er\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count      2010-08-15
19:17:23.000000         Value   UEME_RUNPIDL:%csidl2%\MSN.lnk   1       14N
/A      N/A     2010-06-10 16:10:27.000000
```

windows.registry.hivelist.HiveList

```
sansforensics@siftworkstation: ~/Desktop/hw2/volatility3
$ python3 vol.py -f '/home/sansforensics/Downloads/zeus.vmem/zeus.vmem' win
dows.registry.hivelist.HiveList
Volatility 3 Framework 2.7.0
```

```
Offset  FileFullPath    File output

0xe1e158c0      \Device\HarddiskVolume1\Documents and Settings\Administrato
r\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat        Dis
abled
0xe1da4008      \Device\HarddiskVolume1\Documents and Settings\Administrato
r\NTUSER.DAT    Disabled
0xe1c49008      \Device\HarddiskVolume1\Documents and Settings\LocalService
\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat Disabled
0xe1c41b60      \Device\HarddiskVolume1\Documents and Settings\LocalService
\NTUSER.DAT     Disabled
0xe1a39638      \Device\HarddiskVolume1\Documents and Settings\NetworkServi
ce\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat       Dis
abled
0xe1a33008      \Device\HarddiskVolume1\Documents and Settings\NetworkServi
ce\NTUSER.DAT   Disabled
0xe153ab60      \Device\HarddiskVolume1\WINDOWS\system32\config\software  D
isabled
0xe1542008      \Device\HarddiskVolume1\WINDOWS\system32\config\default Dis
abled
0xe1537b60      \SystemRoot\System32\Config\SECURITY    Disabled
0xe1544008      \Device\HarddiskVolume1\WINDOWS\system32\config\SAM     Dis
abled
0xe13ae580              Disabled
0xe101b008      \Device\HarddiskVolume1\WINDOWS\system32\config\system  Dis
abled
0xe1008978              Disabled
```

windows.registry.hivescan.HiveScan

```
sansforensics@siftworkstation: ~/Desktop/hw2/volatility3
$ python3 vol.py -f '/home/sansforensics/Downloads/zeus.vmem/zeus.vmem' win
dows.registry.hivescan.HiveScan
Volatility 3 Framework 2.7.0
```

```
Offset

0x9728c0
0xf6e008
0x1824978
0x1867008
0x1bbd580
0x1f98008
0x21eb638
0x36dc008
0x4010b60
0x6ae4b60
0x6b7db60
0x6c48008
0x6c4b008
```

windows.registry.printkey.PrintKey

```
sansforensics@siftworkstation: ~/Desktop/hw2/volatility3
$ python3 vol.py -f '/home/sansforensics/Downloads/zeus.vmem/zeus.vmem' win
dows.registry.printkey.PrintKey
Volatility 3 Framework 2.7.0
```

```
Last Write Time Hive Offset     Type    Key     Name    Data    Volatile

2010-06-10 16:12:08.000000      0xe1e158c0      Key     \Device\HarddiskVol
ume1\Documents and Settings\Administrator\Local Settings\Application Data\M
icrosoft\Windows\UsrClass.dat   Software                False
2010-06-10 16:11:42.000000      0xe1da4008      Key     \Device\HarddiskVol
ume1\Documents and Settings\Administrator\NTUSER.DAT    AppEvents         F
alse
2010-06-10 16:11:42.000000      0xe1da4008      Key     \Device\HarddiskVol
ume1\Documents and Settings\Administrator\NTUSER.DAT    Console         Fal
se
2010-06-10 16:13:03.000000      0xe1da4008      Key     \Device\HarddiskVol
ume1\Documents and Settings\Administrator\NTUSER.DAT    Control Panel     F
alse
2010-06-10 16:11:42.000000      0xe1da4008      Key     \Device\HarddiskVol
ume1\Documents and Settings\Administrator\NTUSER.DAT    Environment       F
alse
2010-06-10 16:12:06.000000      0xe1da4008      Key     \Device\HarddiskVol
ume1\Documents and Settings\Administrator\NTUSER.DAT    Identities        F
alse
2010-06-10 16:11:42.000000      0xe1da4008      Key     \Device\HarddiskVol
ume1\Documents and Settings\Administrator\NTUSER.DAT    Keyboard Layout   F
alse
2010-06-10 16:17:08.000000      0xe1da4008      Key     \Device\HarddiskVol
ume1\Documents and Settings\Administrator\NTUSER.DAT    Printers          F
alse
2010-08-11 06:06:48.000000      0xe1da4008      Key     \Device\HarddiskVol
ume1\Documents and Settings\Administrator\NTUSER.DAT    Software          F
```

```
2010-06-10 12:02:25.000000      0xe1542008      Key     \Device\HarddiskVol
ume1\WINDOWS\system32\config\default    Console         False
2010-06-10 12:02:25.000000      0xe1542008      Key     \Device\HarddiskVol
ume1\WINDOWS\system32\config\default    Control Panel           False
2010-06-10 12:02:25.000000      0xe1542008      Key     \Device\HarddiskVol
ume1\WINDOWS\system32\config\default    Environment             False
2010-06-10 16:07:07.000000      0xe1542008      Key     \Device\HarddiskVol
ume1\WINDOWS\system32\config\default    Identities              False
2010-06-10 12:02:25.000000      0xe1542008      Key     \Device\HarddiskVol
ume1\WINDOWS\system32\config\default    Keyboard Layout         False
2010-06-10 16:17:05.000000      0xe1542008      Key     \Device\HarddiskVol
ume1\WINDOWS\system32\config\default    Printers                False
2010-06-10 16:12:53.000000      0xe1542008      Key     \Device\HarddiskVol
ume1\WINDOWS\system32\config\default    Software                False
2010-06-10 12:02:25.000000      0xe1542008      Key     \Device\HarddiskVol
ume1\WINDOWS\system32\config\default    UNICODE Program Groups          Fal
se
2010-06-10 16:04:44.000000      0xe1537b60      Key     \SystemRoot\System3
2\Config\SECURITY       Policy          False
2010-08-11 06:06:26.000000      0xe1537b60      Key     \SystemRoot\System3
2\Config\SECURITY       RXACT           False
2010-06-10 12:01:43.000000      0xe1544008      Key     \Device\HarddiskVol
ume1\WINDOWS\system32\config\SAM        SAM             False
2010-06-10 12:03:02.000000      0xe101b008      Key     \Device\HarddiskVol
ume1\WINDOWS\system32\config\system     ControlSet001           False
2010-06-10 16:11:17.000000      0xe101b008      Key     \Device\HarddiskVol
ume1\WINDOWS\system32\config\system     ControlSet002           False
2010-06-10 16:20:33.000000      0xe101b008      Key     \Device\HarddiskVol
ume1\WINDOWS\system32\config\system     LastKnownGoodRecovery           Fal
```

windows.cmdline.CmdLine

```
$ python3 vol.py -f '/home/sansforensics/Downloads/zeus.vmem/zeus.vmem' win
dows.cmdline.CmdLine
Volatility 3 Framework 2.7.0
```

```
PID     Process Args

4       System  Required memory at 0x10 is not valid (process exited?)
544     smss.exe        \SystemRoot\System32\smss.exe
608     csrss.exe       C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Wind
ows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows ServerDll=
basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:C
onServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16
632     winlogon.exe    winlogon.exe
676     services.exe    C:\WINDOWS\system32\services.exe
688     lsass.exe       C:\WINDOWS\system32\lsass.exe
844     vmacthlp.exe    "C:\Program Files\VMware\VMware Tools\vmacthlp.exe"
856     svchost.exe     C:\WINDOWS\system32\svchost -k DcomLaunch
936     svchost.exe     C:\WINDOWS\system32\svchost -k rpcss
1028    svchost.exe     C:\WINDOWS\System32\svchost.exe -k netsvcs
1088    svchost.exe     C:\WINDOWS\system32\svchost.exe -k NetworkService
1148    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalService
1432    spoolsv.exe     C:\WINDOWS\system32\spoolsv.exe
1668    vmtoolsd.exe    "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
1788    VMUpgradeHelper "C:\Program Files\VMware\VMware Tools\VMUpgradeHelp
er.exe" /service
1968    TPAutoConnSvc.e "C:\Program Files\VMware\VMware Tools\TPAutoConnSvc
.exe"
216     alg.exe C:\WINDOWS\System32\alg.exe
888     wscntfy.exe     C:\WINDOWS\system32\wscntfy.exe
1084    TPAutoConnect.e TPAutoConnect.exe -q -i vmware -a COM1 -F 30
```

```
1732    wuauclt.exe     "C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComSer
ver Local\[404]SUSDS138b3bb6212377429f3e2e8558d9fb16
1724    explorer.exe    C:\WINDOWS\Explorer.EXE
432     VMwareTray.exe  "C:\Program Files\VMware\VMware Tools\VMwareTray.ex
e"
452     VMwareUser.exe  "C:\Program Files\VMware\VMware Tools\VMwareUser.ex
e"
468     wuauclt.exe     "C:\WINDOWS\system32\wuauclt.exe"
124     cmd.exe Required memory at 0x7ffdf010 is not valid (process exited?
)
```

windows.getsids.GetSIDs

```
sansforensics@siftworkstation: ~/Desktop/hw2/volatility3
$ python3 vol.py -f '/home/sansforensics/Downloads/zeus.vmem/zeus.vmem' win
dows.getsids.GetSIDs
Volatility 3 Framework 2.7.0
```

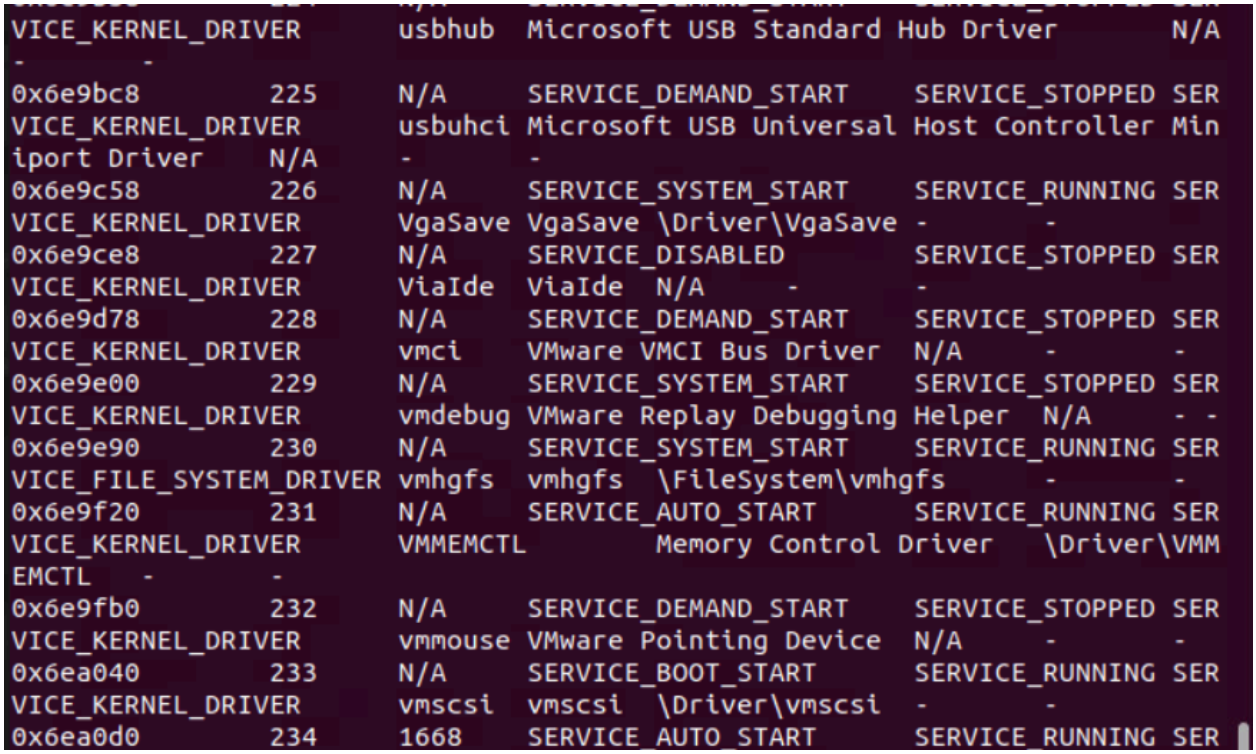
PID	Process	SID	Name
4	System	S-1-5-18	Local System
4	System	S-1-5-32-544	Administrators
4	System	S-1-1-0	Everyone
4	System	S-1-5-11	Authenticated Users
544	smss.exe	S-1-5-18	Local System
544	smss.exe	S-1-5-32-544	Administrators
544	smss.exe	S-1-1-0	Everyone
544	smss.exe	S-1-5-11	Authenticated Users
608	csrss.exe	S-1-5-18	Local System
608	csrss.exe	S-1-5-32-544	Administrators
608	csrss.exe	S-1-1-0	Everyone
608	csrss.exe	S-1-5-11	Authenticated Users
632	winlogon.exe	S-1-5-18	Local System
632	winlogon.exe	S-1-5-32-544	Administrators
632	winlogon.exe	S-1-1-0	Everyone
632	winlogon.exe	S-1-5-11	Authenticated Users
676	services.exe	S-1-5-18	Local System
676	services.exe	S-1-5-32-544	Administrators
676	services.exe	S-1-1-0	Everyone
676	services.exe	S-1-5-11	Authenticated Users
688	lsass.exe	S-1-5-18	Local System
688	lsass.exe	S-1-5-32-544	Administrators
688	lsass.exe	S-1-1-0	Everyone

```
452     VMwareUser.exe  S-1-5-21-1614895754-436374069-839522115-513     Dom
ain Users
452     VMwareUser.exe  S-1-1-0 Everyone
452     VMwareUser.exe  S-1-5-32-544    Administrators
452     VMwareUser.exe  S-1-5-32-545    Users
452     VMwareUser.exe  S-1-5-4 Interactive
452     VMwareUser.exe  S-1-5-11        Authenticated Users
452     VMwareUser.exe  S-1-5-5-0-59917 Logon Session
452     VMwareUser.exe  S-1-2-0 Local (Users with the ability to log in loc
ally)
468     wuauclt.exe     S-1-5-21-1614895754-436374069-839522115-500     Adm
inistrator
468     wuauclt.exe     S-1-5-21-1614895754-436374069-839522115-513     Dom
ain Users
468     wuauclt.exe     S-1-1-0 Everyone
468     wuauclt.exe     S-1-5-32-544    Administrators
468     wuauclt.exe     S-1-5-32-545    Users
468     wuauclt.exe     S-1-5-4 Interactive
468     wuauclt.exe     S-1-5-11        Authenticated Users
468     wuauclt.exe     S-1-5-5-0-59917 Logon Session
468     wuauclt.exe     S-1-2-0 Local (Users with the ability to log in loc
ally)
124     cmd.exe S-1-5-18        Local System
124     cmd.exe S-1-5-32-544    Administrators
124     cmd.exe S-1-1-0 Everyone
124     cmd.exe S-1-5-11        Authenticated Users
```

windows.svcscan.SvcScan

```
sansforensics@siftworkstation: ~/Desktop/hw2/volatility3
$ python3 vol.py -f '/home/sansforensics/Downloads/zeus.vmem/zeus.vmem' win
dows.svcscan.SvcScan
Volatility 3 Framework 2.7.0
```

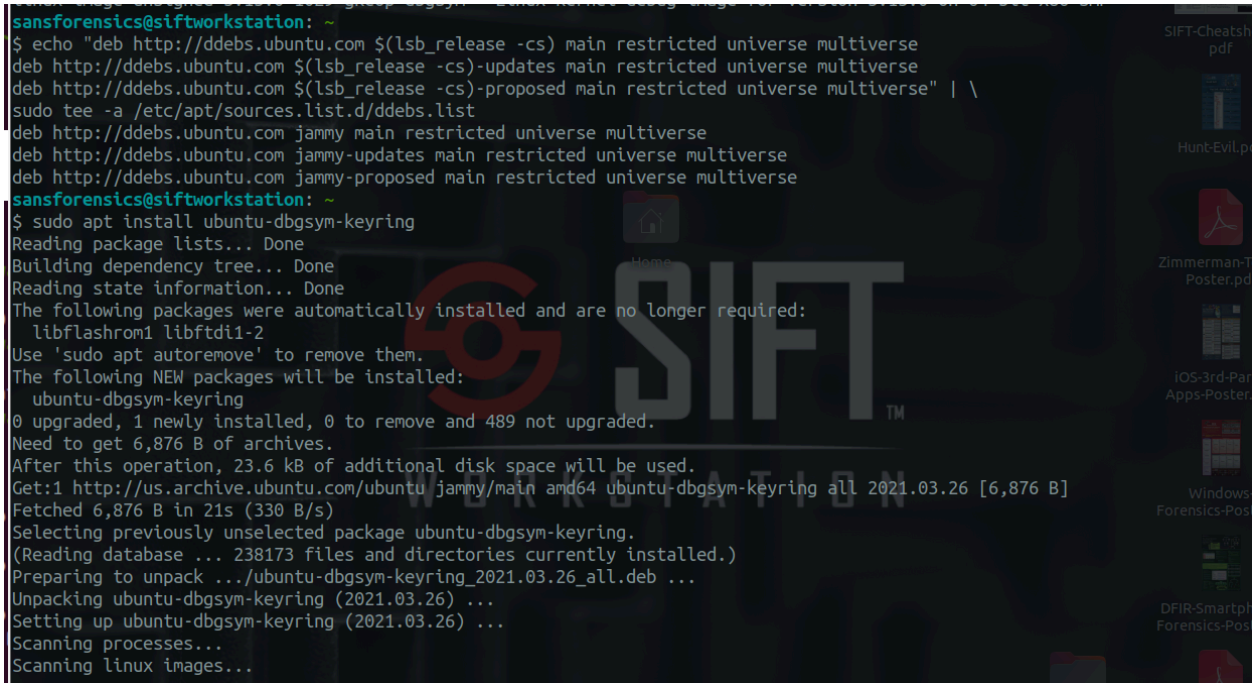
```
Offset  Order   PID     Start   State   Type    Name    Display Binary  Bin
ary (Registry)  Dll

0x6e1e90        1       N/A     SERVICE_DISABLED        SERVICE_STOPPED SER
VICE_KERNEL_DRIVER      Abiosdsk        Abiosdsk        N/A     -       -
0x6e1f20        2       N/A     SERVICE_DISABLED        SERVICE_STOPPED SER
VICE_KERNEL_DRIVER      abp480n5        abp480n5        N/A     -       -
0x6e1fb0        3       N/A     SERVICE_BOOT_START      SERVICE_RUNNING SER
VICE_KERNEL_DRIVER      ACPI    Microsoft ACPI Driver   \Driver\ACPI    - -
0x6e2038        4       N/A     SERVICE_DISABLED        SERVICE_STOPPED SER
VICE_KERNEL_DRIVER      ACPIEC  ACPIEC  N/A     -       -
0x6e20c8        5       N/A     SERVICE_DISABLED        SERVICE_STOPPED SER
VICE_KERNEL_DRIVER      adpu160m        adpu160m        N/A     -       -
0x6e2158        6       N/A     SERVICE_DEMAND_START    SERVICE_STOPPED SER
VICE_KERNEL_DRIVER      aec     Microsoft Kernel Acoustic Echo Canceller  N
/A      -       -
0x6e21e0        7       N/A     SERVICE_SYSTEM_START    SERVICE_RUNNING SER
VICE_KERNEL_DRIVER      AFD     AFD     \Driver\AFD     -       -
0x6e2268        8       N/A     SERVICE_BOOT_START      SERVICE_RUNNING SER
VICE_KERNEL_DRIVER      agp440  Intel AGP Bus Filter    \Driver\agp440  - -
0x6e22f8        9       N/A     SERVICE_DISABLED        SERVICE_STOPPED SER
VICE_KERNEL_DRIVER      Aha154x Aha154x N/A     -       -
0x6e2388        10      N/A     SERVICE_DISABLED        SERVICE_STOPPED SER
VICE_KERNEL_DRIVER      aic78u2 aic78u2 N/A     -       -
0x6e2418        11      N/A     SERVICE_DISABLED        SERVICE_STOPPED SER
VICE_KERNEL_DRIVER      aic78xx aic78xx N/A     -       -
```


VICE_KERNEL_DRIVER usbhub Microsoft USB Standard Hub Driver N/A
- -
0x6e9bc8 225 N/A SERVICE_DEMAND_START SERVICE_STOPPED SER
VICE_KERNEL_DRIVER usbuhci Microsoft USB Universal Host Controller Min
iport Driver N/A - -
0x6e9c58 226 N/A SERVICE_SYSTEM_START SERVICE_RUNNING SER
VICE_KERNEL_DRIVER VgaSave VgaSave \Driver\VgaSave - -
0x6e9ce8 227 N/A SERVICE_DISABLED SERVICE_STOPPED SER
VICE_KERNEL_DRIVER ViaIde ViaIde N/A - -
0x6e9d78 228 N/A SERVICE_DEMAND_START SERVICE_STOPPED SER
VICE_KERNEL_DRIVER vmci VMware VMCI Bus Driver N/A - -
0x6e9e00 229 N/A SERVICE_SYSTEM_START SERVICE_STOPPED SER
VICE_KERNEL_DRIVER vmdebug VMware Replay Debugging Helper N/A - -
0x6e9e90 230 N/A SERVICE_SYSTEM_START SERVICE_RUNNING SER
VICE_FILE_SYSTEM_DRIVER vmhgfs vmhgfs \FileSystem\vmhgfs - -
0x6e9f20 231 N/A SERVICE_AUTO_START SERVICE_RUNNING SER
VICE_KERNEL_DRIVER VMMEMCTL Memory Control Driver \Driver\VMM
EMCTL - -
0x6e9fb0 232 N/A SERVICE_DEMAND_START SERVICE_STOPPED SER
VICE_KERNEL_DRIVER vmmouse VMware Pointing Device N/A - -
0x6ea040 233 N/A SERVICE_BOOT_START SERVICE_RUNNING SER
VICE_KERNEL_DRIVER vmscsi vmscsi \Driver\vmscsi - -
0x6ea0d0 234 1668 SERVICE_AUTO_START SERVICE_RUNNING SER

Part 4 : bonus

```
sansforensics@siftworkstation: ~/Desktop
$ source ~/.profile
sansforensics@siftworkstation: ~/Desktop
$ go version
go version go1.20.3 linux/amd64
```

```
sansforensics@siftworkstation: ~/Desktop
$ cd dwarf2json/
sansforensics@siftworkstation: ~/Desktop/dwarf2json
$ go build
go: downloading github.com/spf13/pflag v1.0.5
sansforensics@siftworkstation: ~/Desktop/dwarf2json
$ ls
dwarf2json  go.mod  go.sum  LICENSE.txt  main.go  README.md
sansforensics@siftworkstation: ~/Desktop/dwarf2json
$ ./dwarf2json linux --help
Usage: dwarf2json linux [OPTIONS]

      --elf PATH           ELF file PATH to extract symbol and type infor
mation
      --elf-symbols PATH   ELF file PATH to extract only symbol informati
on
      --elf-types PATH     ELF file PATH to extract only type information
      --system-map PATH    System.Map file PATH to extract symbol informa
tion
```



I got stuck in this step and I was unable to finish the bonus. I don't know what is the problem