Windows Memory Analysis Using Volatility

1. *Run vol.py -f zeus.vmem imageinfo* using volatility's plugin "imageinfo." What is the suggested type of OS of zeus.vmem and when was the sample was collected? Provide screenshots as your supporting data.

⇒ suggested type of OS**:** WINXPSP2X86 / WINXPSP3X86
⇒ collected on**:** 2010-08-15 19:17:56 or 15:17:56

Results of imageinfo:

2. Run *vol.py –f zeus.vmem pslist* and *vol.py –f zeus.vmem psscan*.

Which one walks through the doubly-linked list of EPROCESS pointed by PsActiveProcessHead?
⇒ **pslist**

- To enumerate processes using pool tag scanning (_POOL_HEADER)
- does not detect hidden or unlinked processes

Which one does not rely on the doubly-list of EPROCESS and can detect unlinked (hidden) processes? Show the hidden processes in a screenshot.
⇒ **psscan**

- can find terminated/inactive processes
- can find processes that have been hidden or unlinked by a rootkit !

Psscan results:

```
sansforensics@siftworkstation -> ~/D/D/1/1
$ vol.py -f zeus.vmem psscan
Volatility Foundation Volatility Framework 2.6
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
0x000000000655fc88 VMUpgradeHelper    1788    676 0x06cc01e0 2010-08-11 06:06:38 UTC+0000
0x00000000066f0978 winlogon.exe        632    544 0x06cc0060 2010-08-11 06:06:23 UTC+0000
0x00000000066f0da0 csrss.exe           608    544 0x06cc0040 2010-08-11 06:06:23 UTC+0000
0x0000000006945da0 spoolsv.exe        1432    676 0x06cc01a0 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
```

Hidden processes (present in psscan but not in pslist)

****Vmip.exe** [psscan pid# 1944 | offset 0x00000000069a7328]

NOTE: This Doesn't show up in a DLL scan and offset commands as suggested in volatility wiki is ineffective [ex: vol.py –f zeus.vmem psscan --offset=0x00000000069a7328]

Alternative: psxview can provide more metrics on the suspected malware

NOTE: Vmip.exe returns nearly all falses [this indicates that most processes are missing]
See image below:

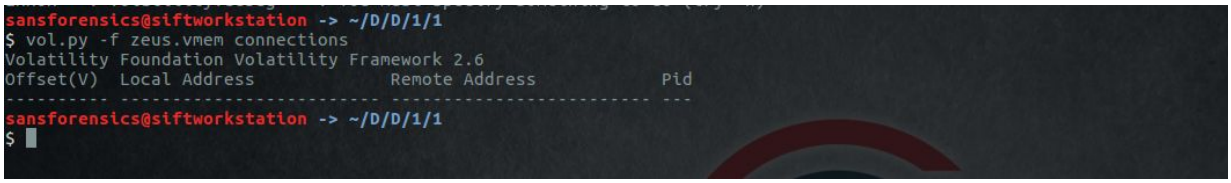
```
sansforensics@siftworkstation -> ~/D/D/1/1
$ vol.py -f zeus.vmem psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
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
```

3. Run *vol.py –f zeus.vmem connections* and *vol.py –f zeus.vmem connscan*. Do you see any active TCP connections or previous connections? Provide screenshots as your supporting data. (Note: both *connections* and *connscan* do not work for Windows Vista and later version memory image. You will use plugin *netscan* instead)

connections ⇒ vol.py –f zeus.vmem connections **[no connections present]**

- used to see TCP connections that were active at the time of the memory acquisition
- walks the singly-linked list of connection structures
- pointed to by a non-exported symbol in the tcpip.sys module

Results of connections [vol.py -f zeus.vmem connections]:



connscan ⇒ vol.py –f zeus.vmem connscan **[2 connections present]**

- Looks for _TCPT_OBJECT structures using pool scanning.
- Can find both active and terminated connections.

Results of connections [vol.py -f zeus.vmem connscan]:

offset	local address	remote address	pid
0x02214988	172.16.176.143.1054	193.104.41.75:80	856
0x06015ab0	0.0.0.1056	193.104.41.75:80	856

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"*.

hivelist ⇒ vol.py –f zeus.vmem hivelist

- Locates virtual addresses of registry hives in memory
- locates full path of the corresponding hive on disk

hivescan ⇒ vol.py –f zeus.vmem hivescan

- finds the physical address of register hives in memory
- works together with hivelist

printkey ⇒ vol.py -f zeus.vmem printkey -K "Microsoft\Windows NT\CurrentVersion\Winlogon"

- searches all hives and prints the key information
- this includes printing a key each time a hive contains it

Which plugin displays the subkeys, values, and data types contained within a specified registry key? Provide screenshots as your supporting data.

⇒ printkey

results of printkey

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.

⇒ hivelist

results of hivelist

```
sansforensics@siftworkstation -> ~/D/D/1/1
$ vol.py -f zeus.vmem hivelist
Volatility Foundation Volatility Framework 2.6
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 -> ~/D/D/1/1
$
```

5. Try other plugins from the Volatility Command Reference, show me one or two other plugins that provide you interesting results.

dlllist ⇒ vol.py –f zeus.vmem dlllist

displays loaded DLLs for a process
walks doubly-linked-list for _LDR_DATA_TABLE_ENTRY pointed to by InLoadOrderModuleList
each time a process uses/loads a DLL, the process is added to the dlllist

results of dlllist

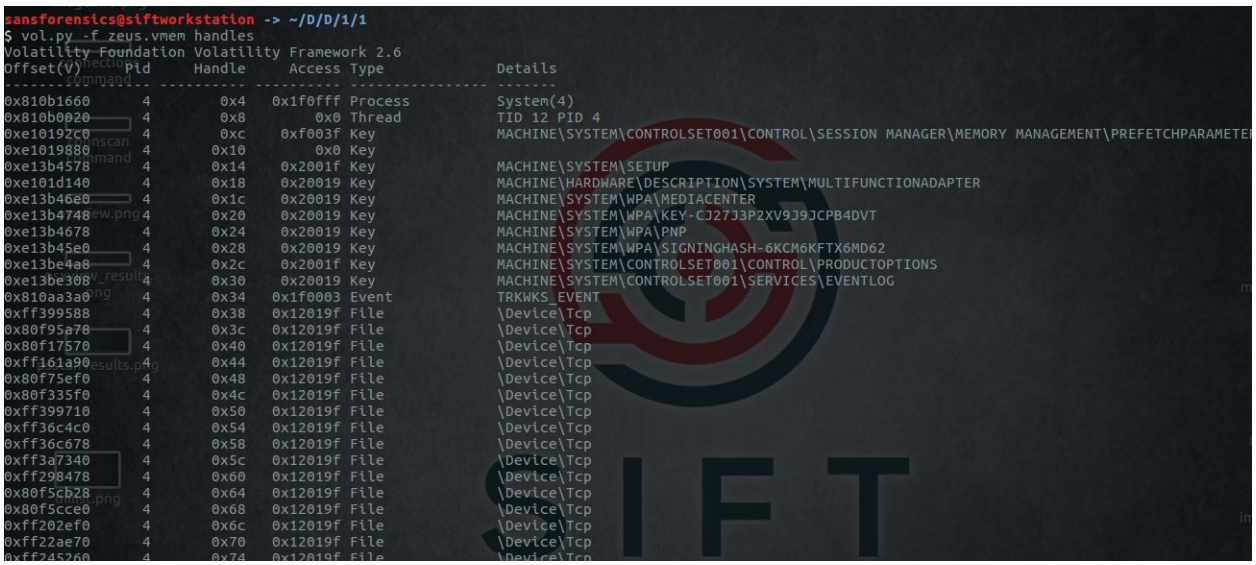
```
************************************************************************
VMwareTray.exe pid:    432
Command line : "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
Service Pack 2

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x00400000    0x21000     0xffff C:\Program Files\VMware\VMware Tools\VMwareTray.exe
0x7c900000    0xb0000     0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf4000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77d40000    0x90000     0xffff C:\WINDOWS\system32\USER32.dll
0x77f10000    0x46000     0xffff C:\WINDOWS\system32\GDI32.dll
0x7c9c0000   0x814000     0xffff C:\WINDOWS\system32\SHELL32.dll
0x77c10000    0x58000     0xffff C:\WINDOWS\system32\msvcrt.dll
0x77dd0000    0x9b000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x91000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77f60000    0x76000     0xffff C:\WINDOWS\system32\SHLWAPI.dll
0x10000000    0x8a000     0xffff C:\Program Files\VMware\VMware Tools\VMControlPanel.cpl
0x774e0000   0x13c000     0xffff C:\WINDOWS\system32\ole32.dll
0x782e0000   0x10f000     0xffff C:\WINDOWS\WinSxS\x86_Microsoft.VC80.MFC_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_3bf8fa05\MFC80U.DLL
0x78130000    0x9b000     0xffff C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_6b128700\MSVCR80.dll
0x763b0000    0x49000     0xffff C:\WINDOWS\system32\COMDLG32.dll
0x773d0000   0x102000     0xffff C:\WINDOWS\WinSxS\X86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.2180_x-ww_a84f1ff9\COMCTL32
0x00340000    0xbe000     0xffff C:\Program Files\VMware\VMware Tools\glib-2.0.dll
0x00440000    0x13000     0xffff C:\Program Files\VMware\VMware Tools\intl.dll
0x00470000   0x10b000     0xffff C:\Program Files\VMware\VMware Tools\iconv.dll
0x71ab0000    0x17000     0xffff C:\WINDOWS\system32\WS2_32.dll
0x71aa0000     0x8000     0xffff C:\WINDOWS\system32\WS2HELP.dll
0x00590000    0x77000     0xffff C:\Program Files\VMware\VMware Tools\vmtools.dll
0x77120000    0x8c000     0xffff C:\WINDOWS\system32\OLEAUT32.dll
```

handles ⇒ vol.py -f zeus.vmem handles

displays open handles in a process
files, registry keys, mutexes, named pipes, events, window stations, desktops, threads etc

results of handles



```
sansforensics@siftworkstation -> ~/D/D/1/1
$ vol.py -f zeus.vmem handles
Volatility Foundation Volatility Framework 2.6
Offset(V)          Pid      Handle     Access Type            Details
------------------ -------- ---------- ---------- --------------- -------
0x810b1660             4        0x4   0x1f0fff Process         System(4)
0x810b0020             4        0x8        0x0 Thread          TID 12 PID 4
0xe1019zc0             4        0xc     0xf003f Key             MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER\MEMORY MANAGEMENT\PREFETCHPARAMETER
0xe1019880             4       0x10        0x0 Key
0xe13b4578             4       0x14     0x2001f Key             MACHINE\SYSTEM\SETUP
0xe101d140             4       0x18     0x20019 Key             MACHINE\HARDWARE\DESCRIPTION\SYSTEM\MULTIFUNCTIONADAPTER
0xe13b46e0             4       0x1c     0x20019 Key             MACHINE\SYSTEM\WPA\MEDIACENTER
0xe13b4748             4       0x20     0x20019 Key             MACHINE\SYSTEM\WPA\KEY-CJ27J3P2XV9J9JCPB4DVT
0xe13b4678             4       0x24     0x20019 Key             MACHINE\SYSTEM\WPA\PNP
0xe13b45e0             4       0x28     0x20019 Key             MACHINE\SYSTEM\WPA\SIGNINGHASH-6KCM6KFTX6MD62
0xe13be4a8             4       0x2c     0x2001f Key             MACHINE\SYSTEM\CONTROLSET001\CONTROL\PRODUCTOPTIONS
0xe13be308             4       0x30     0x20019 Key             MACHINE\SYSTEM\CONTROLSET001\SERVICES\EVENTLOG
0x810aa3a0             4       0x34   0x1f0003 Event           TRKWKS_EVENT
0xff399588             4       0x38   0x12019f File            \Device\Tcp
0x80f95a78             4       0x3c   0x12019f File            \Device\Tcp
0x80f17570             4       0x40   0x12019f File            \Device\Tcp
0xff161a90             4       0x44   0x12019f File            \Device\Tcp
0x80f75ef0             4       0x48   0x12019f File            \Device\Tcp
0x80f335f0             4       0x4c   0x12019f File            \Device\Tcp
0xff399710             4       0x50   0x12019f File            \Device\Tcp
0xff36c4c0             4       0x54   0x12019f File            \Device\Tcp
0xff36c678             4       0x58   0x12019f File            \Device\Tcp
0xff3a7340             4       0x5c   0x12019f File            \Device\Tcp
0xff298478             4       0x60   0x12019f File            \Device\Tcp
0x80f5cb28             4       0x64   0x12019f File            \Device\Tcp
0x80f5cce0             4       0x68   0x12019f File            \Device\Tcp
0xff202ef0             4       0x6c   0x12019f File            \Device\Tcp
0xff22ae70             4       0x70   0x12019f File            \Device\Tcp
0xff245260             4       0x74   0x12019f File            \Device\Tcp
```