CIS-387: Digital Forensics (4 credits)

With Dr. Jinhua Guo

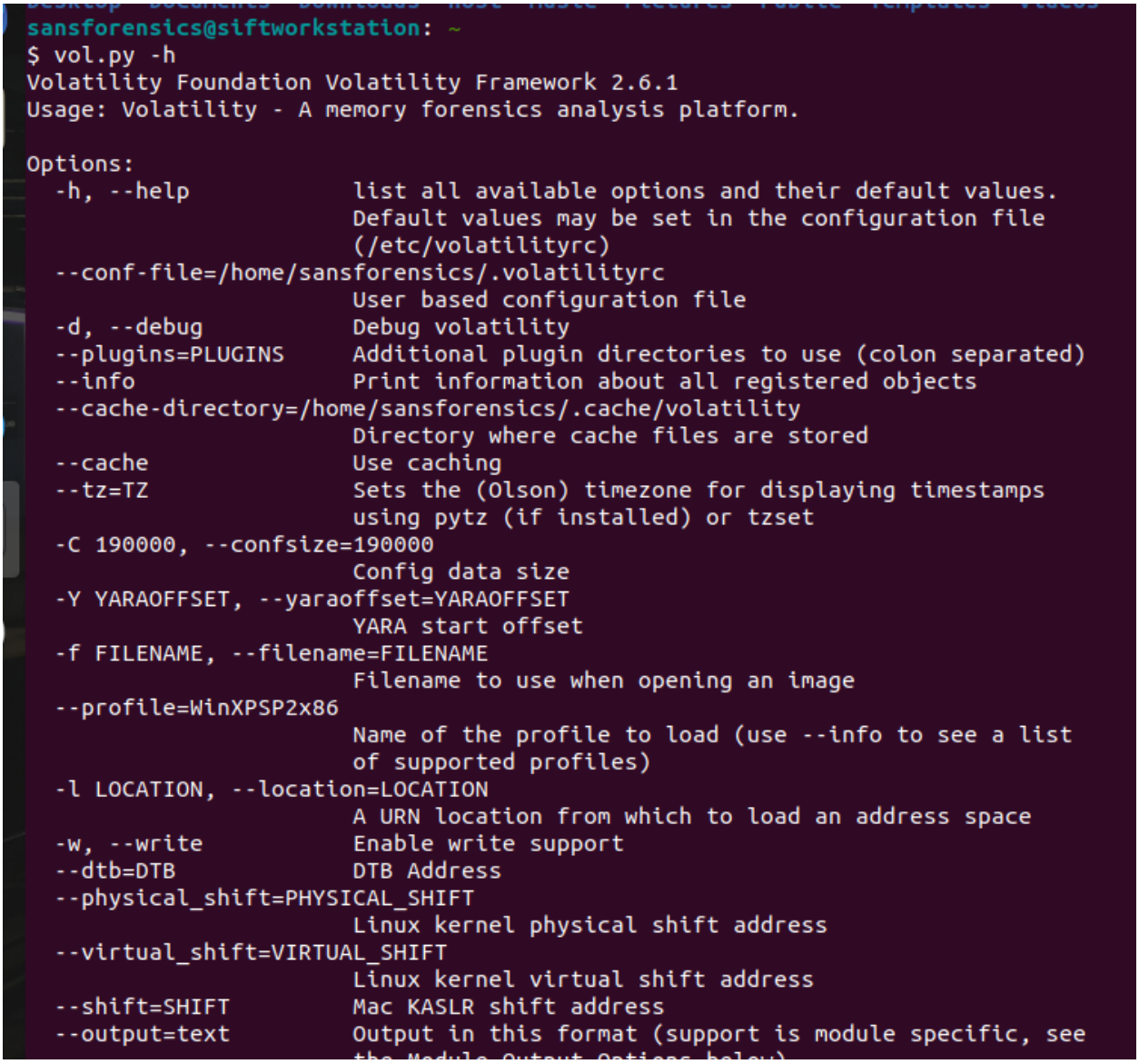
Lab 3

Demetrius Johnson

October 05, 2022

ACTIVITY 1: PRACTICING VOLITILITY (vol.py program)

1) Run vol.py -h to see volatility's options



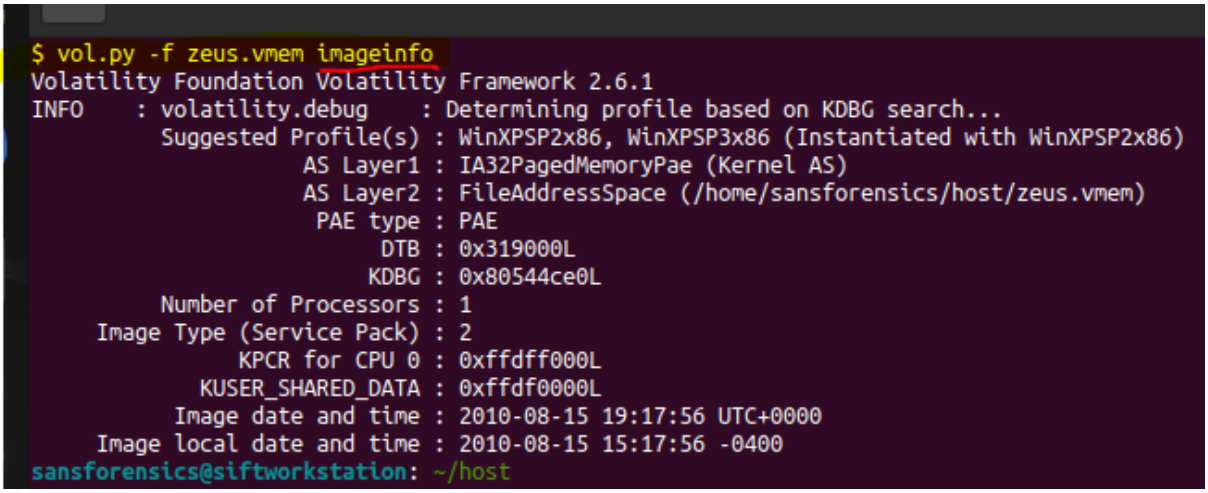
```
sansforensics@siftworkstation: ~
$ vol.py -h
Volatility Foundation Volatility Framework 2.6.1
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=/home/sansforensics/.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (colon separated)
  --info                Print information about all registered objects
  --cache-directory=/home/sansforensics/.cache/volatility
                        Directory where cache files are stored
  --cache               Use caching
  --tz=TZ               Sets the (Olson) timezone for displaying timestamps
                        using pytz (if installed) or tzset
  -C 190000, --confsize=190000
                        Config data size
  -Y YARAOFFSET, --yaraoffset=YARAOFFSET
                        YARA start offset
  -f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
  --profile=WinXPSP2x86
                        Name of the profile to load (use --info to see a list
                        of supported profiles)
  -l LOCATION, --location=LOCATION
                        A URN location from which to load an address space
  -w, --write           Enable write support
  --dtb=DTB             DTB Address
  --physical_shift=PHYSICAL_SHIFT
                        Linux kernel physical shift address
  --virtual_shift=VIRTUAL_SHIFT
                        Linux kernel virtual shift address
  --shift=SHIFT         Mac KASLR shift address
  --output=text         Output in this format (support is module specific, see
```

- Above, showing some of the options of vol.py command line program.

2) Practice these basic plugins to understand how you can use the result for your investigation. For example, vol.py –f zeus.vmem imageinfo

imageinfo

Shows basic system information such as type of OS.



pslist

Lists the processes of a system.

```
$ 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
```

```
0xff364310 wscntfy.exe             888   1028      1       40      0      0 2010-08-11 06:06:49 UTC+0000
0xff38b5f8 TPAutoConnect.e        1084   1968      1       68      0      0 2010-08-11 06:06:52 UTC+0000
0x80f60da0 wuauclt.exe            1732   1028      7      189      0      0 2010-08-11 06:07:44 UTC+0000
0xff3865d0 explorer.exe           1724   1708     13      326      0      0 2010-08-11 06:09:29 UTC+0000
0xff3667e8 VMwareTray.exe          432   1724      1       60      0      0 2010-08-11 06:09:31 UTC+0000
0xff374980 VMwareUser.exe          452   1724      8      207      0      0 2010-08-11 06:09:32 UTC+0000
0x80f94588 wuauclt.exe             468   1028      4      142      0      0 2010-08-11 06:09:37 UTC+0000
0xff224020 cmd.exe                 124   1668      0 --------      0      0 2010-08-15 19:17:55 UTC+0000   2010-08-15 19:17:56 UTC+0000
```

psscan

Finds processes that previously terminated (inactive) and processes that have been hidden or unlinked by a rootkit.

```
sansforensics@siftworkstation: ~/host
$ 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
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
sansforensics@siftworkstation: ~/host
```

pstree

Displays the process listing in tree form connections Shows the TCP connections that were active at the time of the memory acquisition.

```
$ 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+0000
. 0xff2ab020:smss.exe                                544      4      3     21 2010-08-11 06:06:21 UTC+0000
.. 0xff1ec978:winlogon.exe                           632    544     24    536 2010-08-11 06:06:23 UTC+0000
... 0xff255020:lsass.exe                             688    632     21    405 2010-08-11 06:06:24 UTC+0000
... 0xff247020:services.exe                          676    632     16    288 2010-08-11 06:06:24 UTC+0000
.... 0xff1b8b28:vmtoolsd.exe                        1668    676      5    225 2010-08-11 06:06:35 UTC+0000
..... 0xff224020:cmd.exe                             124   1668      0 ------ 2010-08-15 19:17:55 UTC+0000
.... 0x80ff88d8:svchost.exe                          856    676     29    336 2010-08-11 06:06:24 UTC+0000
.... 0xff1d7da0:spoolsv.exe                         1432    676     14    145 2010-08-11 06:06:26 UTC+0000
.... 0x80fbf910:svchost.exe                         1028    676     88   1424 2010-08-11 06:06:24 UTC+0000
..... 0x80f60da0:wuauclt.exe                        1732   1028      7    189 2010-08-11 06:07:44 UTC+0000
..... 0x80f94588:wuauclt.exe                         468   1028      4    142 2010-08-11 06:09:37 UTC+0000
..... 0xff364310:wscntfy.exe                         888   1028      1     40 2010-08-11 06:06:49 UTC+0000
.... 0xff217560:svchost.exe                          936    676     11    288 2010-08-11 06:06:24 UTC+0000
.... 0xff143b28:TPAutoConnSvc.e                     1968    676      5    106 2010-08-11 06:06:39 UTC+0000
..... 0xff38b5f8:TPAutoConnect.e                    1084   1968      1     68 2010-08-11 06:06:52 UTC+0000
.... 0xff22d558:svchost.exe                         1088    676      7     93 2010-08-11 06:06:25 UTC+0000
.... 0xff218230:vmacthlp.exe                         844    676      1     37 2010-08-11 06:06:24 UTC+0000
.... 0xff25a7e0:alg.exe                              216    676      8    120 2010-08-11 06:06:39 UTC+0000
.... 0xff203b80:svchost.exe                         1148    676     15    217 2010-08-11 06:06:26 UTC+0000
.... 0xff1fdc88:VMUpgradeHelper                     1788    676      5    112 2010-08-11 06:06:38 UTC+0000
.. 0xff1ecda0:csrss.exe                              608    544     10    410 2010-08-11 06:06:23 UTC+0000
 0xff3865d0:explorer.exe                            1724   1708     13    326 2010-08-11 06:09:29 UTC+0000
. 0xff374980:VMwareUser.exe                          452   1724      8    207 2010-08-11 06:09:32 UTC+0000
. 0xff3667e8:VMwareTray.exe                          432   1724      1     60 2010-08-11 06:09:31 UTC+0000
sansforensics@siftworkstation: ~/host
```

pstotal (I did this optional command so that I can analyze easier)

Outputs a combination of pslist, psscan, and pstree.

```
sansforensics@siftworkstation: ~/host
$ vol.py -f zeus.vmem pstotal
Volatility Foundation Volatility Framework 2.6.1
Offset (P)  Name            PID    PPID   PDB         Time created                   Time exited                    Interesting
---------- -------------- ------ ------ ---------- ------------------------------ ------------------------------ -----------
0x006499b80 svchost.exe       1148    676 0x006cc0160 2010-08-11 06:06:26 UTC+0000
0x004b5a980 VMwareUser.exe     452   1724 0x006cc0300 2010-08-11 06:09:32 UTC+0000
0x0010f7588 wuauclt.exe        468   1028 0x006cc0180 2010-08-11 06:09:37 UTC+0000
0x00211ab28 TPAutoConnSvc.e   1968    676 0x006cc0260 2010-08-11 06:06:39 UTC+0000
0x001122910 svchost.exe       1028    676 0x006cc0120 2010-08-11 06:06:24 UTC+0000
0x00115b8d8 svchost.exe        856    676 0x006cc00e0 2010-08-11 06:06:24 UTC+0000
0x006945da0 spoolsv.exe       1432    676 0x006cc01a0 2010-08-11 06:06:26 UTC+0000
0x0010c3da0 wuauclt.exe       1732   1028 0x006cc02c0 2010-08-11 06:07:44 UTC+0000
0x0069d5b28 vmtoolsd.exe      1668    676 0x006cc01c0 2010-08-11 06:06:35 UTC+0000
0x005471020 smss.exe           544      4 0x006cc0020 2010-08-11 06:06:21 UTC+0000
0x006384230 vmacthlp.exe       844    676 0x006cc00c0 2010-08-11 06:06:24 UTC+0000
0x00655fc88 VMUpgradeHelper   1788    676 0x006cc01e0 2010-08-11 06:06:38 UTC+0000
0x0066f0da0 csrss.exe          608    544 0x006cc0040 2010-08-11 06:06:23 UTC+0000
0x006015020 services.exe       676    632 0x006cc0080 2010-08-11 06:06:24 UTC+0000
0x005f027e0 alg.exe            216    676 0x006cc0240 2010-08-11 06:06:39 UTC+0000
0x006238020 cmd.exe            124   1668 0x006cc02a0 2010-08-15 19:17:55 UTC+0000 2010-08-15 19:17:56 UTC+0000
0x0069a7328 VMip.exe          1944    124 0x006cc0320 2010-08-15 19:17:55 UTC+0000 2010-08-15 19:17:56 UTC+0000 TRUE
0x004a065d0 explorer.exe      1724   1708 0x006cc0280 2010-08-11 06:09:29 UTC+0000
0x0066f0978 winlogon.exe       632    544 0x006cc0060 2010-08-11 06:06:23 UTC+0000
0x0061ef558 svchost.exe       1088    676 0x006cc0140 2010-08-11 06:06:25 UTC+0000
0x001214660 System               4      0 0x000319000
0x004c2b310 wscntfy.exe        888   1028 0x006cc0200 2010-08-11 06:06:49 UTC+0000
0x004be97e8 VMwareTray.exe     432   1724 0x006cc02e0 2010-08-11 06:09:31 UTC+0000
0x005f47020 lsass.exe          688    632 0x006cc00a0 2010-08-11 06:06:24 UTC+0000
0x0063c5560 svchost.exe        936    676 0x006cc0100 2010-08-11 06:06:24 UTC+0000
0x0049c15f8 TPAutoConnect.e   1084   1968 0x006cc0220 2010-08-11 06:06:52 UTC+0000
sansforensics@siftworkstation: ~/host
```

pstotal --output=dot (I did this optional command so that I can analyze easier)

Outputs a combination of pslist, psscan, and pstree in a graphical way.

```
$ vol.py -f zeus.vmem pstotal --output=dot
Volatility Foundation Volatility Framework 2.6.1
digraph processtree {
graph [rankdir = "TB"];
pid676 -> pid1968 [];
pid1028 -> pid468 [];
pid676 -> pid1788 [];
pid1968 -> pid1084 [];
pid0 -> pid4 [];
pid4 -> pid544 [];
pid676 -> pid936 [];
pid1708 -> pid1724 [];
pid632 -> pid676 [];
pid676 -> pid1148 [];
pid544 -> pid608 [];
pid1724 -> pid452 [];
pid676 -> pid216 [];
pid1668 -> pid124 [];
pid1724 -> pid432 [];
pid1028 -> pid1732 [];
pid676 -> pid1088 [];
pid124 -> pid1944 [];
pid676 -> pid1028 [];
pid676 -> pid844 [];
pid1028 -> pid888 [];
pid544 -> pid632 [];
pid676 -> pid1668 [];
pid676 -> pid1432 [];
pid632 -> pid688 [];
pid676 -> pid856 [];
pid936 [label="{936 | offset (P)\n0x063c5560 | svc
```

```
pid676 -> pid856 [];
pid936 [label="{936 | offset (P)\n0x063c5560 | svchost.exe | created:\n2010-08-11 06:06:24 UTC+0000 |running}" shape="record" ];
pid1724 [label="{1724 | offset (P)\n0x04a065d0 | explorer.exe | created:\n2010-08-11 06:09:29 UTC+0000 |running}" shape="record" ];
pid432 [label="{432 | offset (P)\n0x04be97e8 | VMwareTray.exe | created:\n2010-08-11 06:09:31 UTC+0000 |running}" shape="record" ];
pid544 [label="{544 | offset (P)\n0x05471020 | smss.exe | created:\n2010-08-11 06:06:21 UTC+0000 |running}" shape="record" ];
pid4 [label="{4 | offset (P)\n0x01214660 | System | created:\nnot available |running}" shape="record" ];
pid1148 [label="{1148 | offset (P)\n0x06499b80 | svchost.exe | created:\n2010-08-11 06:06:26 UTC+0000 |running}" shape="record" ];
pid1084 [label="{1084 | offset (P)\n0x049c15f8 | TPAutoConnect.e | created:\n2010-08-11 06:06:52 UTC+0000 |running}" shape="record" ]
pid468 [label="{468 | offset (P)\n0x010f7588 | wuauclt.exe | created:\n2010-08-11 06:09:37 UTC+0000 |running}" shape="record" ];
pid124 [label="{124 | offset (P)\n0x06238020 | cmd.exe | created:\n2010-08-15 19:17:55 UTC+0000 |exited:\n2010-08-15 19:17:56 UTC+000
pid888 [label="{888 | offset (P)\n0x04c2b310 | wscntfy.exe | created:\n2010-08-11 06:06:49 UTC+0000 |running}" shape="record" ];
pid1088 [label="{1088 | offset (P)\n0x061ef558 | svchost.exe | created:\n2010-08-11 06:06:25 UTC+0000 |running}" shape="record" ];
pid216 [label="{216 | offset (P)\n0x05f027e0 | alg.exe | created:\n2010-08-11 06:06:39 UTC+0000 |running}" shape="record" ];
pid1788 [label="{1788 | offset (P)\n0x0655fc88 | VMUpgradeHelper | created:\n2010-08-11 06:06:38 UTC+0000 |running}" shape="record" ]
pid452 [label="{452 | offset (P)\n0x04b5a980 | VMwareUser.exe | created:\n2010-08-11 06:09:32 UTC+0000 |running}" shape="record" ];
pid1668 [label="{1668 | offset (P)\n0x069d5b28 | vmtoolsd.exe | created:\n2010-08-11 06:06:35 UTC+0000 |running}" shape="record" ];
pid1968 [label="{1968 | offset (P)\n0x0211ab28 | TPAutoConnSvc.e | created:\n2010-08-11 06:06:39 UTC+0000 |running}" shape="record" ]
pid632 [label="{632 | offset (P)\n0x066f0978 | winlogon.exe | created:\n2010-08-11 06:06:23 UTC+0000 |running}" shape="record" ];
pid856 [label="{856 | offset (P)\n0x0115b8d8 | svchost.exe | created:\n2010-08-11 06:06:24 UTC+0000 |running}" shape="record" ];
pid844 [label="{844 | offset (P)\n0x06384230 | vmacthlp.exe | created:\n2010-08-11 06:06:24 UTC+0000 |running}" shape="record" ];
pid676 [label="{676 | offset (P)\n0x06015020 | services.exe | created:\n2010-08-11 06:06:24 UTC+0000 |running}" shape="record" ];
pid688 [label="{688 | offset (P)\n0x05f47020 | lsass.exe | created:\n2010-08-11 06:06:24 UTC+0000 |running}" shape="record" ];
pid608 [label="{608 | offset (P)\n0x066f0da0 | csrss.exe | created:\n2010-08-11 06:06:23 UTC+0000 |running}" shape="record" ];
pid1028 [label="{1028 | offset (P)\n0x01122910 | svchost.exe | created:\n2010-08-11 06:06:24 UTC+0000 |running}" shape="record" ];
pid1944 [label="{1944 | offset (P)\n0x069a7328 | VMip.exe | created:\n2010-08-15 19:17:55 UTC+0000 |exited:\n2010-08-15 19:17:56 UTC+
pid1732 [label="{1732 | offset (P)\n0x010c3da0 | wuauclt.exe | created:\n2010-08-11 06:07:44 UTC+0000 |running}" shape="record" ];
pid1432 [label="{1432 | offset (P)\n0x06945da0 | spoolsv.exe | created:\n2010-08-11 06:06:26 UTC+0000 |running}" shape="record" ];
```

```
pid468 [label="{468 | offset (P)\n0x010f7588 | wuauclt.exe | created:\n2010-08-11 06:09:37 UTC+0000 |running}" shape="record" ];
pid124 [label="{124 | offset (P)\n0x06238020 | cmd.exe | created:\n2010-08-15 19:17:55 UTC+0000 |exited:\n2010-08-15 19:17:56 UTC+0000}" shape="record"  style = "filled" fillcolor = "lightgray" ];
pid888 [label="{888 | offset (P)\n0x04c2b310 | wscntfy.exe | created:\n2010-08-11 06:06:49 UTC+0000 |running}" shape="record" ];
```

```
pid1028 [label="{1028 | offset (P)\n0x01122910 | svchost.exe | created:\n2010-08-11 06:06:24 UTC+0000 |running}" shape="record" ];
pid1944 [label="{1944 | offset (P)\n0x069a7328 | VMip.exe | created:\n2010-08-15 19:17:55 UTC+0000 |exited:\n2010-08-15 19:17:56 UTC+0000}" shape="record"  style = "filled" fillcolor = "red" ];
pid1732 [label="{1732 | offset (P)\n0x010c3da0 | wuauclt.exe | created:\n2010-08-11 06:07:44 UTC+0000 |running}" shape="record" ];
```

connscan

Extracts TCP connections that were active at the time of the memory acquisition and previous connections that have since been terminated.

```
sansforensics@siftworkstation: ~/host
$ 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
```

hivelist

Locates the virtual addresses of registry hives in memory and the full paths to the corresponding hive on disk.

```
sansforensics@siftworkstation: ~/host
$ 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
```

- I notice that above there are two registry hives in memory that have no name/path.

hivescan

Displays the physical addresses of registry hives in memory.

```
sansforensics@siftworkstation: ~/host
$ 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
```

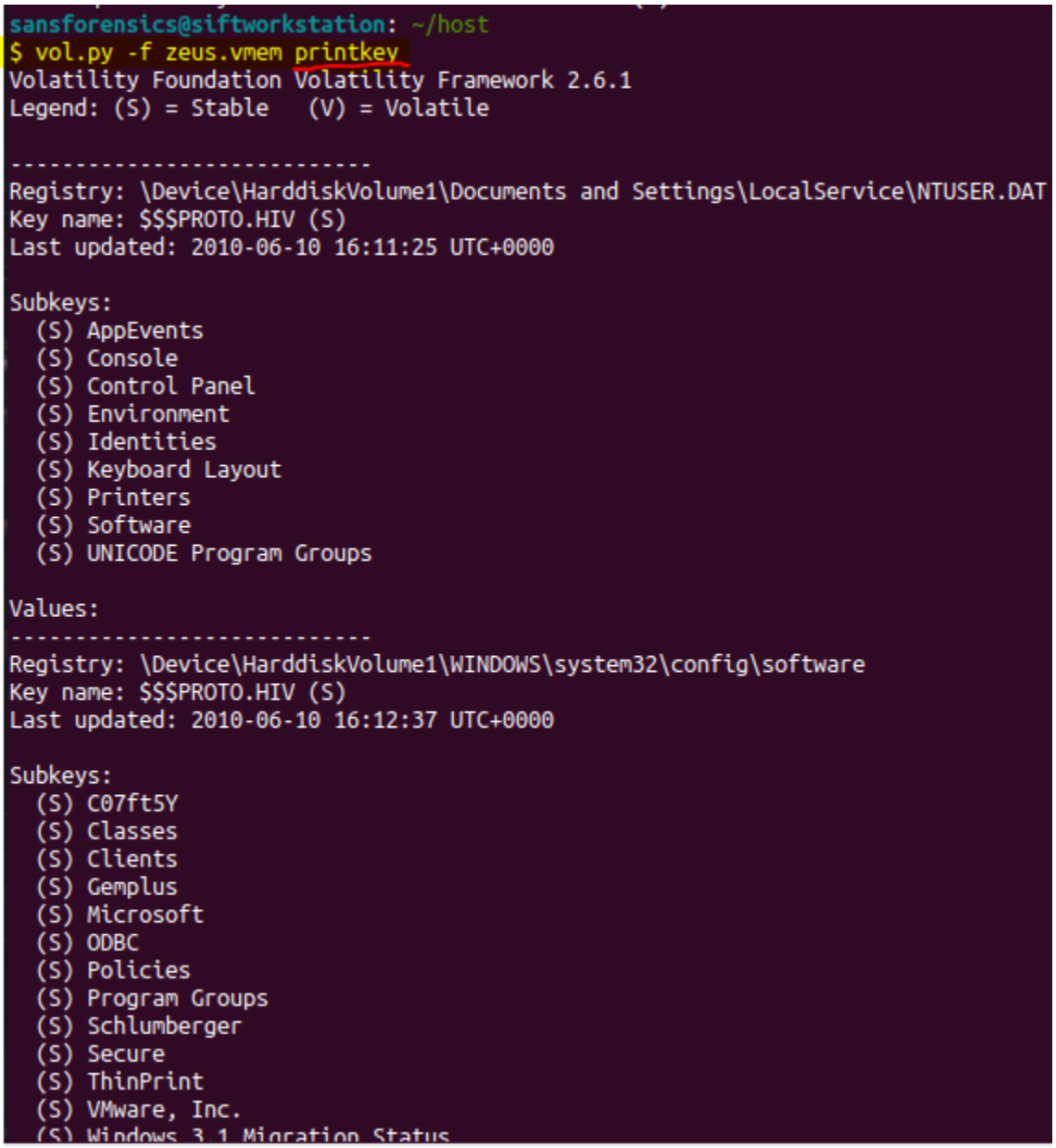
printkey

Displays the subkeys, values, data, and data types contained within a specified registry key, for example:

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

```
$ vol.py -f zeus.vmem printkey -K "Microsoft\Windows NT\CurrentVersion\winlogon"
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: Winlogon (S)
Last updated: 2010-08-15 19:17:23 UTC+0000

Subkeys:
  (S) GPExtensions
  (S) Notify
  (S) SpecialAccounts
  (V) Credentials

Values:
REG_DWORD      AutoRestartShell : (S) 1
REG_SZ         DefaultDomainName : (S) BILLY-DB5B96DD3
REG_SZ         DefaultUserName : (S) Administrator
REG_SZ         LegalNoticeCaption : (S)
REG_SZ         LegalNoticeText : (S)
REG_SZ         PowerdownAfterShutdown : (S) 0
REG_SZ         ReportBootOk    : (S) 1
REG_SZ         Shell           : (S) Explorer.exe
REG_SZ         ShutdownWithoutLogon : (S) 0
REG_SZ         System          : (S)
REG_SZ         Userinit        : (S) C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe,
REG_SZ         VmApplet        : (S) rundll32 shell32,Control_RunDLL "sysdm.cpl"
REG_DWORD      SfcQuota        : (S) 4294967295
REG_SZ         allocatecdroms  : (S) 0
REG_SZ         allocatedasd    : (S) 0
REG_SZ         allocatefloppies : (S) 0
REG_SZ         cachedlogonscount : (S) 10
REG_DWORD      forceunlocklogon : (S) 0
REG_DWORD      passwordexpirywarning : (S) 14
REG_SZ         scremoveoption  : (S) 0
REG_DWORD      AllowMultipleTSSessions : (S) 1
REG_EXPAND_SZ  UIHost          : (S) logonui.exe
REG_DWORD      LogonType       : (S) 1
REG_SZ         Background      : (S) 0 0 0
REG_SZ         AutoAdminLogon  : (S) 0
REG_SZ         DebugServerCommand : (S) no
REG_DWORD      SFCDisable      : (S) 0
REG_SZ         WinStationsDisabled : (S) 0
REG_DWORD      HibernationPreviouslyEnabled : (S) 1
REG_DWORD      ShowLogonOptions : (S) 0
REG_SZ         AltDefaultUserName : (S) Administrator
REG_SZ         AltDefaultDomainName : (S) BILLY-DB5B96DD3
sansforensics@siftworkstation: ~/host
```

now I will run printkey for all registry locations on the zues.vmem image file:



```
  (S) ThinPrint
  (S) VMware, Inc.
  (S) Windows 3.1 Migration Status

Values:
---------------------------
Registry: \SystemRoot\System32\Config\SECURITY
Key name: SECURITY (S)
Last updated: 2010-08-11 06:06:23 UTC+0000

Subkeys:
  (S) Policy
  (S) RXACT

Values:
---------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
Key name: S-1-5-19_Classes (S)
Last updated: 2010-06-10 16:11:25 UTC+0000

Subkeys:

Values:
---------------------------
Registry: [no name]
Key name: REGISTRY (S)
Last updated: 2010-08-11 06:06:08 UTC+0000

Subkeys:
  (S) MACHINE
  (S) USER

Values:
---------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
Key name: S-1-5-21-1614895754-436374069-839522115-500_Classes (S)
Last updated: 2010-06-10 16:12:08 UTC+0000

Subkeys:
  (S) Software

Values:
---------------------------
```

```
Key name: S-1-5-21-1614895754-436374069-839522115-500_Classes (S)
Last updated: 2010-06-10 16:12:08 UTC+0000

Subkeys:
  (S) Software

Values:
---------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
Key name: $$$PROTO.HIV (S)
Last updated: 2010-08-11 06:06:48 UTC+0000

Subkeys:
  (S) AppEvents
  (S) Console
  (S) Control Panel
  (S) Environment
  (S) Identities
  (S) Keyboard Layout
  (S) Printers
  (S) Software
  (S) UNICODE Program Groups
  (V) Volatile Environment

Values:
---------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\default
Key name: $$$PROTO.HIV (S)
Last updated: 2010-06-10 16:07:07 UTC+0000

Subkeys:
  (S) AppEvents
  (S) Console
  (S) Control Panel
  (S) Environment
  (S) Identities
  (S) Keyboard Layout
  (S) Printers
  (S) Software
  (S) UNICODE Program Groups

Values:
---------------------------
```

```
Values:
---------------------------
Registry: [no name]
Key name: HARDWARE (S)
Last updated: 2010-08-11 06:06:08 UTC+0000

Subkeys:

Values:
---------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
Key name: $$$PROTO.HIV (S)
Last updated: 2010-06-10 16:11:21 UTC+0000

Subkeys:
  (S) AppEvents
  (S) Console
  (S) Control Panel
  (S) Environment
  (S) Identities
  (S) Keyboard Layout
  (S) Printers
  (S) Software
  (S) UNICODE Program Groups

Values:
---------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
Key name: S-1-5-20_Classes (S)
Last updated: 2010-06-10 16:11:21 UTC+0000

Subkeys:

Values:
---------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
Key name: $$$PROTO.HIV (S)
Last updated: 2010-08-11 06:06:08 UTC+0000

Subkeys:
  (S) ControlSet001
  (S) ControlSet002
```

```
  (S) Identities
  (S) Keyboard Layout
  (S) Printers
  (S) Software
  (S) UNICODE Program Groups

Values:
---------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
Key name: S-1-5-20_Classes (S)
Last updated: 2010-06-10 16:11:21 UTC+0000

Subkeys:

Values:
---------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
Key name: $$$PROTO.HIV (S)
Last updated: 2010-08-11 06:06:08 UTC+0000

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

Values:
---------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
Key name: SAM (S)
Last updated: 2010-06-10 12:01:43 UTC+0000

Subkeys:
  (S) SAM

Values:
sansforensics@siftworkstation: ~/host
```

Summary/Reflection

The system is possibly compromised because of the svchost.exe. I found that it has multiple processes running, but it is a part of services.exe as a parent process – so perhaps this is normal. I also found that svchost.exe has a TCP connection on port 80 (HTTP), which is typically a protocol used by web browser applications, which svchost.exe is not a web browser application. Lastly, I notice that one of the svchost.exe processes has 1400+ handles, meaning that it is using 1400+ system resources (files, libraries, other binaries and streams…etc.), meaning that it could be a process that is spying, and sending and receiving data about other processes on the machine.