Mr Robot

Saturday, 2 July, 2022 11:32 PM

Scenario:

An employee reported that his machine started to act strangely after receiving a suspicious email for a security update. The incident response team captured a couple of memory dumps from the suspected machines for further inspection.

```
PS C:\Users\60196\Desktop\Cyberdefender\c69-Grrcon2015> .\vmss2core-sb-8456865.exe -W 'C:\Users\60196\Desktop\Cyberdefender\c69-Grrcon2015\target1\Target1-1dd8701f.vmss'
vmss2core version 8456865 Copyright (C) 1998-2017 VMware, Inc. All rights reserved.
... 10 MBs written.
... 20 MBs written.
... 30 MBs written.
... 40 MBs written.
... 50 MBs written.
... 60 MBs written.
... 70 MBs written.
... 80 MBs written.
... 90 MBs written.
... 100 MBs written.
... 110 MBs written.
... 120 MBs written.
... 130 MBs written.
... 140 MBs written.
... 150 MBs written.
PS C:\Users\60196\Desktop\Cyberdefender\c69-Grrcon2015> dir


    Directory: C:\Users\60196\Desktop\Cyberdefender\c69-Grrcon2015


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         2/7/2022  11:32 PM                pos01
d-----         2/7/2022  11:32 PM                target1
d-----         2/7/2022  11:33 PM                target2
-a----         2/7/2022  11:37 PM     1073745920 memory.dmp
-a----         2/7/2022  11:33 PM         641536 vmss2core-sb-8456865.exe
```

```
maman@ubuntu:~/volatility$ vol.py -f memory.dmp imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : WindowsCrashDumpSpace32 (Unnamed AS)
                     AS Layer3 : FileAddressSpace (/home/maman/volatility/memory.dmp)
                      PAE type : PAE
                           DTB : 0x3ecc3260L
                  KUSER_SHARED_DATA : 0xffdf0000L
                Image date and time : 2015-10-09 12:53:02 UTC+0000
          Image local date and time : 2015-10-09 08:53:02 -0400
```

Win7SP1x86_23418

```
maman@ubuntu:~/volatility$ vol.py -f memory.dmp --profile Win7SP1x86_23418 yarascan -Y "From:"
Volatility Foundation Volatility Framework 2.6.1
Rule: r1
Owner: Process OUTLOOK.EXE Pid 3196
0x086dffe1  46 72 6f 6d 3a 20 54 68 65 20 57 68 69 74 33 52   From:.The.Whit3R
0x086dfff1  30 73 33 20 3c 74 68 33 77 68 31 74 33 72 30 73   0s3.<th3wh1t3r0s
0x086e0001  33 40 67 6d 61 69 6c 2e 63 6f 6d 3e 0d 0a 54 6f   3@gmail.com>..To
0x086e0011  3a 20 3c 66 72 6f 6e 74 64 65 73 6b 40 61 6c 6c   :.<frontdesk@all
0x086e0021  73 61 66 65 63 79 62 65 72 73 65 63 2e 63 6f 6d   safecybersec.com
0x086e0031  3e 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a   >..Content-Type:
0x086e0041  20 6d 75 6c 74 69 70 61 72 74 2f 61 6c 74 65 72   .multipart/alter
0x086e0051  6e 61 74 69 76 65 3b 20 62 6f 75 6e 64 61 72 79   native;.boundary
0x086e0061  3d 22 30 30 31 61 31 31 33 34 33 32 37 38 62 64   ="001a11343278bd
0x086e0071  61 30 64 36 30 35 32 31 61 36 31 65 39 35 22 0d   a0d60521a61e95".
0x086e0081  0a 52 65 74 75 72 6e 2d 50 61 74 68 3a 20 74 68   .Return-Path:.th
0x086e0091  33 77 68 31 74 33 72 30 73 33 40 67 6d 61 69 6c   3wh1t3r0s3@gmail
0x086e00a1  2e 63 6f 6d 0d 0a 58 2d 4d 53 2d 45 78 63 68 61   .com..X-MS-Excha
0x086e00b1  6e 67 65 2d 4f 72 67 61 6e 69 7a 61 74 69 6f 6e   nge-Organization
0x086e00c1  2d 4e 65 74 77 6f 72 6b 2d 4d 65 73 73 61 67 65   -Network-Message
0x086e00d1  2d 49 64 3a 20 34 35 35 36 64 33 61 34 2d 33 38   -Id:.4556d3a4-38
```

```
maman@ubuntu:~/volatility$ vol.py -f memory.dmp --profile Win7SP1x86_23418 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x83d334e8 System                    4      0     94      500 ------      0 2015-10-09 11:30:44 UTC+0000
0x84edcbf0 smss.exe                276      4      2       30 ------      0 2015-10-09 11:30:44 UTC+0000
0x84ecbb18 csrss.exe               368    360      9      366      0      0 2015-10-09 11:30:47 UTC+0000
0x84f97628 wininit.exe             420    360      3       77      0      0 2015-10-09 11:30:48 UTC+0000
0x855f6d40 csrss.exe               432    412     11      366      1      0 2015-10-09 11:30:48 UTC+0000
0x8561d030 winlogon.exe            480    412      3      115      1      0 2015-10-09 11:30:48 UTC+0000
0x84e979f8 services.exe            528    420      9      200      0      0 2015-10-09 11:30:48 UTC+0000
0x8583b030 lsass.exe               536    420      9      851      0      0 2015-10-09 11:30:48 UTC+0000
0x8583d960 lsm.exe                 544    420     10      163      0      0 2015-10-09 11:30:48 UTC+0000
0x8586fd40 svchost.exe             644    528     11      351      0      0 2015-10-09 11:30:48 UTC+0000
0x84e01448 svchost.exe             720    528      6      276      0      0 2015-10-09 11:30:50 UTC+0000
0x85935030 svchost.exe             796    528     19      446      0      0 2015-10-09 11:30:51 UTC+0000
0x85969030 svchost.exe             836    528     17      405      0      0 2015-10-09 11:30:52 UTC+0000
0x85978940 svchost.exe             864    528     30     1036      0      0 2015-10-09 11:30:52 UTC+0000
0x859cc2c0 svchost.exe            1008    528     13      650      0      0 2015-10-09 11:30:52 UTC+0000
0x85a138f0 svchost.exe            1124    528     16      484      0      0 2015-10-09 11:30:53 UTC+0000
0x8582c8d8 spoolsv.exe            1228    528     12      273      0      0 2015-10-09 11:30:53 UTC+0000
0x85a55d40 svchost.exe            1256    528     17      304      0      0 2015-10-09 11:30:53 UTC+0000
0x85ae3030 vmtoolsd.exe           1432    528      8      274      0      0 2015-10-09 11:30:54 UTC+0000
0x85976318 svchost.exe            1784    528      5       99      0      0 2015-10-09 11:30:54 UTC+0000
0x85ae0cb0 dllhost.exe            1888    528     13      196      0      0 2015-10-09 11:30:54 UTC+0000
0x858b69e8 msdtc.exe              1980    528     12      145      0      0 2015-10-09 11:30:55 UTC+0000
0x85c09968 dwm.exe                2088    836      3       93      1      0 2015-10-09 11:31:04 UTC+0000
0x85c1e5f8 explorer.exe           2116   2060     23      912      1      0 2015-10-09 11:31:04 UTC+0000
0x85c39030 taskhost.exe           2252    528      7      150      1      0 2015-10-09 11:31:04 UTC+0000
0x859281f0 vmtoolsd.exe           2388   2116      7      164      1      0 2015-10-09 11:31:04 UTC+0000
0x8598c920 SearchIndexer.         2544    528     13      670      0      0 2015-10-09 11:31:10 UTC+0000
0x85d0d030 iexplore.exe           2996   2984      6      463      1      0 2015-10-09 11:31:27 UTC+0000
0x85cd3d40 OUTLOOK.EXE            3196   2116     22     1678      1      0 2015-10-09 11:31:32 UTC+0000
0x85d01510 svchost.exe            3232    528      9      131      0      0 2015-10-09 11:31:34 UTC+0000
0x85b43a58 sppsvc.exe             3900    528      4      153      0      0 2015-10-09 11:32:54 UTC+0000
0x83eb5d40 cmd.exe                2496   2116      1       22      1      0 2015-10-09 11:33:42 UTC+0000
0x83e5cd40 conhost.exe             916    432      3       83      1      0 2015-10-09 11:33:42 UTC+0000
0x83f105f0 cmd.exe                1856   2996      1       33      1      0 2015-10-09 11:35:15 UTC+0000
0x83f13d40 conhost.exe            1624    432      3       81      1      0 2015-10-09 11:35:15 UTC+0000
0x83fb86a8 cmd.exe                3064   2116      1       22      1      0 2015-10-09 11:37:32 UTC+0000
0x83fa9030 conhost.exe             676    432      3       83      1      0 2015-10-09 11:37:32 UTC+0000
0x83fb2d40 cmd.exe                3784   2196      1       24      1      0 2015-10-09 11:39:22 UTC+0000
0x83fc7c08 conhost.exe            1824    432      3       85      1      0 2015-10-09 11:39:22 UTC+0000
0x84013598 TeamViewer.exe         2680   1696     28      632      1      0 2015-10-09 12:08:46 UTC+0000
0x84017d40 tv_w32.exe             4064   2680      2       83      1      0 2015-10-09 12:08:47 UTC+0000
```

```
maman@ubuntu:~/volatility$ vol.py -f memory.dmp --profile Win7SP1x86_23418 pslist | grep -i outlook
Volatility Foundation Volatility Framework 2.6.1
0x85cd3d40 OUTLOOK.EXE           3196   2116     22     1678      1      0 2015-10-09 11:31:32 UTC+0000
```

```
maman@ubuntu:~/volatility$ vol.py -f memory.dmp --profile Win7SP1x86_23418 memdump --dump-dir . -p 3196
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
Writing OUTLOOK.EXE [  3196] to 3196.dmp
maman@ubuntu:~/volatility$
```

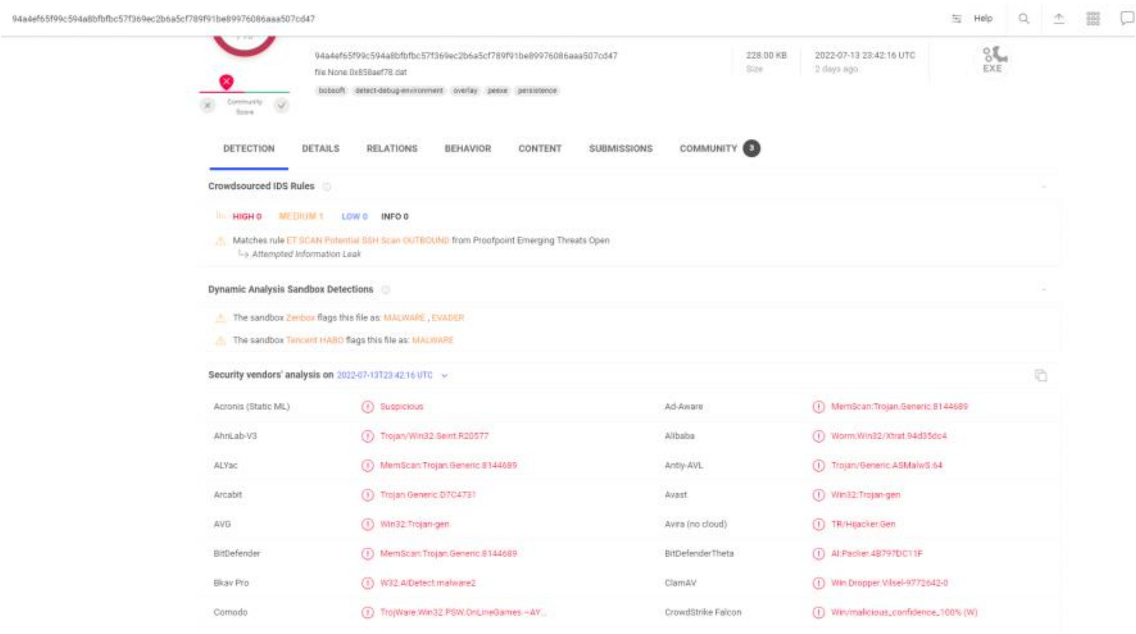
```
maman@ubuntu:~/volatility$ strings -n 10 3196.dmp | grep -i ".exe"
C:\Program Files\Microsoft Office\Office15\OUTLOOK.EXE
ComSpec=C:\Windows\system32\cmd.exe
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
ComSpec=C:\Windows\system32\cmd.exe
ComSpec=C:\Windows\system32\cmd.exe
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
"C:\Program Files\Microsoft Office\Office15\OUTLOOK.EXE"
C:\PROGRA~1\MICROS~1\Office15\OUTLOOK.EXE
am Files\Microsoft Office\Office15\OUTLOOK.EXE
        C:\Program Files\Microsoft Office\Office15\OUTLOOK.EXE
OUTLOOK.EXE
ETOOA:ExecuteAction IsVisible
ETOOA:ExecuteAction IsBigButton
ETOOA:ExecuteAction Hosted
ETOOA:ExecuteAction IsLabelVisible
C:\Program Files\Microsoft Office\Office15\OUTLOOK.EXE
ComSpec=C:\Windows\system32\cmd.exe
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
2015/10/09 08:08:47.466  2680  2416 H32  teamviewer.exe: SharedMem Connected (seg = 0x2b30000, refcnt = 2)
2015/10/09 08:11:15.885  2116  2120 H32  explorer.exe: ResumeAllThreads: resumed 30 threads, max count 30
2015/10/09 08:11:15.885  2116  2120 H32  explorer.exe: DragInterceptor: interception successful (new interface)
SetExemptValue
GetExemptValue
infopath.exe
OUTLOOK.EXE
outlook.exe
outlook.exe
```

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"><div dir="ltr">Hello Mr. Wellick,<div><br></div><div>In order to provide the best service, in the most secure manner, AllSafe has recently updated our remote VPN software. Please download the update from the link below.</div><div><br></div><div><a href="http://180.76.254.120/AnyConnectInstaller.exe">http://180.76.254.120/AnyConnectInstaller.exe</a></div><div><br></div><div>If you have any questions please don't hesitate to contact IT support.</div><div><br></div><div>Thanks and have a great day!</div><div>AllSafe IT Support Desk</div></div>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"><div dir="ltr">Hello Mr. Wellick,<div><br></div><div>In order to provide the best service, in the most secure manner, AllSafe has recently updated our remote VPN software. Please download the update from the link below.</div><div><br></div><div><a href="http://180.76.254.120/AnyConnectInstaller.exe">http://180.76.254.120/AnyConnectInstaller.exe</a></div><div><br></div><div>If you have any questions please don't hesitate to contact IT support.</div><div><br></div><div>Thanks and have a great day!</div><div>AllSafe IT Support Desk</div></div>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"><div dir="ltr">Hello Mr. Wellick,<div><br></div><div>In order to provide the best service, in the most secure manner, AllSafe has recently updated our remote VPN software. Please download the update from the link below.</div><div><br></div><div><a href="http://180.76.254.120/AnyConnectInstaller.exe">http://180.76.254.120/AnyConnectInstaller.exe</a></div><div><br></div><div>If you have any questions please don't hesitate to contact IT support.</div><div><br></div><div>Thanks and have a great day!</div><div>AllSafe IT Support Desk</div></div>
```

```
maman@ubuntu:~/volatility$ vol.py -f memory.dmp --profile Win7SP1x86_23418 filescan | grep -i Anyconnect
Volatility Foundation Volatility Framework 2.6.1
0x000000003debbf80      8      0 R--r-- \Device\HarddiskVolume2\Windows\Prefetch\ANYCONNECTINSTALLER.EXE-BF8040D4.pf
0x000000003df12dd0      2      0 RW-rwd \Device\HarddiskVolume2\Users\anyconnect\AnyConnect\AnyConnectInstaller.exe
0x000000003df1cf00      4      0 R--r-d \Device\HarddiskVolume2\Users\anyconnect\AnyConnect\AnyConnectInstaller.exe
0x000000003e0bc5e0      7      0 R--r-d \Device\HarddiskVolume2\Users\frontdesk\Downloads\AnyConnectInstaller.exe
0x000000003e2559b0      8      0 R--rwd \Device\HarddiskVolume2\Users\frontdesk\Downloads\AnyConnectInstaller.exe
0x000000003e2ae8e0      8      0 RWD--- \Device\HarddiskVolume2\Users\anyconnect\AnyConnect\AnyConnectInstaller.exe
0x000000003ed57968      4      0 R--r-d \Device\HarddiskVolume2\Users\frontdesk\Downloads\AnyConnectInstaller.exe
0x000000003fc3c8c0      8      0 R--r-- \Device\HarddiskVolume2\Windows\Prefetch\ANYCONNECTINSTALLER.EXE-F5AF5299.pf
```

```
maman@ubuntu:~/volatility$ vol.py -f memory.dmp --profile Win7SP1x86_23418 dumpfiles --dump-dir=./ -Q 0x3df1cf00
Volatility Foundation Volatility Framework 2.6.1
ImageSectionObject 0x3df1cf00   None   \Device\HarddiskVolume2\Users\anyconnect\AnyConnect\AnyConnectInstaller.exe
DataSectionObject 0x3df1cf00   None   \Device\HarddiskVolume2\Users\anyconnect\AnyConnect\AnyConnectInstaller.exe
maman@ubuntu:~/volatility$ ls
3196.dmp      CHANGELOG.txt  dist                      get-pip.py   Makefile     PKG-INFO     pyinstaller.spec  setup.py  tools                 vol.py
AUTHORS.txt   contrib        file.None.0x85d12b18.dat  LEGAL.txt    MANIFEST.in  pos01        README.txt        target1   volatility
build         CREDITS.txt    file.None.0x85d1c6c0.img  LICENSE.txt  memory.dmp   pyinstaller  resources         target2   volatility.egg-info
maman@ubuntu:~/volatility$
```

```
maman@ubuntu:~/volatility$ sha256sum file.None.0x85d12b18.dat
94a4ef65f99c594a8bfbfbc57f369ec2b6a5cf789f91be89976086aaa507cd47  file.None.0x85d12b18.dat
maman@ubuntu:~/volatility$
```



```
maman@ubuntu:~/volatility$ vol.py  -f memory.dmp --profile=Win7SP1x86_23418 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                 Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x84ecbb18:csrss.exe                                368    360      9    366 2015-10-09 11:30:47 UTC+0000
 0x84f97628:wininit.exe                              420    360      3     77 2015-10-09 11:30:48 UTC+0000
. 0x84e979f8:services.exe                            528    420      9    200 2015-10-09 11:30:48 UTC+0000
.. 0x85ae0cb0:dllhost.exe                           1888    528     13    196 2015-10-09 11:30:54 UTC+0000
.. 0x8586fd40:svchost.exe                            644    528     11    351 2015-10-09 11:30:48 UTC+0000
.. 0x85ae3030:vmtoolsd.exe                          1432    528      8    274 2015-10-09 11:30:54 UTC+0000
.. 0x85935030:svchost.exe                            796    528     19    446 2015-10-09 11:30:51 UTC+0000
.. 0x85d01510:svchost.exe                           3232    528      9    131 2015-10-09 11:31:34 UTC+0000
.. 0x858b69e8:msdtc.exe                             1980    528     12    145 2015-10-09 11:30:55 UTC+0000
.. 0x85978940:svchost.exe                            864    528     30   1036 2015-10-09 11:30:52 UTC+0000
.. 0x85969030:svchost.exe                            836    528     17    405 2015-10-09 11:30:52 UTC+0000
... 0x85c09968:dwm.exe                              2088    836      3     93 2015-10-09 11:31:04 UTC+0000
.. 0x85c39030:taskhost.exe                          2252    528      7    150 2015-10-09 11:31:04 UTC+0000
.. 0x8582c8d8:spoolsv.exe                           1228    528     12    273 2015-10-09 11:30:53 UTC+0000
.. 0x84e01448:svchost.exe                            720    528      6    276 2015-10-09 11:30:50 UTC+0000
.. 0x85a138f0:svchost.exe                           1124    528     16    484 2015-10-09 11:30:53 UTC+0000
.. 0x85a55d40:svchost.exe                           1256    528     17    304 2015-10-09 11:30:53 UTC+0000
.. 0x85b43a58:sppsvc.exe                            3900    528      4    153 2015-10-09 11:32:54 UTC+0000
.. 0x859cc2c0:svchost.exe                           1008    528     13    650 2015-10-09 11:30:52 UTC+0000
.. 0x8598c920:SearchIndexer.                        2544    528     13    670 2015-10-09 11:31:10 UTC+0000
.. 0x85976318:svchost.exe                           1784    528      5     99 2015-10-09 11:30:54 UTC+0000
. 0x8583b030:lsass.exe                               536    420      9    851 2015-10-09 11:30:48 UTC+0000
. 0x8583d960:lsm.exe                                 544    420     10    163 2015-10-09 11:30:48 UTC+0000
 0x83d334e8:System                                     4      0     94    500 2015-10-09 11:30:44 UTC+0000
. 0x84edcbf0:smss.exe                                276      4      2     30 2015-10-09 11:30:44 UTC+0000
 0x84013598:TeamViewer.exe                           2680   1696     28    632 2015-10-09 12:08:46 UTC+0000
. 0x858bc278:TeamViewer_Des                          1092   2680     16    405 2015-10-09 12:10:56 UTC+0000
. 0x84017d40:tv_w32.exe                              4064   2680      2     83 2015-10-09 12:08:47 UTC+0000
 0x85c1e5f8:explorer.exe                             2116   2060     23    912 2015-10-09 11:31:04 UTC+0000
. 0x83eb5d40:cmd.exe                                 2496   2116      1     22 2015-10-09 11:33:42 UTC+0000
. 0x83f1ed40:mstsc.exe                               2844   2116     11    484 2015-10-09 12:12:03 UTC+0000
. 0x83fb86a8:cmd.exe                                 3064   2116      1     22 2015-10-09 11:37:32 UTC+0000
. 0x859281f0:vmtoolsd.exe                            2388   2116      7    164 2015-10-09 11:31:04 UTC+0000
. 0x85cd3d40:OUTLOOK.EXE                             3196   2116     22   1678 2015-10-09 11:31:32 UTC+0000
 0x855f6d40:csrss.exe                                 432    412     11    366 2015-10-09 11:30:48 UTC+0000
. 0x83f13d40:conhost.exe                             1624    432      3     81 2015-10-09 11:35:15 UTC+0000
. 0x83fa9030:conhost.exe                              676    432      3     83 2015-10-09 11:37:32 UTC+0000
. 0x83e5cd40:conhost.exe                              916    432      3     83 2015-10-09 11:33:42 UTC+0000
. 0x83fc7c08:conhost.exe                             1824    432      3     85 2015-10-09 11:39:22 UTC+0000
 0x8561d030:winlogon.exe                              480    412      3    115 2015-10-09 11:30:48 UTC+0000
 0x85d0d030:iexplore.exe                             2996   2984      6    463 2015-10-09 11:31:27 UTC+0000
. 0x83f105f0:cmd.exe                                 1856   2996      1     33 2015-10-09 11:35:15 UTC+0000
 0x83fb2d40:cmd.exe                                  3784   2196      1     24 2015-10-09 11:39:22 UTC+0000
```

```
maman@ubuntu:~/volatility$ grep -i "\Users" filescan.txt | grep -v front
0x000000003de54038      7      0 R--rwd \Device\HarddiskVolume2\Users\Public\desktop.ini
0x000000003de575d0      7      0 R--rwd \Device\HarddiskVolume2\Users\desktop.ini
0x000000003de5c1a0      2      1 R--rwd \Device\HarddiskVolume2\Users\Public\Desktop
0x000000003de5cef0      2      1 R--rwd \Device\HarddiskVolume2\Users\Public\Desktop
0x000000003de77800      8      0 R--rwd \Device\HarddiskVolume2\Users\zerocool\AppData\Roaming\Microsoft\Windows\SendTo\Desktop.ini
0x000000003de8c680      7      0 R--rwd \Device\HarddiskVolume2\Users\Public\Music\desktop.ini
0x000000003de8d998      7      0 R--rwd \Device\HarddiskVolume2\Users\Public\Pictures\desktop.ini
0x000000003dec4a88      1      1 -W-rw- \Device\HarddiskVolume2\Users\FRONTD~1\AppData\Local\Temp\FXSAPIDebugLogFile.txt
0x000000003dec6c58      2      0 R--rwd \Device\HarddiskVolume2\Users\Public\Videos\desktop.ini
0x000000003df12dd0      2      0 RW-rwd \Device\HarddiskVolume2\Users\anyconnect\AnyConnect\AnyConnectInstaller.exe
0x000000003df1cf00      4      0 R--r-d \Device\HarddiskVolume2\Users\anyconnect\AnyConnect\AnyConnectInstaller.exe
0x000000003e1e5f40     10      1 RW-rw- \Device\HarddiskVolume2\Users\FRONTD~1\AppData\Local\Temp\ExchangePerflog_8484fa318652fe45c4ce420b.dat
0x000000003e2ae8e0      8      0 RWD--- \Device\HarddiskVolume2\Users\anyconnect\AnyConnect\AnyConnectInstaller.exe
0x000000003e7c63b8      7      0 R--rwd \Device\HarddiskVolume2\Users\Public\Desktop\desktop.ini
0x000000003ef2caf8      7      0 R--rwd \Device\HarddiskVolume2\Users\Public\Documents\desktop.ini
0x000000003fa1edb0      8      0 R--r-d \Device\HarddiskVolume2\Users\FRONTD~1\AppData\Local\Temp\TeamViewer\TeamViewer_Desktop.exe
0x000000003fa4f5d0      4      0 R--r-d \Device\HarddiskVolume2\Users\FRONTD~1\AppData\Local\Temp\TeamViewer\tv_w32.exe
0x000000003fd2a3a0      5      0 R--r-d \Device\HarddiskVolume2\Users\FRONTD~1\AppData\Local\Temp\TeamViewer\TeamViewer_StaticRes.dll
0x000000003fd304b0      3      0 R--r-d \Device\HarddiskVolume2\Users\FRONTD~1\AppData\Local\Temp\TeamViewer\tv_w32.dll
0x000000003fd57ae8      6      0 R--r-d \Device\HarddiskVolume2\Users\FRONTD~1\AppData\Local\Temp\TeamViewer\TeamViewer.exe
0x000000003fda7430      8      0 R--rwd \Device\HarddiskVolume2\Users\zerocool\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
0x000000003fdb1cf8      2      0 R--rwd \Device\HarddiskVolume2\Users\Public\Libraries\desktop.ini
0x000000003fdcab70      8      0 RW-rwd \Device\HarddiskVolume2\Users\FRONTD~1\AppData\Local\Temp\TeamViewer\tvinfo.ini
0x000000003fdcb4f0      3      0 R--r-d \Device\HarddiskVolume2\Users\FRONTD~1\AppData\Local\Temp\TeamViewer\TeamViewer_Resource_en.dll
0x000000003fdd5f80      1      1 R--rw- \Device\Mup\;Z:000000000002e898\10.1.1.21\c$\Users\gideon
0x000000003fded840      1      1 R--rw- \Device\HarddiskVolume2\Users\FRONTD~1\AppData\Local\Temp\TeamViewer
```

https://en.wikipedia.org › wiki › Hackers_(film)

Hackers (film) - Wikipedia

Hackers is a 1995 American crime thriller film directed by Iain Softley and starring Jonny ... On August 10, 1988, 11-year-old Dade "**Zero Cool**" Murphy's family is...

Images for zero cool

```
maman@ubuntu:~/volatility$ vol.py  -f memory.dmp --profile=Win7SP1x86_23418 hashdump
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:79402b7671c317877b8b954b3311fa82:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
front-desk:1000:aad3b435b51404eeaad3b435b51404ee:2ae4c526659523d58350e4d70107fc11:::
```

```
Cmd #1 @ 0x2efeb0: cd Temp
Cmd #2 @ 0x2f58a0: dir
Cmd #3 @ 0x2f6bb8: wce.exe -w
Cmd #4 @ 0x2fe400: wce.exe -w > w.tmp
Cmd #36 @ 0x2c00c4: -?0?,???,
Cmd #37 @ 0x2f6008: 0?-???????/
**************************************************
CommandProcess: conhost.exe Pid: 1624
CommandHistory: 0x1c0ab0 Application: cmd.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
Cmd #36 @ 0x1900c4: ?????
Cmd #37 @ 0x1900c4: ?????
**************************************************
CommandProcess: conhost.exe Pid: 676
CommandHistory: 0x349ff8 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 @ 0x33fe58: cd ..
Cmd #1 @ 0x33fe70: cd Temp
Cmd #2 @ 0x3477a8: wce.exe -w
Cmd #3 @ 0x3487b8: runas /profile /user:Administrator
Cmd #4 @ 0x34e500: runas /profile /user:Administrator cmd
Cmd #6 @ 0x340034: ??????
Cmd #14 @ 0x330038: ?63?
Cmd #36 @ 0x3100c4: 4?5?1????1
Cmd #37 @ 0x346be8: 5?1??E????4
**************************************************
CommandProcess: conhost.exe Pid: 1824
CommandHistory: 0x2d90d0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0x2cfe88: cd ..
Cmd #1 @ 0x2cfea0: cd Temp
Cmd #2 @ 0x2d6de0: dir
Cmd #3 @ 0x2d67f0: wce.exe -w
Cmd #4 @ 0x2bbc10: wce.exe -w > w.tmp
Cmd #12 @ 0x2d0031: S
Cmd #17 @ 0x2d0037: ??????
Cmd #36 @ 0x2a00c4: -?.?*???*
Cmd #37 @ 0x2d5c28: .?-???????-
```

```
maman@ubuntu:~/volatility$ vol.py  -f memory.dmp --profile=Win7SP1x86_23418 console
Volatility Foundation Volatility Framework 2.6.1
**************************************************
ConsoleProcess: conhost.exe Pid: 916
Console: 0x1381c0 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: cmd
Title: Administrator: cmd
AttachedProcess: cmd.exe Pid: 2496 Handle: 0x5c
----
CommandHistory: 0x2fa238 Application: wce.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0x2f9098 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 at 0x2efe98: cd ..
Cmd #1 at 0x2efeb0: cd Temp
Cmd #2 at 0x2f58a0: dir
Cmd #3 at 0x2f6bb8: wce.exe -w
Cmd #4 at 0x2fe400: wce.exe -w > w.tmp
----
Screen 0x2dfeb0 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd ..

C:\Windows>cd Temp

C:\Windows\Temp>dir
```

```
C:\Windows\Temp>
C:\Windows\Temp>dir
 Volume in drive C has no label.
 Volume Serial Number is FE0F-F423

 Directory of C:\Windows\Temp

10/09/2015  07:29 AM    <DIR>          .
10/09/2015  07:29 AM    <DIR>          ..
10/09/2015  01:27 AM                 0 DMIE58D.tmp
10/09/2015  06:57 AM            50,176 getlsasrvaddr.exe
10/09/2015  02:02 AM             7,572 MpCmdRun.log
10/09/2015  12:07 AM             4,636 MpSigStub.log
10/09/2015  03:37 AM    <DIR>          MPTelemetrySubmit
10/09/2015  06:45 AM            36,864 nbtscan.exe
10/09/2015  06:44 AM           503,800 Rar.exe
10/09/2015  01:28 AM           180,224 TS_A16D.tmp
10/09/2015  01:28 AM           196,608 TS_A3BF.tmp
10/09/2015  01:28 AM           376,832 TS_A42D.tmp
10/09/2015  01:28 AM           114,688 TS_A528.tmp
10/09/2015  01:28 AM           425,984 TS_A5C5.tmp
10/09/2015  01:28 AM           131,072 TS_A807.tmp
10/09/2015  01:28 AM           655,360 TS_A911.tmp
10/09/2015  01:28 AM           114,688 TS_AA79.tmp
10/09/2015  01:28 AM           180,224 TS_AF79.tmp
10/08/2015  11:43 PM    <DIR>          vmware-SYSTEM
10/09/2015  07:34 AM               333 w.tmp
10/09/2015  06:45 AM           199,168 wce.exe
              17 File(s)      3,178,229 bytes
               4 Dir(s)  22,603,194,368 bytes free
```

```
Administrator\front-desk-PC:flagadmin@1234
frontdesk\ALLSAFECYBERSEC:THzV7mpz
FRONT-DESK-PC$\ALLSAFECYBERSEC:o0&77qj:^zctL2T]ljn3<nlK2Kbql`(:LeBoO7zE>'d8<>J"P
K;\*5IS@Oxg:rC:P:z Y!%fUiIX0y_J& uNUTJ?%:Y;qJY,xq/:)%5^f&zDK.)F%H;V?.^Z

C:\Windows\Temp>wce.exe -w > w.tmp

C:\Windows\Temp>
maman@ubuntu:~/volatility$
```

```
maman@ubuntu:~/volatility$ vol.py  -f memory.dmp --profile=Win7SP1x86_23418 timeliner | grep -i nbtscan.exe
Volatility Foundation Volatility Framework 2.6.1
2015-10-09 10:45:12 UTC+0000|[SHIMCACHE]| \??\C:\Windows\Temp\nbtscan.exe|
maman@ubuntu:~/volatility$
```

```
maman@ubuntu:~/volatility$ grep -i nbs filescan.txt
0x00000003fdb7808      8      0 -W-r-- \Device\HarddiskVolume2\Windows\Temp\nbs.txt
maman@ubuntu:~/volatility$
```

```
maman@ubuntu:~/volatility$ vol.py  -f memory.dmp --profile=Win7SP1x86_23418 dumpfiles -n -Q 0x3fdb7808 --dump-dir=./output
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3fdb7808   None   \Device\HarddiskVolume2\Windows\Temp\nbs.txt
maman@ubuntu:~/volatility$ cd output/
maman@ubuntu:~/volatility/output$ ls
2996.dmp  file.None.0x83eda598.nbs.txt.dat  strings.asc  strings.txt
maman@ubuntu:~/volatility/output$ cat file.None.0x83eda598.nbs.txt.dat
10.1.1.2        ALLSAFECYBERSEC\AD01            SHARING DC
10.1.1.3        ALLSAFECYBERSEC\EX01            SHARING
10.1.1.20       ALLSAFECYBERSEC\FRONT-DESK-PC   SHARING
10.1.1.21       ALLSAFECYBERSEC\GIDEON-PC       SHARING
maman@ubuntu:~/volatility/output$
```

```
maman@ubuntu:~/volatility$ vol.py  -f memory.dmp --profile=Win7SP1x86_23418 netscan | grep -i iexplore.exe
Volatility Foundation Volatility Framework 2.6.1
0x3e0eedf8         TCPv4    10.1.1.20:49205               180.76.254.120:22    ESTABLISHED      2996     iexplore.exe
maman@ubuntu:~/volatility$
```

```
maman@ubuntu:~/volatility$ vol.py  -f memory.dmp --profile=Win7SP1x86_23418 netscan | grep -i mstsc.exe
Volatility Foundation Volatility Framework 2.6.1
0x3fb7a560         TCPv4    10.1.1.20:49301               10.1.1.21:3389       ESTABLISHED      2844     mstsc.exe
maman@ubuntu:~/volatility$
```

```
----
CommandHistory: 0xe9198 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 18 LastAdded: 17 LastDisplayed: 17
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 at 0xe6030: cd C:\Users
Cmd #1 at 0xe6ea8: dir
Cmd #2 at 0xee3d0: wce.exe -w > gideon/w.tmp
Cmd #3 at 0xe0170: who ami
Cmd #4 at 0xe0188: whoami
Cmd #5 at 0xea3c8: net use z: \\10.1.1.2\c$
Cmd #6 at 0xe01b8: cd z:
Cmd #7 at 0xe6ed8: dir
Cmd #8 at 0xe6070: cd gideon
Cmd #9 at 0xe6ef8: dir
Cmd #10 at 0xe6f08: z:
Cmd #11 at 0xe6f18: dir
Cmd #12 at 0xf2418: copy c:\users\gideon\rar.exe z:\crownjewels
Cmd #13 at 0xe0cb8: cd crownjewels
Cmd #14 at 0xe6f28: dir
Cmd #15 at 0xe6f38: rar
Cmd #16 at 0xf2478: rar crownjewlez.rar *.txt -hp123qwe!@#
Cmd #17 at 0xf24d0: rar a -hp123!@#qwe crownjewlez.rar *.txt
----
Screen 0xd0038 X:80 Y:300
Dump:

maman@ubuntu:~/volatility/target2$
```

```
maman@ubuntu:~/volatility/target2$ grep -i w.tmp filescan.txt
0x000000003fcf2798      8      0 -W-r-- \Device\HarddiskVolume2\Users\gideon\w.tmp
maman@ubuntu:~/volatility/target2$
```

```
maman@ubuntu:~/volatility/target2$ cat consoles.txt
**************************************************
ConsoleProcess: conhost.exe Pid: 2888
Console: 0x4a81c0 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe
AttachedProcess: cmd.exe Pid: 3488 Handle: 0x60
----
CommandHistory: 0x2da180 Application: ipconfig.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0x2d9ff0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 at 0x2d77a0: ipconfig
----
Screen 0x2bfe68 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\gideon.ALLSAFECYBERSEC>ipconfig

Windows IP Configuration
```

```
CommandHistory: 0xe9198 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 18 LastAdded: 17 LastDisplayed: 17
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 at 0xe6030: cd C:\Users
Cmd #1 at 0xe6ea8: dir
Cmd #2 at 0xee3d0: wce.exe -w > gideon/w.tmp
Cmd #3 at 0xe0170: who ami
Cmd #4 at 0xe0188: whoami
Cmd #5 at 0xea3c8: net use z: \\10.1.1.2\c$
Cmd #6 at 0xe01b8: cd z:
Cmd #7 at 0xe6ed8: dir
Cmd #8 at 0xe6070: cd gideon
Cmd #9 at 0xe6ef8: dir
Cmd #10 at 0xe6f08: z:
Cmd #11 at 0xe6f18: dir
Cmd #12 at 0xf2418: copy c:\users\gideon\rar.exe z:\crownjewels
Cmd #13 at 0xe0cb8: cd crownjewels
Cmd #14 at 0xe6f28: dir
Cmd #15 at 0xe6f38: rar
Cmd #16 at 0xf2478: rar crownjewlez.rar *.txt -hp123qwe!@#
Cmd #17 at 0xf24d0: rar a -hp123!@#qwe crownjewlez.rar *.txt
----
Screen 0xd0038 X:80 Y:300
Dump:
```

```
maman@ubuntu:~/volatility/target2$ cat filescan.txt | grep -i "System32\\tasks\\\\"
0x000000003d86af80      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\WindowsColorSystem\Calibration Loader
0x000000003d8a5d58      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Task Manager\Interactive
0x000000003db79318      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Media Center\PBDADiscoveryW2
0x000000003dddb160      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Media Center\mcupdate
0x000000003dddb6a0      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\GoogleUpdateTaskMachineUA
0x000000003decdda0      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\SideShow\SessionAgent
0x000000003e022998      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Media Center\ReindexSearchRoot
0x000000003e037340      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Media Center\PvrScheduleTask
0x000000003e077c20      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\CertificateServicesClient\UserTask-Roam
0x000000003e08d820      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Multimedia\SystemSoundsService
0x000000003e0ae7a8      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\PerfTrack\BackgroundConfigSurveyor
0x000000003e15ebb0      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\MemoryDiagnostic\DecompressionFailureDetector
0x000000003e165f80      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Autochk\Proxy
0x000000003e16b428      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Time Synchronization\SynchronizeTime
0x000000003e193320      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Active Directory Rights Management Services Client\AD RMS Rights Policy Template Management
)
0x000000003e347488      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Windows Filtering Platform\BfeOnServiceStartTypeChange
0x000000003e367bf0      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Windows Error Reporting\QueueReporting
0x000000003e3fe420      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows Defender\MP Scheduled Scan
0x000000003ec30448      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Application Experience\ProgramDataUpdater
0x000000003edad5c0      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Media Center\PBDADiscoveryW1
0x000000003f06ce28      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\NetTrace\GatherNetworkInfo
0x000000003f4029e0      8      0 R--rwd \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\RAC\RacTask
0x000000003f42c498      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Office\Office 15 Subscription Heartbeat
0x000000003f4506a8      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\AppID\PolicyConverter
0x000000003fa00278      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\SideShow\SystemDataProviders
0x000000003fa0c658      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Customer Experience Improvement Program\Consolidator
0x000000003fa43d60      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Shell\WindowsParentalControls
0x000000003fa45af8      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Offline Files\Background Synchronization
0x000000003fa7f2c0      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\WDI\ResolutionHost
0x000000003fa803a0      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Media Center\RegisterSearch
0x000000003fa98510      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Media Center\DispatchRecoveryTasks
0x000000003faa4398      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticResolver
0x000000003faa6758      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\MobilePC\HotStart
0x000000003fac7f80      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Shell\WindowsParentalControlsMigration
0x000000003fae5ef0      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\SystemRestore\SR
0x000000003fae6480      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Application Experience\AitAgent
0x000000003faeaeb8      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Windows Media Sharing\UpdateLibrary
0x000000003faf0ba0      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Maintenance\WinSAT
0x000000003fafbc40      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Tcpip\IpAddressConflict2
0x000000003fb007e8      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Active Directory Rights Management Services Client\AD RMS Rights Policy Template Management
ated)
0x000000003fb10408      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\CertificateServicesClient\UserTask
```

```
0x000000003fb10408      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\CertificateServicesClient\UserTask
0x000000003fb21e88      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\TextServicesFramework\MsCtfMonitor
0x000000003fb37bc0      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\User Profile Service\HiveUploadTask
0x000000003fb395d8      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Media Center\SqlLiteRecoveryTask
0x000000003fb587c0      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Power Efficiency Diagnostics\AnalyzeSystem
0x000000003fb58ec8      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\RemoteAssistance\RemoteAssistanceTask
0x000000003fb5b470      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Media Center\RecordingRestart
0x000000003fb92038      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Office\OfficeTelemetryAgentLogOn
0x000000003fb92708      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\CertificateServicesClient\SystemTask
0x000000003fbaef80      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Tcpip\IpAddressConflict1
0x000000003fbb7e00      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\GoogleUpdateTaskMachineCore
0x000000003fbb7f80      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\MUI\LPRemove
0x000000003fc399b8      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\At1
0x000000003fc436a8      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Media Center\MediaCenterRecoveryTask
```

```
maman@ubuntu:~/volatility/target2$ vol.py  -f target2-6186fe9f.vmss --profile=Win7SP1x86_23418 dumpfiles -n -Q 0x000000003fc399b8 --dump-dir=./dumpfiles
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3fc399b8   None    \Device\HarddiskVolume2\Windows\System32\Tasks\At1
maman@ubuntu:~/volatility/target2$
```

```
maman@ubuntu:~/volatility/target2$ vol.py  -f target2-6186fe9f.vmss --profile=Win7SP1x86_23418 dumpfiles -n -Q 0x000000003fc399b8 --dump-dir=./dumpfiles
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3fc399b8   None    \Device\HarddiskVolume2\Windows\System32\Tasks\At1
maman@ubuntu:~/volatility/target2$ cd dumpfiles/
maman@ubuntu:~/volatility/target2/dumpfiles$ ls
file.None.0x85a35da0.w.tmp.dat  file.None.0x85a86af0.At1.dat
maman@ubuntu:~/volatility/target2/dumpfiles$ cat file.None.0x85a86af0.At1.dat
ÿþ<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.0" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo />
  <Triggers>
    <TimeTrigger>
      <StartBoundary>2015-10-09T08:00:00</StartBoundary>
    </TimeTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <UserId>@AtServiceAccount</UserId>
      <LogonType>InteractiveTokenOrPassword</LogonType>
      <RunLevel>HighestAvailable</RunLevel>
    </Principal>
  </Principals>
  <Actions Context="Author">
    <Exec>
      <Command>c:\users\gideon\1.bat</Command>
    </Exec>
  </Actions>
</Task>maman@ubuntu:~/volatility/target2/dumpfiles$ ^C
```

```
maman@ubuntu:~/volatility/target2$ vol.py -f target2-6186fe9f.vmss --profile=Win7SP1x86_23418 cmdscan
Volatility Foundation Volatility Framework 2.6.1
**************************************************
CommandProcess: conhost.exe Pid: 2888
CommandHistory: 0x2d9ff0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0x2d77a0: ipconfig
Cmd #1 @ 0x2d0031: ???
Cmd #12 @ 0x2d0032: ???
Cmd #17 @ 0x2d0035: ?
Cmd #36 @ 0x2a00c4: -?-?*???*
Cmd #37 @ 0x2d6be0: -?*???????-
**************************************************
CommandProcess: conhost.exe Pid: 3048
CommandHistory: 0xe9198 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 18 LastAdded: 17 LastDisplayed: 17
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0xe6030: cd C:\Users
Cmd #1 @ 0xe6ea8: dir
Cmd #2 @ 0xee3d0: wce.exe -w > gideon/w.tmp
Cmd #3 @ 0xe0170: who ami
Cmd #4 @ 0xe0188: whoami
Cmd #5 @ 0xea3c8: net use z: \\10.1.1.2\c$
Cmd #6 @ 0xe01b8: cd z:
Cmd #7 @ 0xe6ed8: dir
Cmd #8 @ 0xe6070: cd gideon
Cmd #9 @ 0xe6ef8: dir
Cmd #10 @ 0xe6f08: z:
Cmd #11 @ 0xe6f18: dir
Cmd #12 @ 0xf2418: copy c:\users\gideon\rar.exe z:\crownjewels
Cmd #13 @ 0xe0cb8: cd crownjewels
Cmd #14 @ 0xe6f28: dir
Cmd #15 @ 0xe6f38: rar
Cmd #16 @ 0xf2478: rar crownjewlez.rar *.txt -hp123qwe!@#
Cmd #17 @ 0xf24d0: rar a -hp123!@#qwe crownjewlez.rar *.txt
Cmd #36 @ 0xb00c4: ??
                   ???

Cmd #37 @ 0xe5d48: ?
                   ???????
```

```
maman@ubuntu:~/volatility/target2$ vol.py -f target2-6186fe9f.vmss --profile=Win7SP1x86_23418 memdump -p 3048 --dump-dir=.
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
Writing conhost.exe [  3048] to 3048.dmp
```

```
maman@ubuntu:~/volatility/target2$ strings --encoding=l 3048.dmp | grep -i crown
  c-           Disable comments show                                    cfg-          Disable read configuration                                    cl            Convert names to lower case
                    cu            Convert names to upper case                                    df            Delete files after archiving                                    dh
         Open shared files                                    dr            Delete files to Recycle Bin                                    ds            Disable name sort for solid archi
ve                       dw            Wipe files after archiving                                    e[+]<attr>    Set file exclude and include attributes                                    ed
    Do not add empty directories                                    en            Do not put 'end of archive' block                                    ep            Exclude paths from names
                    ep1           Exclude base directory from names                                    ep2           Expand paths to full                                    ep3           Ex
pand paths to full including the drive letter                    f             Freshen files                                    hp[password]  Encrypt both file data and headers
                ht[b|c]       Select hash type [BLAKE2,CRC32] for file checksum                id[c,d,p,q]   Disable messages                                    ieml[addr]    Send arc
hive by email                                    ierr          Send all messages to stderr                                    ilog[name]    Log errors to file (registered versions only)
             inul          Disable all messages                                    ioff          Turn PC off after completing an operation                                    isnd          Enable sound
                                    k             Lock archive                                    kb            Keep broken extracted files
        log[f][=name] Write names to log file                    m<0..5>       Set compression level (0-store...3-default...5-maximal)        ma[4|5]       Specify a version of
 archiving format                    mc<par>       Set advanced compression parameters                    md<n>[k,m,g]  Dictionary size in KB, MB or GB
   ms[ext;ext]   Specify file types to store                                    mt<threads>   Set the number of threads                                    n<file>       Additionally filter includ
ed files                                    n@            Read additional filter masks from stdin                                    n@<list>      Read additional filter masks from list file                    o[+
|-]        Set the overwrite mode                                    oc            Set NTFS Compressed attribute                                    oh            Save hard links as the link inst
ead of the file                    oi[0-4][:min] Save identical files as references                                    ol[a]         Process symbolic links as the link [absolute paths]            or
     Rename files automatically                                    os            Save NTFS streams                                    ow            Save or restore file owner and group
                        p[password]   Set password                                    p-            Do not query password                                    qo[-|+]       A
dd quick open information [none|force]                    r             Recurse subdirectories                    r-            Disable recursion
                    r0            Recurse subdirectories for wildcard names only                ri<P>[:<S>]   Set priority (0-default,1-min..15-max) and sleep time in ms       rr[N]         Add dat
a recovery record                                    rv[N]         Create recovery volumes                                    s[<N>,v[-],e] Create solid archive
                s-            Disable solid archiving                                    sc<chr>[obj]  Specify the character set                                    sfx[name]     Create SFX ar
chive                                    si[name]      Read data from standard input (stdin)                                    sl<size>      Process files with size less than specified
          sm<size>      Process files with size more than specified                    t             Test files after archiving                                    ta<date>      Process files modif
ied after <date> in YYYYMMDDHHMMSS format      tb<date>      Process files modified before <date> in YYYYMMDDHHMMSS format     tk            Keep original archive time
    tl            Set archive time to latest file                                    tn<time>      Process files newer than <time>                                    to<time>      Process files older than
<time>                        ts<m,c,a>[N]  Save or restore file time (modification, creation, access)        u             Update files                                    v<
size>[k,b]  Create volumes with size=<size>*1000 [*1024, *1]                    vd            Erase disk contents before creating volume                    ver[n]        File version control
                        vn            Use the old style volume naming scheme                    vp            Pause before each volume                                    w<path>
      Assign work directory                                    x<file>       Exclude specified file                                    x@            Read file names to exclude from stdin
                    x@<list>      Exclude files listed in specified list file                    y             Assume Yes on all queries                                    z[file]
Read archive comment from file                                                                                                    Z:\crownjewels>rar a -hp123!@#qwe crownjewlez.rar *.txt
                                                                                                RAR 5.30 beta 5   Copyright (c) 1993-2015 Alexander Roshal   8 Oct 2015         Trial version
    Type RAR -? for help                                                                                                                Evaluation copy. Please register.
                                                                                                Creating archive crownjewlez.rar
                                                Adding    SecretSauce1.txt                                                OK        Adding    SecretSauce2.txt                                                O
K        Adding    SecretSauce3.txt                                                OK        Done
                                                Z:\crownjewels>                                                Volume Serial Number is 68F8-C163
                                                                                Directory of Z:\
                                            10/09/2015  02:49 AM    <DIR>          crownjewels                                    10/08/2015  05:21 PM    <DIR>          inetpub                                    08/
22/2013  11:52 AM    <DIR>          PerfLogs                                    10/08/2015  05:21 PM    <DIR>          Program Files                                    10/08/2015  05:22 PM    <DIR>          Program
 Files (x86)                    10/08/2015  05:24 PM    <DIR>          Users                                    10/08/2015  05:24 PM    <DIR>          Windows                                    10/07/201
5  12:14 AM    <DIR>          Windows.old                                                0 File(s)              0 bytes                                                8 Dir(s)  11,368,648,704 bytes free
```

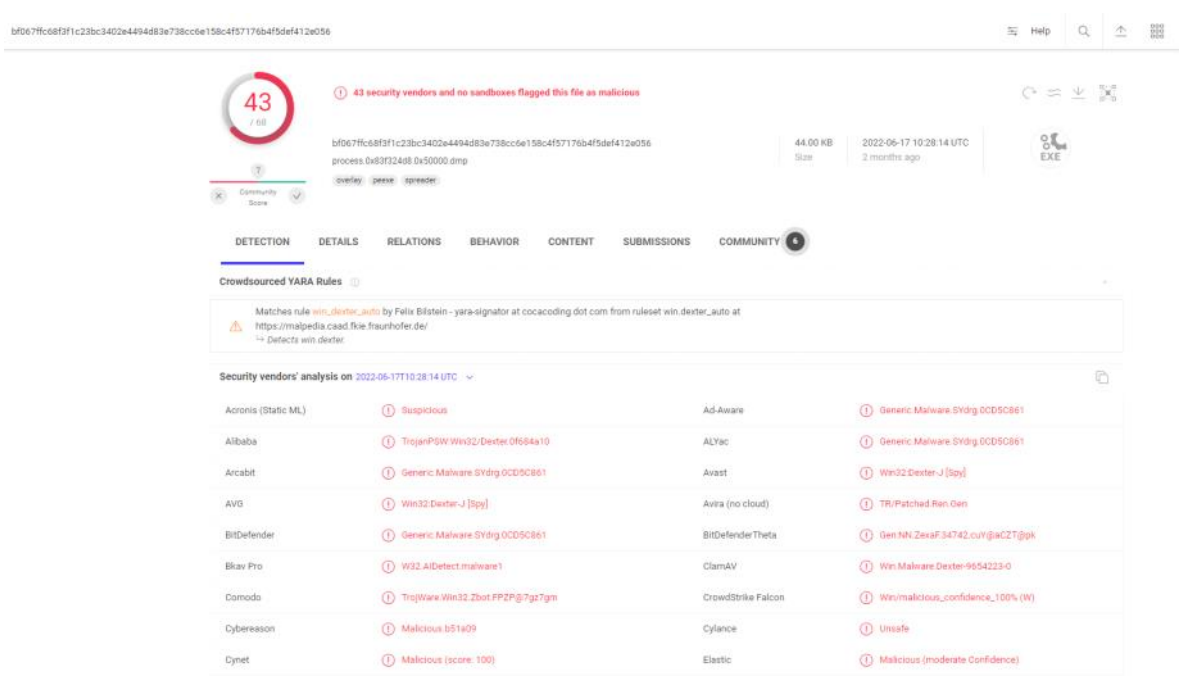
```
maman@ubuntu:~/volatility/pos01$ vol.py  -f POS-01-c4e8f786.vmss imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : VMWareAddressSpace (Unnamed AS)
                     AS Layer3 : FileAddressSpace (/home/maman/volatility/pos01/POS-01-c4e8f786.vmss)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82763be8L
          Number of Processors : 2
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0x82764c00L
                KPCR for CPU 1 : 0x807c5000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2015-10-09 12:52:56 UTC+0000
     Image local date and time : 2015-10-09 08:52:56 -0400
```

```
maman@ubuntu:~/volatility/pos01$ vol.py  -f POS-01-c4e8f786.vmss --profile=Win7SP1x86_23418 netscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x3e00bf50         UDPv4    127.0.0.1:63206                *:*                                   3544     svchost.exe    2015-10-09 12:18:42 UTC+0000
0x3e15daf0         UDPv4    127.0.0.1:51984                *:*                                   3376     OUTLOOK.EXE    2015-10-09 06:21:39 UTC+0000
0x3e17f008         UDPv6    ::1:1900                       *:*                                   3544     svchost.exe    2015-10-09 12:18:41 UTC+0000
0x3e2262c0         UDPv4    0.0.0.0:0                      *:*                                   536      lsass.exe      2015-10-09 03:38:56 UTC+0000
0x3e2262c0         UDPv6    :::0                           *:*                                   536      lsass.exe      2015-10-09 03:38:56 UTC+0000
0x3e22aec0         UDPv4    0.0.0.0:0                      *:*                                   536      lsass.exe      2015-10-09 03:38:56 UTC+0000
0x3e236e20         UDPv4    127.0.0.1:56547                *:*                                   536      lsass.exe      2015-10-09 03:38:56 UTC+0000
0x3e23d6e8         UDPv4    127.0.0.1:61346                *:*                                   3740     WINWORD.EXE    2015-10-09 05:21:28 UTC+0000
0x3e256580         UDPv4    0.0.0.0:0                      *:*                                   536      lsass.exe      2015-10-09 03:38:56 UTC+0000
0x3e256580         UDPv6    :::0                           *:*                                   536      lsass.exe      2015-10-09 03:38:56 UTC+0000
0x3e2569c0         UDPv4    0.0.0.0:0                      *:*                                   536      lsass.exe      2015-10-09 03:38:56 UTC+0000
0x3e2e4378         UDPv4    127.0.0.1:49798                *:*                                   900      svchost.exe    2015-10-09 03:39:04 UTC+0000
0x3e33cc10         UDPv4    127.0.0.1:59590                *:*                                   1116     svchost.exe    2015-10-09 03:38:58 UTC+0000
0x3e3b36c8         UDPv4    0.0.0.0:0                      *:*                                   1008     svchost.exe    2015-10-09 03:39:01 UTC+0000
0x3e3b9d98         UDPv4    0.0.0.0:0                      *:*                                   1008     svchost.exe    2015-10-09 03:39:01 UTC+0000
0x3e3b9d98         UDPv6    :::0                           *:*                                   1008     svchost.exe    2015-10-09 03:39:01 UTC+0000
0x3e0773d0         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        736      svchost.exe
0x3e078af8         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        736      svchost.exe
0x3e078af8         TCPv6    :::135                         :::0                 LISTENING        736      svchost.exe
0x3e07f008         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        432      wininit.exe
0x3e07f008         TCPv6    :::49152                       :::0                 LISTENING        432      wininit.exe
0x3e0816c8         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        432      wininit.exe
0x3e092bf0         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        824      svchost.exe
0x3e092bf0         TCPv6    :::49153                       :::0                 LISTENING        824      svchost.exe
0x3e092d50         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        824      svchost.exe
0x3e0ca170         TCPv4    0.0.0.0:49179                  0.0.0.0:0            LISTENING        536      lsass.exe
0x3e0cb028         TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING        4        System
0x3e0cb028         TCPv6    :::445                         :::0                 LISTENING        4        System
0x3e0cb0d0         TCPv4    0.0.0.0:49169                  0.0.0.0:0            LISTENING        528      services.exe
0x3e0cb240         TCPv4    0.0.0.0:49169                  0.0.0.0:0            LISTENING        528      services.exe
0x3e0cb240         TCPv6    :::49169                       :::0                 LISTENING        528      services.exe
0x3e6cf058         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        900      svchost.exe
0x3e6cf058         TCPv6    :::49154                       :::0                 LISTENING        900      svchost.exe
0x3e6cf270         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        900      svchost.exe
0x3e0f90e8         TCPv4    10.1.1.10:64532                10.1.1.3:80          ESTABLISHED      3376     OUTLOOK.EXE
0x3e135df8         TCPv4    10.1.1.10:58751                54.84.237.92:80      CLOSE_WAIT       3208     iexplore.exe
0x3e24c7d0         TCPv4    10.1.1.10:49201                23.203.149.112:443   CLOSE_WAIT       2464     jusched.exe
0x3e611b10         TCPv4    -:49887                        108.162.232.200:49155 CLOSED          536      lsass.exe
0x3e6fe830         TCPv4    10.1.1.10:64530                10.1.1.3:80          ESTABLISHED      3376     OUTLOOK.EXE
0x3ec374e8         UDPv4    127.0.0.1:65038                *:*                                   -1                2015-10-09 11:05:05 UTC+0000
0x3ecc27f0         UDPv4    10.1.1.10:137                  *:*                                   4        System   2015-10-09 12:18:41 UTC+0000
```

```
maman@ubuntu:~/volatility/pos01$ vol.py -f POS-01-c4e8f786.vmss --profile=Win7SP1x86_23418 malfind -p 3208
Volatility Foundation Volatility Framework 2.6.1
Process: iexplore.exe Pid: 3208 Address: 0x50000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 11, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000000050000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x0000000000050010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x0000000000050020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x0000000000050030  00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00   ................

0x0000000000050000 4d              DEC EBP
0x0000000000050001 5a              POP EDX
0x0000000000050002 90              NOP
0x0000000000050003 0003            ADD [EBX], AL
0x0000000000050005 0000            ADD [EAX], AL
0x0000000000050007 000400          ADD [EAX+EAX], AL
0x000000000005000a 0000            ADD [EAX], AL
0x000000000005000c ff              DB 0xff
0x000000000005000d ff00            INC DWORD [EAX]
0x000000000005000f 00b800000000    ADD [EAX+0x0], BH
0x0000000000050015 0000            ADD [EAX], AL
0x0000000000050017 004000          ADD [EAX+0x0], AL
0x000000000005001a 0000            ADD [EAX], AL
0x000000000005001c 0000            ADD [EAX], AL
0x000000000005001e 0000            ADD [EAX], AL
0x0000000000050020 0000            ADD [EAX], AL
0x0000000000050022 0000            ADD [EAX], AL
0x0000000000050024 0000            ADD [EAX], AL
0x0000000000050026 0000            ADD [EAX], AL
0x0000000000050028 0000            ADD [EAX], AL
0x000000000005002a 0000            ADD [EAX], AL
0x000000000005002c 0000            ADD [EAX], AL
0x000000000005002e 0000            ADD [EAX], AL
0x0000000000050030 0000            ADD [EAX], AL
0x0000000000050032 0000            ADD [EAX], AL
0x0000000000050034 0000            ADD [EAX], AL
0x0000000000050036 0000            ADD [EAX], AL
0x0000000000050038 0000            ADD [EAX], AL
0x000000000005003a 0000            ADD [EAX], AL
0x000000000005003c d800            FADD DWORD [EAX]
0x000000000005003e 0000            ADD [EAX], AL

maman@ubuntu:~/volatility/pos01$
```

```
maman@ubuntu:~/volatility/pos01$ vol.py -f POS-01-c4e8f786.vmss --profile=Win7SP1x86_23418 malfind -p 3208 -D dump/
Volatility Foundation Volatility Framework 2.6.1
Process: iexplore.exe Pid: 3208 Address: 0x50000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 11, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000000050000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x0000000000050010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x0000000000050020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x0000000000050030  00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00   ................

0x0000000000050000 4d              DEC EBP
0x0000000000050001 5a              POP EDX
0x0000000000050002 90              NOP
0x0000000000050003 0003            ADD [EBX], AL
0x0000000000050005 0000            ADD [EAX], AL
0x0000000000050007 000400          ADD [EAX+EAX], AL
0x000000000005000a 0000            ADD [EAX], AL
0x000000000005000c ff              DB 0xff
0x000000000005000d ff00            INC DWORD [EAX]
0x000000000005000f 00b800000000    ADD [EAX+0x0], BH
0x0000000000050015 0000            ADD [EAX], AL
0x0000000000050017 004000          ADD [EAX+0x0], AL
0x000000000005001a 0000            ADD [EAX], AL
0x000000000005001c 0000            ADD [EAX], AL
0x000000000005001e 0000            ADD [EAX], AL
0x0000000000050020 0000            ADD [EAX], AL
0x0000000000050022 0000            ADD [EAX], AL
0x0000000000050024 0000            ADD [EAX], AL
0x0000000000050026 0000            ADD [EAX], AL
0x0000000000050028 0000            ADD [EAX], AL
0x000000000005002a 0000            ADD [EAX], AL
0x000000000005002c 0000            ADD [EAX], AL
0x000000000005002e 0000            ADD [EAX], AL
0x0000000000050030 0000            ADD [EAX], AL
0x0000000000050032 0000            ADD [EAX], AL
0x0000000000050034 0000            ADD [EAX], AL
0x0000000000050036 0000            ADD [EAX], AL
0x0000000000050038 0000            ADD [EAX], AL
0x000000000005003a 0000            ADD [EAX], AL
0x000000000005003c d800            FADD DWORD [EAX]
0x000000000005003e 0000            ADD [EAX], AL
```

```
maman@ubuntu:~/volatility/pos01/dump$ ls
process.0x83f324d8.0x50000.dmp
maman@ubuntu:~/volatility/pos01/dump$ sha256sum process.0x83f324d8.0x50000.dmp
bf867ffc68f3f1c23bc3402e4494d83e738cc6e158c4f57176b4f5def412e056  process.0x83f324d8.0x50000.dmp
maman@ubuntu:~/volatility/pos01/dump$
```




```
maman@ubuntu:~/volatility/pos01$ vol.py -f POS-01-c4e8f786.vmss --profile=Win7SP1x86_23418 pslist | grep -i 3208
Volatility Foundation Volatility Framework 2.6.1
0x83f324d8 iexplore.exe           3208   3324     11      214      2      0 2015-10-09 12:35:57 UTC+0000
0x855d86d0 iexplore.exe           3136   3208      2       32      2      0 2015-10-09 12:35:57 UTC+0000
```

```
maman@ubuntu:~/volatility/pos01$ vol.py -f POS-01-c4e8f786.vmss --profile=Win7SP1x86_23418 malfind -p 3208
Volatility Foundation Volatility Framework 2.6.1
Process: iexplore.exe Pid: 3208 Address: 0x50000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 11, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000000050000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x0000000000050010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x0000000000050020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x0000000000050030  00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00   ................

0x0000000000050000 4d               DEC EBP
0x0000000000050001 5a               POP EDX
0x0000000000050002 90               NOP
0x0000000000050003 0003             ADD [EBX], AL
0x0000000000050005 0000             ADD [EAX], AL
0x0000000000050007 000400           ADD [EAX+EAX], AL
0x000000000005000a 0000             ADD [EAX], AL
0x000000000005000c ff               DB 0xff
0x000000000005000d ff00             INC DWORD [EAX]
0x000000000005000f 00b800000000     ADD [EAX+0x0], BH
0x0000000000050015 0000             ADD [EAX], AL
0x0000000000050017 004000           ADD [EAX+0x0], AL
0x000000000005001a 0000             ADD [EAX], AL
0x000000000005001c 0000             ADD [EAX], AL
0x000000000005001e 0000             ADD [EAX], AL
0x0000000000050020 0000             ADD [EAX], AL
0x0000000000050022 0000             ADD [EAX], AL
0x0000000000050024 0000             ADD [EAX], AL
0x0000000000050026 0000             ADD [EAX], AL
0x0000000000050028 0000             ADD [EAX], AL
0x000000000005002a 0000             ADD [EAX], AL
0x000000000005002c 0000             ADD [EAX], AL
0x000000000005002e 0000             ADD [EAX], AL
0x0000000000050030 0000             ADD [EAX], AL
0x0000000000050032 0000             ADD [EAX], AL
0x0000000000050034 0000             ADD [EAX], AL
0x0000000000050036 0000             ADD [EAX], AL
0x0000000000050038 0000             ADD [EAX], AL
0x000000000005003a 0000             ADD [EAX], AL
0x000000000005003c d800             FADD DWORD [EAX]
0x000000000005003e 0000             ADD [EAX], AL
```

```
maman@ubuntu:~/volatility/pos01$ vol.py -f POS-01-c4e8f786.vmss --profile=Win7SP1x86_23418 dlldump -p 3208 --base=0x50000 -D sample/
Volatility Foundation Volatility Framework 2.6.1
Process(V) Name                  Module Base Module Name          Result
---------- -------------------- ----------- -------------------- ------
0x83f324d8 iexplore.exe         0x00050000 UNKNOWN              OK: module.3208.3fd324d8.50000.dll
maman@ubuntu:~/volatility/pos01$
```

```
maman@ubuntu:~/volatility/pos01/sample$ strings -a module.3208.3fd324d8.50000.dll
!This program cannot be run in DOS mode.
RichH
.text
.data
.idata
@.rsrc
@.reloc
allsafe_protector.exe
svchost.exe
iexplore.exe
explorer.exe
System
smss.exe
csrss.exe
winlogon.exe
lsass.exe
spoolsv.exe
alg.exe
wuauclt.exe
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
SeDebugPrivilege
NtQueryInformationProcess
NTDLL.DLL
54.84.237.92
gateway.php
GetNativeSystemInfo
kernel32.dll
Windows 2000
Windows XP
Windows XP Professional x64
Windows Server 2003
Windows Home Server
Windows Server 2003 R2
Windows Vista
Windows Server 2008
Windows Server R2
Windows 7
64 Bit
32 Bit
Machines
Mozilla/4.0(compatible; MSIE 7.0b; Windows NT 6.0)
POST
Content-Type:application/x-www-form-urlencoded
http://%s%s
Software\Microsoft\Windows\CurrentVersion\Policies\Associations
LowRiskFileTypes
```

```
maman@ubuntu:~/volatility/pos01$ vol.py -f POS-01-c4e8f786.vmss --profile=Win7SP1x86_23418 timeliner | grep "54.84.237.92"
Volatility Foundation Volatility Framework 2.6.1
2015-10-09 12:35:55 UTC+0000|[IEHISTORY]| explorer.exe->Visited: pos@http://54.84.237.92/allsafe_update.exe| PID: 1836/Cache type "URL " at 0x1c05300 End: 2015-10-09 12:35:55 UTC+0000
2015-10-09 12:35:57 UTC+0000|[IEHISTORY]| explorer.exe->Visited: pos@http://54.84.237.92/allsafe_update.exe| PID: 1836/Cache type "URL " at 0x1c05400 End: 2015-10-09 12:35:57 UTC+0000
2015-10-09 08:35:55 UTC+0000|[IEHISTORY]| explorer.exe->:2015100920151010: pos@http://54.84.237.92/allsafe_update.exe| PID: 1836/Cache type "URL " at 0x1db5400 End: 2015-10-09 12:35:55 UTC+0000
2015-10-09 08:35:55 UTC+0000|[IEHISTORY]| explorer.exe->:2015100920151010: pos@:Host: 54.84.237.92| PID: 1836/Cache type "URL " at 0x1db5500 End: 2015-10-09 12:35:55 UTC+0000
2015-10-09 08:35:57 UTC+0000|[IEHISTORY]| explorer.exe->:2015100920151010: pos@http://54.84.237.92/allsafe_update.exe| PID: 1836/Cache type "URL " at 0x1db5600 End: 2015-10-09 12:35:57 UTC+0000
2015-10-09 12:35:55 UTC+0000|[IEHISTORY]| OUTLOOK.EXE->Visited: pos@http://54.84.237.92/allsafe_update.exe| PID: 3376/Cache type "URL " at 0x3a85300 End: 2015-10-09 12:35:55 UTC+0000
2015-10-09 12:35:57 UTC+0000|[IEHISTORY]| OUTLOOK.EXE->Visited: pos@http://54.84.237.92/allsafe_update.exe| PID: 3376/Cache type "URL " at 0x3a85400 End: 2015-10-09 12:35:57 UTC+0000
```