Practical-3

AIM: Memory analysis of malware samples using tools such as Volatility.

```
──(root㉿kali)-[/home/Downloads]
└─# ls
sample.vmem  stuxnet.zip  volatility-installation-main  volatility-installation-main.zip

┌──(root㉿kali)-[/home/Downloads]
└─# cd volatility-installation-main

┌──(root㉿kali)-[/home/Downloads/volatility-installation-main]
└─# chmod +x volatility-installation.sh

┌──(root㉿kali)-[/home/Downloads/volatility-installation-main]
└─# ./volatility-installation.sh
volatility is not found
Cloning into 'volatility'...
remote: Enumerating objects: 27411, done.
remote: Total 27411 (delta 0), reused 0 (delta 0), pack-reused 27411 (from 1)
Receiving objects: 100% (27411/27411), 21.10 MiB | 9.60 MiB/s, done.
Resolving deltas: 100% (19758/19758), done.
volatility is cloned at /opt directory
Volatility Foundation Volatility Framework 2.6.1
^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B*** Failed to import
volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named
Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named
Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name
'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module
named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module
named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named
Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module
named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named
Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named
Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module
named Crypto.Hash)
```

```
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
ERROR   : volatility.debug    : You must specify something to do (try -h)
python2-dev is available. Installing...
Reading package lists... Done[[B^[[B
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libpython2-dev libpython2.7 libpython2.7-dev python2.7-dev
The following NEW packages will be installed:
  libpython2-dev libpython2.7 libpython2.7-dev python2-dev python2.7-dev
0 upgraded, 5 newly installed, 0 to remove and 52 not upgraded.
Need to get 3475 kB of archives.
After this operation, 16.2 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 libpython2.7 amd64 2.7.18-13.2 [1015 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 python2.7-dev amd64 2.7.18-13.2 [291 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 python2-dev amd64 2.7.18-3 [1216 B]
Get:3 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 libpython2-dev amd64 2.7.18-3 [21.3 kB]
Get:2 http://mirror.kku.ac.th/kali kali-rolling/main amd64 libpython2.7-dev amd64 2.7.18-13.2 [2145 kB]
Fetched 3475 kB in 4s (930 kB/s)
Selecting previously unselected package libpython2.7:amd64.
(Reading database ... 415865 files and directories currently installed.)
Preparing to unpack .../libpython2.7_2.7.18-13.2_amd64.deb ...
```

```
Unpacking libpython2.7:amd64 (2.7.18-13.2) ...
Selecting previously unselected package libpython2.7-dev:amd64.
Preparing to unpack .../libpython2.7-dev_2.7.18-13.2_amd64.deb ...
Unpacking libpython2.7-dev:amd64 (2.7.18-13.2) ...
Selecting previously unselected package libpython2-dev:amd64.
Preparing to unpack .../libpython2-dev_2.7.18-3_amd64.deb ...
Unpacking libpython2-dev:amd64 (2.7.18-3) ...
Selecting previously unselected package python2.7-dev.
Preparing to unpack .../python2.7-dev_2.7.18-13.2_amd64.deb ...
Unpacking python2.7-dev (2.7.18-13.2) ...
Selecting previously unselected package python2-dev.
Preparing to unpack .../python2-dev_2.7.18-3_amd64.deb ...
Unpacking python2-dev (2.7.18-3) ...
Setting up libpython2.7:amd64 (2.7.18-13.2) ...
Setting up libpython2.7-dev:amd64 (2.7.18-13.2) ...
Setting up libpython2-dev:amd64 (2.7.18-3) ...
Setting up python2.7-dev (2.7.18-13.2) ...
Setting up python2-dev (2.7.18-3) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...
Processing triggers for libc-bin (2.40-3) ...
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 1863k  100 1863k    0     0  5550k      0 --:--:-- --:--:-- --:--:-- 5562k
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please
upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop
support for Python 2.7 in January 2021. More details about Python 2 support in pip
can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-
support pip 21.0 will remove support for this functionality.
Collecting pip<21.0
  Downloading pip-20.3.4-py2.py3-none-any.whl (1.5 MB)
     |████████████████████████████████| 1.5 MB 2.2 MB/s
Collecting wheel
  Downloading wheel-0.37.1-py2.py3-none-any.whl (35 kB)
Installing collected packages: pip, wheel
Successfully installed pip-20.3.4 wheel-0.37.1
setuptools not found. Installing setuptools...
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please
upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop
support for Python 2.7 in January 2021. More details about Python 2 support in pip
can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-
support pip 21.0 will remove support for this functionality.
Collecting setuptools
  Downloading setuptools-44.1.1-py2.py3-none-any.whl (583 kB)
     |████████████████████████████████| 583 kB 3.8 MB/s
Installing collected packages: setuptools
Successfully installed setuptools-44.1.1
python2-dev is already installed.
pycrypto not found. Installing pycrypto...
```

```
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please
upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop
support for Python 2.7 in January 2021. More details about Python 2 support in pip
can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-
support pip 21.0 will remove support for this functionality.
Collecting pycrypto
  Downloading pycrypto-2.6.1.tar.gz (446 kB)
     |████████████████████████████████| 446 kB 2.7 MB/s
Building wheels for collected packages: pycrypto
  Building wheel for pycrypto (setup.py) ... done
  Created wheel for pycrypto: filename=pycrypto-2.6.1-cp27-cp27mu-
linux_x86_64.whl size=526420
sha256=1ee19bde1414614d81c276ba52a98bf2b34b275aae97b2d7b3d8069df57a0792
  Stored in directory:
/root/.cache/pip/wheels/b6/e6/c8/d1eca13628952ceec1d40d96e0a7a1380460d2349ce
0b85312
Successfully built pycrypto
Installing collected packages: pycrypto
Successfully installed pycrypto-2.6.1
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please
upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop
support for Python 2.7 in January 2021. More details about Python 2 support in pip
can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-
support pip 21.0 will remove support for this functionality.
WARNING: Package(s) not found: distorm3
distorm3 version 3.4.4 not found. Installing distorm3...
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please
upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop
support for Python 2.7 in January 2021. More details about Python 2 support in pip
can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-
support pip 21.0 will remove support for this functionality.
Collecting distorm3==3.4.4
  Downloading distorm3-3.4.4.tar.gz (134 kB)
     |████████████████████████████████| 134 kB 2.5 MB/s
Building wheels for collected packages: distorm3
  Building wheel for distorm3 (setup.py) ... done
  Created wheel for distorm3: filename=distorm3-3.4.4-cp27-cp27mu-
linux_x86_64.whl size=104823
sha256=974fa6162c39fe5dfa3eac17aee04f55c2e03d945268f2ad8e603402e77de112
  Stored in directory:
/root/.cache/pip/wheels/93/14/6f/aaeed0f34af1f5028e3ed4b7929b094caf7e4a62fcbf3e
3623
Successfully built distorm3
Installing collected packages: distorm3
Successfully installed distorm3-3.4.4
Pillow not found. Installing Pillow...
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please
upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop
support for Python 2.7 in January 2021. More details about Python 2 support in pip
```

```
can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
Collecting Pillow
  Downloading Pillow-6.2.2-cp27-cp27mu-manylinux1_x86_64.whl (2.1 MB)
     |████████████████████████████████| 2.1 MB 2.7 MB/s
Installing collected packages: Pillow
Successfully installed Pillow-6.2.2
Yara not found. Installing YARA...
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
Collecting yara-python==3.7.0
  Downloading yara-python-3.7.0.tar.gz (313 kB)
     |████████████████████████████████| 313 kB 2.7 MB/s
Building wheels for collected packages: yara-python
  Building wheel for yara-python (setup.py) ... done
  Created wheel for yara-python: filename=yara_python-3.7.0-cp27-cp27mu-linux_x86_64.whl size=318504 sha256=bbcec7a26e15914a9134466a796728681fad752c963b9e600183f9b4841b8cec
  Stored in directory: /root/.cache/pip/wheels/ee/b3/cb/f965b3725871e865a08fa76bb565c02d838afd0e9f0052c8c0
Successfully built yara-python
Installing collected packages: yara-python
Successfully installed yara-python-3.7.0
Volatility Foundation Volatility Framework 2.6.1
ERROR   : volatility.debug    : You must specify something to do (try -h)
Volatility is installed at /opt/volatility

┌──(root㉿kali)-[/home/Downloads]
└─# mv sample.vmem /opt/volatility/

┌──(root㉿kali)-[/]
└─# cd /opt/volatility/

┌──(root㉿kali)-[/opt/volatility]
└─# python2 vol.py -f sample.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/opt/volatility/sample.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80545ae0L
          Number of Processors : 1
```

```
    Image Type (Service Pack) : 3
            KPCR for CPU 0 : 0xffdff000L
         KUSER_SHARED_DATA : 0xffdf0000L
       Image date and time : 2011-06-03 04:31:36 UTC+0000
    Image local date and time : 2011-06-03 00:31:36 -0400

┌──(root㉿kali)-[/opt/volatility]
└─# python2 vol.py -f sample.vmem --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
- ------------------------------
0x823c8830 System                  4      0     59      403 ------      0
0x820df020 smss.exe              376      4      3       19 ------      0 2010-10-29 17:08:53
UTC+0000
0x821a2da0 csrss.exe             600    376     11      395      0      0 2010-10-29 17:08:54
UTC+0000
0x81da5650 winlogon.exe          624    376     19      570      0      0 2010-10-29
17:08:54 UTC+0000
0x82073020 services.exe          668    624     21      431      0      0 2010-10-29
17:08:54 UTC+0000
0x81e70020 lsass.exe             680    624     19      342      0      0 2010-10-29 17:08:54
UTC+0000
0x823315d8 vmacthlp.exe          844    668      1       25      0      0 2010-10-29
17:08:55 UTC+0000
0x81db8da0 svchost.exe           856    668     17      193      0      0 2010-10-29
17:08:55 UTC+0000
0x81e61da0 svchost.exe           940    668     13      312      0      0 2010-10-29
17:08:55 UTC+0000
0x822843e8 svchost.exe          1032    668     61     1169      0      0 2010-10-29
17:08:55 UTC+0000
0x81e18b28 svchost.exe          1080    668      5       80      0      0 2010-10-29
17:08:55 UTC+0000
0x81ff7020 svchost.exe          1200    668     14      197      0      0 2010-10-29
17:08:55 UTC+0000
0x81fee8b0 spoolsv.exe          1412    668     10      118      0      0 2010-10-29
17:08:56 UTC+0000
0x81e0eda0 jqs.exe              1580    668      5      148      0      0 2010-10-29 17:09:05
UTC+0000
0x81fe52d0 vmtoolsd.exe         1664    668      5      284      0      0 2010-10-29
17:09:05 UTC+0000
0x821a0568 VMUpgradeHelper      1816    668      3       96      0      0 2010-10-29
17:09:08 UTC+0000
0x8205ada0 alg.exe               188    668      6      107      0      0 2010-10-29 17:09:09
UTC+0000
0x820ec7e8 explorer.exe         1196   1728     16      582      0      0 2010-10-29
17:11:49 UTC+0000
0x820ecc10 wscntfy.exe          2040   1032      1       28      0      0 2010-10-29
17:11:49 UTC+0000
```

```
0x81e86978 TSVNCache.exe          324   1196      7        54      0        0 2010-10-29
17:11:49 UTC+0000
0x81fc5da0 VMwareTray.exe        1912   1196      1        50      0        0 2010-10-29
17:11:50 UTC+0000
0x81e6b660 VMwareUser.exe        1356   1196      9       251      0        0 2010-10-29
17:11:50 UTC+0000
0x8210d478 jusched.exe           1712   1196      1        26      0        0 2010-10-29
17:11:50 UTC+0000
0x82279998 imapi.exe              756    668      4       116      0        0 2010-10-29
17:11:54 UTC+0000
0x822b9a10 wuauclt.exe            976   1032      3       133      0        0 2010-10-29
17:12:03 UTC+0000
0x81c543a0 Procmon.exe            660   1196     13       189      0        0 2011-06-03
04:25:56 UTC+0000
0x81fa5390 wmiprvse.exe          1872    856      5       134      0        0 2011-06-03
04:25:58 UTC+0000
0x81c498c8 lsass.exe          868    668      2      23      0      0 2011-06-03 04:26:55
UTC+0000
0x81c47c00 lsass.exe         1928    668      4      65      0      0 2011-06-03 04:26:55
UTC+0000
0x81c0cda0 cmd.exe            968   1664      0 --------      0      0 2011-06-03 04:31:35
UTC+0000   2011-06-03 04:31:36 UTC+0000
0x81f14938 ipconfig.exe           304    968      0 --------       0       0 2011-06-03
04:31:35 UTC+0000   2011-06-03 04:31:36 UTC+0000
```

```
┌──(root㉿kali)-[/opt/volatility]
└─# python2 vol.py -f sample.vmem --profile=WinXPSP2x86 psscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Name                PID   PPID PDB        Time created                   Time
exited
------------------ ---------------- ------ ------ ---------- ------------------------------ -------------
-----------------
0x000000001e0cda0 cmd.exe              968   1664 0x0a9403a0 2011-06-03 04:31:35
UTC+0000   2011-06-03 04:31:36 UTC+0000
0x0000000001e47c00 lsass.exe          1928    668 0x0a9403c0 2011-06-03 04:26:55
UTC+0000
0x0000000001e498c8 lsass.exe           868    668 0x0a940360 2011-06-03 04:26:55
UTC+0000
0x0000000001e543a0  Procmon.exe              660      1196  0x0a940260  2011-06-03
04:25:56 UTC+0000
0x0000000001fa5650 winlogon.exe        624    376 0x0a940060 2010-10-29 17:08:54
UTC+0000
0x0000000001fb8da0 svchost.exe         856    668 0x0a9400e0 2010-10-29 17:08:55
UTC+0000
0x000000000200eda0 jqs.exe            1580    668 0x0a9401e0 2010-10-29 17:09:05
UTC+0000
0x0000000002018b28 svchost.exe        1080    668 0x0a940140 2010-10-29 17:08:55
UTC+0000
0x0000000002061da0 svchost.exe         940    668 0x0a940100 2010-10-29 17:08:55
UTC+0000
```

```
0x000000000206b660  VMwareUser.exe        1356     1196  0x0a9402e0  2010-10-29
17:11:50 UTC+0000
0x0000000002070020 lsass.exe            680     624 0x0a9400a0 2010-10-29 17:08:54
UTC+0000
0x0000000002086978  TSVNCache.exe          324     1196  0x0a940180  2010-10-29
17:11:49 UTC+0000
0x0000000002114938 ipconfig.exe        304     968 0x0a940380 2011-06-03 04:31:35
UTC+0000   2011-06-03 04:31:36 UTC+0000
0x00000000021a5390  wmiprvse.exe           1872       856  0x0a9401c0  2011-06-03
04:25:58 UTC+0000
0x00000000021c5da0  VMwareTray.exe        1912     1196  0x0a9402c0  2010-10-29
17:11:50 UTC+0000
0x00000000021e52d0  vmtoolsd.exe           1664       668  0x0a940200  2010-10-29
17:09:05 UTC+0000
0x00000000021ee8b0 spoolsv.exe        1412     668 0x0a9401a0 2010-10-29 17:08:56
UTC+0000
0x00000000021f7020 svchost.exe        1200     668 0x0a940160 2010-10-29 17:08:55
UTC+0000
0x000000000225ada0 alg.exe             188     668 0x0a940240 2010-10-29 17:09:09
UTC+0000
0x0000000002273020 services.exe        668     624 0x0a940080 2010-10-29 17:08:54
UTC+0000
0x00000000022df020 smss.exe             376       4 0x0a940020 2010-10-29 17:08:53
UTC+0000
0x00000000022ec7e8 explorer.exe       1196    1728 0x0a940280 2010-10-29 17:11:49
UTC+0000
0x00000000022ecc10 wscntfy.exe        2040    1032 0x0a9402a0 2010-10-29 17:11:49
UTC+0000
0x000000000230d478 jusched.exe        1712    1196 0x0a940300 2010-10-29 17:11:50
UTC+0000
0x00000000023a0568  VMUpgradeHelper       1816       668  0x0a940220  2010-10-29
17:09:08 UTC+0000
0x00000000023a2da0 csrss.exe           600     376 0x0a940040 2010-10-29 17:08:54
UTC+0000
0x0000000002479998 imapi.exe           756     668 0x0a940320 2010-10-29 17:11:54
UTC+0000
0x00000000024843e8 svchost.exe        1032     668 0x0a940120 2010-10-29 17:08:55
UTC+0000
0x00000000024b9a10 wuauclt.exe         976    1032 0x0a940340 2010-10-29 17:12:03
UTC+0000
0x00000000025315d8 vmacthlp.exe        844     668 0x0a9400c0 2010-10-29 17:08:55
UTC+0000
0x00000000025c8830 System              4       0 0x00319000
```