ASSIGNMENT NO 3 : MUHAMMAD HAMAD

Result of all command are present in "stuxnet-commands-results" folder and "newimage-commands-results" folder

1-Imageinfo

The command will tell us about the possible operating system running on system when image was created and tell us about number of processors of the respective system and also gives time and date of image created

```
D:\digital forensic\Assignment 3\volatility_2.5.win.standalone>volatility-2.5.st
andalone.exe -f stuxnet.vmem imageinfo
Volatility Foundation Volatility Framework 2.5
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with Win
XPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (D:\digital forensic\Assignmen
t 3\volatility_2.5.win.standalone\stuxnet.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
```

2-KDBGSCAN

Provides correct kdbg profile and give memory address of kdbg and kdbg header it displayed two structures one of which is correct.

```
D:\digital forensic\Assignment 3\volatility_2.5.win.standalone>volatility-2.5.st
andalone.exe --profile=WinXPSP2x86 -f stuxnet.vmem kdbgscan
Volatility Foundation Volatility Framework 2.5
**************************************************
Instantiating KDBG using: Kernel AS WinXPSP2x86 (5.1.0 32bit)
Offset (V)                    : 0x80545ae0
Offset (P)                    : 0x545ae0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): WinXPSP3x86
Version64                     : 0x80545ab8 (Major: 15, Minor: 2600)
Service Pack (CmNtCSDVersion) : 3
Build string (NtBuildLab)     : 2600.xpsp.080413-2111
PsActiveProcessHead           : 0x8055a158 (31 processes)
PsLoadedModuleList            : 0x80553fc0 (122 modules)
KernelBase                    : 0x804d7000 (Matches MZ: True)
Major (OptionalHeader)        : 5
Minor (OptionalHeader)        : 1
KPCR                          : 0xffdff000 (CPU 0)

**************************************************
Instantiating KDBG using: Kernel AS WinXPSP2x86 (5.1.0 32bit)
Offset (V)                    : 0x80545ae0
Offset (P)                    : 0x545ae0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): WinXPSP2x86
Version64                     : 0x80545ab8 (Major: 15, Minor: 2600)
Service Pack (CmNtCSDVersion) : 3
Build string (NtBuildLab)     : 2600.xpsp.080413-2111
PsActiveProcessHead           : 0x8055a158 (31 processes)
PsLoadedModuleList            : 0x80553fc0 (122 modules)
KernelBase                    : 0x804d7000 (Matches MZ: True)
Major (OptionalHeader)        : 5
Minor (OptionalHeader)        : 1
KPCR                          : 0xffdff000 (CPU 0)
```

3-PSLIST

Display list of all processes along with their process id and parent id and also gives the creation time of processes. In the current scenario their exist three processes with name lsaas.exe and it seems that 2 of them are malicious, for this purpose we checked the parent id's and creation time of all 3 processes one of them with process id 680 is created by winlogon.exe at the same time when winlogon.exe was created and other 2 are created by services.exe and creation time of services.exe and lsaas.exe is different, so these 2 are malicious.

```
D:\digital forensic\Assignment 3\volatility_2.5.win.standalone>volatility-2.5.st
andalone -f stuxnet.vmem pslist pslist.txt
Volatility Foundation Volatility Framework 2.5
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Star
t                           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
```

4-PSSCAN

This can find processes that previously terminated (inactive) and processes that have been hidden or unlinked by a rootkit. The downside is that rootkits can still hide by overwriting the pool tag values.

Offset(P)	Name	PID	PPID	PDB	Time created	Time exited
0x0000000001e0cda0	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	
0x000000000024b9a10	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		

5-PSTREE

To view the process listing in tree form, use the pstree command. This enumerates processes using the same technique as pslist, so it will also not show hidden or unlinked processes. Child process are indicated using indention and periods.

```
Name                                                 Pid   PPid   Thds   Hnds Time
---------------------------------------------------- ------ ------ ------ ------ ----
 0x823c8830:System                                      4      0     59    403 1970-01-01 00:00:00 UTC+0000
. 0x820df020:smss.exe                                 376      4      3     19 2010-10-29 17:08:53 UTC+0000
.. 0x821a2da0:csrss.exe                               600    376     11    395 2010-10-29 17:08:54 UTC+0000
.. 0x81da5650:winlogon.exe                            624    376     19    570 2010-10-29 17:08:54 UTC+0000
... 0x82073020:services.exe                           668    624     21    431 2010-10-29 17:08:54 UTC+0000
.... 0x81fe52d0:vmtoolsd.exe                         1664    668      5    284 2010-10-29 17:09:05 UTC+0000
..... 0x81c0cda0:cmd.exe                              968   1664      0 ------ 2011-06-03 04:31:35 UTC+0000
...... 0x81f14938:ipconfig.exe                        304    968      0 ------ 2011-06-03 04:31:35 UTC+0000
.... 0x822843e8:svchost.exe                          1032    668     61   1169 2010-10-29 17:08:55 UTC+0000
..... 0x822b9a10:wuauclt.exe                          976   1032      3    133 2010-10-29 17:12:03 UTC+0000
..... 0x820ecc10:wscntfy.exe                         2040   1032      1     28 2010-10-29 17:11:49 UTC+0000
.... 0x81e61da0:svchost.exe                           940    668     13    312 2010-10-29 17:08:55 UTC+0000
.... 0x81db8da0:svchost.exe                           856    668     17    193 2010-10-29 17:08:55 UTC+0000
..... 0x81fa5390:wmiprvse.exe                        1872    856      5    134 2011-06-03 04:25:58 UTC+0000
.... 0x821a0568:VMUpgradeHelper                      1816    668      3     96 2010-10-29 17:09:08 UTC+0000
.... 0x81fee8b0:spoolsv.exe                          1412    668     10    118 2010-10-29 17:08:56 UTC+0000
.... 0x81ff7020:svchost.exe                          1200    668     14    197 2010-10-29 17:08:55 UTC+0000
.... 0x81c47c00:lsass.exe                            1928    668      4     65 2011-06-03 04:26:55 UTC+0000
.... 0x81e18b28:svchost.exe                          1080    668      5     80 2010-10-29 17:08:55 UTC+0000
.... 0x8205ada0:alg.exe                               188    668      6    107 2010-10-29 17:09:09 UTC+0000
.... 0x823315d8:vmacthlp.exe                          844    668      1     25 2010-10-29 17:08:55 UTC+0000
.... 0x81e0eda0:jqs.exe                              1580    668      5    148 2010-10-29 17:09:05 UTC+0000
.... 0x81c498c8:lsass.exe                             868    668      2     23 2011-06-03 04:26:55 UTC+0000
.... 0x82279998:imapi.exe                             756    668      4    116 2010-10-29 17:11:54 UTC+0000
... 0x81e70020:lsass.exe                              680    624     19    342 2010-10-29 17:08:54 UTC+0000
 0x820ec7e8:explorer.exe                             1196   1728     16    582 2010-10-29 17:11:49 UTC+0000
. 0x81c543a0:Procmon.exe                             660   1196     13    189 2011-06-03 04:25:56 UTC+0000
. 0x81e86978:TSVNCache.exe                           324   1196      7     54 2010-10-29 17:11:49 UTC+0000
. 0x81e6b660:VMwareUser.exe                         1356   1196      9    251 2010-10-29 17:11:50 UTC+0000
. 0x8210d478:jusched.exe                            1712   1196      1     26 2010-10-29 17:11:50 UTC+0000
. 0x81fc5da0:VMwareTray.exe                         1912   1196      1     50 2010-10-29 17:11:50 UTC+0000
```

6-GETSIDS

To view the SIDs (Security Identifiers) associated with a process, use the getsids command. Among other things, this can help you identify processes which have maliciously escalated privileges and which processes belong to specific users

Here all three processes have same privileges, but according to us only original lsaas.exe should have these privileges

```
D:\digital forensic\Assignment 3\volatility_2.5.win.standalone>volatility-2.5.st
andalone --profile=WinXPSP3x86 -f stuxnet.vmem getsids -p 1928,868,680
Volatility Foundation Volatility Framework 2.5
lsass.exe (680): S-1-5-18 (Local System)
lsass.exe (680): S-1-5-32-544 (Administrators)
lsass.exe (680): S-1-1-0 (Everyone)
lsass.exe (680): S-1-5-11 (Authenticated Users)
lsass.exe (868): S-1-5-18 (Local System)
lsass.exe (868): S-1-5-32-544 (Administrators)
lsass.exe (868): S-1-1-0 (Everyone)
lsass.exe (868): S-1-5-11 (Authenticated Users)
lsass.exe (1928): S-1-5-18 (Local System)
lsass.exe (1928): S-1-5-32-544 (Administrators)
lsass.exe (1928): S-1-1-0 (Everyone)
lsass.exe (1928): S-1-5-11 (Authenticated Users)
```

7-Malfind

The malfind command helps find hidden or injected code/DLLs in user mode memory, based on characteristics such as VAD tag and page permissions.

Here this command found that malicious signatures have been matched to the processes given in the command and also it provides the command in assembly languages. Snapshot is not complete please concern the text file malfind.txt

```
Process: lsass.exe Pid: 868 Address: 0x80000
Vad Tag: Vad  Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x00080000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x00080010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x00080020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00080030  00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00   ................

0x00080000 4d              DEC EBP
0x00080001 5a              POP EDX
0x00080002 90              NOP
0x00080003 0003            ADD [EBX], AL
0x00080005 0000            ADD [EAX], AL
0x00080007 000400          ADD [EAX+EAX], AL
0x0008000a 0000            ADD [EAX], AL
0x0008000c ff              DB 0xff
0x0008000d ff00            INC DWORD [EAX]
0x0008000f 00b800000000    ADD [EAX+0x0], BH
0x00080015 0000            ADD [EAX], AL
0x00080017 004000          ADD [EAX+0x0], AL
0x0008001a 0000            ADD [EAX], AL
0x0008001c 0000            ADD [EAX], AL
0x0008001e 0000            ADD [EAX], AL
0x00080020 0000            ADD [EAX], AL
0x00080022 0000            ADD [EAX], AL
0x00080024 0000            ADD [EAX], AL
0x00080026 0000            ADD [EAX], AL
0x00080028 0000            ADD [EAX], AL
0x0008002a 0000            ADD [EAX], AL
0x0008002c 0000            ADD [EAX], AL
0x0008002e 0000            ADD [EAX], AL
0x00080030 0000            ADD [EAX], AL
0x00080032 0000            ADD [EAX], AL
0x00080034 0000            ADD [EAX], AL
0x00080036 0000            ADD [EAX], AL
```

8-Malfind –D malcode

Save the memory dumps of processes provided in command in malcode directory , windows defender found it suspicious and immediately deleted all that dumps.

Dumps are present in malcode folder.

9-VADINFO

The vadinfo command displays extended information about a process's VAD nodes. In particular, it shows:

- The address of the MMVAD structure in kernel memory
- The starting and ending virtual addresses in process memory that the MMVAD structure pertains to
- The VAD Tag
- The VAD flags, control flags, etc
- The name of the memory mapped file (if one exists)
- The memory protection constant (permissions).

```
D:\digital forensic\Assignment 3\volatility_2.5.win.standalone>volatility-2.5.st
andalone --profile=WinXPSP3x86 -f stuxnet.vmem -p 1928,868,680 -p 868 vadinfo
Volatility Foundation Volatility Framework 2.5
**************************************************************************
Pid:    868
VAD node @ 0x81f459d0 Start 0x00210000 End 0x0021ffff Tag Vad
Flags: Protection: 4
Protection: PAGE_READWRITE
ControlArea @8211ec60 Segment e12e2a48
NumberOfSectionReferences:          0 NumberOfPfnReferences:           0
NumberOfMappedViews:                2 NumberOfUserReferences:          2
Control Flags: HadUserReference: 1, Reserve: 1
First prototype PTE: e12e2a88 Last contiguous PTE: e12e2b00
Flags2:

VAD node @ 0x822e7e70 Start 0x00080000 End 0x000f9fff Tag Vad
Flags: Protection: 6
Protection: PAGE_EXECUTE_READWRITE
ControlArea @81de9890 Segment e2b7dbf0
NumberOfSectionReferences:          0 NumberOfPfnReferences:           0
NumberOfMappedViews:                1 NumberOfUserReferences:          1
Control Flags: Commit: 1, HadUserReference: 1
First prototype PTE: e2b7dc30 Last contiguous PTE: e2b7dff8
Flags2: Inherit: 1

VAD node @ 0x81fc8520 Start 0x00010000 End 0x00010fff Tag VadS
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 4
Protection: PAGE_READWRITE

VAD node @ 0x82122368 Start 0x00020000 End 0x00020fff Tag VadS
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 4
Protection: PAGE_READWRITE

VAD node @ 0x82297138 Start 0x00030000 End 0x0006ffff Tag VadS
Flags: CommitCharge: 7, PrivateMemory: 1, Protection: 4
Protection: PAGE_READWRITE

VAD node @ 0x820817c0 Start 0x00070000 End 0x00072fff Tag Vad
Flags: NoChange: 1, Protection: 1
Protection: PAGE_READONLY
ControlArea @8210e110 Segment e11ab260
NumberOfSectionReferences:          1 NumberOfPfnReferences:           0
NumberOfMappedViews:               12 NumberOfUserReferences:         13
Control Flags: Commit: 1, HadUserReference: 1
First prototype PTE: e11ab2a0 Last contiguous PTE: e11ab2b0
Flags2: Inherit: 1, SecNoChange: 1

VAD node @ 0x81f65b60 Start 0x00100000 End 0x001fffff Tag VadS
Flags: CommitCharge: 6, PrivateMemory: 1, Protection: 4
Protection: PAGE_READWRITE
```

10-ldrmodules

There are many ways to hide a DLL. One of the ways involves unlinking the DLL from one (or all) of the linked lists in the PEB. However, when this is done, there is still information contained within the VAD (Virtual Address Descriptor) which identifies the base address of the DLL and its full path on disk. To cross-reference this information (known as memory mapped files) with the 3 PEB lists, use the ldrmodules command.

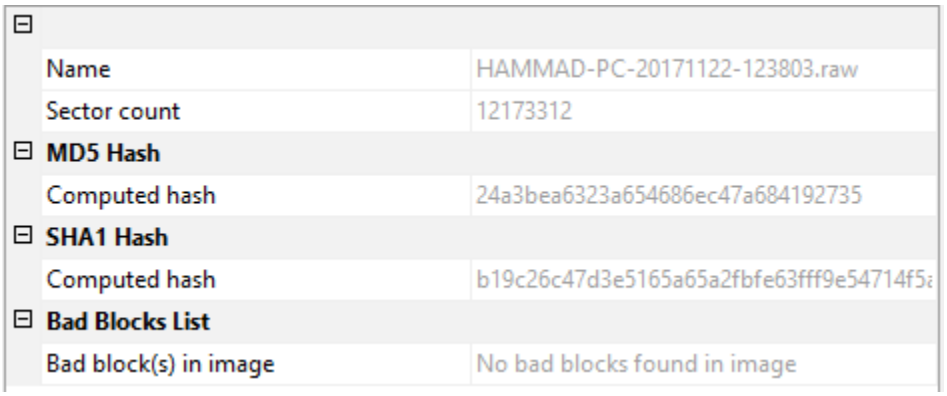
For each memory mapped PE file, the ldrmodules command prints True or False if the PE exists in the PEB lists.

```
Pid      Process              Base       InLoad InInit InMem MappedPath
-------- -------------------- ---------- ------ ------ ----- ----------
     868 lsass.exe            0x00080000 False  False  False
     868 lsass.exe            0x7c900000 True   True   True  \WINDOWS\system32\ntdll.dll
  Load Path: C:\WINDOWS\system32\ntdll.dll : ntdll.dll
  Init Path: C:\WINDOWS\system32\ntdll.dll : ntdll.dll
  Mem Path:  C:\WINDOWS\system32\ntdll.dll : ntdll.dll
     868 lsass.exe            0x77e70000 True   True   True  \WINDOWS\system32\rpcrt4.dll
  Load Path: C:\WINDOWS\system32\RPCRT4.dll : RPCRT4.dll
  Init Path: C:\WINDOWS\system32\RPCRT4.dll : RPCRT4.dll
  Mem Path:  C:\WINDOWS\system32\RPCRT4.dll : RPCRT4.dll
     868 lsass.exe            0x7c800000 True   True   True  \WINDOWS\system32\kernel32.dll
  Load Path: C:\WINDOWS\system32\kernel32.dll : kernel32.dll
  Init Path: C:\WINDOWS\system32\kernel32.dll : kernel32.dll
  Mem Path:  C:\WINDOWS\system32\kernel32.dll : kernel32.dll
     868 lsass.exe            0x77fe0000 True   True   True  \WINDOWS\system32\secur32.dll
  Load Path: C:\WINDOWS\system32\Secur32.dll : Secur32.dll
  Init Path: C:\WINDOWS\system32\Secur32.dll : Secur32.dll
  Mem Path:  C:\WINDOWS\system32\Secur32.dll : Secur32.dll
     868 lsass.exe            0x7e410000 True   True   True  \WINDOWS\system32\user32.dll
  Load Path: C:\WINDOWS\system32\USER32.dll : USER32.dll
  Init Path: C:\WINDOWS\system32\USER32.dll : USER32.dll
  Mem Path:  C:\WINDOWS\system32\USER32.dll : USER32.dll
     868 lsass.exe            0x01000000 True   False  True
  Load Path: C:\WINDOWS\system32\lsass.exe : lsass.exe
  Mem Path:  C:\WINDOWS\system32\lsass.exe : lsass.exe
     868 lsass.exe            0x77f10000 True   True   True  \WINDOWS\system32\gdi32.dll
  Load Path: C:\WINDOWS\system32\GDI32.dll : GDI32.dll
  Init Path: C:\WINDOWS\system32\GDI32.dll : GDI32.dll
  Mem Path:  C:\WINDOWS\system32\GDI32.dll : GDI32.dll
     868 lsass.exe            0x77dd0000 True   True   True  \WINDOWS\system32\advapi32.dll
  Load Path: C:\WINDOWS\system32\ADVAPI32.dll : ADVAPI32.dll
  Init Path: C:\WINDOWS\system32\ADVAPI32.dll : ADVAPI32.dll
  Mem Path:  C:\WINDOWS\system32\ADVAPI32.dll : ADVAPI32.dll
```

PART 2 - System Image

STEP 2- Image location: volatility_2.5.win.standalone\DumpIt\oldimage.raw

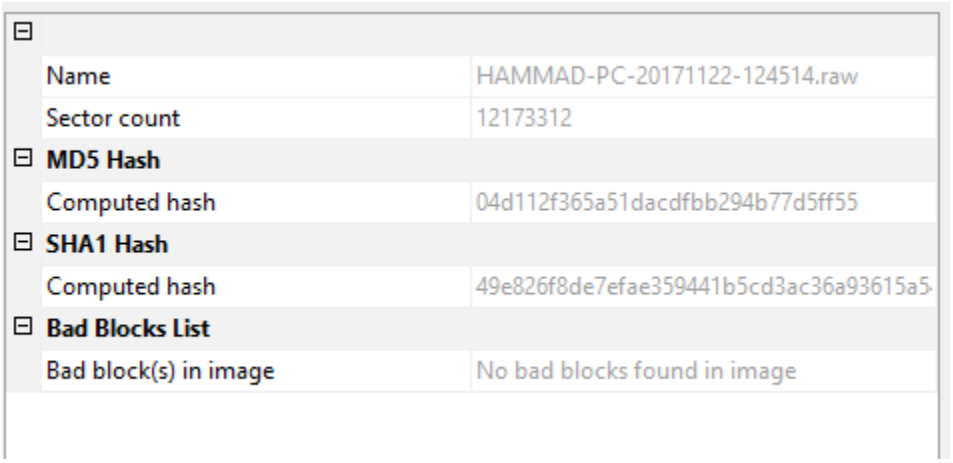
Hash of old image



Name	HAMMAD-PC-20171122-123803.raw
Sector count	12173312
MD5 Hash	
Computed hash	24a3bea6323a654686ec47a684192735
SHA1 Hash	
Computed hash	b19c26c47d3e5165a65a2fbfe63fff9e54714f5
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

STEP 3- Image location: volatility_2.5.win.standalone\newimage.raw

Hash of new image:

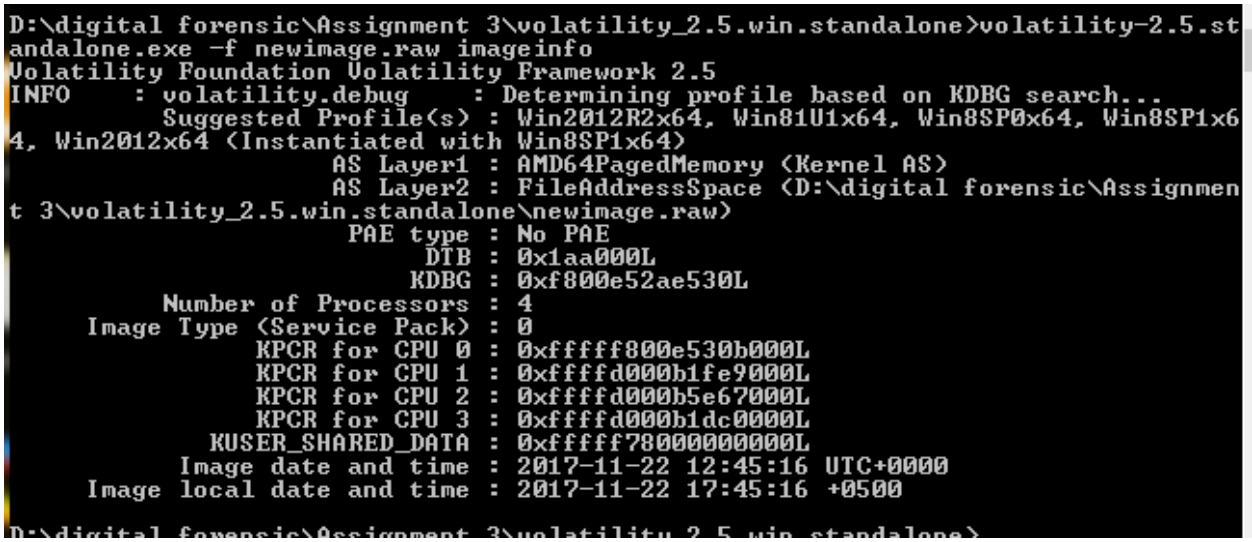


Name	HAMMAD-PC-20171122-124514.raw
Sector count	12173312
MD5 Hash	
Computed hash	04d112f365a51dacdfbb294b77d5ff55
SHA1 Hash	
Computed hash	49e826f8de7efae359441b5cd3ac36a93615a5
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

The hash values of newimage and oldimage are diffirent because the memory state is continuously changes

1-IMAGEINFO

It displays the suggested profiles/ operating system that were running on this system, in current scenario there are 5 suggested profiles. The number of processors in the system, and date, time of acquired image is also provided.



2-KDBGSCAN

As opposed to imageinfo which simply provides profile suggestions, kdbgscan is designed to positively identify the correct profile and the correct KDBG address (if there happen to be multiple). This plugin scans for the KDBGHeader signatures linked to Volatility profiles and applies sanity checks to reduce false positives.

Here it has shown just profile when command was executed.

```
**************************************************
Instantiating KDBG using: Unnamed AS Win8SP1x64 (6.3.9600 64bit)
Offset (V)                    : 0xf800e52ae530
Offset (P)                    : 0x1702ae530
KdCopyDataBlock (V)           : 0xf800e51e67e4
Block encoded                 : Yes
Wait never                    : 0xd01f92ce00913bf6
Wait always                   : 0x489ddd634c96d80
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win8SP1x64
Version64                     : 0xf800e52aee60 (Major: 15, Minor: 9600)
Service Pack (CmNtCSDVersion) : 0
Build string (NtBuildLab)     : 9600.18821.amd64fre.winblue_ltsb
PsActiveProcessHead           : 0xfffff800e52c7340 (75 processes)
PsLoadedModuleList            : 0xfffff800e52e1650 (158 modules)
KernelBase                    : 0xfffff800e500f000 (Matches MZ: True)
Major (OptionalHeader)        : 6
Minor (OptionalHeader)        : 3
KPCR                          : 0xfffff800e530b000 (CPU 0)
KPCR                          : 0xffffd000b1fe9000 (CPU 1)
KPCR                          : 0xffffd000b5e67000 (CPU 2)
KPCR                          : 0xffffd000b1dc0000 (CPU 3)
```

3-PSLIST

Displays all the system processes running on the system when memory acquisition of system was performed along with there process id’s and there parent process id’s

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start
0xffffe001f9802600	System	4	0	124	0	------	0	2017-11-19 06:05:48 UTC+0000
0xffffe001fb427380	smss.exe	340	4	2	0	------	0	2017-11-19 06:05:48 UTC+0000
0xffffe001fcb7f580	csrss.exe	472	460	10	0	0	0	2017-11-19 06:05:55 UTC+0000
0xffffe001fcdee080	wininit.exe	520	460	1	0	0	0	2017-11-19 06:05:56 UTC+0000
0xffffe001fce648c0	services.exe	620	520	4	0	0	0	2017-11-19 06:05:56 UTC+0000
0xffffe001fce941c0	lsass.exe	628	520	7	0	0	0	2017-11-19 06:05:56 UTC+0000
0xffffe001fcf8f8c0	svchost.exe	704	620	7	0	0	0	2017-11-19 06:05:58 UTC+0000
0xffffe001fcf83780	svchost.exe	740	620	9	0	0	0	2017-11-19 06:05:59 UTC+0000
0xffffe001fcfc9080	svchost.exe	856	620	24	0	0	0	2017-11-19 06:05:59 UTC+0000
0xffffe001fd000640	svchost.exe	884	620	44	0	0	0	2017-11-19 06:05:59 UTC+0000
0xffffe001fd05a080	svchost.exe	948	620	21	0	0	0	2017-11-19 06:05:59 UTC+0000
0xffffe001fb7e88c0	igfxCUIService	368	620	2	0	0	0	2017-11-19 06:06:03 UTC+0000
0xffffe001fd10c300	svchost.exe	384	620	15	0	0	0	2017-11-19 06:06:03 UTC+0000
0xffffe001fd188080	svchost.exe	80	620	16	0	0	0	2017-11-19 06:06:03 UTC+0000
0xffffe001fd3358c0	aerohost.exe	1224	884	2	0	0	0	2017-11-19 06:06:05 UTC+0000
0xffffe001fd317800	spoolsv.exe	1232	620	13	0	0	0	2017-11-19 06:06:05 UTC+0000
0xffffe001fd368300	svchost.exe	1256	620	22	0	0	0	2017-11-19 06:06:05 UTC+0000
0xffffe001fd420580	OfficeClickToR	1412	620	17	0	0	0	2017-11-19 06:06:06 UTC+0000
0xffffe001fd4a9080	svchost.exe	1448	620	9	0	0	0	2017-11-19 06:06:08 UTC+0000
0xffffe001fd4608c0	dasHost.exe	1472	384	3	0	0	0	2017-11-19 06:06:08 UTC+0000
0xffffe001fd521200	app_updater.ex	1488	620	57	0	0	1	2017-11-19 06:06:08 UTC+0000
0xffffe001fd5cb8c0	FoxitConnected	1772	620	9	0	0	1	2017-11-19 06:06:10 UTC+0000
0xffffe001fd4078c0	sqlwriter.exe	1988	620	2	0	0	0	2017-11-19 06:06:11 UTC+0000
0xffffe001fd490080	ss_conn_servic	2044	620	5	0	0	1	2017-11-19 06:06:11 UTC+0000
0xffffe001fdf086c0	svchost.exe	1292	620	6	0	0	0	2017-11-19 06:06:11 UTC+0000
0xffffe001fdeb08c0	MsMpEng.exe	1852	620	3	0	0	0	2017-11-19 06:06:11 UTC+0000
0xffffe001fe1634c0	svchost.exe	2628	620	3	0	0	0	2017-11-19 06:06:22 UTC+0000
0xffffe001fe15c780	svchost.exe	2648	620	16	0	0	0	2017-11-19 06:06:22 UTC+0000
0xffffe001fe7038c0	PresentationFo	3076	620	4	0	0	0	2017-11-19 06:06:28 UTC+0000
0xffffe001fea248c0	SearchIndexer.	3792	620	15	0	0	0	2017-11-19 06:06:36 UTC+0000
0xffffe001fde5d080	GoogleCrashHan	4596	3148	3	0	0	1	2017-11-19 06:07:23 UTC+0000
0xffffe001fc3f7800	GoogleCrashHan	4612	3148	3	0	0	0	2017-11-19 06:07:23 UTC+0000
0xffffe001fae164c0	Encrypto.Servi	3788	620	6	0	0	0	2017-11-19 06:08:19 UTC+0000
0xffffe001fe967080	VirtualBox.exe	1996	4932	0	--------	1	0	2017-11-19 06:08:25 UTC+0000

4-PSSCAN

This can find processes that previously terminated (inactive) and processes that have been hidden or unlinked by a rootkit. The downside is that rootkits can still hide by overwriting the pool tag values.

Offset(P)	Name	PID	PPID	PDB	Time created
0x00000000020ce8c0	dllhost.exe	304	704	0x0000000133edb000	2017-11-22 12:45:14 UTC+0000
0x0000000003f931c0	lsass.exe	628	520	0x00000000425b3000	2017-11-19 06:05:56 UTC+0000
0x000000000a951300	svchost.exe	384	620	0x0000000121ddc000	2017-11-19 06:06:03 UTC+0000
0x000000000efdb080	WmiPrvSE.exe	4912	704	0x000000002a869000	2017-11-22 12:23:09 UTC+0000
0x000000001021d080	igfxEM.exe	3560	4944	0x0000000138d14000	2017-11-22 12:13:46 UTC+0000
0x00000000172308c0	services.exe	620	520	0x000000007dced000	2017-11-19 06:05:56 UTC+0000
0x000000001d4d0340	onenoteim.exe	3204	704	0x000000001cbd9000	2017-11-22 12:16:41 UTC+0000
0x00000000287ec640	svchost.exe	884	620	0x000000011c198000	2017-11-19 06:05:59 UTC+0000
0x0000000031228080	explorer.exe	2876	5248	0x0000000135709000	2017-11-22 12:13:45 UTC+0000
0x00000000367258c0	ProductUpdater	3804	5320	0x00000001186b9000	2017-11-22 12:13:52 UTC+0000
0x000000003bc8c080	svchost.exe	80	620	0x0000000122f41000	2017-11-19 06:06:03 UTC+0000
0x000000003da39200	app_updater.ex	1488	620	0x000000012aff3000	2017-11-19 06:06:08 UTC+0000
0x000000003db5d8c0	conhost.exe	3160	3300	0x0000000080077000	2017-11-22 12:28:28 UTC+0000
0x000000003ef46080	svchost.exe	1448	620	0x000000012aded000	2017-11-19 06:06:08 UTC+0000
0x000000003fef4080	VirtualBox.exe	1484	1996	0x000000001f85e000	2017-11-19 06:08:26 UTC+0000
0x00000000443958c0	conhost.exe	5812	5548	0x00000000007e4000	2017-11-22 12:14:00 UTC+0000
0x000000004b225800	spoolsv.exe	1232	620	0x0000000126c0c000	2017-11-19 06:06:05 UTC+0000
0x000000005272f8c0	hpwuschd2.exe	3852	5320	0x000000007f9dc000	2017-11-22 12:13:51 UTC+0000
0x00000000589a78c0	FoxitConnected	1772	620	0x000000012eabf000	2017-11-19 06:06:10 UTC+0000
0x0000000058b37080	GoogleCrashHan	4596	3148	0x0000000022877000	2017-11-19 06:07:23 UTC+0000
0x0000000058d908c0	MsMpEng.exe	1852	620	0x00000000133d1000	2017-11-19 06:06:11 UTC+0000
0x0000000059b9c6c0	svchost.exe	1292	620	0x0000000132d04000	2017-11-19 06:06:11 UTC+0000
0x000000006024d580	OfficeClickToR	1412	620	0x00000001287a8000	2017-11-19 06:06:06 UTC+0000
0x0000000063bfc8c0	cmd.exe	3300	2876	0x000000006fe68000	2017-11-22 12:28:28 UTC+0000
0x00000000653ad8c0	rundll32.exe	1944	2876	0x0000000011847000	2017-11-22 12:13:50 UTC+0000
0x00000000653d1080	splwow64.exe	6056	2396	0x0000000101ca4000	2017-11-22 12:30:21 UTC+0000
0x000000006815f8c0	chrome.exe	2108	5124	0x000000016cfd1000	2017-11-22 12:35:05 UTC+0000
0x0000000069020180	dwm.exe	648	2292	0x000000002a7f5000	2017-11-21 13:38:46 UTC+0000
0x00000000715a38c0	aerohost.exe	1224	884	0x0000000126b96000	2017-11-19 06:06:05 UTC+0000
0x0000000074d5e080	wininit.exe	520	460	0x000000010f4c3000	2017-11-19 06:05:56 UTC+0000
0x0000000075fb68c0	PresentationFo	3076	620	0x000000014d4e1000	2017-11-19 06:06:28 UTC+0000
0x0000000076c8d8c0	sqlwriter.exe	1988	620	0x0000000013165a000	2017-11-19 06:06:11 UTC+0000
0x00000000771c6080	svchost.exe	948	620	0x000000011c968000	2017-11-19 06:05:59 UTC+0000
0x000000007965c780	svchost.exe	2648	620	0x0000000143d72000	2017-11-19 06:06:22 UTC+0000

5-PSTREE

Displays all the processes in the tree structure, and indentation and dots are used to show parent child relation.

```
Name                                                  Pid   PPid   Thds   Hnds Time
----------------------------------------------------- ------ ------ ------ ------ ----
 0xffffe001fcdee080:wininit.exe                       520    460      1      0 2017-11-19 06:05:56 UTC+0000
. 0xffffe001fce648c0:services.exe                     620    520      4      0 2017-11-19 06:05:56 UTC+0000
.. 0xffffe001fd10c300:svchost.exe                     384    620     15      0 2017-11-19 06:06:03 UTC+0000
... 0xffffe001fd4608c0:dasHost.exe                   1472    384      3      0 2017-11-19 06:06:08 UTC+0000
.. 0xffffe001fdf086c0:svchost.exe                     1292    620      6      0 2017-11-19 06:06:11 UTC+0000
.. 0xffffe001fe1634c0:svchost.exe                     2628    620      3      0 2017-11-19 06:06:22 UTC+0000
.. 0xffffe001fd521200:app_updater.ex                  1488    620     57      0 2017-11-19 06:06:08 UTC+0000
.. 0xffffe001fd420580:OfficeClickToR                  1412    620     17      0 2017-11-19 06:06:06 UTC+0000
.. 0xffffe001fd4a9080:svchost.exe                     1448    620      9      0 2017-11-19 06:06:08 UTC+0000
.. 0xffffe001fd05a080:svchost.exe                      948    620     21      0 2017-11-19 06:05:59 UTC+0000
.. 0xffffe001fd000640:svchost.exe                      884    620     44      0 2017-11-19 06:05:59 UTC+0000
... 0xffffe001fe87c080:taskhostex.exe                 1904    884      8      0 2017-11-22 12:13:45 UTC+0000
... 0xffffe001fd3358c0:aerohost.exe                   1224    884      2      0 2017-11-19 06:06:05 UTC+0000
.. 0xffffe001fdeb08c0:MsMpEng.exe                     1852    620      3      0 2017-11-19 06:06:11 UTC+0000
.. 0xffffe001fcf8f8c0:svchost.exe                      704    620      7      0 2017-11-19 06:05:58 UTC+0000
... 0xffffe001fc4f6080:WmiPrvSE.exe                    848    704      6      0 2017-11-22 12:45:15 UTC+0000
... 0xffffe001fd143600:RuntimeBroker.                 4188    704      3      0 2017-11-22 12:16:48 UTC+0000
... 0xffffe001ff178080:WmiPrvSE.exe                   4912    704      3      0 2017-11-22 12:23:09 UTC+0000
... 0xffffe001fad27200:WmiPrvSE.exe                   4192    704      5      0 2017-11-22 12:29:05 UTC+0000
... 0xffffe001f9e81340:onenoteim.exe                  3204    704     25      0 2017-11-22 12:16:41 UTC+0000
.. 0xffffe001fd4078c0:sqlwriter.exe                   1988    620      2      0 2017-11-19 06:06:11 UTC+0000
.. 0xffffe001fe15c780:svchost.exe                     2648    620     16      0 2017-11-19 06:06:22 UTC+0000
.. 0xffffe001fae164c0:Encrypto.Servi                  3788    620      6      0 2017-11-19 06:08:19 UTC+0000
.. 0xffffe001fd188080:svchost.exe                       80    620     16      0 2017-11-19 06:06:03 UTC+0000
.. 0xffffe001fcfc9080:svchost.exe                      856    620     24      0 2017-11-19 06:05:59 UTC+0000
... 0xffffe001f9f368c0:audiodg.exe                     852    856      5      0 2017-11-21 12:45:32 UTC+0000
.. 0xffffe001fea248c0:SearchIndexer.                  3792    620     15      0 2017-11-19 06:06:36 UTC+0000
.. 0xffffe001fe7038c0:PresentationFo                  3076    620      4      0 2017-11-19 06:06:28 UTC+0000
.. 0xffffe001fd317800:spoolsv.exe                     1232    620     13      0 2017-11-19 06:06:05 UTC+0000
.. 0xffffe001fcf83780:svchost.exe                      740    620      9      0 2017-11-19 06:05:59 UTC+0000
.. 0xffffe001fd368300:svchost.exe                     1256    620     22      0 2017-11-19 06:06:05 UTC+0000
.. 0xffffe001fd5cb8c0:FoxitConnected                  1772    620      9      0 2017-11-19 06:06:10 UTC+0000
.. 0xffffe001fb7e88c0:igfxCUIService                   368    620      2      0 2017-11-19 06:06:03 UTC+0000
.. 0xffffe001fd490080:ss_conn_servic                  2044    620      5      0 2017-11-19 06:06:11 UTC+0000
```

6-GETSIDS

To view the SIDs (Security Identifiers) associated with a process, use the getsids command.

```
FoxitConnected (1772): S-1-5-18 (Local System)
FoxitConnected (1772): S-1-5-32-544 (Administrators)
FoxitConnected (1772): S-1-1-0 (Everyone)
FoxitConnected (1772): S-1-5-11 (Authenticated Users)
FoxitConnected (1772): S-1-16-16384 (System Mandatory Level)
chrome.exe (3704): S-1-5-21-2756749756-3125308804-953656174-1001
chrome.exe (3704): S-1-5-21-2756749756-3125308804-953656174-513 (Domain Users)
chrome.exe (3704): S-1-1-0 (Everyone)
chrome.exe (3704): S-1-5-114 (Local Account (Member of Administrators))
chrome.exe (3704): S-1-5-32-544 (Administrators)
chrome.exe (3704): S-1-5-32-559 (BUILTIN\Performance Log Users)
chrome.exe (3704): S-1-5-32-545 (Users)
chrome.exe (3704): S-1-5-4 (Interactive)
chrome.exe (3704): S-1-2-1 (Console Logon (Users who are logged onto the physical console))
chrome.exe (3704): S-1-5-11 (Authenticated Users)
chrome.exe (3704): S-1-5-15 (This Organization)
chrome.exe (3704): S-1-5-113 (Local Account)
chrome.exe (3704): S-1-5-5-0-36544772 (Logon Session)
chrome.exe (3704): S-1-2-0 (Local (Users with the ability to log in locally))
chrome.exe (3704): S-1-5-64-10 (NTLM Authentication)
chrome.exe (3704): S-1-16-8192 (Medium Mandatory Level)
WINWORD.EXE (2396): S-1-5-21-2756749756-3125308804-953656174-1001
WINWORD.EXE (2396): S-1-5-21-2756749756-3125308804-953656174-513 (Domain Users)
WINWORD.EXE (2396): S-1-1-0 (Everyone)
WINWORD.EXE (2396): S-1-5-114 (Local Account (Member of Administrators))
WINWORD.EXE (2396): S-1-5-32-544 (Administrators)
WINWORD.EXE (2396): S-1-5-32-559 (BUILTIN\Performance Log Users)
WINWORD.EXE (2396): S-1-5-32-545 (Users)
WINWORD.EXE (2396): S-1-5-4 (Interactive)
WINWORD.EXE (2396): S-1-2-1 (Console Logon (Users who are logged onto the physical console))
WINWORD.EXE (2396): S-1-5-11 (Authenticated Users)
WINWORD.EXE (2396): S-1-5-15 (This Organization)
WINWORD.EXE (2396): S-1-5-113 (Local Account)
WINWORD.EXE (2396): S-1-5-5-0-36544772 (Logon Session)
WINWORD.EXE (2396): S-1-2-0 (Local (Users with the ability to log in locally))
WINWORD.EXE (2396): S-1-5-64-10 (NTLM Authentication)
```

7-MALFIND

Checks if some malware signature matches with the processes given in the command, here in my case winword process has some malicious pattern that is being matched with signature present in volatility

Processes used in command are 2396, 3704,1772 . Signature of 2396 has been matched .2396 is winword process

```
Process: WINWORD.EXE Pid: 2396 Address: 0x1f20000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: PrivateMemory: 1, Protection: 6

0x01f20000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ........
0x01f20010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ........
0x01f20020  00 00 00 00 00 00 f2 01 00 00 00 00 00 00 00 00   ........
0x01f20030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ........

0x01f20000 0000              ADD [EAX], AL
0x01f20002 0000              ADD [EAX], AL
0x01f20004 0000              ADD [EAX], AL
0x01f20006 0000              ADD [EAX], AL
0x01f20008 0000              ADD [EAX], AL
0x01f2000a 0000              ADD [EAX], AL
0x01f2000c 0000              ADD [EAX], AL
0x01f2000e 0000              ADD [EAX], AL
0x01f20010 0000              ADD [EAX], AL
0x01f20012 0000              ADD [EAX], AL
0x01f20014 0000              ADD [EAX], AL
0x01f20016 0000              ADD [EAX], AL
0x01f20018 0000              ADD [EAX], AL
0x01f2001a 0000              ADD [EAX], AL
0x01f2001c 0000              ADD [EAX], AL
0x01f2001e 0000              ADD [EAX], AL
0x01f20020 0000              ADD [EAX], AL
0x01f20022 0000              ADD [EAX], AL
0x01f20024 0000              ADD [EAX], AL
0x01f20026 f20100            ADD [EAX], EAX
0x01f20029 0000              ADD [EAX], AL
0x01f2002b 0000              ADD [EAX], AL
0x01f2002d 0000              ADD [EAX], AL
0x01f2002f 0000              ADD [EAX], AL
0x01f20031 0000              ADD [EAX], AL
0x01f20033 0000              ADD [EAX], AL
0x01f20035 0000              ADD [EAX], AL
```

8-MALFIND –d

Save the memory dumps of processes provided in command in malcode directory , windows defender found it suspicious and immediately deleted all that dumps.

Newimagemalcode folder is location of dump

9-VADINFO

Provides extended information about processes virtual address descriptor

```
**********************************************************************
Pid:   2396
VAD node @ 0xffffe001fad6da20 Start 0x0000000003ac0000 End 0x0000000003acffff Tag VadS
Flags: PrivateMemory: 1, Protection: 4
Protection: PAGE_READWRITE
Vad Type: VadNone

VAD node @ 0xffffe001fe928940 Start 0x00000000025e0000 End 0x00000000025effff Tag VadS
Flags: PrivateMemory: 1, Protection: 4
Protection: PAGE_READWRITE
Vad Type: VadNone

VAD node @ 0xffffe001fb8baa00 Start 0x0000000001d80000 End 0x0000000001d8ffff Tag VadS
Flags: PrivateMemory: 1, Protection: 4
Protection: PAGE_READWRITE
Vad Type: VadNone

VAD node @ 0xffffe001fef68570 Start 0x0000000000440000 End 0x000000000053ffff Tag VadS
Flags: PrivateMemory: 1, Protection: 4
Protection: PAGE_READWRITE
Vad Type: VadNone

VAD node @ 0xffffe001fcf886f0 Start 0x0000000000300000 End 0x000000000030ffff Tag VadS
Flags: PrivateMemory: 1, Protection: 4
Protection: PAGE_READWRITE
Vad Type: VadNone

VAD node @ 0xffffe001fd1175a0 Start 0x0000000000100000 End 0x000000000013ffff Tag VadS
Flags: PrivateMemory: 1, Protection: 4
Protection: PAGE_READWRITE
Vad Type: VadNone

VAD node @ 0xffffe001fee20460 Start 0x00000000000d0000 End 0x00000000000dffff Tag VadS
Flags: PrivateMemory: 1, Protection: 4
Protection: PAGE_READWRITE
Vad Type: VadNone
```

10-ldrmodule

There are many ways to hide a DLL. One of the ways involves unlinking the DLL from one (or all) of the linked lists in the PEB. However, when this is done, there is still information contained within the VAD (Virtual Address Descriptor) which identifies the base address of the DLL and its full path on disk. To cross-reference this information (known as memory mapped files) with the 3 PEB lists, use the ldrmodules command.

For each memory mapped PE file, the ldrmodules command prints True or False if the PE exists in the PEB lists.

```
Pid      Process              Base               InLoad InInit InMem MappedPath
-------- -------------------- ------------------ ------ ------ ----- ----------
    2396 WINWORD.EXE          0x0000000001f90000 False  False  False \Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\Cultures\OFFICE.ODF
    2396 WINWORD.EXE          0x0000000003860000 False  False  False \Program Files (x86)\Common Files\Microsoft Shared\OFFICE11\1033\msxml5r.dll
    2396 WINWORD.EXE          0x0000000060740000 False  False  False \Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\MSPTLS.DLL
    2396 WINWORD.EXE          0x0000[ Search ]10000 False  False  False \Windows\SysWOW64\iertutil.dll
    2396 WINWORD.EXE          0x0000000061900000 False  False  False \Program Files (x86)\Microsoft Office\Office12\OART.DLL
    2396 WINWORD.EXE          0x0000000074060000 False  False  False \Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9600.17810_none_7c5b61
    2396 WINWORD.EXE          0x0000000063eb0000 False  False  False \Program Files (x86)\Microsoft Office\Office12\MSOSTYLE.DLL
    2396 WINWORD.EXE          0x00000000600e0000 False  False  False \Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\MSORES.DLL
    2396 WINWORD.EXE          0x0000000073d00000 False  False  False \Windows\SysWOW64\dwmapi.dll
    2396 WINWORD.EXE          0x00000000699a0000 False  False  False \Windows\SysWOW64\propsys.dll
    2396 WINWORD.EXE          0x00000000735c0000 False  False  False \Windows\SysWOW64\userenv.dll
    2396 WINWORD.EXE          0x0000000059bd0000 False  False  False \Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.8428_none_d08a11e2442dc25d\msvcp
    2396 WINWORD.EXE          0x00000000637f0000 False  False  False \Windows\apppatch\AcGenral.dll
    2396 WINWORD.EXE          0x0000000075990000 False  False  False \Windows\SysWOW64\KernelBase.dll
    2396 WINWORD.EXE          0x0000000073030000 False  False  False \Windows\SysWOW64\rsaenh.dll
    2396 WINWORD.EXE          0x0000000058260000 False  False  False \Program Files (x86)\Microsoft Office\Office12\NLSLEXICONS0009_SP.dll
    2396 WINWORD.EXE          0x0000000074b20000 False  False  False \Windows\SysWOW64\version.dll
    2396 WINWORD.EXE          0x0000000072d50000 False  False  False \Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9600.18006_none_a9ec6aa
    2396 WINWORD.EXE          0x0000000077360000 True   True   True  \Windows\System32\wow64cpu.dll
  Load Path: C:\Windows\system32\wow64cpu.dll : wow64cpu.dll
  Init Path: C:\Windows\system32\wow64cpu.dll : wow64cpu.dll
  Mem Path:  C:\Windows\system32\wow64cpu.dll : wow64cpu.dll
    2396 WINWORD.EXE          0x0000000074ba0000 False  False  False \Windows\SysWOW64\cryptbase.dll
    2396 WINWORD.EXE          0x0000000075a70000 False  False  False \Windows\SysWOW64\cfgmgr32.dll
    2396 WINWORD.EXE          0x000000003f100000 False  False  False \Program Files (x86)\Common Files\Microsoft Shared\PROOF\1033\MSGR3EN.DLL
    2396 WINWORD.EXE          0x0000000073d20000 False  False  False \Windows\SysWOW64\uxtheme.dll
    2396 WINWORD.EXE          0x0000000072330000 False  False  False \Windows\SysWOW64\msi.dll
    2396 WINWORD.EXE          0x0000000075940000 False  False  False \Windows\SysWOW64\ws2_32.dll
    2396 WINWORD.EXE          0x00000000005ff50000 False  False  False \Program Files (x86)\Microsoft Office\Office12\USP10.DLL
    2396 WINWORD.EXE          0x00000000005ffd0000 False  False  False \Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\RICHED20.DLL
    2396 WINWORD.EXE          0x00000000735e0000 False  False  False \Windows\SysWOW64\wininet.dll
    2396 WINWORD.EXE          0x0000000072bf0000 False  False  False \Windows\SysWOW64\sxs.dll
    2396 WINWORD.EXE          0x00000000755b0000 False  False  False \Windows\SysWOW64\combase.dll
    2396 WINWORD.EXE          0x0000000077 1d0000 False  False  False \Windows\SysWOW64\msctf.dll
```

	PID	Image name & hash	PPID	Psexplorer/psmoniter sysinternals	Malicious/benign comments
1	PID=2876 explorer.exe	Newimage.raw	5248	I took the image somedays ago so processes have diffirent pid when I use psexplorer	
2	PID=2396 WINWORD.EXE	Newimage.raw	2876		

Dump of winword process is present in **volatility_2.5.win.standalone\procc** , but this image was acquired some days ago so I am not able to provide dump of original source.

```
D:\digital forensic\Assignment 3\volatility_2.5.win.standalone>volatility-2.5.st
andalone.exe --profile=Win8SP1x64 -f newimage.raw procdump -D procc -p 2396
Volatility Foundation Volatility Framework 2.5
Process(V)          ImageBase           Name                 Result
------------------ ------------------ -------------------- ------
0xffffe001fb10f080 0x000000002f170000 WINWORD.EXE          OK: executable.2396.e
xe
```