**Module Title**

**Introduction to Forensic**

**Assessment Weightage & Type**

**Portfolio Coursework**

**Year**

**2024-25**

**Student Name: Sujal Adhikari**

**UWE ID: 24030183**

**Assignment Submission Date:**

**Dumpme Volatility2**

# SCENARIO:

A SOC analyst took a memory dump from a machine infected with a meterpreter malware. As a Digital Forensicators, your job is to analyze the dump, extract the available indicators of compromise (IOCs) and answer the provided questions.

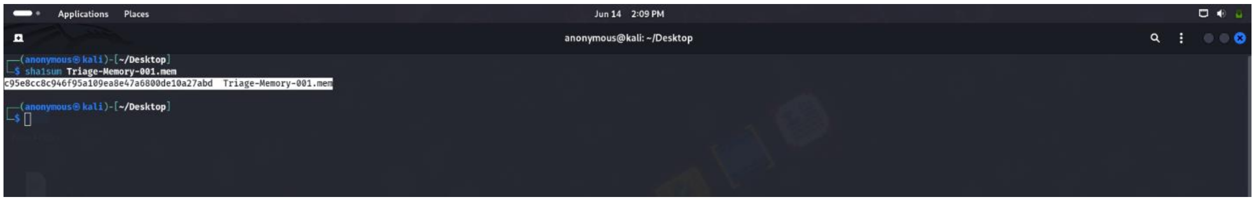
# TOOLS:

Volalitity2

SHA1

**First question:** What is the SHA1 hash of Triage-Memory.mem (memory dump)?

So we need to find hash of memory dump. For that we will use the tool called SHA1. The command for that tool is “sha1sum Triage-Memory-001.mem”

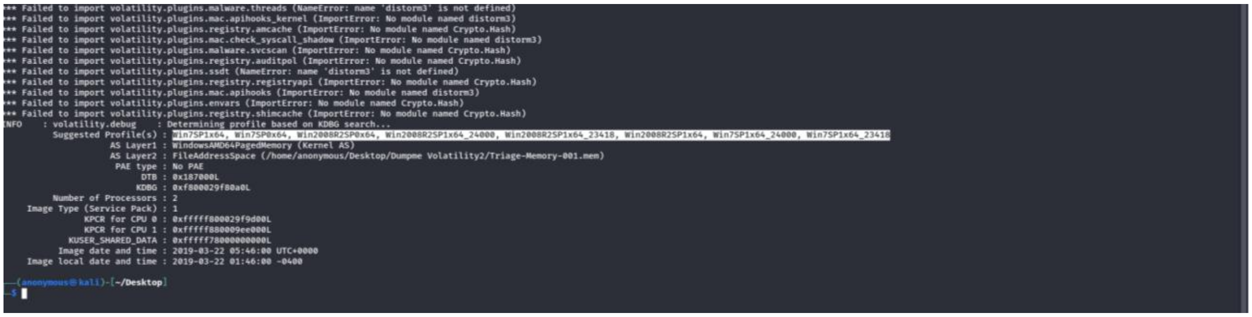


```
┌──(anonymous㉿kali)-[~/Desktop]
└─$ sha1sum Triage-Memory-001.mem
c95e8cc8c946f95a109ea8e47a6800de10a27abd  Triage-Memory-001.mem

┌──(anonymous㉿kali)-[~/Desktop]
└─$ ▯
```

**Second question:** What volatility profile is the most appropriate for this machine? (ex: Win10x86_14393)

Now, we need to do start our understand what profile are we dealing with. Then there is plugin called image info. For this we will use the command “python2 volatility/vol.py –f /home/anonymous/Desktop/Dumpme\Volatility2/Triage-Memory.-001.mem imageinfo”

Our profile is **Win7SP1x64**



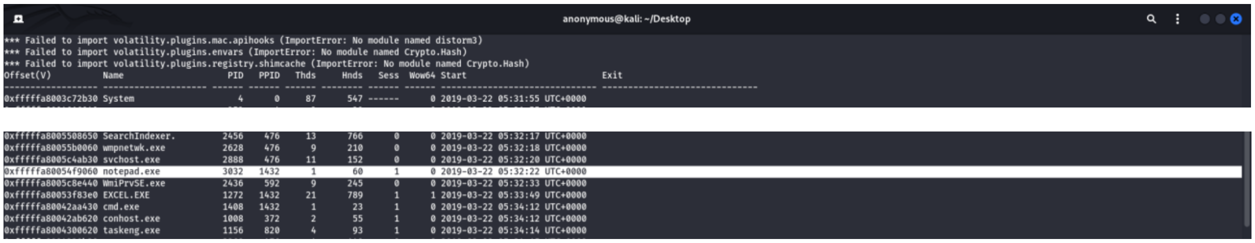
```
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** 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)
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/anonymous/Desktop/Dumpme Volatility2/Triage-Memory-001.mem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800029f80a0L
          Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff800029f9d00L
                KPCR for CPU 1 : 0xfffff880009ee000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2019-03-22 05:46:00 UTC+0000
     Image local date and time : 2019-03-22 01:46:00 -0400

┌──(anonymous㉿kali)-[~/Desktop]
└─$ █
```

**Third question:** What was the process ID of notepad.exe?

From here, we can use plugin called pslist to list our processes during memory dump. We will use the command “python2 volatility/vol.py –f /home/anonymous/Desktop/Dumpme\Volatility2/Triage-Memory.-001.mem pslist”

Parent process id for notepad is 1432 and process id of notepad is 3032

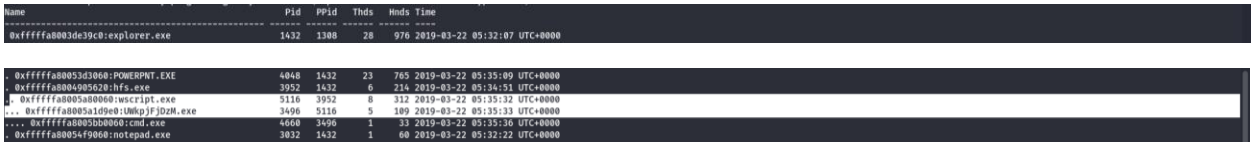
Then answer is **3032**



```
*** 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)
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8003c72b30 System                    4      0     87      547 ------      0 2019-03-22 05:31:55 UTC+0000

0xfffffa8005508650 SearchIndexer.         2456    476     13      766      0      0 2019-03-22 05:32:17 UTC+0000
0xfffffa80055b0060 wmpnetwk.exe           2628    476      9      210      0      0 2019-03-22 05:32:18 UTC+0000
0xfffffa8005c4ab30 svchost.exe            2888    476     11      152      0      0 2019-03-22 05:32:20 UTC+0000
0xfffffa80054f9060 notepad.exe            3032   1432      1       60      1      0 2019-03-22 05:32:22 UTC+0000
0xfffffa8005c8e440 WmiPrvSE.exe           2436    592      9      245      0      0 2019-03-22 05:32:33 UTC+0000
0xfffffa80053f83e0 EXCEL.EXE              1272   1432     21      789      1      1 2019-03-22 05:33:49 UTC+0000
0xfffffa80042aa430 cmd.exe                1408   1432      1       23      1      0 2019-03-22 05:34:12 UTC+0000
0xfffffa80042ab620 conhost.exe            1008    372      2       55      1      0 2019-03-22 05:34:12 UTC+0000
0xfffffa8004300620 taskeng.exe            1156    820      4       93      1      0 2019-03-22 05:34:14 UTC+0000
```

**Fourth question:** Name the child process of wscript.exe.

The question need us to understand more about process called wscript.exe and not just to know the process id but to also know what this process wscript.exe has open other process once it was open in windows 7. We can use the same plugin as in third question but we can do better by using pstree as it shows clearly. So the command will be “python2 volatility/vol.py –f /home/anonymous/Desktop/Dumpme\Volatility2/Triage-Memory.-001.mem pstree”



```
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa8003de39c0:explorer.exe                     1432   1308     28    976 2019-03-22 05:32:07 UTC+0000

. 0xfffffa80053d3060:POWERPNT.EXE                    4048   1432     23    765 2019-03-22 05:35:09 UTC+0000
. 0xfffffa8004905620:hfs.exe                         3952   1432      6    214 2019-03-22 05:34:51 UTC+0000
.. 0xfffffa8005a80060:wscript.exe                    5116   3952      8    312 2019-03-22 05:35:32 UTC+0000
... 0xfffffa8005a1d9e0:UWkpjFjDzM.exe                3496   5116      5    109 2019-03-22 05:35:33 UTC+0000
.... 0xfffffa8005bb0060:cmd.exe                      4660   3496      1     33 2019-03-22 05:35:36 UTC+0000
. 0xfffffa80054f9060:notepad.exe                     3032   1432      1     60 2019-03-22 05:32:22 UTC+0000
```

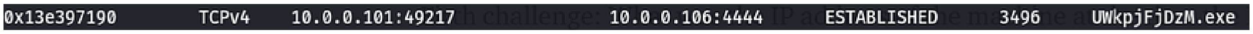
How do we define child process? we can define by the dot. the one with one dot is process that stand itself meaning that it is not child process. the one with two dots makes it to be child process of process with one dot and even the one with three dot makes it to be child process of process with two dots. things

we can see even the process wscript.exe is child process of hfs.exe which is not easily to see these process wscript.exe with pslist escecially if there are lot of processes. Then these process wscript.exe open another process UWkpjFjDzM.exe which in turn open cmd process which is very dangerous

Our answer is **UWkpjFjDzM.exe**

**Fifth question:** What was the IP address of the machine at the time the RAM dump was created?

We can try to use connscan, connections,sockscan. but here we can use net scan as it works and try to focus to applications that have established network to outside. So we will use the command “python2 volatility/vol.py –f /home/anonymous/Desktop/Dumpme\Volatility2/Triage-Memory.-001.mem net scan”



```
0x13e397190         TCPv4    10.0.0.101:49217              10.0.0.106:4444      ESTABLISHED      3496     UWkpjFjDzM.exe
```

Our first established network in the analysis is UWkpjFjDzM.exe and these must give the impression or confirmation that this process is more suspicious

therefore, answer is **10.0.0.101**

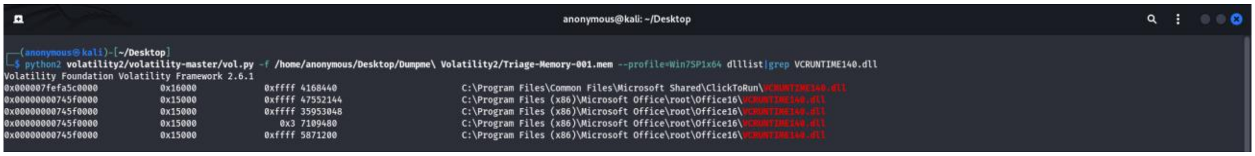
**Sixth question:** Based on the answer regarding the infected PID, can you determine the IP of the attacker?

Now that we know our suspicious process from fifth challenge and from our previous screenshot, we can see the ip address of remote is 10.0.0.106.

the answer is **10.0.0.106**

**Seventh question:** How many processes are associated with VCRUNTIME140.dll?

We can use plugin dlllist to see what process the dll is interact with and grep that |grep VCRUNTIME140.dll to get how many processes that dll interact with the command “python2 volatility/vol.py –f /home/anonymous/Desktop/Dumpme\Volatility2/Triage-Memory.-001.mem –profile=Win7SP1x64 dlllist|grep VCRUNTIME140.dll”

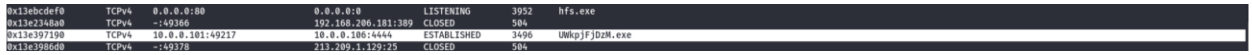


```
┌──(anonymous㉿kali)-[~/Desktop]
└─$ python2 volatility2/volatility-master/vol.py -f /home/anonymous/Desktop/Dumpme\ Volatility2/Triage-Memory-001.mem --profile=Win7SP1x64 dlllist|grep VCRUNTIME140.dll
Volatility Foundation Volatility Framework 2.6.1
0x000007fefa5c0000          0x16000          0xffff 4168440                C:\Program Files\Common Files\Microsoft Shared\ClickToRun\VCRUNTIME140.dll
0x00000000745f0000          0x15000          0xffff 47552144               C:\Program Files (x86)\Microsoft Office\root\Office16\VCRUNTIME140.dll
0x00000000745f0000          0x15000          0xffff 35953048               C:\Program Files (x86)\Microsoft Office\root\Office16\VCRUNTIME140.dll
0x00000000745f0000          0x15000             0x3 7109480                C:\Program Files (x86)\Microsoft Office\root\Office16\VCRUNTIME140.dll
0x00000000745f0000          0x15000          0xffff 5871200                C:\Program Files (x86)\Microsoft Office\root\Office16\VCRUNTIME140.dll
```

**Our answer is that there are 5 processes**

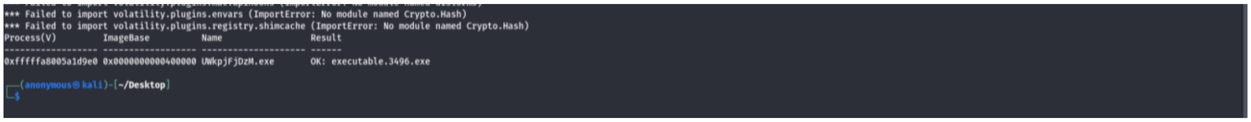
## Eighth Challenge question: After dumping the infected process, what is its md5 hash?

We know our infected process is UWkpjFjDzM.exe then we need to know process id of that infected process and we can use the plugin pstree with command “python2 volatility/vol.py –f /home/anonymous/Desktop/Dumpme\Volatility2/Triage-Memory.-001.mem pstree” and see our pid is 3496

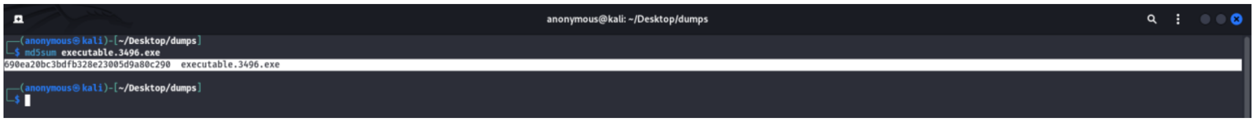


```
0x13ebcdef0        TCPv4    0.0.0.0:80                    0.0.0.0:0              LISTENING        3952     hfs.exe
0x13e2348a0        TCPv4    -:49366                       192.168.206.181:389    CLOSED           504
0x13e397190        TCPv4    10.0.0.101:49217              10.0.0.106:4444        ESTABLISHED      3496     UWkpjFjDzM.exe
0x13e3986d0        TCPv4    -:49378                       213.209.1.129:25       CLOSED           504
```

Now that we have pid and we do the dump of that process with plugin called procdump COMMAND: “python2 volatility/vol.py –f/home/anonymous/Desktop/Dumpme\Volatility2/Triage-Memory.-001.mem procdump -p3496 — dump-dir . Now that we have dump the process and we do md5sum according to question



```
*** 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)
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
0xfffffa8005a1d9e0 0x0000000000400000 UWkpjFjDzM.exe       OK: executable.3496.exe

┌──(anonymous㉿kali)-[~/Desktop]
└─$
```



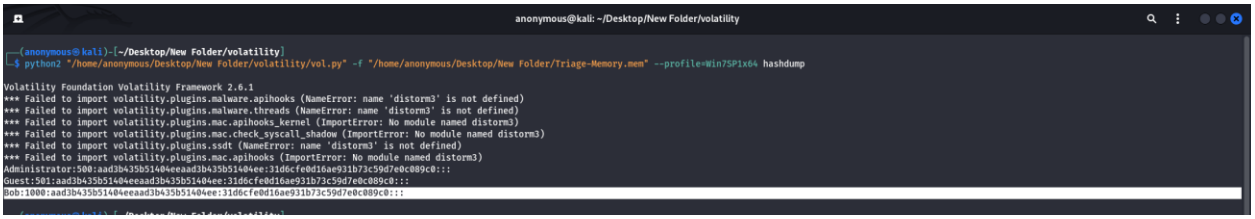
anonymous@kali: ~/Desktop/dumps

```
┌──(anonymous㉿kali)-[~/Desktop/dumps]
└─$ md5sum executable.3496.exe
690ea20bc3bdfb328e23005d9a80c290  executable.3496.exe

┌──(anonymous㉿kali)-[~/Desktop/dumps]
└─$ █
```

**our answer is 690ea20bc3bdfb328e23005d9a80c290**

## Ninth question: What is the LM hash of Bob's account?

In this question, it wants us find LM hash. In here, we can use plugin called hashdump to dump hashes. The command will be “python2 “/home/anonymous/Desktop/New Folder/volatility/vol.py” –f “/home/anonymous/Desktop/New Folder/triage-Memory.mem” –profile=Win7SP1x64 hashdump”



anonymous@kali: ~/Desktop/New Folder/volatility

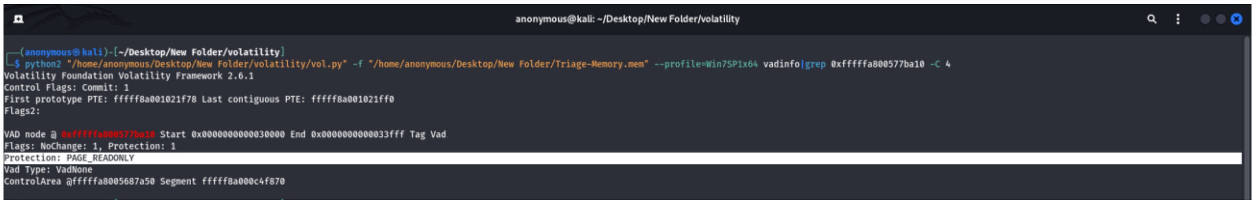
```
┌──(anonymous㉿kali)-[~/Desktop/New Folder/volatility]
└─$ python2 "/home/anonymous/Desktop/New Folder/volatility/vol.py" -f "/home/anonymous/Desktop/New Folder/Triage-Memory.mem" --profile=Win7SP1x64 hashdump

Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** 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.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Bob:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Now we can see two hashes, first hash from left side is LM hash and second hash is password hash. Then our LM hash of **Bob is aad3b435b51404eeaad3b435b51404ee**

**Tenth question:** What memory protection constants does the VAD node at 0xfffffa800577ba10 have?

VAD is used by the Windows memory manager to describe memory ranges used by a process as they are allocated. When a process allocates memory with VirutalAlloc, the memory manager creates an entry in the VAD tree. Plugin that we can use is ladino.

Command "python2 "/home/anonymous/Desktop/New Folder/triage-Memory.mem" –profile=Win7SP1x64 vadinfo|grep 0xfffffa800577ba10 -C 4"

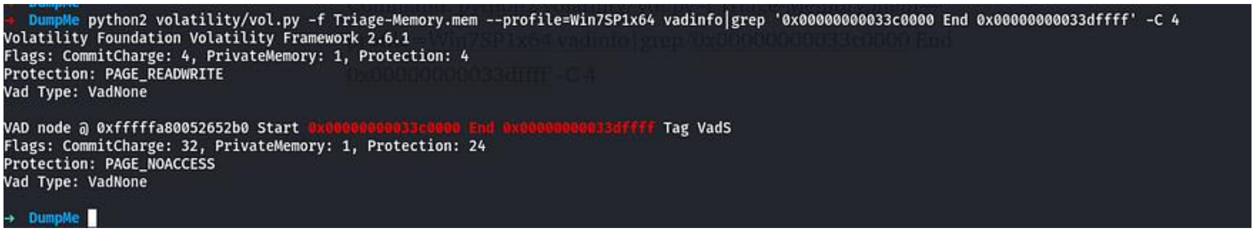


```
┌──(anonymous㉿kali)-[~/Desktop/New Folder/volatility]
└─$ python2 "/home/anonymous/Desktop/New Folder/volatility/vol.py" -f "/home/anonymous/Desktop/New Folder/Triage-Memory.mem" --profile=Win7SP1x64 vadinfo|grep 0xfffffa800577ba10 -C 4
Volatility Foundation Volatility Framework 2.6.1
Control Flags: Commit: 1
First prototype PTE: fffff8a001021f78 Last contiguous PTE: fffff8a001021ff0
Flags2:

VAD node @ 0xfffffa800577ba10 Start 0x0000000000030000 End 0x0000000000033fff Tag Vad
Flags: NoChange: 1, Protection: 1
Protection: PAGE_READONLY
Vad Type: VadNone
ControlArea @fffffa8005687a50 Segment fffff8a000c4f870
```

Now we can see protection is **PAGE_READONLY**

**Eleventh question:** What memory protection did the VAD starting at 0x00000000033c0000 and ending at 0x00000000033dffff have?

Command "python2 "/home/anonymous/Desktop/New Folder/triage-Memory.mem" –profile=Win7SP1x64 vadinfo|grep '0x00000000033c0000 End 0x00000000033dffff' -C 4

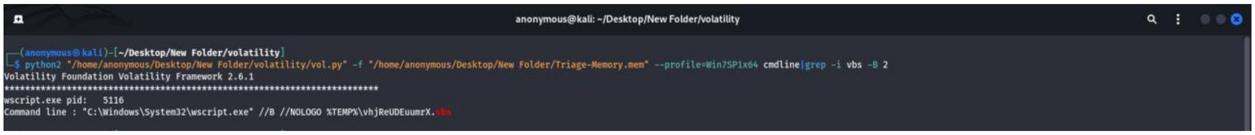


```
➜  DumpMe python2 volatility/vol.py -f Triage-Memory.mem --profile=Win7SP1x64 vadinfo|grep '0x00000000033c0000 End 0x00000000033dffff' -C 4
Volatility Foundation Volatility Framework 2.6.1
Flags: CommitCharge: 4, PrivateMemory: 1, Protection: 4
Protection: PAGE_READWRITE
Vad Type: VadNone

VAD node @ 0xfffffa80052652b0 Start 0x00000000033c0000 End 0x00000000033dffff Tag VadS
Flags: CommitCharge: 32, PrivateMemory: 1, Protection: 24
Protection: PAGE_NOACCESS
Vad Type: VadNone

➜  DumpMe
```

Our permission now is **PAGE_NOACCESS**

**Twelve question:** There was a VBS script that ran on the machine. What is the name of the script? (submit without file extension)

Run on the machine meaning that we should check the one that execute in a certain command with path. the plugin cmdline is useful in this situation



anonymous@kali: ~/Desktop/New Folder/volatility

```
┌──(anonymous㉿kali)-[~/Desktop/New Folder/volatility]
└─$ python2 "/home/anonymous/Desktop/New Folder/volatility/vol.py" -f "/home/anonymous/Desktop/New Folder/Triage-Memory.mem" --profile=Win7SP1x64 cmdline|grep -i vbs -B 2
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
wscript.exe pid:   5116
Command line : "C:\Windows\System32\wscript.exe" //B //NOLOGO %TEMP%\vhjReUDEuumrX.vbs
```

Command: “python2 “/home/anonymous/Desktop/New Folder/triage-Memory.mem” –profile=Win7SP1x64 cmdline|grep -i vbs -B 2”

Name of script is **vhjReUDEuumrX**

**Thirteen question:** An application was run at 2019-03-07 23:06:58 UTC. What is the name of the program? (Include extension)

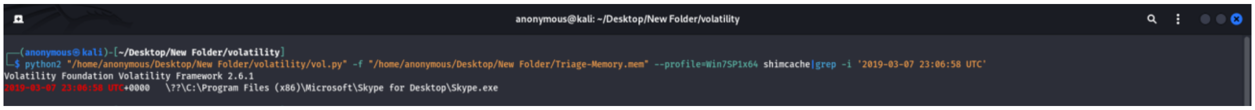
we can try the application using cmdline and consoles which fails.

CMDLINE: it fails because the program was closed and also they specified the word ‘was’

CONSOLES: It fails because the program was not only closed but the history of command for that process does not exist and maybe they turn off PC so i wont exist

Now we can use plugin shimcache to check for that process that was last modified

Command: “python2 “/home/anonymous/Desktop/New Folder/triage-Memory.mem” –profile=Win7SP1x64 shimcache|grep -i ‘2019–03–07 23:06:58 UTC”



anonymous@kali: ~/Desktop/New Folder/volatility

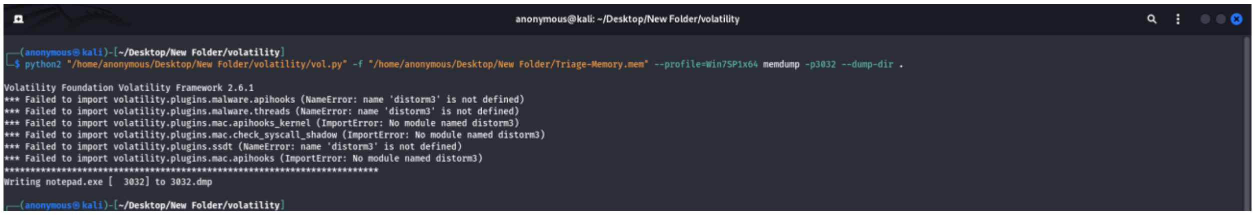
```
┌──(anonymous㉿kali)-[~/Desktop/New Folder/volatility]
└─$ python2 "/home/anonymous/Desktop/New Folder/volatility/vol.py" -f "/home/anonymous/Desktop/New Folder/Triage-Memory.mem" --profile=Win7SP1x64 shimcache|grep -i '2019-03-07 23:06:58 UTC'
Volatility Foundation Volatility Framework 2.6.1
2019-03-07 23:06:58 UTC+0000   \??\C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe
```

**It is Skype.exe**

**Fourth teen question:** What was written in notepad.exe at the time when the memory dump was captured?

we know pid process of notepad as we already done and it is 3032

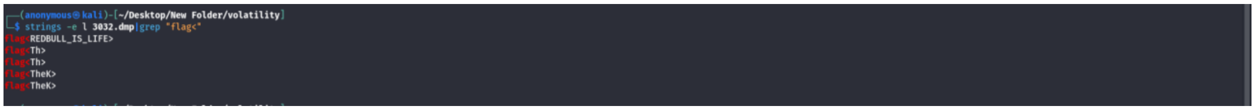
command “ python2 “/home/anonymous/Desktop/New Folder/triage-Memory.mem” –profile=Win7SP1x64 memdump -p3032 — dump-dir .”



```
┌──(anonymous㉿kali)-[~/Desktop/New Folder/volatility]
└─$ python2 "/home/anonymous/Desktop/New Folder/volatility/vol.py" -f "/home/anonymous/Desktop/New Folder/Triage-Memory.mem" --profile=Win7SP1x64 memdump -p3032 --dump-dir .

Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** 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.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
************************************************************************
Writing notepad.exe [  3032] to 3032.dmp

┌──(anonymous㉿kali)-[~/Desktop/New Folder/volatility]
```

and

"strings -e l 3032.dmp|grep "flage<"



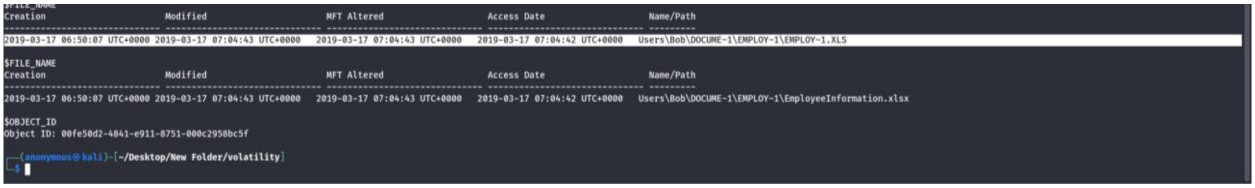
```
┌──(anonymous㉿kali)-[~/Desktop/New Folder/volatility]
└─$ strings -e l 3032.dmp|grep "flag<"
flag<REDBULL_IS_LIFE>
flag<Th>
flag<Th>
flag<TheK>
flag<TheK>
```

flag is flag<REDBULL_IS_LIFE>

**fifteen teen Challenge question:** What is the short name of the file at file record 59045?

For file record, we can use plugin called mftparser to do the job

Command "python2 "/home/anonymous/Desktop/New Folder/triage-Memory.mem" –profile=Win7SP1x64 mftparser|grep 59045 -C 20"



```
Creation                       Modified                       MFT Altered                    Access Date                    Name/Path
------------------------------ ------------------------------ ------------------------------ ------------------------------ ---------
2019-03-17 06:50:07 UTC+0000 2019-03-17 07:04:43 UTC+0000   2019-03-17 07:04:43 UTC+0000   2019-03-17 07:04:42 UTC+0000   Users\Bob\DOCUME~1\EMPLOY~1\EMPLOY~1.XLS

$FILE_NAME
Creation                       Modified                       MFT Altered                    Access Date                    Name/Path
------------------------------ ------------------------------ ------------------------------ ------------------------------ ---------
2019-03-17 06:50:07 UTC+0000 2019-03-17 07:04:43 UTC+0000   2019-03-17 07:04:43 UTC+0000   2019-03-17 07:04:42 UTC+0000   Users\Bob\DOCUME~1\EMPLOY~1\EmployeeInformation.xlsx

$OBJECT_ID
Object ID: 00fe50d2-4841-e911-8751-000c2958bc5f

┌──(anonymous㉿kali)-[~/Desktop/New Folder/volatility]
└─$ 
```

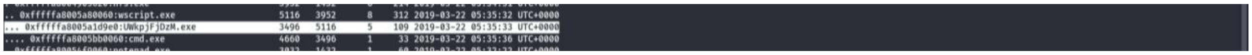
the name is **EMPLOY~1.XLS**

**Sixth teen question:** This box was exploited and is running meterpreter. What was the infected PID?

we already did this one

command: "python2 volatility/vol.py –f /home/anonymous/Desktop/Dumpme\Volatility2/Triage-Memory.-001.mem pslist"

Suscioup process was UWkpjFjDzM.exe



```
.. 0xfffffa8005a80060:wscript.exe        5116   3952      8    312 2019-03-22 05:35:32 UTC+0000
... 0xfffffa8005a1d9e0:UWkpjFjDzM.exe    3496   5116      5    109 2019-03-22 05:35:33 UTC+0000
.... 0xfffffa8005bb0060:cmd.exe          4660   3496      1     33 2019-03-22 05:35:36 UTC+0000
```

then our pid is **3496**