

# Digital Forensics-Lab09

I22-1609 Ahmad Abdullah

## Introduction

Today in this lab task we were given a memory dump of a windows-7 x64, which we can see after running the image info module of the volatility. The profile given after running the command was Win7SP1x64 which we used throughout the Lab to find out different flags.

```
(kali@kali)-[~/Downloads/volatility]
$ python2 vol.py -f memdump_challenge.mem imageinfo

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.ssd (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64_24000, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/kali/Downloads/volatility/memdump_challenge.mem)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf800028410a0L
Number of Processors : 4
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff80002842d00L
KPCR for CPU 1 : 0xfffff800009eb000L
KPCR for CPU 2 : 0xfffff80002ea9000L
KPCR for CPU 3 : 0xfffff80002f1f000L
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2023-04-02 14:37:16 UTC+0000
Image local date and time : 2023-04-02 19:37:16 +0500
```

## Clipboard

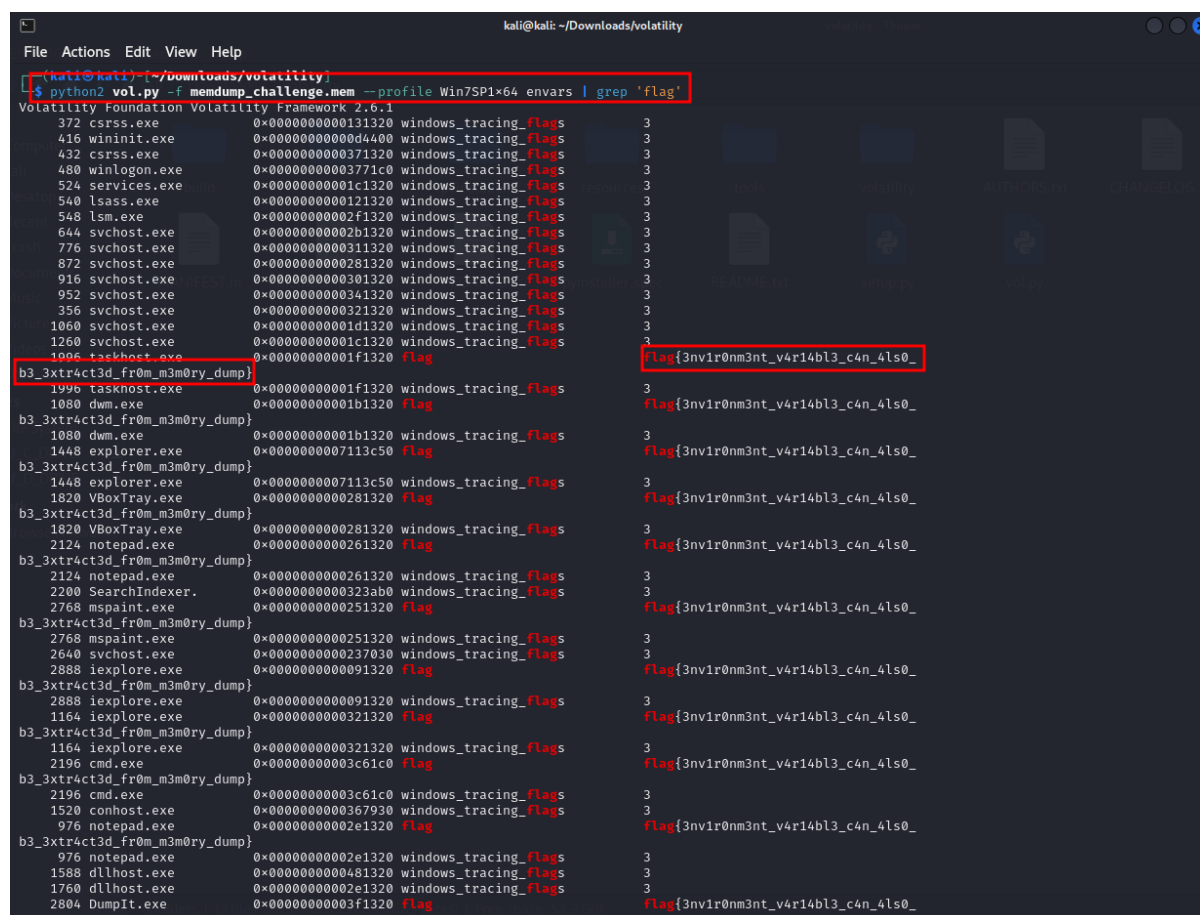
We were tasked with finding if there was a flag in the clipboard which is stored in memory as long as it is in the clipboard. We just used the module clipboard and easily enough there was a flag.

```
(kali@kali)-[~/Downloads/volatility]
$ python2 vol.py -f memdump_challenge.mem --profile Win7SP1x64 clipboard

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.ssd (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Session WindowStation Format Handle Object Data
-----
1 WinSta0 CF_UNICODETEXT 0x18027b 0xfffff900c1e6d260 flag{s0m3_stuff_c0p13d_1n_th3_cl1
pb0ard}
1 WinSta0 CF_TEXT 0x10
1 WinSta0 0xa0103L 0x200000000000
1 WinSta0 CF_TEXT 0x1
1 0xa0103 0xfffff900c210e780
```

## Environmental Variables

Next, we needed to find the flag in the environmental variables and by using the module envvars and using its output as input for grep the terminal shows all the flags that were stored in the environmental variables. Since they all were the same flags, I highlighted only one.



```
kali@kali: ~/Downloads/volatility
File Actions Edit View Help
(kali@kali)~/Downloads/volatility
$ python2 vol.py -f memdump_challenge.mem --profile Win7SP1x64 envvars | grep 'flag'
Volatility Foundation Volatility Framework 2.6.1
372 csrss.exe 0x0000000000131320 windows_tracing_flags 3
416 wininit.exe 0x00000000000d4400 windows_tracing_flags 3
432 csrss.exe 0x0000000000371320 windows_tracing_flags 3
480 winlogon.exe 0x00000000003771c0 windows_tracing_flags 3
524 services.exe 0x00000000001c1320 windows_tracing_flags 3
540 lsass.exe 0x0000000000121320 windows_tracing_flags 3
548 lsm.exe 0x00000000002f1320 windows_tracing_flags 3
644 svchost.exe 0x00000000002b1320 windows_tracing_flags 3
776 svchost.exe 0x0000000000311320 windows_tracing_flags 3
872 svchost.exe 0x0000000000281320 windows_tracing_flags 3
916 svchost.exe 0x0000000000301320 windows_tracing_flags 3
952 svchost.exe 0x0000000000341320 windows_tracing_flags 3
356 svchost.exe 0x0000000000321320 windows_tracing_flags 3
1060 svchost.exe 0x00000000001d1320 windows_tracing_flags 3
1260 svchost.exe 0x00000000001c1320 windows_tracing_flags 3
1096 taskhost.exe 0x00000000001f1320 flag flag{3nv1r0nm3nt_v4r14bl3_c4n_4ls0_}
b3_3xtr4ct3d_fr0m_m3m0ry_dump}
1996 taskhost.exe 0x00000000001f1320 windows_tracing_flags 3
1080 dwm.exe 0x00000000001b1320 flag flag{3nv1r0nm3nt_v4r14bl3_c4n_4ls0_}
b3_3xtr4ct3d_fr0m_m3m0ry_dump}
1080 dwm.exe 0x00000000001b1320 windows_tracing_flags 3
1448 explorer.exe 0x00000000007113c50 flag flag{3nv1r0nm3nt_v4r14bl3_c4n_4ls0_}
b3_3xtr4ct3d_fr0m_m3m0ry_dump}
1448 explorer.exe 0x00000000007113c50 windows_tracing_flags 3
1820 VBoxTray.exe 0x0000000000281320 flag flag{3nv1r0nm3nt_v4r14bl3_c4n_4ls0_}
b3_3xtr4ct3d_fr0m_m3m0ry_dump}
1820 VBoxTray.exe 0x0000000000281320 windows_tracing_flags 3
2124 notepad.exe 0x0000000000261320 flag flag{3nv1r0nm3nt_v4r14bl3_c4n_4ls0_}
b3_3xtr4ct3d_fr0m_m3m0ry_dump}
2124 notepad.exe 0x0000000000261320 windows_tracing_flags 3
2200 SearchIndexer. 0x0000000000323ab0 windows_tracing_flags 3
2768 mspaint.exe 0x0000000000251320 flag flag{3nv1r0nm3nt_v4r14bl3_c4n_4ls0_}
b3_3xtr4ct3d_fr0m_m3m0ry_dump}
2768 mspaint.exe 0x0000000000251320 windows_tracing_flags 3
2640 svchost.exe 0x0000000000237030 windows_tracing_flags 3
2888 iexplore.exe 0x0000000000091320 flag flag{3nv1r0nm3nt_v4r14bl3_c4n_4ls0_}
b3_3xtr4ct3d_fr0m_m3m0ry_dump}
2888 iexplore.exe 0x0000000000091320 windows_tracing_flags 3
1164 iexplore.exe 0x0000000000321320 flag flag{3nv1r0nm3nt_v4r14bl3_c4n_4ls0_}
b3_3xtr4ct3d_fr0m_m3m0ry_dump}
1164 iexplore.exe 0x0000000000321320 windows_tracing_flags 3
2196 cmd.exe 0x00000000003c61c0 flag flag{3nv1r0nm3nt_v4r14bl3_c4n_4ls0_}
b3_3xtr4ct3d_fr0m_m3m0ry_dump}
2196 cmd.exe 0x00000000003c61c0 windows_tracing_flags 3
1520 conhost.exe 0x0000000000367930 windows_tracing_flags 3
976 notepad.exe 0x00000000002e1320 flag flag{3nv1r0nm3nt_v4r14bl3_c4n_4ls0_}
b3_3xtr4ct3d_fr0m_m3m0ry_dump}
976 notepad.exe 0x00000000002e1320 windows_tracing_flags 3
1588 dllhost.exe 0x0000000000481320 windows_tracing_flags 3
1760 dllhost.exe 0x00000000002e1320 windows_tracing_flags 3
2804 DumpIt.exe 0x00000000003f1320 flag flag{3nv1r0nm3nt_v4r14bl3_c4n_4ls0_}
```

## Executed Commands

Further, we needed to find what commands were run recently that were stored. Simply we added a module cmdscan with grep 'flag' and it gave us what we were looking for.

```
(kali@kali)-[~/Downloads/volatility]
$ python2 vol.py -f memdump_challenge.mem --profile Win7SP1x64 cmdscan | grep 'flag'
Volatility Foundation Volatility Framework 2.6.1
Cmd #0 @ 0x38cf70: echo ZmxhZ3tnMDBkXzBsZF9jMG5zMGwzX2gxc3Qwcnl9 > flag.txt && notepad.exe flag.txt
(kali@kali)-[~/Downloads/volatility]
$
```

The flag was encrypted and echoed in a txt flag so we had to paste it into cyber-chef to decrypt us.

Input

ZmxhZ3tnMDBkXzBsZF9jMG5zMGwzX2gxc3Qwcnl9

Output

flag{g00d\_0ld\_c0ns0l3\_h1st0ry}

## Internet Search

For this, we used the module iehistory to look for internet search history.

```
(kali@kali)-[~/Downloads/volatility]
$ python2 vol.py -f memdump_challenge.mem --profile Win7SP1x64 iehistory | grep 'flag'
Volatility Foundation Volatility Framework 2.6.1
Location: Visited: w@file:///C:/Users/w/Desktop/flag.txt.txt
Location: Visited: w@http://example.com/?flag=flag{1nt3rn3t_3xpl0r3r_h1st0ry_1n_m3m0ry_dump}
Location: Visited: w@http://example.com/?flag=flag{1nt3rn3t_3xpl0r3r_h1st0ry_1n_m3m0ry_dump}
Location: http://example.com/?flag=flag{1nt3rn3t_3xpl0r3r_h1st0ry_1n_m3m0ry_dump}
Location: Visited: w@http://example.com/?flag=flag{1nt3rn3t_3xpl0r3r_h1st0ry_1n_m3m0ry_dump}
(kali@kali)-[~/Downloads/volatility]
$
```

## MSPaint

This task was an interesting one. The flag was actually drawn in mspaint.exe, but a file was not saved so the application was still open and flag drawn without any save file. For this we had to dump mspaint's data in memory and open it into a software GIMP

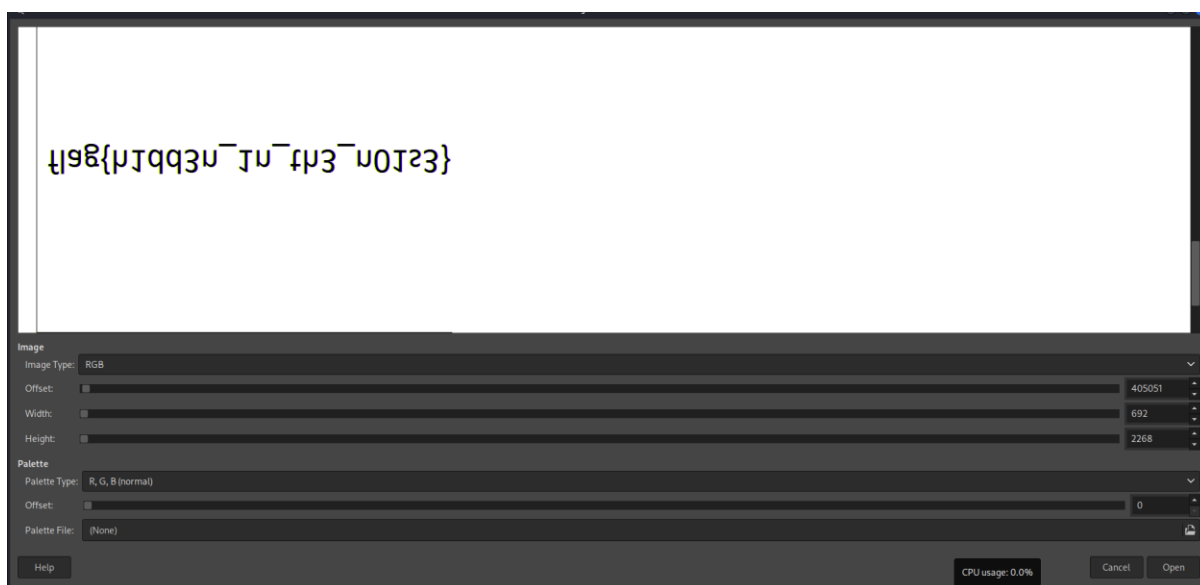
```
(kali@kali)-[~/Downloads/volatility]
$ python2 vol.py -f memdump_challenge.mem --profile Win7SP1x64 psscan | grep 'mspaint'
Volatility Foundation Volatility Framework 2.6.1
0x000000001eedc920 mspaint.exe 2768 1448 0x00000000183a2000 2023-04-02 14:09:01 UTC+0000

(kali@kali)-[~/Downloads/volatility]
$ python2 vol.py -f memdump_challenge.mem --profile Win7SP1x64 memdump -p 2768 -D .
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.ssd (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*****
Writing mspaint.exe [ 2768] to 2768.dmp

(kali@kali)-[~/Downloads/volatility]
$
```

We changed the extension of the dump file to .data

And located the file at given offsets, width and height.



Flag{h1dd3n\_1n\_th3\_n01se}

