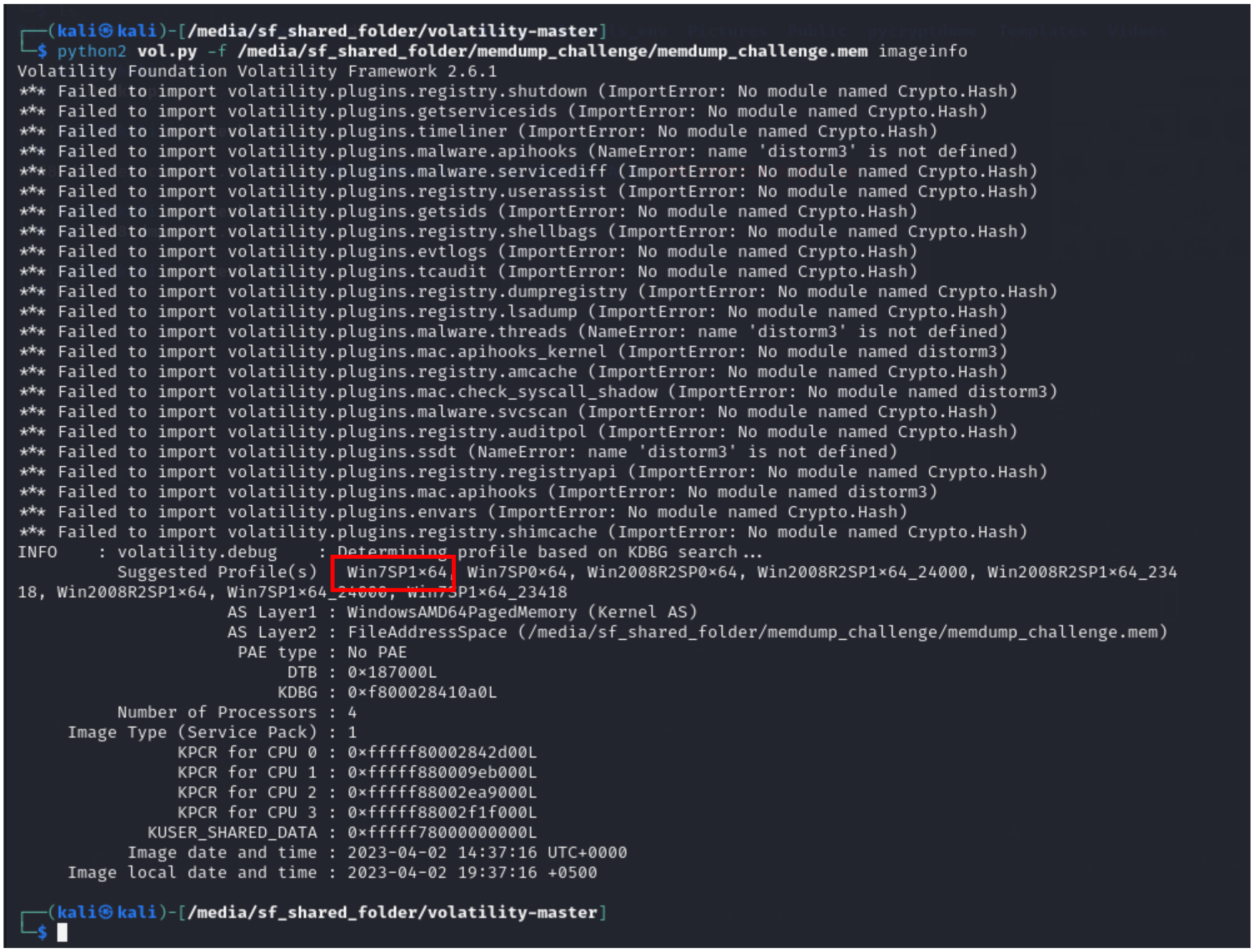
LAB 09

Abdul Sami Qasim

22i-1725

CY-D

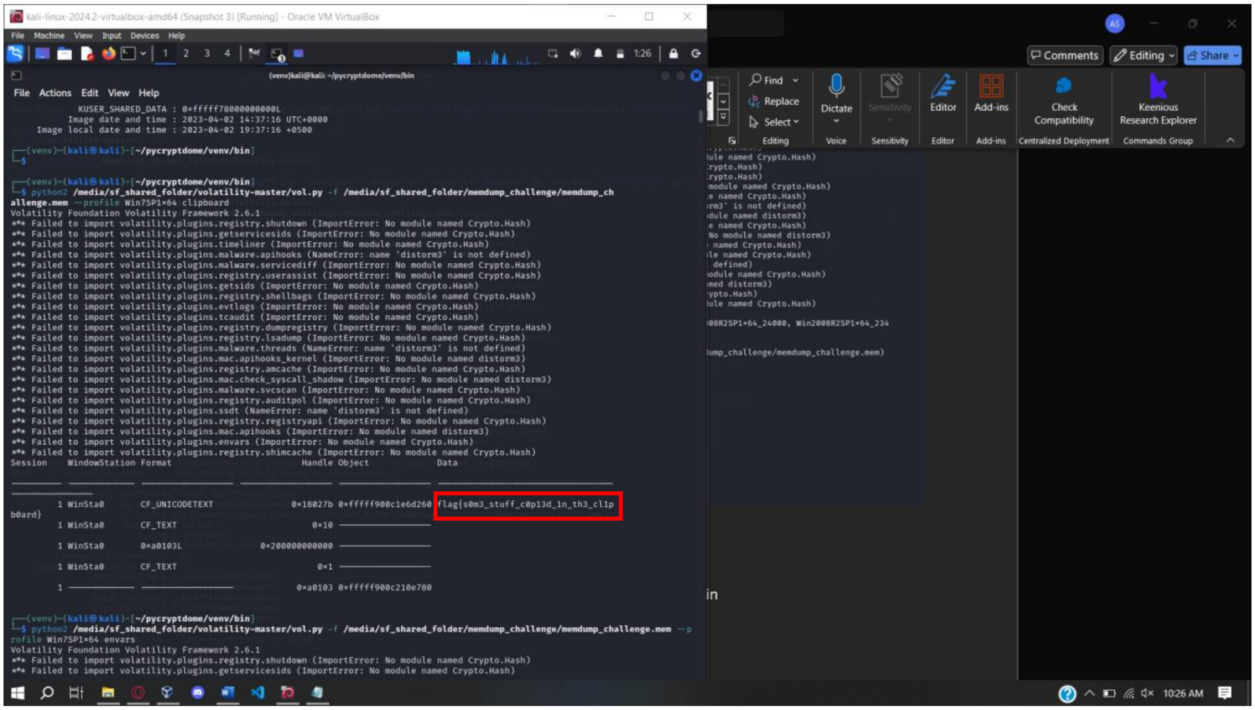
First of all, finding the memdump profile using plugin imageinfo



```
┌──(kali㉿kali)-[/media/sf_shared_folder/volatility-master]
└─$ python2 vol.py -f /media/sf_shared_folder/memdump_challenge/memdump_challenge.mem imageinfo
Volatility Foundation Volatility Framework 2.6.1
*** 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)
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_234
18, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/media/sf_shared_folder/memdump_challenge/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 : 0xfffff880009eb000L
                KPCR for CPU 2 : 0xfffff88002ea9000L
                KPCR for CPU 3 : 0xfffff88002f1f000L
             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

┌──(kali㉿kali)-[/media/sf_shared_folder/volatility-master]
└─$ 
```

Q1)

To find the clipboard info, we use the clipboard plugin



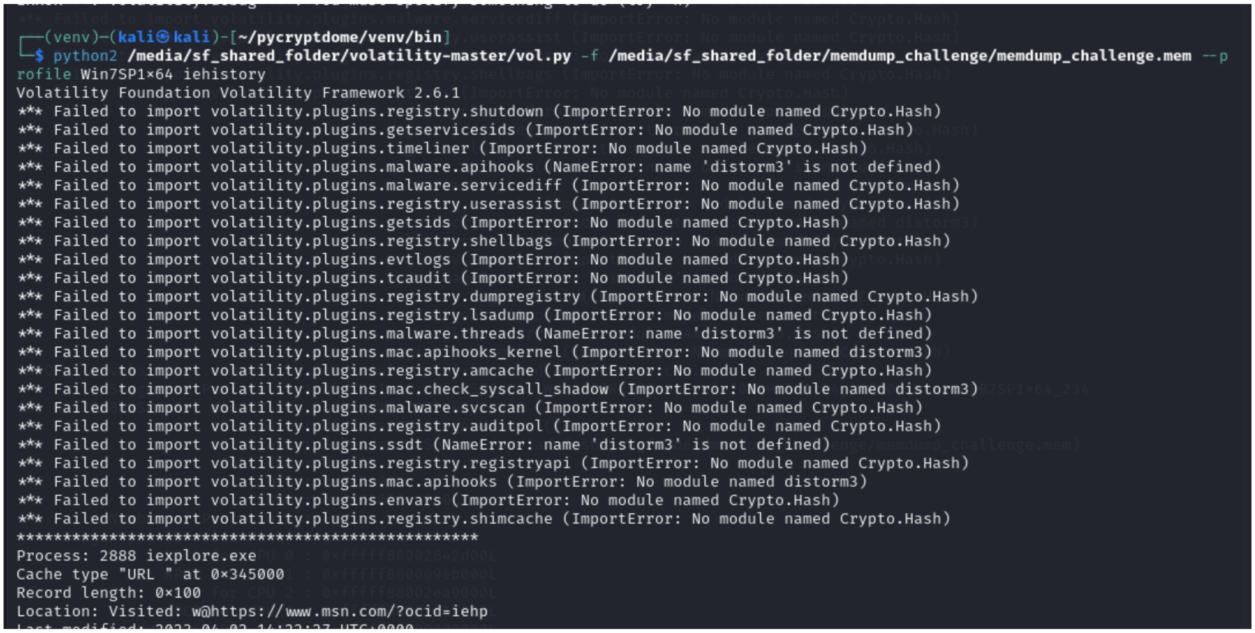
kali-linux-2024.2-virtualbox-amd64 (Snapshot 3) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
(venv)kali@kali: ~/pycryptdome/venv/bin
File Actions Edit View Help
Comments
Editing
Share
Find
Replace
Select
Editing
Dictate
Voice
Sensitivity
Editor
Add-ins
Check Compatibility
Centralized Deployment
Keenious Research Explorer
Commands Group
10:26 AM

```
         KUSER_SHARED_DATA : 0×fffff78000000000L
       Image date and time : 2023-04-02 14:37:16 UTC+0000
 Image local date and time : 2023-04-02 19:37:16 +0500

┌──(venv)─(kali㉿kali)-[~/pycryptdome/venv/bin]
└─$ 

┌──(venv)─(kali㉿kali)-[~/pycryptdome/venv/bin]
└─$ python2 /media/sf_shared_folder/volatility-master/vol.py -f /media/sf_shared_folder/memdump_challenge/memdump_ch
allenge.mem --profile Win7SP1×64 clipboard
Volatility Foundation Volatility Framework 2.6.1
*** 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)
Session    WindowStation Format                 Handle Object             Data
────────── ───────────── ────────────────── ────────────── ────────────── ──────────────────────────────────
────────────
         1 WinSta0       CF_UNICODETEXT           0×18027b 0×fffff900c1e6d260 flag{s0m3_stuff_c0p13d_1n_th3_cl1p
b0ard}
         1 WinSta0       CF_TEXT                      0×10 ──────────────

         1 WinSta0       0×a0103L          0×200000000000 ──────────────

         1 WinSta0       CF_TEXT                       0×1 ──────────────

         1 ───────────── ──────────────────        0×a0103 0×fffff900c210e780

┌──(venv)─(kali㉿kali)-[~/pycryptdome/venv/bin]
└─$ python2 /media/sf_shared_folder/volatility-master/vol.py -f /media/sf_shared_folder/memdump_challenge/memdump_challenge.mem --p
rofile Win7SP1×64 envars
Volatility Foundation Volatility Framework 2.6.1
*** 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)
```

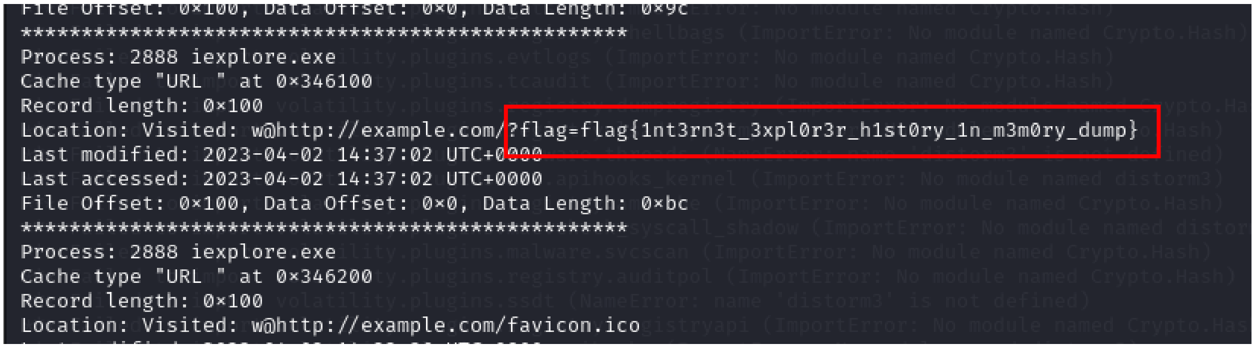
Flag: flag{s0m3_stuff_c0p13d_1n_th3_cl1pb0ard}

Q2)

To find it in the internet explorer search history we use the iehistory plugin



```
┌──(venv)─(kali㉿kali)-[~/pycryptdome/venv/bin]
└─$ python2 /media/sf_shared_folder/volatility-master/vol.py -f /media/sf_shared_folder/memdump_challenge/memdump_challenge.mem --p
rofile Win7SP1×64 iehistory
Volatility Foundation Volatility Framework 2.6.1
*** 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)
**************************************************
Process: 2888 iexplore.exe
Cache type "URL " at 0×345000
Record length: 0×100
Location: Visited: w@https://www.msn.com/?ocid=iehp
Last modified: 2023-04-02 14:23:27 UTC+0000
```



```
File Offset: 0×100, Data Offset: 0×0, Data Length: 0×9c
**************************************************
Process: 2888 iexplore.exe
Cache type "URL " at 0×346100
Record length: 0×100
Location: Visited: w@http://example.com/?flag=flag{1nt3rn3t_3xpl0r3r_h1st0ry_1n_m3m0ry_dump}
Last modified: 2023-04-02 14:37:02 UTC+0000
Last accessed: 2023-04-02 14:37:02 UTC+0000
File Offset: 0×100, Data Offset: 0×0, Data Length: 0×bc
**************************************************
Process: 2888 iexplore.exe
Cache type "URL " at 0×346200
Record length: 0×100
Location: Visited: w@http://example.com/favicon.ico
```

Flag: flag{1nt3rn3t_3xpl0r3r_h1st0ry_1n_m3m0ry_dump}

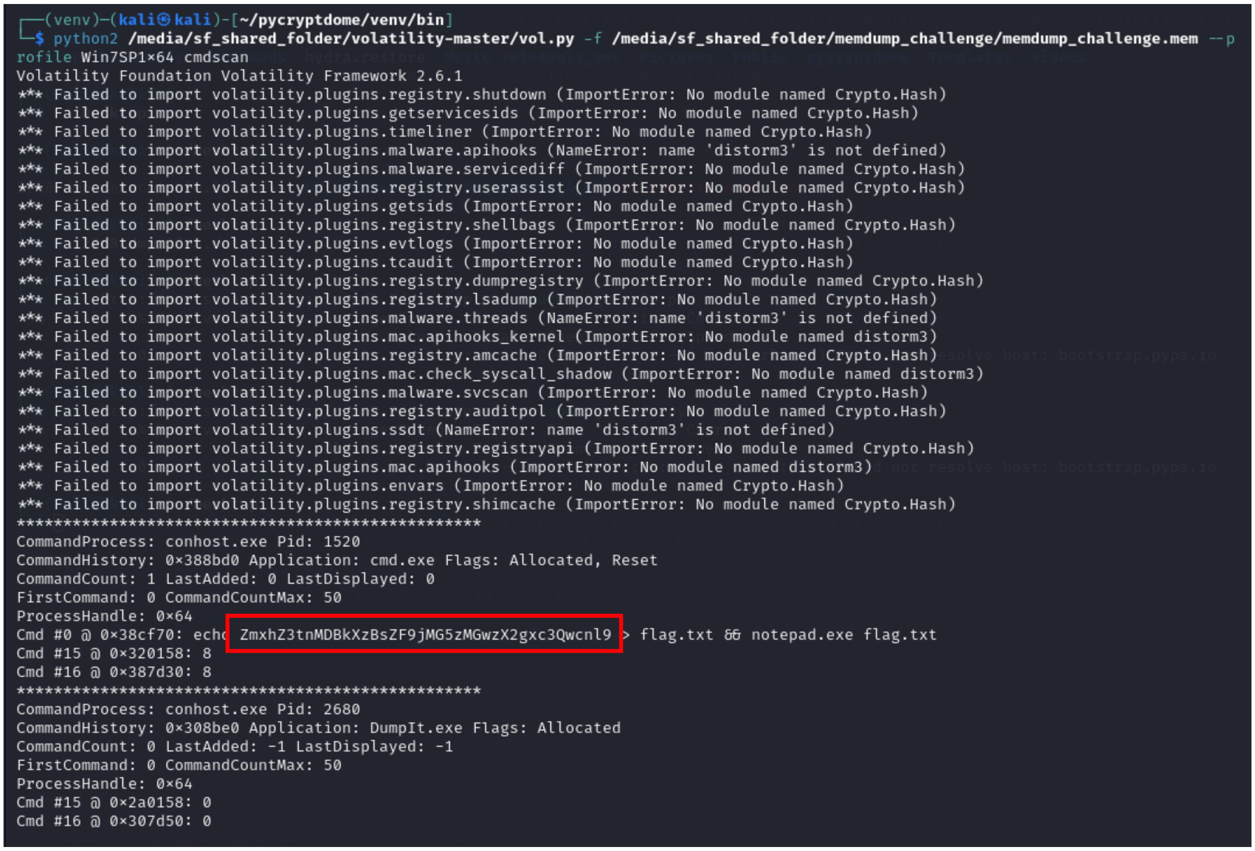
Q3)

This involves using the envars plugin which required pycryptodome

Flag:

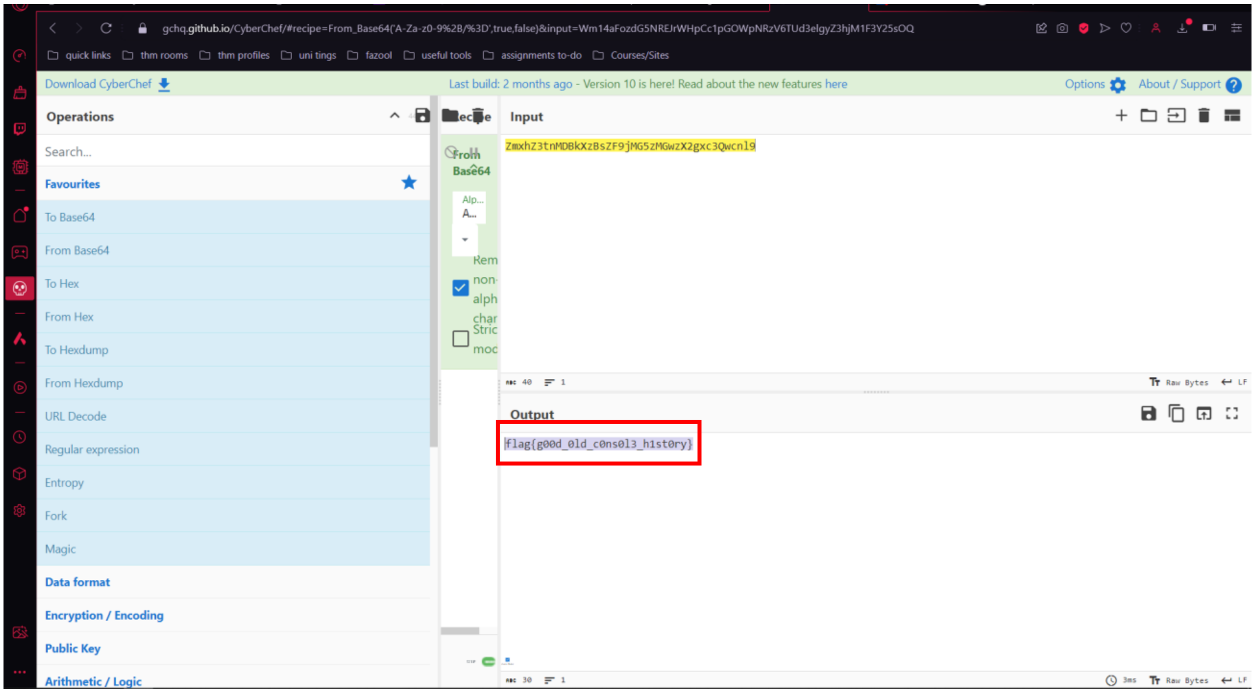
Q4)

This involves the plugin cmdscan



```
┌──(venv)─(kali㉿kali)-[~/pycryptdome/venv/bin]
└─$ python2 /media/sf_shared_folder/volatility-master/vol.py -f /media/sf_shared_folder/memdump_challenge/memdump_challenge.mem --p
rofile Win7SP1x64 cmdscan
Volatility Foundation Volatility Framework 2.6.1
*** 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)
**************************************************
CommandProcess: conhost.exe Pid: 1520
CommandHistory: 0x388bd0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
Cmd #0 @ 0x38cf70: echo ZmxhZ3tnMDBkXzBsZF9jMG5zMGwzX2gxc3Qwcnl9 > flag.txt && notepad.exe flag.txt
Cmd #15 @ 0x320158: 8
Cmd #16 @ 0x387d30: 8
**************************************************
CommandProcess: conhost.exe Pid: 2680
CommandHistory: 0x308be0 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
Cmd #15 @ 0x2a0158: 0
Cmd #16 @ 0x307d50: 0
```

This is an encrypted flag that we decrypt on cyberchef



gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=Wm14aFozdG5NREJrWHpCc1pGOWpNRzV6TUd3elgyZ3hjM1F3Y25sOQ

☑ Rem non- alph char

□ Stric moc

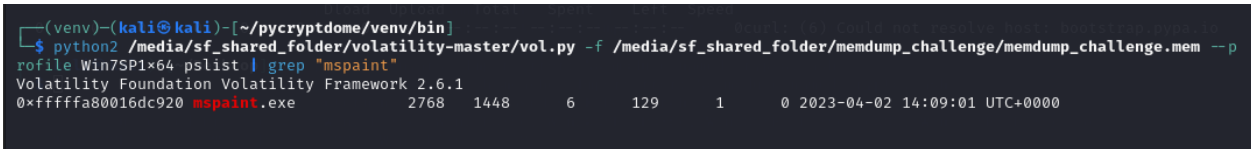
```
ZmxhZ3tnMDBkXzBsZF9jMG5zMGwzX2gxc3Qwcnl9
```

```
flag{g00d_0ld_c0ns0l3_h1st0ry}
```

Flag: flag{g00d_0ld_c0ns0l3_h1st0ry}

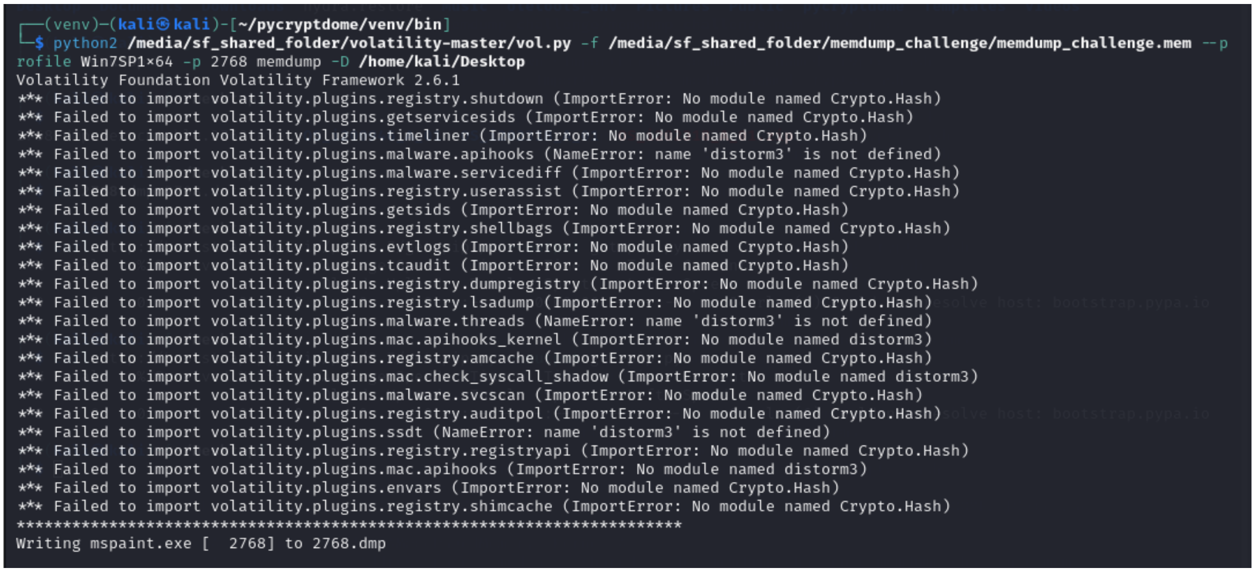
Q5)

First of all, finding the PID for mspaint



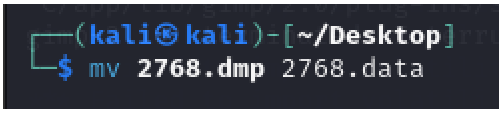
```
┌──(venv)─(kali㉿kali)-[~/pycryptdome/venv/bin]
└─$ python2 /media/sf_shared_folder/volatility-master/vol.py -f /media/sf_shared_folder/memdump_challenge/memdump_challenge.mem --p
rofile Win7SP1x64 pslist | grep "mspaint"
Volatility Foundation Volatility Framework 2.6.1
0xfffffa80016dc920 mspaint.exe            2768   1448      6      129      1      0 2023-04-02 14:09:01 UTC+0000
```

It is 2768. Now, exporting it's data



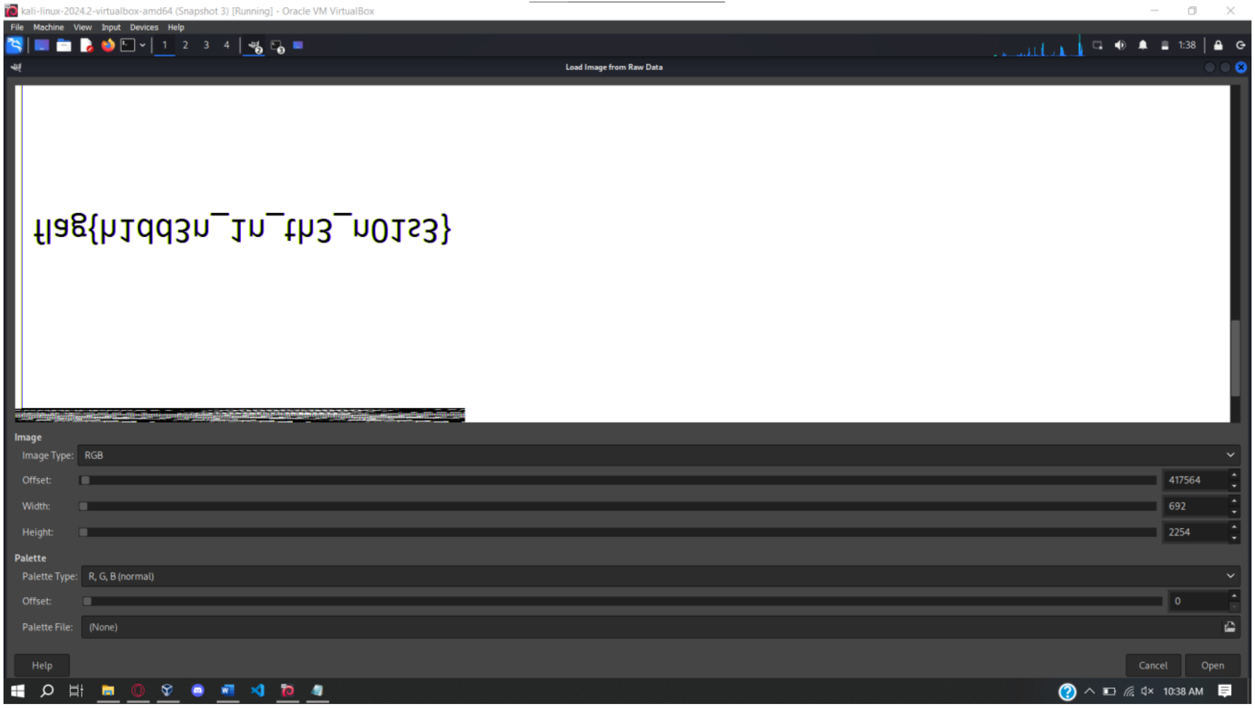
```
┌──(venv)─(kali㉿kali)-[~/pycryptdome/venv/bin]
└─$ python2 /media/sf_shared_folder/volatility-master/vol.py -f /media/sf_shared_folder/memdump_challenge/memdump_challenge.mem --p
rofile Win7SP1x64 -p 2768 memdump -D /home/kali/Desktop
Volatility Foundation Volatility Framework 2.6.1
*** Failed to 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)
************************************************************************
Writing mspaint.exe [  2768] to 2768.dmp
```

Changing the format



```
┌──(kali㉿kali)-[~/Desktop]
└─$ mv 2768.dmp 2768.data
```

Now opening it in GIMP, we get this



kali-linux-2024.2-virtualbox-amd64 (Snapshot 3) [Running] - Oracle VM VirtualBox

Load Image from Raw Data

Image

Image Type: RGB

Offset: 417564

Width: 692

Height: 2254

Palette

Palette Type: R, G, B (normal)

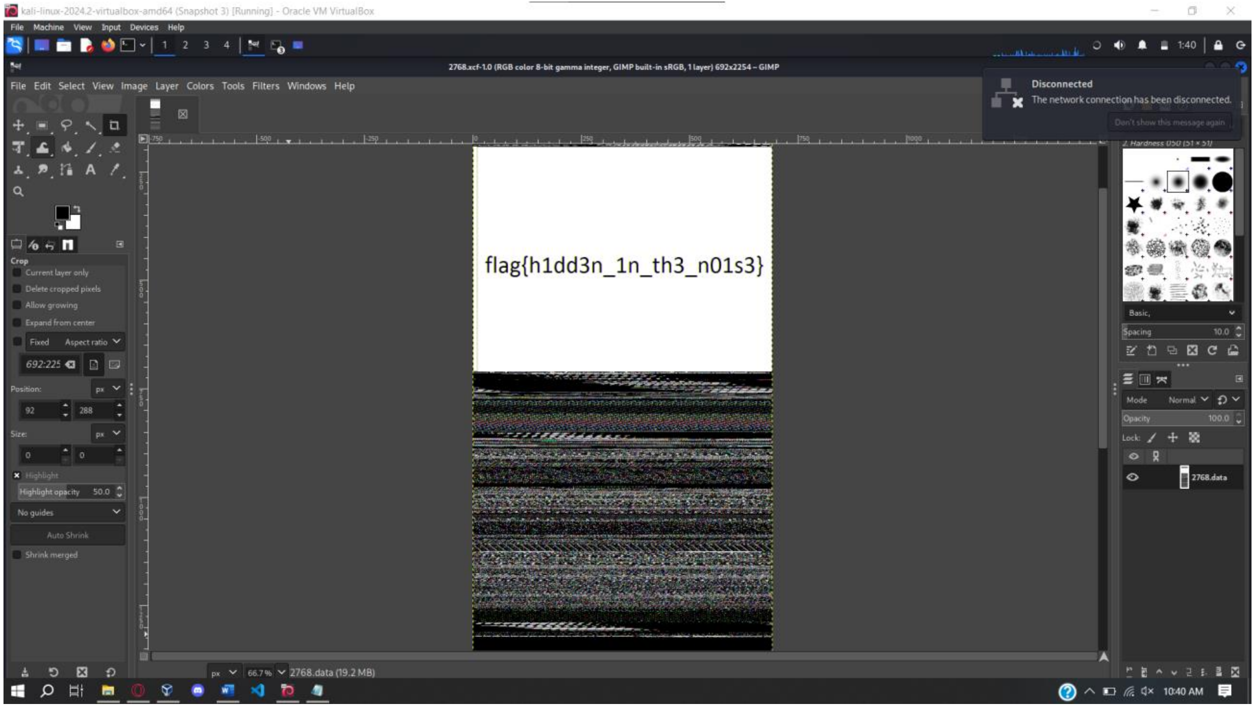
Offset: 0

Palette File: (None)

We opened the .data and then changed width till the font is visible, it was unintelligible first.

Then we moved the offset slider till the flag was completely visible.

Inverted the image to get this



kali-linux-2024.2-virtualbox-amd64 (Snapshot 3) [Running] - Oracle VM VirtualBox

2768.xcf-1.0 (RGB color 8-bit gamma integer, GIMP built-in sRGB, 1 layer) 692x2254 – GIMP

flag{h1dd3n_1n_th3_n01s3}

Disconnected

The network connection has been disconnected.

2768.data (19.2 MB)

The image is inverted from layer->transform->flip vertically

Flag: flag{h1dd3n_1n_th3_n01s3}