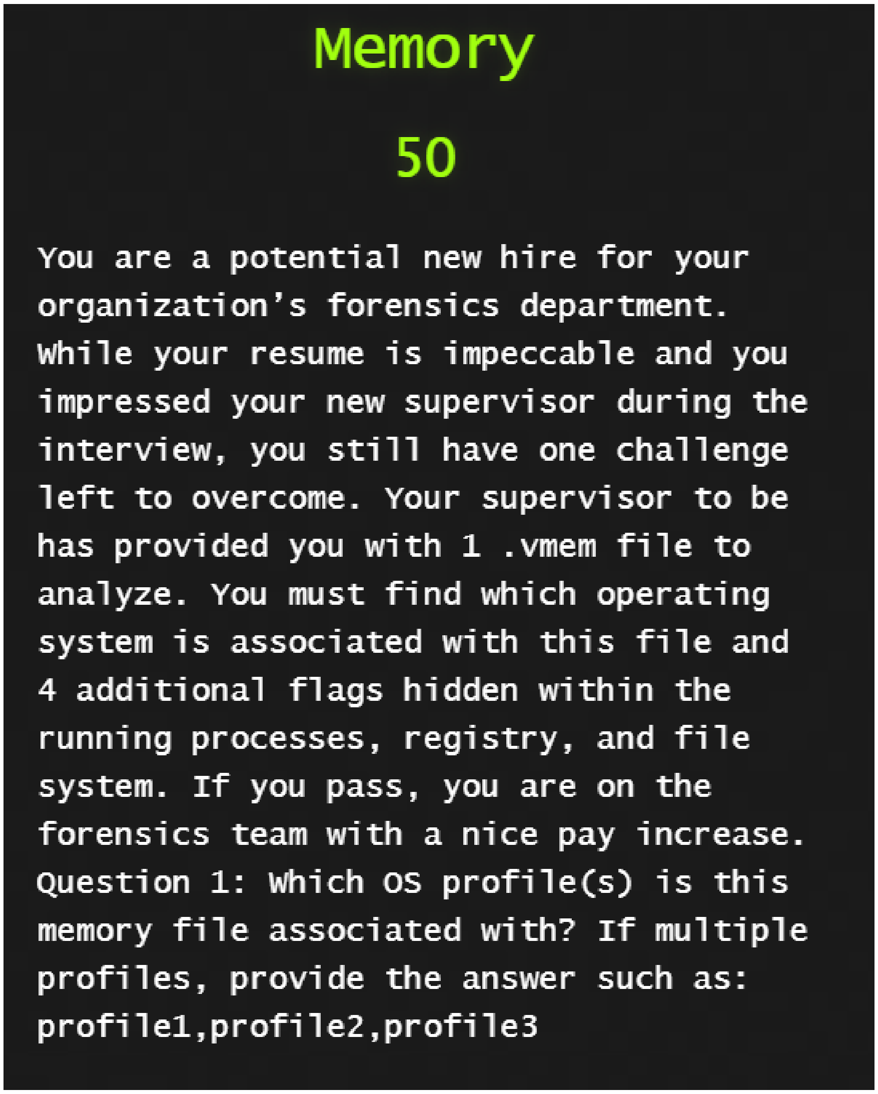
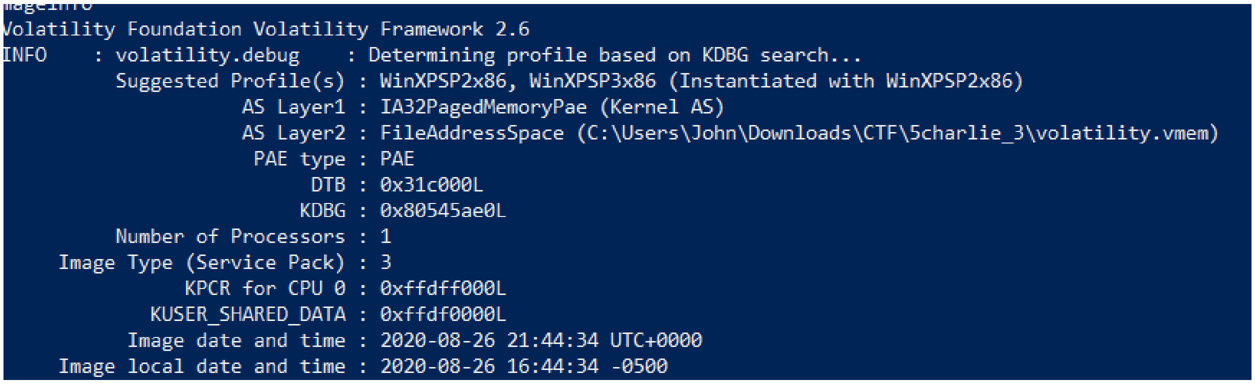


Memory

50

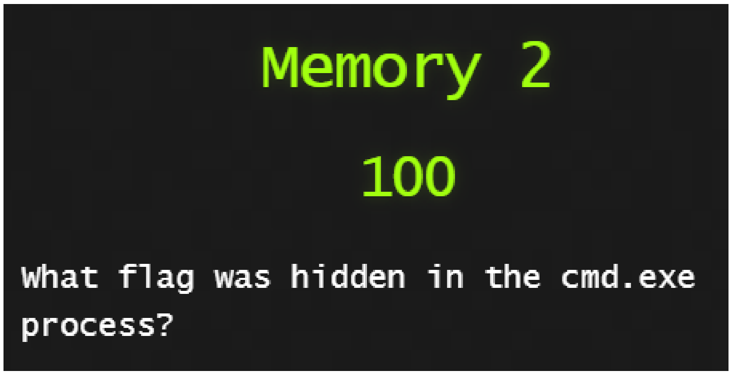
You are a potential new hire for your organization’s forensics department. While your resume is impeccable and you impressed your new supervisor during the interview, you still have one challenge left to overcome. Your supervisor to be has provided you with 1 .vmem file to analyze. You must find which operating system is associated with this file and 4 additional flags hidden within the running processes, registry, and file system. If you pass, you are on the forensics team with a nice pay increase. Question 1: Which OS profile(s) is this memory file associated with? If multiple profiles, provide the answer such as: profile1,profile2,profile3

Plugin to run: imageinfo



```
mageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\John\Downloads\CTF\5charlie_3\volatility.vmem)
                      PAE type : PAE
                           DTB : 0x31c000L
                          KDBG : 0x80545ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2020-08-26 21:44:34 UTC+0000
     Image local date and time : 2020-08-26 16:44:34 -0500
```

Flag: WinXPSP2x86,WINXPSP3x86

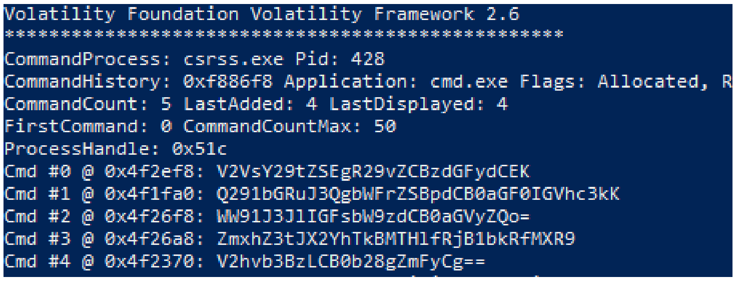


Memory 2

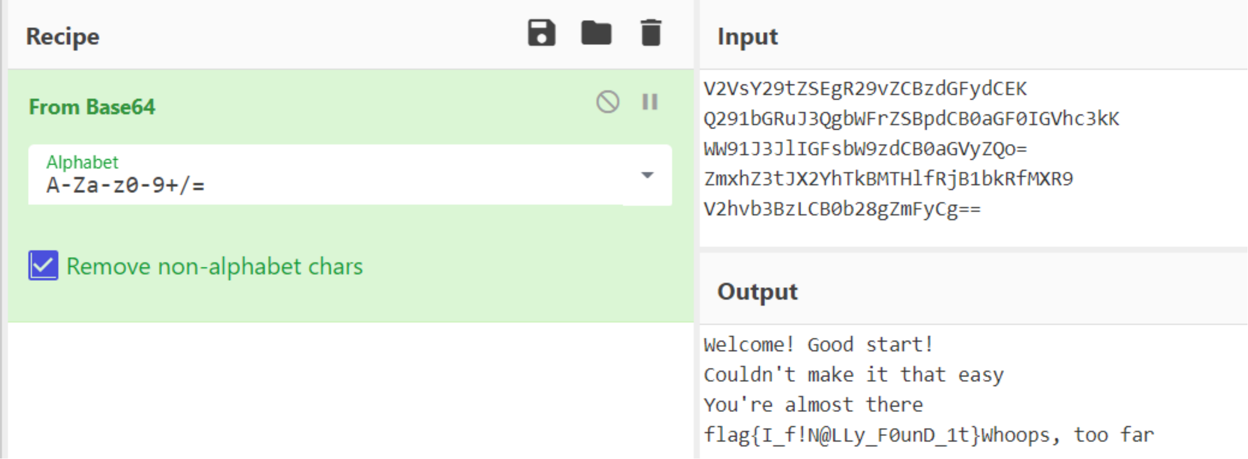
100

What flag was hidden in the cmd.exe process?

Volatility has a cmdscan to pull command line history.



```
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: csrss.exe Pid: 428
CommandHistory: 0xf886f8 Application: cmd.exe Flags: Allocated, R
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x51c
Cmd #0 @ 0x4f2ef8: V2VsY29tZSEgR29vZCBzdGFydCEK
Cmd #1 @ 0x4f1fa0: Q291bGRuJ3QgbWFrZSBpdCB0aGF0IGVhc3kK
Cmd #2 @ 0x4f26f8: WW91J3JlIGFsbW9zdCB0aGVyZQo=
Cmd #3 @ 0x4f26a8: ZmxhZ3tJX2YhTkBMTHlfRjB1bkRfMXR9
Cmd #4 @ 0x4f2370: V2hvb3BzLCB0b28gZmFyCg==
```



Recipe

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

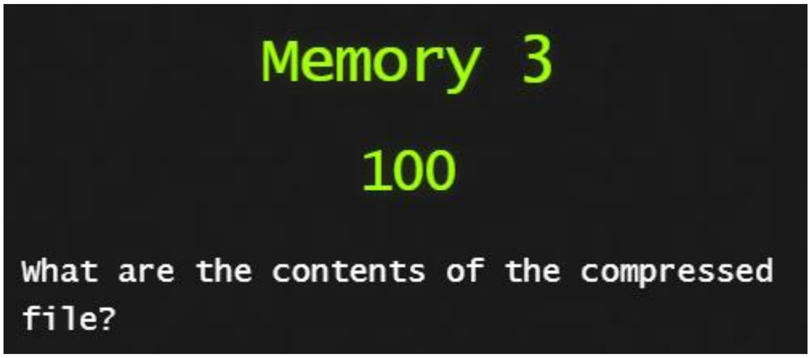
Input

```
V2VsY29tZSEgR29vZCBzdGFydCEK
Q291bGRuJ3QgbWFrZSBpdCB0aGF0IGVhc3kK
WW91J3JlIGFsbW9zdCB0aGVyZQo=
ZmxhZ3tJX2YhTkBMTHlfRjB1bkRfMXR9
V2hvb3BzLCB0b28gZmFyCg==
```

Output

```
Welcome! Good start!
Couldn't make it that easy
You're almost there
flag{I_f!N@LLy_F0unD_1t}Whoops, too far
```

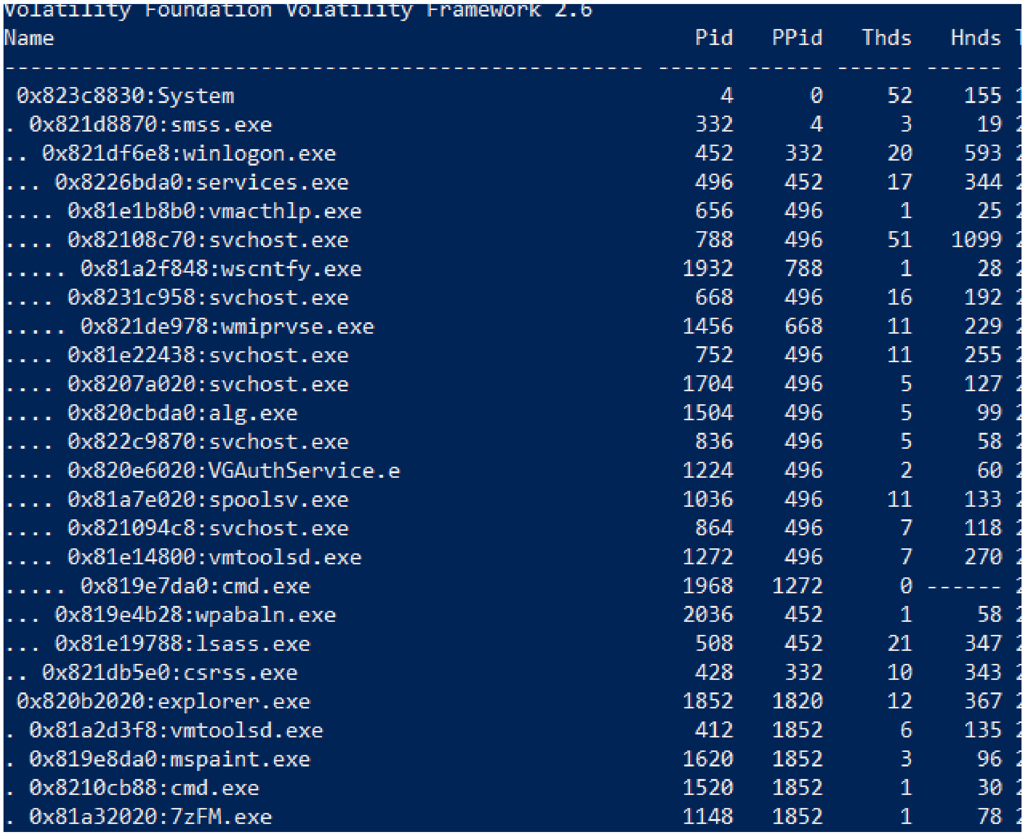
Flag: flag{I_f!N@LLy_F0unD_1t}



Memory 3

100

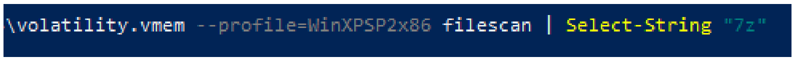
What are the contents of the compressed file?



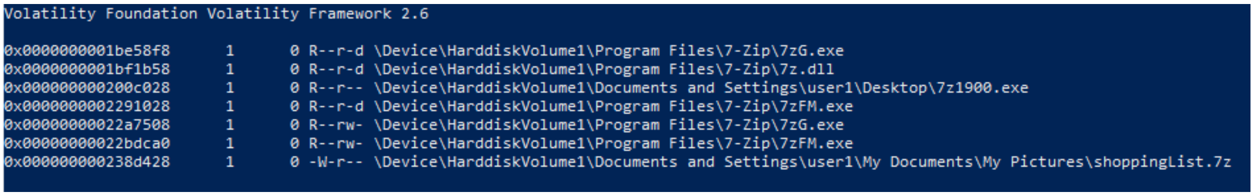
```
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds
-------------------------------------------------- ------ ------ ------ ------
 0x823c8830:System                                      4      0     52    155
. 0x821d8870:smss.exe                                 332      4      3     19
.. 0x821df6e8:winlogon.exe                            452    332     20    593
... 0x8226bda0:services.exe                           496    452     17    344
.... 0x81e1b8b0:vmacthlp.exe                          656    496      1     25
.... 0x82108c70:svchost.exe                           788    496     51   1099
..... 0x81a2f848:wscntfy.exe                         1932    788      1     28
.... 0x8231c958:svchost.exe                           668    496     16    192
..... 0x821de978:wmiprvse.exe                        1456    668     11    229
.... 0x81e22438:svchost.exe                           752    496     11    255
.... 0x8207a020:svchost.exe                          1704    496      5    127
.... 0x820cbda0:alg.exe                              1504    496      5     99
.... 0x822c9870:svchost.exe                           836    496      5     58
.... 0x820e6020:VGAuthService.e                      1224    496      2     60
.... 0x81a7e020:spoolsv.exe                          1036    496     11    133
.... 0x821094c8:svchost.exe                           864    496      7    118
.... 0x81e14800:vmtoolsd.exe                         1272    496      7    270
..... 0x819e7da0:cmd.exe                             1968   1272      0 ------
... 0x819e4b28:wpabaln.exe                           2036    452      1     58
... 0x81e19788:lsass.exe                              508    452     21    347
.. 0x821db5e0:csrss.exe                               428    332     10    343
 0x820b2020:explorer.exe                             1852   1820     12    367
. 0x81a2d3f8:vmtoolsd.exe                             412   1852      6    135
. 0x819e8da0:mspaint.exe                             1620   1852      3     96
. 0x8210cb88:cmd.exe                                 1520   1852      1     30
. 0x81a32020:7zFM.exe                                1148   1852      1     78
```

The compression program used in this is the 7zFM.exe (7Zip). We can look into this process.

We can do a filescan for files that are used in the 7zip extension (.7z)

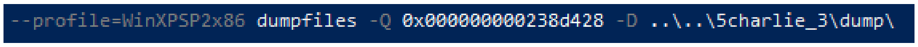


```
\volatility.vmem --profile=WinXPSP2x86 filescan | Select-String "7z"
```

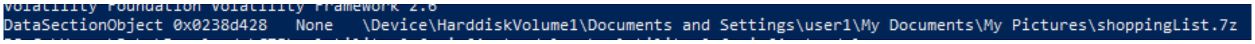


```
Volatility Foundation Volatility Framework 2.6

0x0000000001be58f8      1      0 R--r-d \Device\HarddiskVolume1\Program Files\7-Zip\7zG.exe
0x0000000001bf1b58      1      0 R--r-d \Device\HarddiskVolume1\Program Files\7-Zip\7z.dll
0x000000000200c028      1      0 R--r-- \Device\HarddiskVolume1\Documents and Settings\user1\Desktop\7z1900.exe
0x0000000002291028      1      0 R--r-d \Device\HarddiskVolume1\Program Files\7-Zip\7zFM.exe
0x00000000022a7508      1      0 R--rw- \Device\HarddiskVolume1\Program Files\7-Zip\7zG.exe
0x00000000022bdca0      1      0 R--rw- \Device\HarddiskVolume1\Program Files\7-Zip\7zFM.exe
0x000000000238d428      1      0 -W-r-- \Device\HarddiskVolume1\Documents and Settings\user1\My Documents\My Pictures\shoppingList.7z
```

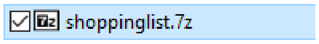
Next, we want to extract the shoppinglist.7z @ 238d428 offset



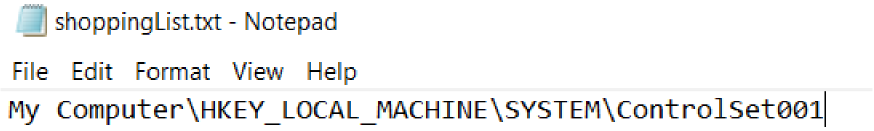
```
--profile=WinXPSP2x86 dumpfiles -Q 0x000000000238d428 -D ..\..\5charlie_3\dump\
```



```
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x0238d428   None   \Device\HarddiskVolume1\Documents and Settings\user1\My Documents\My Pictures\shoppingList.7z
```

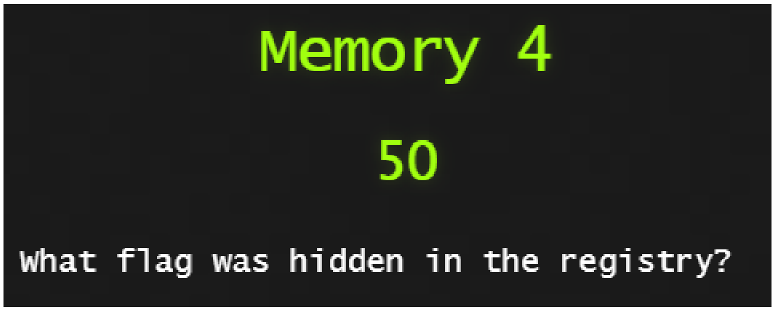


☑ shoppinglist.7z



```
My Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001
```

Flag: My Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001



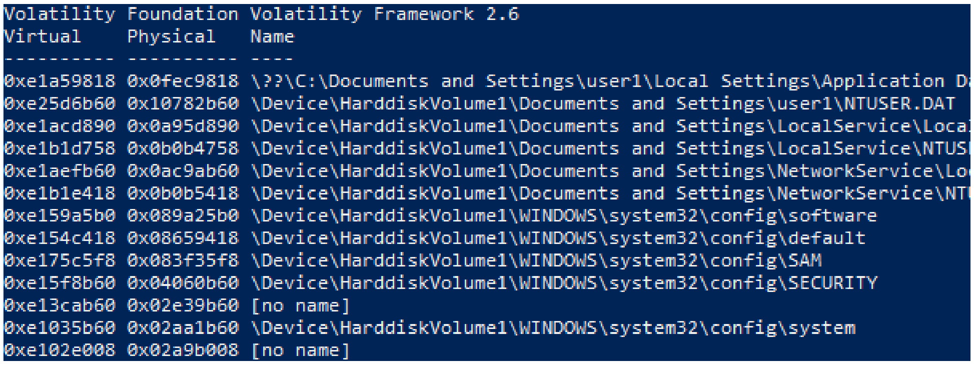
Memory 4

50

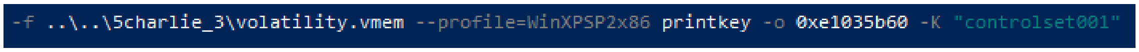
What flag was hidden in the registry?

Run the hivelist to look at the location of the registry hives.

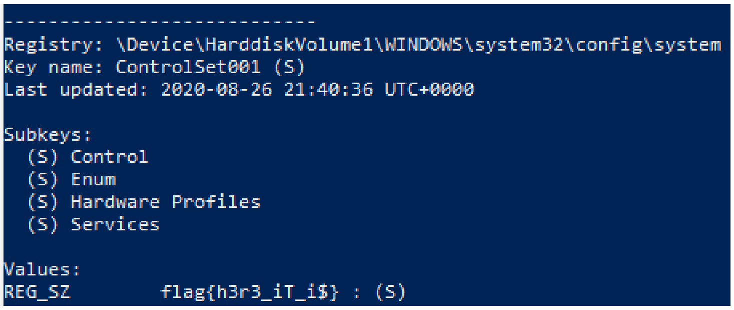
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001



```
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe1a59818 0x0fec9818 \??\C:\Documents and Settings\user1\Local Settings\Application D
0xe25d6b60 0x10782b60 \Device\HarddiskVolume1\Documents and Settings\user1\NTUSER.DAT
0xe1acd890 0x0a95d890 \Device\HarddiskVolume1\Documents and Settings\LocalService\Loca
0xe1b1d758 0x0b0b4758 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUS
0xe1aefb60 0x0ac9ab60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Lo
0xe1b1e418 0x0b0b5418 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NT
0xe159a5b0 0x089a25b0 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe154c418 0x08659418 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe175c5f8 0x083f35f8 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe15f8b60 0x04060b60 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe13cab60 0x02e39b60 [no name]
0xe1035b60 0x02aa1b60 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe102e008 0x02a9b008 [no name]
```

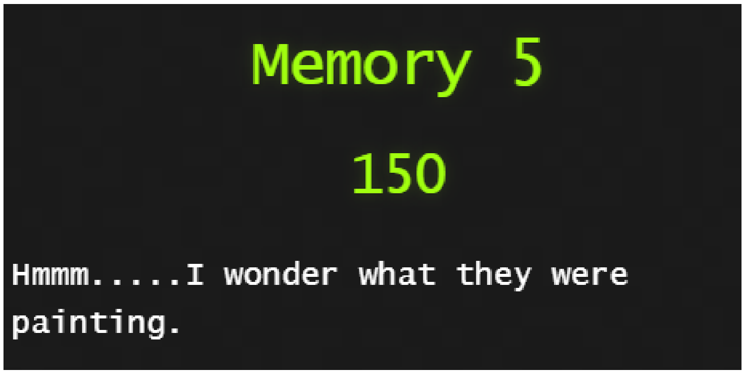


```
-f ..\..\5charlie_3\volatility.vmem --profile=WinXPSP2x86 printkey -o 0xe1035b60 -K "controlset001"
```



```
----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
Key name: ControlSet001 (S)
Last updated: 2020-08-26 21:40:36 UTC+0000

Subkeys:
  (S) Control
  (S) Enum
  (S) Hardware Profiles
  (S) Services

Values:
REG_SZ        flag{h3r3_iT_i$} : (S)
```

Flag: flag{h3r3_iT_i$}

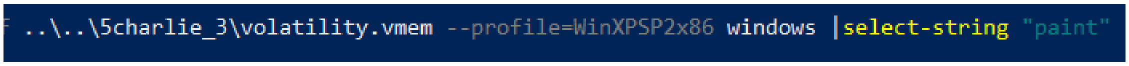


Memory 5

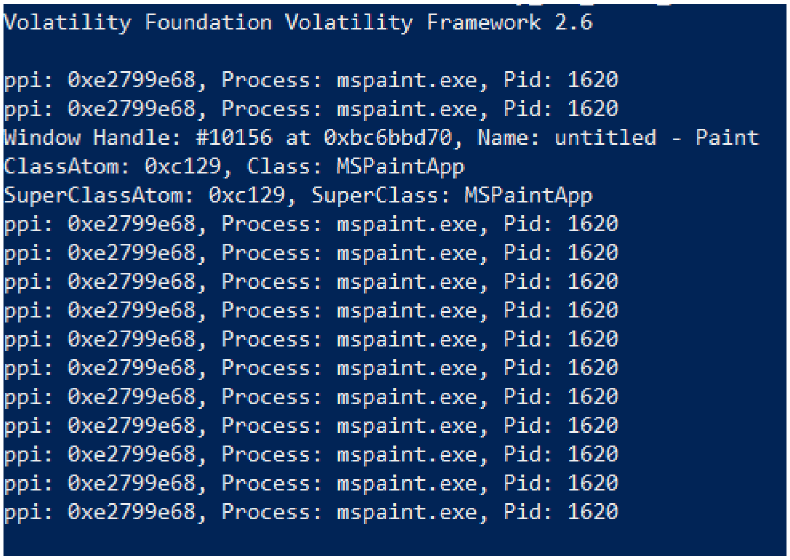
150

Hmmm.....I wonder what they were painting.

I rand the windows command to look for any open windows on the desktop. I also dropped anything that did not have the word paint in it.

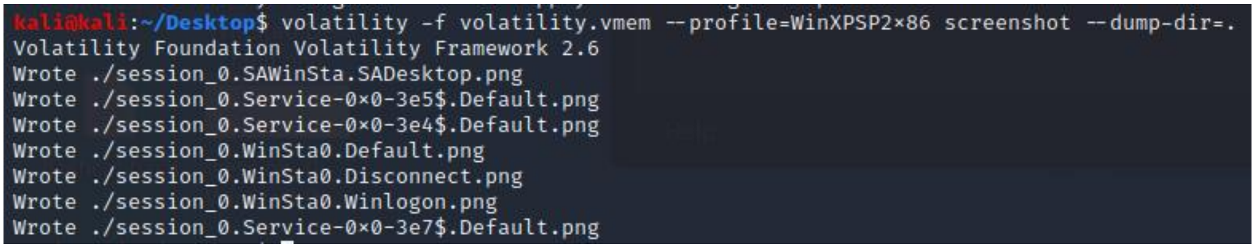


```
f ..\..\5charlie_3\volatility.vmem --profile=WinXPSP2x86 windows |select-string "paint"
```



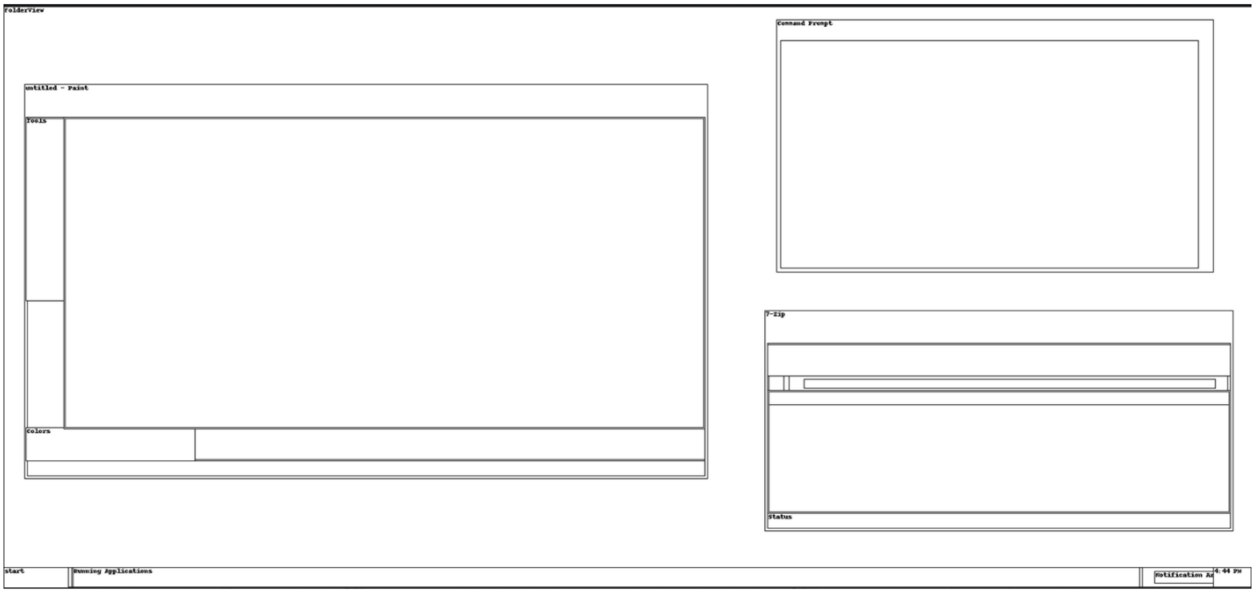
```
Volatility Foundation Volatility Framework 2.6

ppi: 0xe2799e68, Process: mspaint.exe, Pid: 1620
ppi: 0xe2799e68, Process: mspaint.exe, Pid: 1620
Window Handle: #10156 at 0xbc6bbd70, Name: untitled - Paint
ClassAtom: 0xc129, Class: MSPaintApp
SuperClassAtom: 0xc129, SuperClass: MSPaintApp
ppi: 0xe2799e68, Process: mspaint.exe, Pid: 1620
ppi: 0xe2799e68, Process: mspaint.exe, Pid: 1620
ppi: 0xe2799e68, Process: mspaint.exe, Pid: 1620
ppi: 0xe2799e68, Process: mspaint.exe, Pid: 1620
ppi: 0xe2799e68, Process: mspaint.exe, Pid: 1620
ppi: 0xe2799e68, Process: mspaint.exe, Pid: 1620
ppi: 0xe2799e68, Process: mspaint.exe, Pid: 1620
ppi: 0xe2799e68, Process: mspaint.exe, Pid: 1620
ppi: 0xe2799e68, Process: mspaint.exe, Pid: 1620
ppi: 0xe2799e68, Process: mspaint.exe, Pid: 1620
ppi: 0xe2799e68, Process: mspaint.exe, Pid: 1620
```

I had to switch to linux for a minute due to the lack of a library in widows to extract screenshots



```
kali@kali:~/Desktop$ volatility -f volatility.vmem --profile=WinXPSP2x86 screenshot --dump-dir=.
Volatility Foundation Volatility Framework 2.6
Wrote ./session_0.SAWinSta.SADesktop.png
Wrote ./session_0.Service-0x0-3e5$.Default.png
Wrote ./session_0.Service-0x0-3e4$.Default.png
Wrote ./session_0.WinSta0.Default.png
Wrote ./session_0.WinSta0.Disconnect.png
Wrote ./session_0.WinSta0.Winlogon.png
Wrote ./session_0.Service-0x0-3e7$.Default.png
```

It dumped out 7 images, but only one was not blank.



Right click and look at the properties.

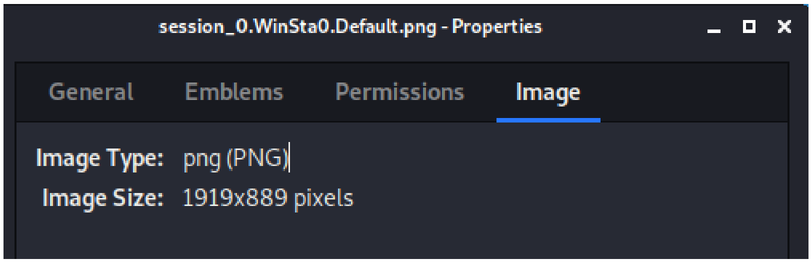
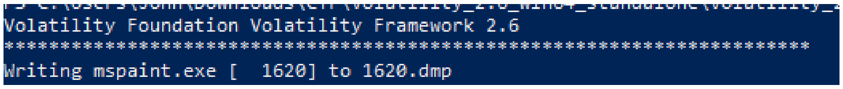

session_0.WinSta0.Default.png - Properties

Image Type: png (PNG)

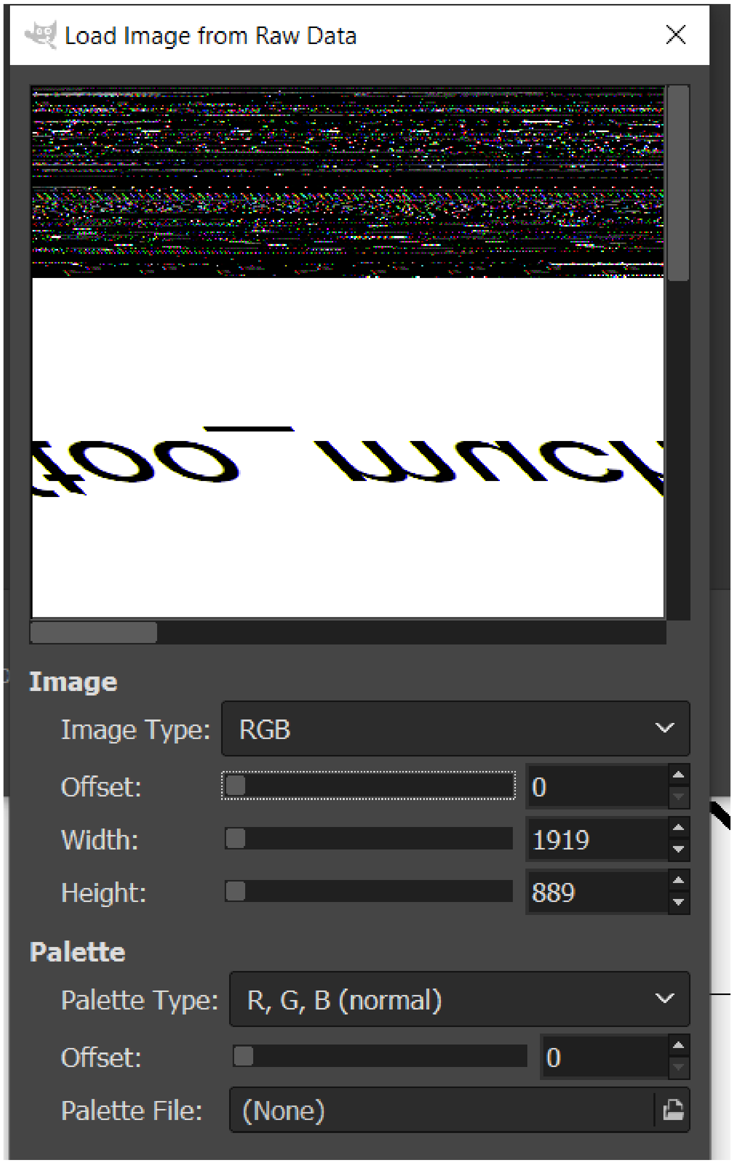
Image Size: 1919x889 pixels

Remember the image size.



```
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing mspaint.exe [  1620] to 1620.dmp
```

Change the .dmp to .data to be read into GIMP



Load Image from Raw Data

Image

Image Type: RGB

Offset: 0

Width: 1919

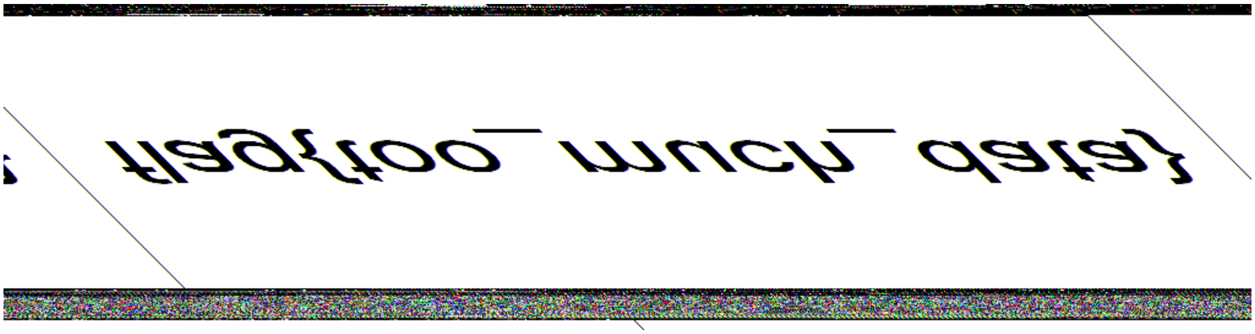
Height: 889

Palette

Palette Type: R, G, B (normal)

Offset: 0

Palette File: (None)



Flip and Rotate:

flag{too_much_data}

Flag: flag{too_much_data}