National University
of computer and emerging sciences

Lab 09

CYL2002 Digital Forensics - Lab

Name : Mirza Humayun Masood(i22-1749)

Section : CY-A

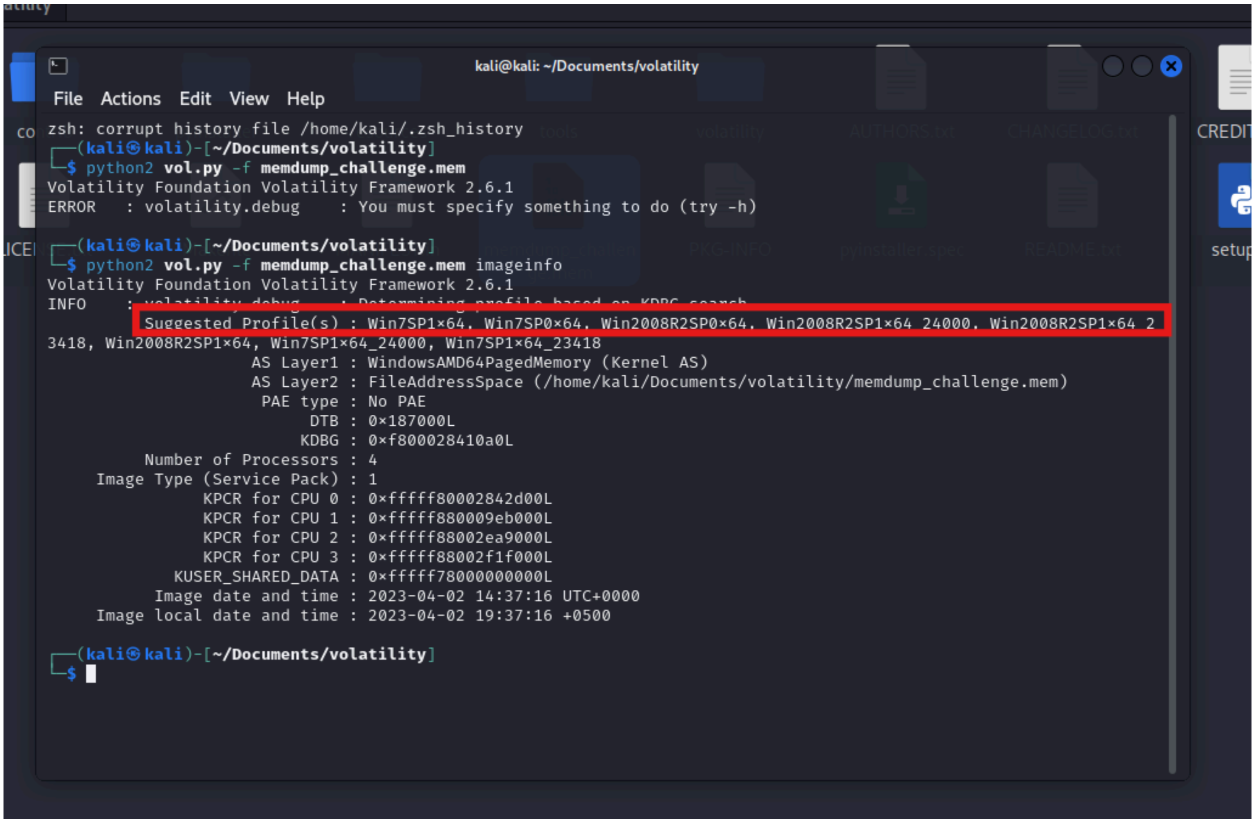
Submitted to: Sir Ubaid Ullah

Department of Cyber Security BS(CY)

FAST-NUCES Islamabad

In this lab we had to do forensics on a memory dump. For that we used votailtiy.

So first i ran volatility on the image file to see its info.



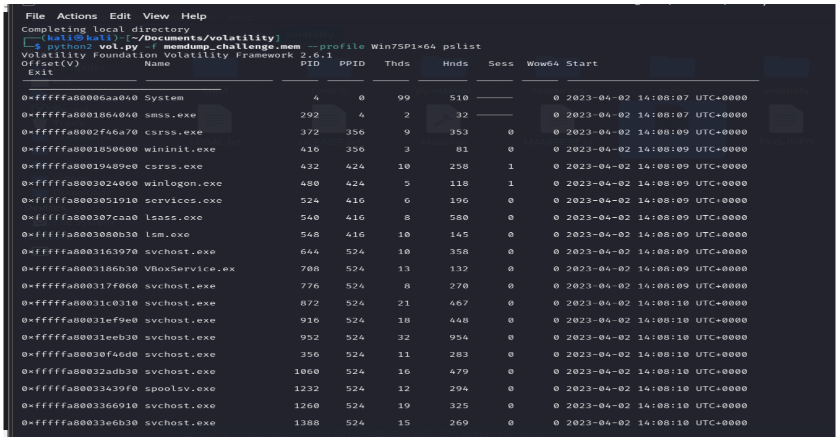
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~/Documents/volatility]
└─$ python2 vol.py -f memdump_challenge.mem
Volatility Foundation Volatility Framework 2.6.1
ERROR   : volatility.debug    : You must specify something to do (try -h)

┌──(kali㉿kali)-[~/Documents/volatility]
└─$ python2 vol.py -f memdump_challenge.mem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_2
3418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Documents/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 : 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)-[~/Documents/volatility]
└─$
```

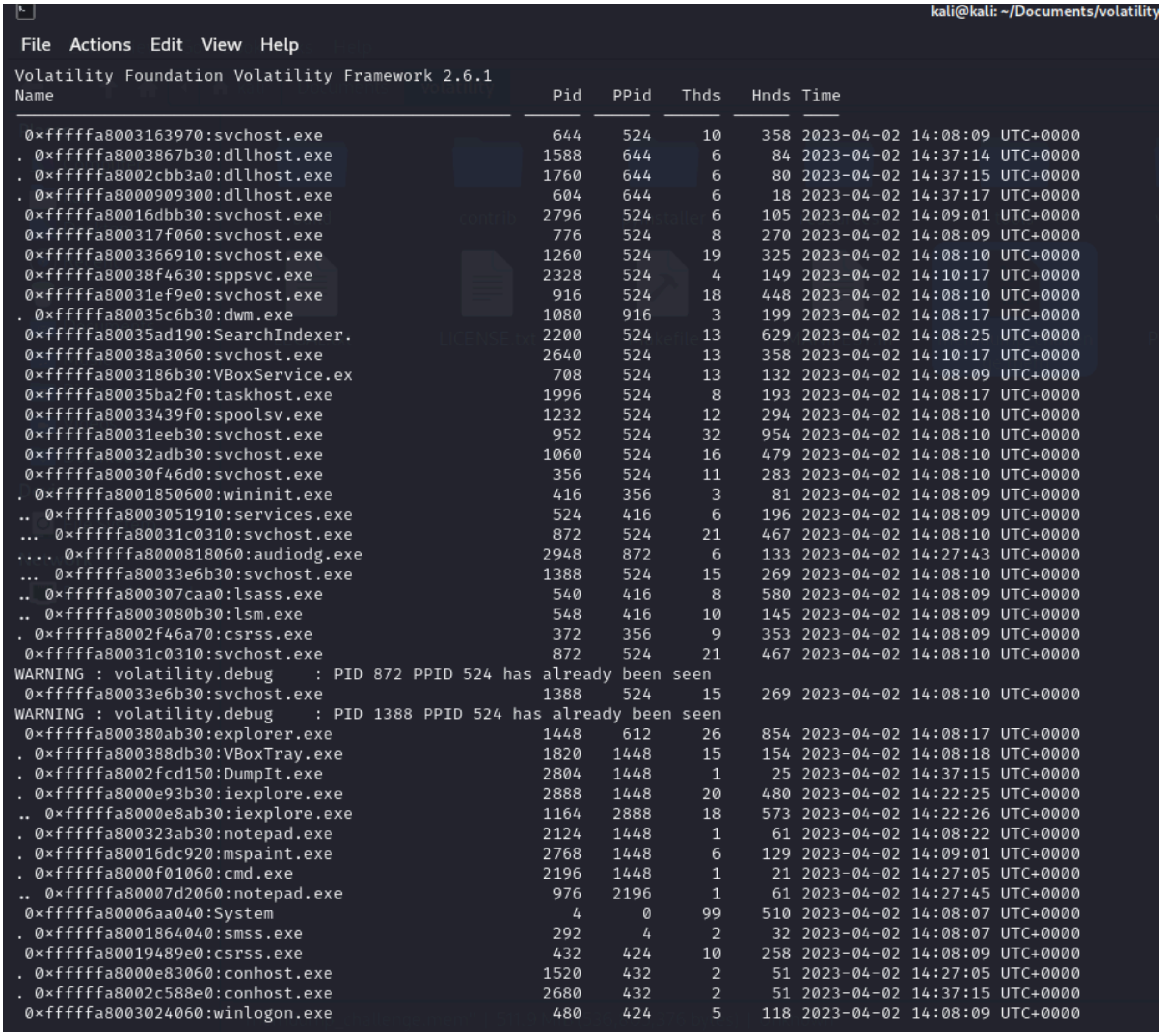
So as we can see the suggested profile is Win7SP1x64 , so we would be using that profile in this task.

So now we will run pslist using this profile to see what processes are being run.



```
Completing local directory
┌──(kali㉿kali)-[~/Documents/volatility]
└─$ python2 vol.py -f memdump_challenge.mem --profile Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
 Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
 ------------------------------
0xfffffa80006aa040 System                    4      0     99      510 ------      0 2023-04-02 14:08:07 UTC+0000
0xfffffa8001864040 smss.exe                292      4      2       32 ------      0 2023-04-02 14:08:07 UTC+0000
0xfffffa8002f46a70 csrss.exe               372    356      9      353      0      0 2023-04-02 14:08:09 UTC+0000
0xfffffa8001850600 wininit.exe             416    356      3       81      0      0 2023-04-02 14:08:09 UTC+0000
0xfffffa80019489e0 csrss.exe               432    424     10      258      1      0 2023-04-02 14:08:09 UTC+0000
0xfffffa8003024060 winlogon.exe            480    424      5      118      1      0 2023-04-02 14:08:09 UTC+0000
0xfffffa8003051910 services.exe            524    416      6      196      0      0 2023-04-02 14:08:09 UTC+0000
0xfffffa800307caa0 lsass.exe               540    416      8      580      0      0 2023-04-02 14:08:09 UTC+0000
0xfffffa8003080b30 lsm.exe                 548    416     10      145      0      0 2023-04-02 14:08:09 UTC+0000
0xfffffa8003163970 svchost.exe             644    524     10      358      0      0 2023-04-02 14:08:09 UTC+0000
0xfffffa8003186b30 VBoxService.ex          708    524     13      132      0      0 2023-04-02 14:08:09 UTC+0000
0xfffffa800317f060 svchost.exe             776    524      8      270      0      0 2023-04-02 14:08:09 UTC+0000
0xfffffa80031c0310 svchost.exe             872    524     21      467      0      0 2023-04-02 14:08:10 UTC+0000
0xfffffa80031ef9e0 svchost.exe             916    524     18      448      0      0 2023-04-02 14:08:10 UTC+0000
0xfffffa80031eeb30 svchost.exe             952    524     32      954      0      0 2023-04-02 14:08:10 UTC+0000
0xfffffa80030f46d0 svchost.exe             356    524     11      283      0      0 2023-04-02 14:08:10 UTC+0000
0xfffffa80032adb30 svchost.exe            1060    524     16      479      0      0 2023-04-02 14:08:10 UTC+0000
0xfffffa80033439f0 spoolsv.exe            1232    524     12      294      0      0 2023-04-02 14:08:10 UTC+0000
0xfffffa8003366910 svchost.exe            1260    524     19      325      0      0 2023-04-02 14:08:10 UTC+0000
0xfffffa80033e6b30 svchost.exe            1388    524     15      269      0      0 2023-04-02 14:08:10 UTC+0000
```

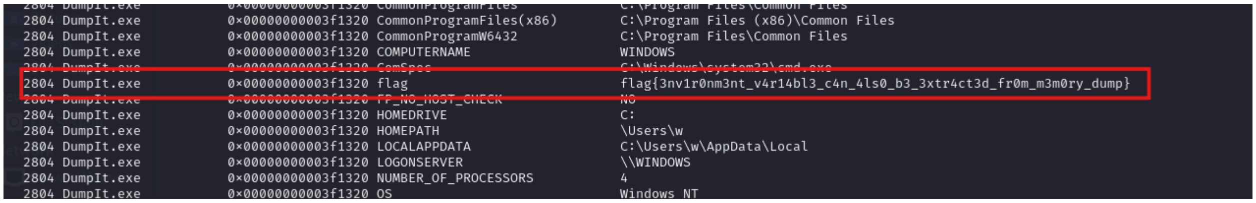
So after that as i ran pstree.


kali@kali: ~/Documents/volatility
File Actions Edit View Help

```
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa8003163970:svchost.exe                       644    524     10    358 2023-04-02 14:08:09 UTC+0000
. 0xfffffa8003867b30:dllhost.exe                     1588    644      6     84 2023-04-02 14:37:14 UTC+0000
. 0xfffffa8002cbb3a0:dllhost.exe                     1760    644      6     80 2023-04-02 14:37:15 UTC+0000
. 0xfffffa8000909300:dllhost.exe                      604    644      6     18 2023-04-02 14:37:17 UTC+0000
 0xfffffa80016dbb30:svchost.exe                      2796    524      6    105 2023-04-02 14:09:01 UTC+0000
 0xfffffa800317f060:svchost.exe                       776    524      8    270 2023-04-02 14:08:09 UTC+0000
 0xfffffa8003366910:svchost.exe                      1260    524     19    325 2023-04-02 14:08:10 UTC+0000
 0xfffffa80038f4630:sppsvc.exe                       2328    524      4    149 2023-04-02 14:10:17 UTC+0000
 0xfffffa80031ef9e0:svchost.exe                       916    524     18    448 2023-04-02 14:08:10 UTC+0000
. 0xfffffa80035c6b30:dwm.exe                         1080    916      3    199 2023-04-02 14:08:17 UTC+0000
 0xfffffa80035ad190:SearchIndexer.                   2200    524     13    629 2023-04-02 14:08:25 UTC+0000
 0xfffffa80038a3060:svchost.exe                      2640    524     13    358 2023-04-02 14:10:17 UTC+0000
 0xfffffa8003186b30:VBoxService.ex                    708    524     13    132 2023-04-02 14:08:09 UTC+0000
 0xfffffa80035ba2f0:taskhost.exe                     1996    524      8    193 2023-04-02 14:08:17 UTC+0000
 0xfffffa80033439f0:spoolsv.exe                      1232    524     12    294 2023-04-02 14:08:10 UTC+0000
 0xfffffa80031eeb30:svchost.exe                       952    524     32    954 2023-04-02 14:08:10 UTC+0000
 0xfffffa80032adb30:svchost.exe                      1060    524     16    479 2023-04-02 14:08:10 UTC+0000
 0xfffffa80030f46d0:svchost.exe                       356    524     11    283 2023-04-02 14:08:10 UTC+0000
. 0xfffffa8001850600:wininit.exe                      416    356      3     81 2023-04-02 14:08:09 UTC+0000
.. 0xfffffa8003051910:services.exe                    524    416      6    196 2023-04-02 14:08:09 UTC+0000
... 0xfffffa80031c0310:svchost.exe                    872    524     21    467 2023-04-02 14:08:10 UTC+0000
.... 0xfffffa8000818060:audiodg.exe                  2948    872      6    133 2023-04-02 14:27:43 UTC+0000
... 0xfffffa80033e6b30:svchost.exe                   1388    524     15    269 2023-04-02 14:08:10 UTC+0000
.. 0xfffffa800307caa0:lsass.exe                       540    416      8    580 2023-04-02 14:08:09 UTC+0000
.. 0xfffffa8003080b30:lsm.exe                         548    416     10    145 2023-04-02 14:08:09 UTC+0000
. 0xfffffa8002f46a70:csrss.exe                        372    356      9    353 2023-04-02 14:08:09 UTC+0000
 0xfffffa80031c0310:svchost.exe                       872    524     21    467 2023-04-02 14:08:10 UTC+0000
WARNING : volatility.debug    : PID 872 PPID 524 has already been seen
 0xfffffa80033e6b30:svchost.exe                      1388    524     15    269 2023-04-02 14:08:10 UTC+0000
WARNING : volatility.debug    : PID 1388 PPID 524 has already been seen
 0xfffffa800380ab30:explorer.exe                     1448    612     26    854 2023-04-02 14:08:17 UTC+0000
. 0xfffffa800388db30:VBoxTray.exe                    1820   1448     15    154 2023-04-02 14:08:18 UTC+0000
. 0xfffffa8002fcd150:DumpIt.exe                      2804   1448      1     25 2023-04-02 14:37:15 UTC+0000
. 0xfffffa8000e93b30:iexplore.exe                    2888   1448     20    480 2023-04-02 14:22:25 UTC+0000
.. 0xfffffa8000e8ab30:iexplore.exe                   1164   2888     18    573 2023-04-02 14:22:26 UTC+0000
. 0xfffffa800323ab30:notepad.exe                     2124   1448      1     61 2023-04-02 14:08:22 UTC+0000
. 0xfffffa80016dc920:mspaint.exe                     2768   1448      6    129 2023-04-02 14:09:01 UTC+0000
. 0xfffffa8000f01060:cmd.exe                         2196   1448      1     21 2023-04-02 14:27:05 UTC+0000
.. 0xfffffa80007d2060:notepad.exe                     976   2196      1     61 2023-04-02 14:27:45 UTC+0000
 0xfffffa80006aa040:System                              4      0     99    510 2023-04-02 14:08:07 UTC+0000
. 0xfffffa8001864040:smss.exe                         292      4      2     32 2023-04-02 14:08:07 UTC+0000
 0xfffffa80019489e0:csrss.exe                         432    424     10    258 2023-04-02 14:08:09 UTC+0000
. 0xfffffa8000e83060:conhost.exe                     1520    432      2     51 2023-04-02 14:27:05 UTC+0000
. 0xfffffa8002c588e0:conhost.exe                     2680    432      2     51 2023-04-02 14:37:15 UTC+0000
 0xfffffa8003024060:winlogon.exe                      480    424      5    118 2023-04-02 14:08:09 UTC+0000
```

Flag 1: so i ran this command , and got the environment variable.

python2 vol.py -f memdump_challenge.mem --profile Win7SP1x64 envars

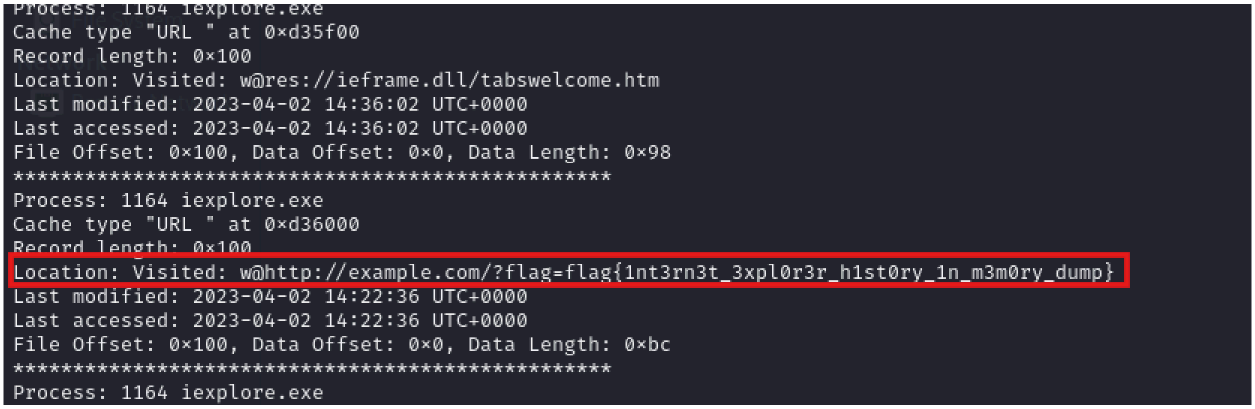


```
2804 DumpIt.exe          0x00000000003f1320 CommonProgramFiles          C:\Program Files\Common Files
2804 DumpIt.exe          0x00000000003f1320 CommonProgramFiles(x86)     C:\Program Files (x86)\Common Files
2804 DumpIt.exe          0x00000000003f1320 CommonProgramW6432          C:\Program Files\Common Files
2804 DumpIt.exe          0x00000000003f1320 COMPUTERNAME                WINDOWS
2804 DumpIt.exe          0x00000000003f1320 ComSpec                     C:\Windows\system32\cmd.exe
2804 DumpIt.exe          0x00000000003f1320 flag                        flag{3nv1r0nm3nt_v4r14bl3_c4n_4ls0_b3_3xtr4ct3d_fr0m_m3m0ry_dump}
2804 DumpIt.exe          0x00000000003f1320 FP_NO_HOST_CHECK            NO
2804 DumpIt.exe          0x00000000003f1320 HOMEDRIVE                   C:
2804 DumpIt.exe          0x00000000003f1320 HOMEPATH                    \Users\w
2804 DumpIt.exe          0x00000000003f1320 LOCALAPPDATA                C:\Users\w\AppData\Local
2804 DumpIt.exe          0x00000000003f1320 LOGONSERVER                 \\WINDOWS
2804 DumpIt.exe          0x00000000003f1320 NUMBER_OF_PROCESSORS        4
2804 DumpIt.exe          0x00000000003f1320 OS                          Windows NT
```

flag{3nv1r0nm3nt_v4r14bl3_c4n_4ls0_b3_3xtr4ct3d_fr0m_m3m0ry_dump}

Flag2: So for the internet history ran command and here it is.

python2 vol.py -f memdump_challenge.mem --profile Win7SP1x64 iehistory

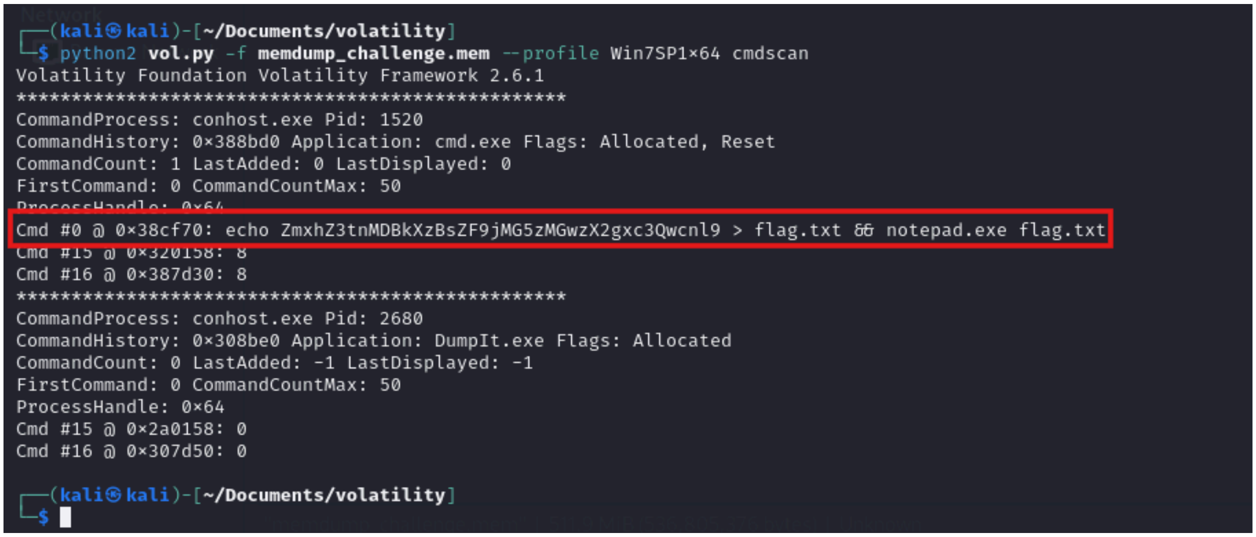


```
Process: 1164 iexplore.exe
Cache type "URL " at 0xd35f00
Record length: 0x100
Location: Visited: w@res://ieframe.dll/tabswelcome.htm
Last modified: 2023-04-02 14:36:02 UTC+0000
Last accessed: 2023-04-02 14:36:02 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0x98
**************************************************
Process: 1164 iexplore.exe
Cache type "URL " at 0xd36000
Record length: 0x100
Location: Visited: w@http://example.com/?flag=flag{1nt3rn3t_3xpl0r3r_h1st0ry_1n_m3m0ry_dump}
Last modified: 2023-04-02 14:22:36 UTC+0000
Last accessed: 2023-04-02 14:22:36 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xbc
**************************************************
Process: 1164 iexplore.exe
```

Flag{1nt3rn3t_3xpl0r3r_h1st0ry_1n_m3m0ry_dump}

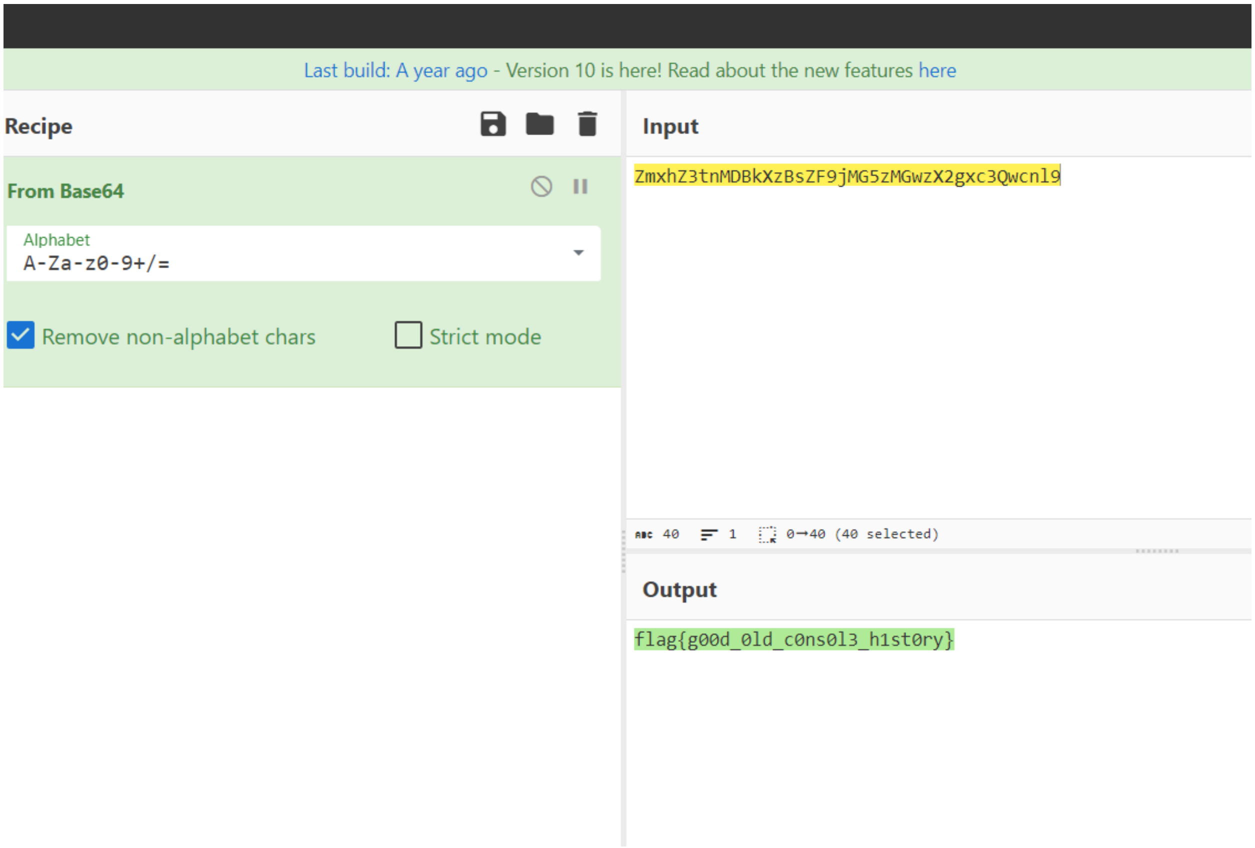
Flag 3: For this flag i saw the command history of cmd, and found the flag in base 64, so i decrypt it using cyberchef.

python2 vol.py -f memdump_challenge.mem --profile Win7SP1x64 cmdscan



```
┌──(kali㉿kali)-[~/Documents/volatility]
└─$ python2 vol.py -f memdump_challenge.mem --profile Win7SP1x64 cmdscan
Volatility Foundation Volatility Framework 2.6.1
**************************************************
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

┌──(kali㉿kali)-[~/Documents/volatility]
└─$ 
```


Last build: A year ago - Version 10 is here! Read about the new features here
Recipe
Input
Output

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

```
ZmxhZ3tnMDBkXzBsZF9jMG5zMGwzX2gxc3Qwcnl9
```

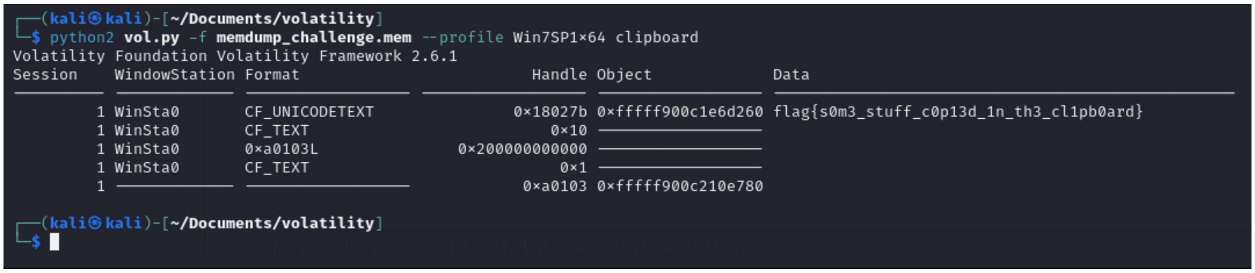
```
abc 40   1   0→40 (40 selected)
```

```
flag{g00d_0ld_c0ns0l3_h1st0ry}
```

Flag{g00d_0ld_c0ns0l3_h1st0ry}

Flag 4: For this i saw the clipboard , and found the flag there.

python2 vol.py -f memdump_challenge.mem --profile Win7SP1x64 clipboard

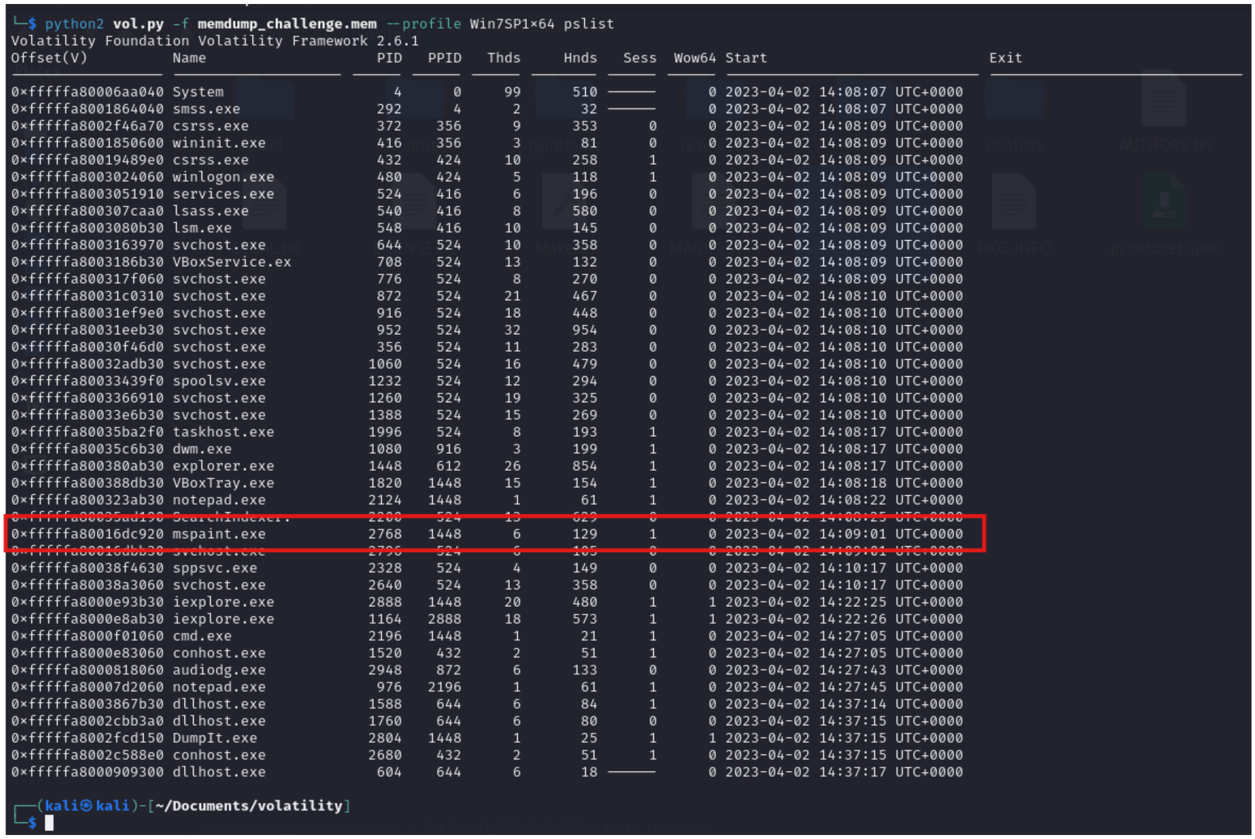


```
┌──(kali㉿kali)-[~/Documents/volatility]
└─$ python2 vol.py -f memdump_challenge.mem --profile Win7SP1x64 clipboard
Volatility Foundation Volatility Framework 2.6.1
Session    WindowStation Format                           Handle Object             Data
────────── ───────────── ────────────────── ──────────────────── ────────────────── ──────────────────────────────────────────────────
         1 WinSta0       CF_UNICODETEXT                 0x18027b 0xfffff900c1e6d260 flag{s0m3_stuff_c0p13d_1n_th3_cl1pb0ard}
         1 WinSta0       CF_TEXT                            0x10 ──────────────────
         1 WinSta0       0xa0103L                 0x200000000000 ──────────────────
         1 WinSta0       CF_TEXT                             0x1 ──────────────────
         1 ───────────── ──────────────────              0xa0103 0xfffff900c210e780

┌──(kali㉿kali)-[~/Documents/volatility]
└─$ █
```

Flag{s0m3_stuff_c0p13d_1n_th3_cl1pb0ard}

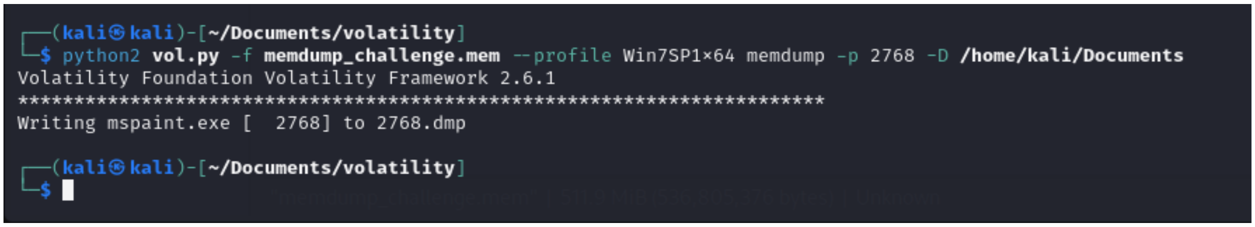
Flag 5 : For ths mspaint, first i saw the pid of it, then i ran the command.



```
└─$ python2 vol.py -f memdump_challenge.mem --profile Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa80006aa040 System                    4      0     99      510 ------      0 2023-04-02 14:08:07 UTC+0000
0xfffffa8001864040 smss.exe                292      4      2       32 ------      0 2023-04-02 14:08:07 UTC+0000
0xfffffa8002f46a70 csrss.exe               372    356      9      353      0      0 2023-04-02 14:08:09 UTC+0000
0xfffffa8001850600 wininit.exe             416    356      3       81      0      0 2023-04-02 14:08:09 UTC+0000
0xfffffa80019489e0 csrss.exe               432    424     10      258      1      0 2023-04-02 14:08:09 UTC+0000
0xfffffa8003024060 winlogon.exe            480    424      5      118      1      0 2023-04-02 14:08:09 UTC+0000
0xfffffa8003051910 services.exe            524    416      6      196      0      0 2023-04-02 14:08:09 UTC+0000
0xfffffa800307caa0 lsass.exe               540    416      8      580      0      0 2023-04-02 14:08:09 UTC+0000
0xfffffa8003080b30 lsm.exe                 548    416     10      145      0      0 2023-04-02 14:08:09 UTC+0000
0xfffffa8003163970 svchost.exe             644    524     10      358      0      0 2023-04-02 14:08:09 UTC+0000
0xfffffa8003186b30 VBoxService.ex          708    524     13      132      0      0 2023-04-02 14:08:09 UTC+0000
0xfffffa800317f060 svchost.exe             776    524      8      270      0      0 2023-04-02 14:08:09 UTC+0000
0xfffffa80031c0310 svchost.exe             872    524     21      467      0      0 2023-04-02 14:08:10 UTC+0000
0xfffffa80031ef9e0 svchost.exe             916    524     18      448      0      0 2023-04-02 14:08:10 UTC+0000
0xfffffa80031eeb30 svchost.exe             952    524     32      954      0      0 2023-04-02 14:08:10 UTC+0000
0xfffffa80030f46d0 svchost.exe             356    524     11      283      0      0 2023-04-02 14:08:10 UTC+0000
0xfffffa80032adb30 svchost.exe            1060    524     16      479      0      0 2023-04-02 14:08:10 UTC+0000
0xfffffa80033439f0 spoolsv.exe            1232    524     12      294      0      0 2023-04-02 14:08:10 UTC+0000
0xfffffa8003366910 svchost.exe            1260    524     19      325      0      0 2023-04-02 14:08:10 UTC+0000
0xfffffa80033e6b30 svchost.exe            1388    524     15      269      0      0 2023-04-02 14:08:10 UTC+0000
0xfffffa80035ba2f0 taskhost.exe           1996    524      8      193      1      0 2023-04-02 14:08:17 UTC+0000
0xfffffa80035c6b30 dwm.exe                1080    916      3      199      1      0 2023-04-02 14:08:17 UTC+0000
0xfffffa800380ab30 explorer.exe           1448    612     26      854      1      0 2023-04-02 14:08:17 UTC+0000
0xfffffa800388db30 VBoxTray.exe           1820   1448     15      154      1      0 2023-04-02 14:08:18 UTC+0000
0xfffffa800323ab30 notepad.exe            2124   1448      1       61      1      0 2023-04-02 14:08:22 UTC+0000
0xfffffa80035ad190 SearchIndexer.         2200    524     13      629      0      0 2023-04-02 14:08:25 UTC+0000
0xfffffa80016dc920 mspaint.exe            2768   1448      6      129      1      0 2023-04-02 14:09:01 UTC+0000
0xfffffa80016dbb30 svchost.exe            2796    524      6      105      0      0 2023-04-02 14:09:01 UTC+0000
0xfffffa80038f4630 sppsvc.exe             2328    524      4      149      0      0 2023-04-02 14:10:17 UTC+0000
0xfffffa80038a3060 svchost.exe            2640    524     13      358      0      0 2023-04-02 14:10:17 UTC+0000
0xfffffa8000e93b30 iexplore.exe           2888   1448     20      480      1      1 2023-04-02 14:22:25 UTC+0000
0xfffffa8000e8ab30 iexplore.exe           1164   2888     18      573      1      1 2023-04-02 14:22:26 UTC+0000
0xfffffa8000f01060 cmd.exe                2196   1448      1       21      1      0 2023-04-02 14:27:05 UTC+0000
0xfffffa8000e83060 conhost.exe            1520    432      2       51      1      0 2023-04-02 14:27:05 UTC+0000
0xfffffa8000818060 audiodg.exe            2948    872      6      133      0      0 2023-04-02 14:27:43 UTC+0000
0xfffffa80007d2060 notepad.exe             976   2196      1       61      1      0 2023-04-02 14:27:45 UTC+0000
0xfffffa8003867b30 dllhost.exe            1588    644      6       84      1      0 2023-04-02 14:37:14 UTC+0000
0xfffffa8002cbb3a0 dllhost.exe            1760    644      6       80      0      0 2023-04-02 14:37:15 UTC+0000
0xfffffa8002fcd150 DumpIt.exe             2804   1448      1       25      1      1 2023-04-02 14:37:15 UTC+0000
0xfffffa8002c588e0 conhost.exe            2680    432      2       51      1      0 2023-04-02 14:37:15 UTC+0000
0xfffffa8000909300 dllhost.exe             604    644      6       18 ------      0 2023-04-02 14:37:17 UTC+0000

┌──(kali㉿kali)-[~/Documents/volatility]
└─$ 
```

And outputed the memory dump of that specific process.



```
┌──(kali㉿kali)-[~/Documents/volatility]
└─$ python2 vol.py -f memdump_challenge.mem --profile Win7SP1x64 memdump -p 2768 -D /home/kali/Documents
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
Writing mspaint.exe [  2768] to 2768.dmp

┌──(kali㉿kali)-[~/Documents/volatility]
└─$ 
```

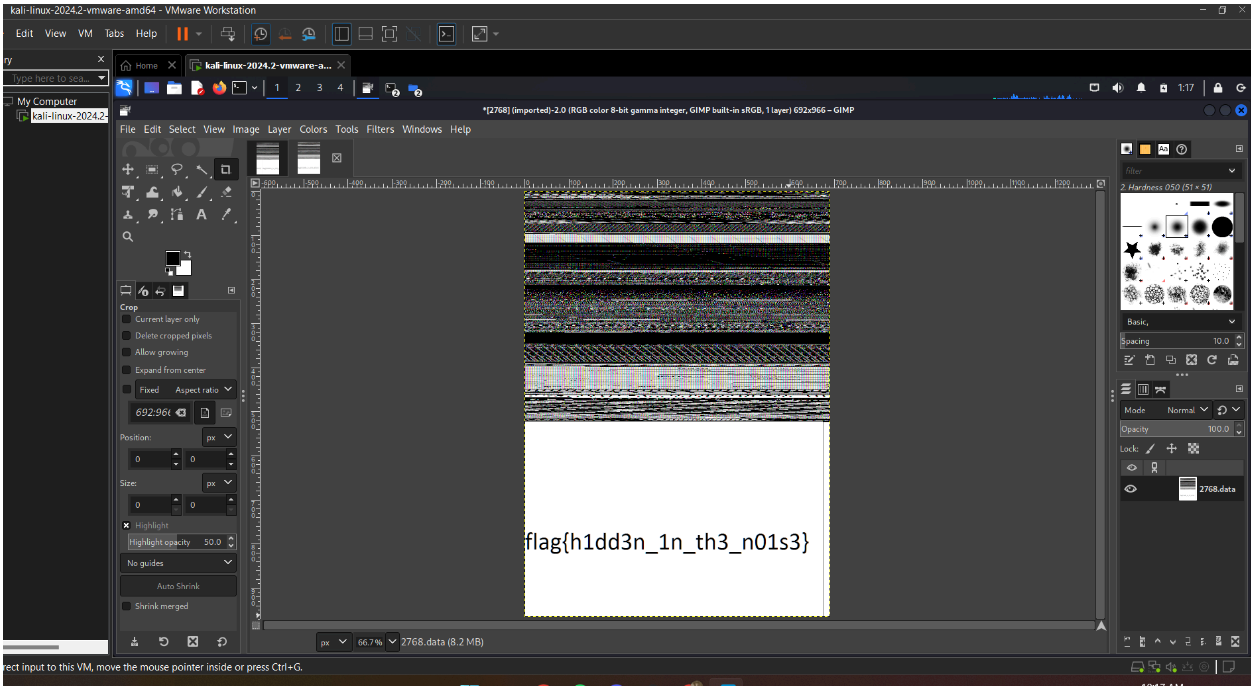
Then after that, I changed the .dmp to .data , so I could open the file in GIMP.

So as I opened the file in GIMP, I put the offset, width and height, and flipped the image vertically. There was the flag.

Offset : 3776058

Width : 692

Height : 966


Edit View VM Tabs Help
Home
kali-linux-2024.2-vmware-a...
My Computer
kali-linux-2024.2-
1 2 3 4
1:17
File Edit Select View Image Layer Colors Tools Filters Windows Help
Auto Shrink
Basic,
2768.data

kali-linux-2024.2-vmware-amd64 - VMware Workstation

*[2768] (imported)-2.0 (RGB color 8-bit gamma integer, GIMP built-in sRGB, 1 layer) 692x966 – GIMP

Crop
- ☐ Current layer only
- ☐ Delete cropped pixels
- ☐ Allow growing
- ☐ Expand from center
- ☐ Fixed Aspect ratio
- 692:966
- Position: px 0 0
- Size: px 0 0
- ☒ Highlight
- Highlight opacity 50.0
- No guides
- ☐ Shrink merged

2. Hardness 050 (51 × 51)

Spacing 10.0

Mode Normal

Opacity 100.0

flag{h1dd3n_1n_th3_n01s3}

px 66.7 % 2768.data (8.2 MB)

rect input to this VM, move the mouse pointer inside or press Ctrl+G.

flag{h1dd3n_1n_th3_n01s3}