DIGITAL FORENSICS 2

MEMORY

BY ROBBIN OOI

$WHOAMI



@WARLOCKSMURF

- Cybersecurity analyst @ MoneyLion
- BSc (Hons) IT graduate from Sunway University
- CTF player for L3ak and M53 focusing on forensics, OSINT and blockchain
- Participated in several local CTFs last time (im old...)
- Challenge creator for SunCTF and GCTF

WHAT IS MEMORY?

Memory is where data and information stored in a system and retrieved when needed.

Non-Volatile Memory: This type of memory retains data even after the power is turned off.

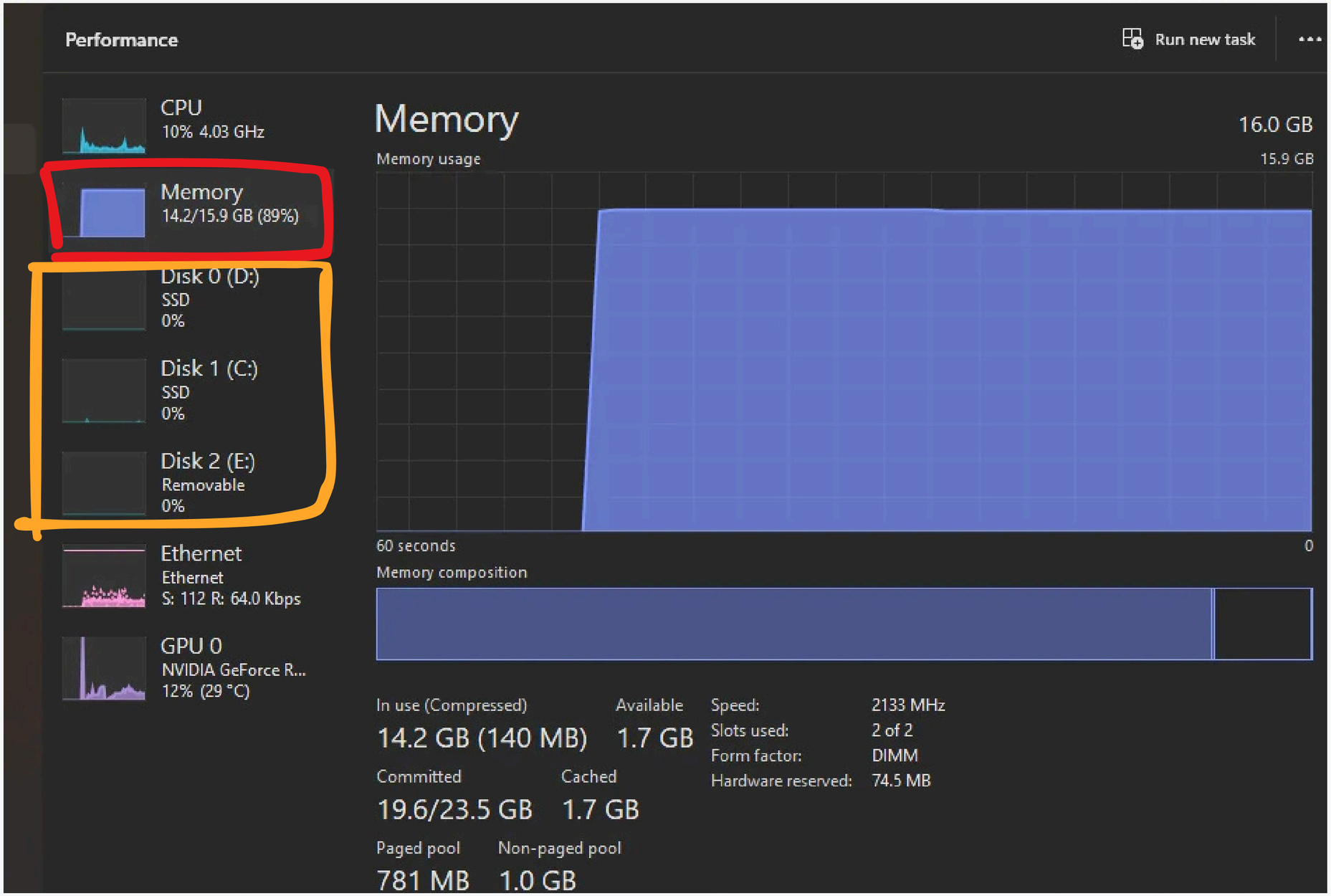
Volatile Memory: This temporary memory is usually stored to be processed by CPU and loses data when the power is turned off.



MEMORY != DISK STORAGE

Although both the hard drive and RAM are memory, people will usually refer to RAM as "memory" and a hard drive as "storage"




Performance
Run new task
CPU
10% 4.03 GHz
Memory
14.2/15.9 GB (89%)
Disk 0 (D:)
SSD
0%
Disk 1 (C:)
SSD
0%
Disk 2 (E:)
Removable
0%
Ethernet
Ethernet
S: 112 R: 64.0 Kbps
GPU 0
NVIDIA GeForce R...
12% (29 °C)
Memory
16.0 GB
Memory usage
15.9 GB
60 seconds
0
Memory composition
In use (Compressed)
14.2 GB (140 MB)
Available
1.7 GB
Committed
19.6/23.5 GB
Cached
1.7 GB
Paged pool
781 MB
Non-paged pool
1.0 GB
Speed:
2133 MHz
Slots used:
2 of 2
Form factor:
DIMM
Hardware reserved:
74.5 MB

MEMORY FORENSICS

- One of the most essential aspect in digital forensics.
- The process of acquiring, preserving, and analyzing volatile data stored in a computer’s RAM.
- Can be done on any OS (Windows, Linux, macOS)

VOLATILE IN NATURE

- Volatile data is **transient** and will be flushed if the system loses power/restarted.

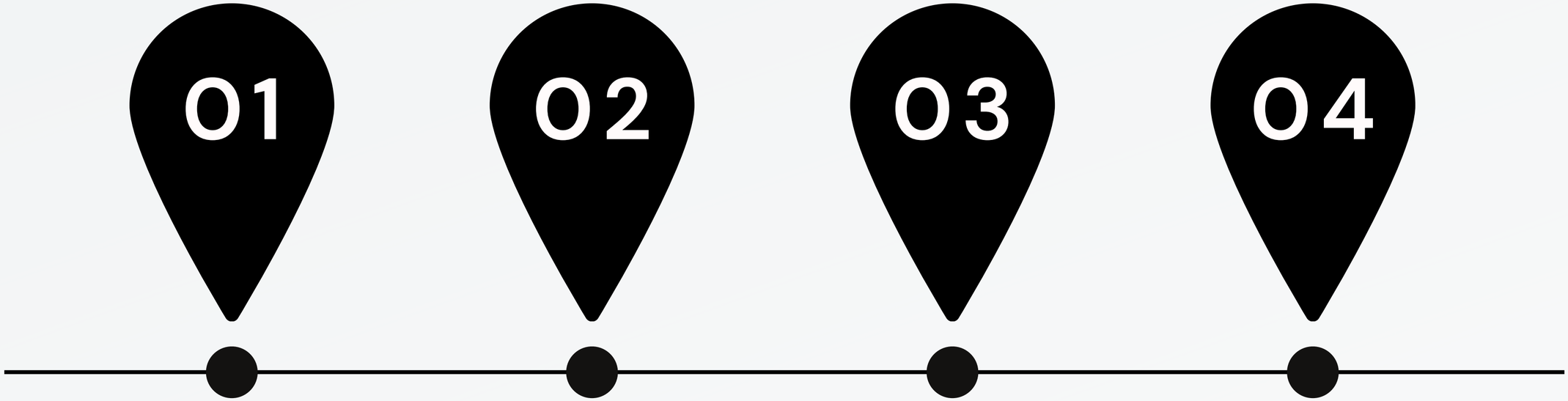
- Time is critical in memory forensics, the longer the delay in acquiring memory, the higher the chances of losing valuable evidence



WHY?

- Uncover evidence of malware infections and other malicious attacks that leave footprints in a system and better understand an attacker’s TTPs.
- Identify fileless malware, rootkits, code injections etc.
- In CTFs, just a challenge of identifying the flag




01
02
03
04
RUNNING PROCESSES
NETWORK CONNECTIONS
SYSTEM OS INFORMATION
COMMAND HISTORY

05

REGISTRY KEYS

06

MEMORY MAPPED FILES

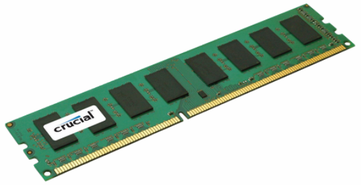
07

CACHE (URLS, PASSWORDS, CLIPBOARD)

08

INJECTED CODE/DLLS

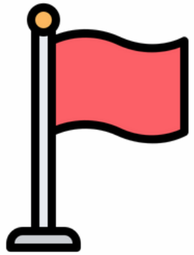
OVERVIEW



ACQUISITION



ANALYSIS



CONCLUSION

ACQUISITION

- The first step in memory forensics is to create a memory dump of the target system.
- A memory dump is a snapshot of the system’s RAM at a specific point in time.
- Tools: FTK Imager, Winpmem, Belkasoft, LiME (Linux)

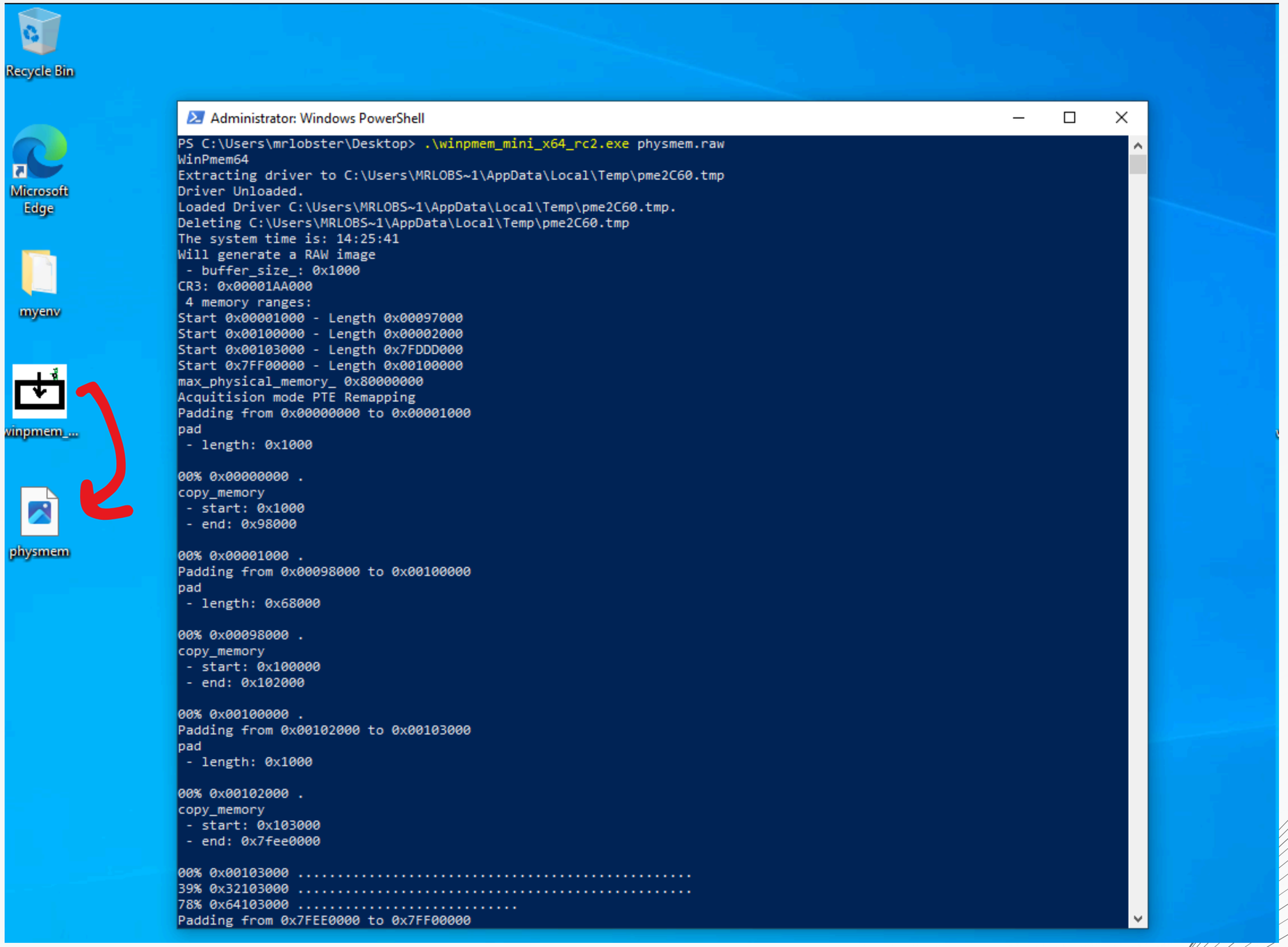
MEMORY DUMP

RAW DUMP
.RAW .MEM .BIN .VMEM

WINDOWS CRASH DUMP
.DMP

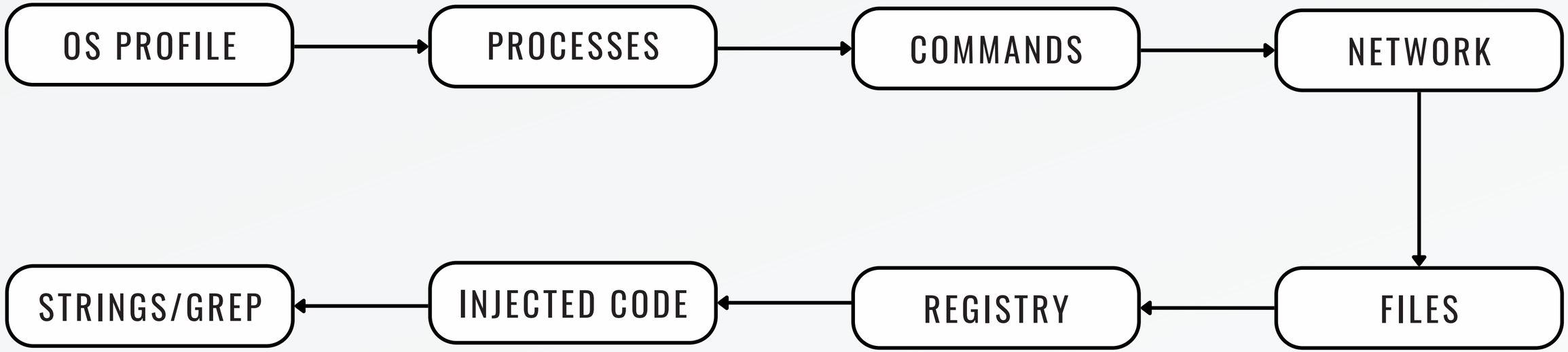
WINDOWS HIBERNATION FILE
HIBERFIL.SYS

PAGE AND SWAP FILES
PAGEFILE.SYS SWAPFILE.SYS


Recycle Bin
Microsoft Edge
myenv
winpmem_...
physmem
Administrator: Windows PowerShell
PS C:\Users\mrlobster\Desktop> .\winpmem_mini_x64_rc2.exe physmem.raw
WinPmem64
Extracting driver to C:\Users\MRLOBS~1\AppData\Local\Temp\pme2C60.tmp
Driver Unloaded.
Loaded Driver C:\Users\MRLOBS~1\AppData\Local\Temp\pme2C60.tmp.
Deleting C:\Users\MRLOBS~1\AppData\Local\Temp\pme2C60.tmp
The system time is: 14:25:41
Will generate a RAW image
- buffer_size_: 0x1000
CR3: 0x00001AA000
4 memory ranges:
Start 0x00001000 - Length 0x00097000
Start 0x00100000 - Length 0x00002000
Start 0x00103000 - Length 0x7FDDD000
Start 0x7FF00000 - Length 0x00100000
max_physical_memory_ 0x80000000
Acquitision mode PTE Remapping
Padding from 0x00000000 to 0x00001000
pad
- length: 0x1000
00% 0x00000000 .
copy_memory
- start: 0x1000
- end: 0x98000
00% 0x00001000 .
Padding from 0x00098000 to 0x00100000
pad
- length: 0x68000
00% 0x00098000 .
copy_memory
- start: 0x100000
- end: 0x102000
00% 0x00100000 .
Padding from 0x00102000 to 0x00103000
pad
- length: 0x1000
00% 0x00102000 .
copy_memory
- start: 0x103000
- end: 0x7fee0000
00% 0x00103000 .....
39% 0x32103000 .....
78% 0x64103000 .....
Padding from 0x7FEE0000 to 0x7FF00000

ANALYSIS

- Once memory is acquired and preserved, the analysis begins.
- Tools: Volatility2/3, MemProcFS, bulkextractor
- But...how should I start my search?


OS PROFILE
PROCESSES
COMMANDS
NETWORK
FILES
REGISTRY
INJECTED CODE
STRINGS/GREP

OS PROFILE

- Vol2 (imageinfo, kdbgscan), Vol3 (windows.info)

```
┌──(kali㉿kali)-[~/Desktop/volatility3]
└─$ python3 vol.py -f ~/Desktop/memdump/memdump.raw windows.info
Volatility 3 Framework 2.10.0
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0×f80066a00000
DTB     0×1aa000
Symbols file:///home/kali/Desktop/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/D9424FC4861E47C10FAD1B35DEC6DCC8-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0×f8006760f400
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      2
SystemTime      2024-09-10 13:58:14+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Mon Dec  9 11:07:51 2019
```

PROCESSES

- Vol2 (pslist), Vol3 (pslist, psscan, pstree)

```
┌──(kali㉿kali)-[~/Desktop/volatility3]
└─$ python3 vol.py -f ~/Desktop/memdump/memdump.raw windows.pslist
Volatility 3 Framework 2.10.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0×868b7ce85200  136     -       N/A     False   2024-09-10 13:56:19.000000 UTC  N/A     Disabled
92      4       Registry        0×868b7cef1080  4       -       N/A     False   2024-09-10 13:56:14.000000 UTC  N/A     Disabled
308     4       smss.exe        0×868b7df9f040  3       -       N/A     False   2024-09-10 13:56:19.000000 UTC  N/A     Disabled
424     416     csrss.exe       0×868b804d7140  12      -       0       False   2024-09-10 13:56:19.000000 UTC  N/A     Disabled
500     416     wininit.exe     0×868b80cfd080  5       -       0       False   2024-09-10 13:56:19.000000 UTC  N/A     Disabled
520     492     csrss.exe       0×868b80ea8080  14      -       1       False   2024-09-10 13:56:19.000000 UTC  N/A     Disabled
596     492     winlogon.exe    0×868b80f09080  6       -       1       False   2024-09-10 13:56:19.000000 UTC  N/A     Disabled
616     500     services.exe    0×868b80f0e080  12      -       0       False   2024-09-10 13:56:19.000000 UTC  N/A     Disabled
660     500     lsass.exe       0×868b80f2a080  12      -       0       False   2024-09-10 13:56:19.000000 UTC  N/A     Disabled
768     500     fontdrvhost.ex  0×868b80fa1140  5       -       0       False   2024-09-10 13:56:20.000000 UTC  N/A     Disabled
764     596     fontdrvhost.ex  0×868b80fa3140  5       -       1       False   2024-09-10 13:56:20.000000 UTC  N/A     Disabled
780     616     svchost.exe     0×868b80fa7240  26      -       0       False   2024-09-10 13:56:20.000000 UTC  N/A     Disabled
888     616     svchost.exe     0×868b80d382c0  19      -       0       False   2024-09-10 13:56:20.000000 UTC  N/A     Disabled
936     616     svchost.exe     0×868b80d67240  6       -       0       False   2024-09-10 13:56:20.000000 UTC  N/A     Disabled
1008    596     dwm.exe 0×868b80daf080  19      -       1       False   2024-09-10 13:56:20.000000 UTC  N/A     Disabled
496     616     svchost.exe     0×868b80de8240  6       -       0       False   2024-09-10 13:56:20.000000 UTC  N/A     Disabled
572     616     svchost.exe     0×868b8010e300  5       -       0       False   2024-09-10 13:56:20.000000 UTC  N/A     Disabled
996     616     svchost.exe     0×868b816782c0  4       -       0       False   2024-09-10 13:56:20.000000 UTC  N/A     Disabled
1068    616     svchost.exe     0×868b816af280  5       -       0       False   2024-09-10 13:56:20.000000 UTC  N/A     Disabled
```

- Vol2 (memdump), Vol3 (memmap)

```
┌──(kali㉿kali)-[~/Desktop/volatility3]
└─$ python3 vol.py -f ~/Desktop/memdump/memdump.raw -o ~/Desktop windows.memmap --dump --pid 1008
Volatility 3 Framework 2.10.0
Progress:  100.00               PDB scanning finished
Virtual Physical        Size    Offset in File  File output

0×7ffe0000      0×5128000       0×1000  0×0     pid.1008.dmp
0×7ffea000      0×d000  0×1000  0×1000  pid.1008.dmp
0×ee8ef0c000    0×1142db000     0×1000  0×2000  pid.1008.dmp
0×ee8ef0d000    0×118d12000     0×1000  0×3000  pid.1008.dmp
0×ee8ef0e000    0×118c13000     0×1000  0×4000  pid.1008.dmp
0×ee8ef0f000    0×116003000     0×1000  0×5000  pid.1008.dmp
0×ee8efa8000    0×11e1a5000     0×1000  0×6000  pid.1008.dmp
0×ee8efa9000    0×11e17a000     0×1000  0×7000  pid.1008.dmp
0×ee8efaa000    0×10ba33000     0×1000  0×8000  pid.1008.dmp
0×ee8efab000    0×11a2c6000     0×1000  0×9000  pid.1008.dmp
0×ee8efac000    0×11e270000     0×1000  0×a000  pid.1008.dmp
0×ee8efad000    0×11f39a000     0×1000  0×b000  pid.1008.dmp
0×ee8efae000    0×11f240000     0×1000  0×c000  pid.1008.dmp
0×ee8efaf000    0×118f3f000     0×1000  0×d000  pid.1008.dmp
0×ee8f1a6000    0×115cf4000     0×1000  0×e000  pid.1008.dmp
0×ee8f1a7000    0×115cff000     0×1000  0×f000  pid.1008.dmp
0×ee8f1a8000    0×115c00000     0×1000  0×10000 pid.1008.dmp
0×ee8f1af000    0×118f3d000     0×2000  0×11000 pid.1008.dmp
0×ee8f1b3000    0×1133cc000     0×1000  0×13000 pid.1008.dmp
0×ee8f1b4000    0×115dcd000     0×1000  0×14000 pid.1008.dmp
0×ee8f1b5000    0×119809000     0×1000  0×15000 pid.1008.dmp
```

COMMAND HISTORY

- Vol2 (cmdline, consoles), Vol3 (cmdline)
- **cmdline** = Extract command line arguments that were passed to a executed process when it was launched.
- **consoles** = Extract commands typed into CMD or executed by program

```
┌──(kali㉿kali)-[~/Desktop/volatility3]
└─$ python3 vol.py -f ~/Desktop/memdump/memdump.raw windows.cmdline
Volatility 3 Framework 2.10.0
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  Required memory at 0x20 is not valid (process exited?)
92      Registry        Required memory at 0x20 is not valid (process exited?)
308     smss.exe        \SystemRoot\System32\smss.exe
424     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,204
rv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThr
500     wininit.exe     wininit.exe
520     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,204
rv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThr
596     winlogon.exe    winlogon.exe
616     services.exe    C:\Windows\system32\services.exe
660     lsass.exe       C:\Windows\system32\lsass.exe
768     fontdrvhost.ex  "fontdrvhost.exe"
764     fontdrvhost.ex  "fontdrvhost.exe"
780     svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch -p
888     svchost.exe     C:\Windows\system32\svchost.exe -k RPCSS -p
936     svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
1008    dwm.exe "dwm.exe"
496     svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
572     svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
```

```
night-wolf@ubuntu:~/MemLabs$ volatility -f MemoryDump_Lab1.raw --profile Win7SP1x64 consoles
Volatility Foundation Volatility Framework 2.6.1
**************************************************
ConsoleProcess: conhost.exe Pid: 2692
Console: 0xff756200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe - St4G3$1
AttachedProcess: cmd.exe Pid: 1984 Handle: 0x60
----
CommandHistory: 0x1fe9c0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 at 0x1de3c0: St4G3$1
----
Screen 0x1e0f70 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\SmartNet>St4G3$1
ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=
Press any key to continue . . .
**************************************************
```

NETWORK CONNECTIONS

- Vol2 (netscan, netstat), Vol3 (netscan, netstat)

```
┌──(kali㉿kali)-[~/Desktop/volatility3]
└─$ python3 vol.py -f ~/Desktop/memdump/memdump.raw windows.netscan
Volatility 3 Framework 2.10.0
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0×868b7ce8a5d0  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2280    spoolsv.exe     2024-09-10 13:56:21.000000 UTC
0×868b7ce8a5d0  TCPv6   ::      49668   ::      0       LISTENING       2280    spoolsv.exe     2024-09-10 13:56:21.000000 UTC
0×868b7ce8ab50  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2280    spoolsv.exe     2024-09-10 13:56:21.000000 UTC
0×868b7d4f2230  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       500     wininit.exe     2024-09-10 13:56:20.000000 UTC
0×868b7d4f2230  TCPv6   ::      49665   ::      0       LISTENING       500     wininit.exe     2024-09-10 13:56:20.000000 UTC
0×868b80372050  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1168    svchost.exe     2024-09-10 13:56:20.000000 UTC
0×868b803721b0  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1168    svchost.exe     2024-09-10 13:56:20.000000 UTC
0×868b803721b0  TCPv6   ::      49667   ::      0       LISTENING       1168    svchost.exe     2024-09-10 13:56:20.000000 UTC
0×868b803725d0  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       500     wininit.exe     2024-09-10 13:56:20.000000 UTC
0×868b80372890  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1152    svchost.exe     2024-09-10 13:56:20.000000 UTC
0×868b80372890  TCPv6   ::      49666   ::      0       LISTENING       1152    svchost.exe     2024-09-10 13:56:20.000000 UTC
0×868b803729f0  TCPv4   192.168.111.136 139     0.0.0.0 0       LISTENING       4       System  2024-09-10 13:56:20.000000 UTC
0×868b80373650  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       660     lsass.exe       2024-09-10 13:56:20.000000 UTC
0×868b80373910  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       660     lsass.exe       2024-09-10 13:56:20.000000 UTC
0×868b80373910  TCPv6   ::      49664   ::      0       LISTENING       660     lsass.exe       2024-09-10 13:56:20.000000 UTC
0×868b80373a70  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       888     svchost.exe     2024-09-10 13:56:20.000000 UTC
0×868b80373bd0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       888     svchost.exe     2024-09-10 13:56:20.000000 UTC
0×868b80373bd0  TCPv6   ::      135     ::      0       LISTENING       888     svchost.exe     2024-09-10 13:56:20.000000 UTC
0×868b80373e90  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1152    svchost.exe     2024-09-10 13:56:20.000000 UTC
0×868b80d61010  TCPv4   192.168.111.136 49674   20.198.119.143  443     ESTABLISHED     3216    svchost.exe     2024-09-10 13:56:25.000000 UTC
0×868b80e97960  UDPv4   0.0.0.0 0       *       0               1520    svchost.exe     2024-09-10 13:56:21.000000 UTC
0×868b80e97960  UDPv6   ::      0       *       0               1520    svchost.exe     2024-09-10 13:56:21.000000 UTC
0×868b816058a0  TCPv4   192.168.111.136 49719   146.75.26.172   80      ESTABLISHED     7944    svchost.exe     2024-09-10 13:57:41.000000 UTC
0×868b816d84d0  TCPv4   192.168.111.136 49718   204.79.197.239  443     ESTABLISHED     6248    msedge.exe      2024-09-10 13:57:41.000000 UTC
0×868b817d2440  UDPv6   fe80::cdf9:234:1133:e5eb        546     *       0               1396    svchost.exe     2024-09-10 13:56:20.000000 UTC
0×868b817d4510  UDPv4   192.168.111.136 137     *       0               4       System  2024-09-10 13:56:20.000000 UTC
```

FILES

- Vol2 (filescan), Vol3 (filescan)

```
┌──(kali㉿kali)-[~/Desktop/volatility3]
└─$ python3 vol.py -f ~/Desktop/memdump/memdump.raw windows.filescan
Volatility 3 Framework 2.10.0
Progress:  100.00               PDB scanning finished
Offset  Name

0×868b7cea93e0  \$Directory
0×868b7ceb2ab0  \Windows\System32\drivers\storqosflt.sys
0×868b7d4cf0b0  \Windows\System32\drivers\dxgkrnl.sys
0×868b7d4cf500  \Windows\System32\DriverStore\FileRepository\basicdisplay.inf_amd64_19e58b6267591a82\BasicDisplay.sys
0×868b7d4cf7e0  \Windows\System32\drivers\beep.sys
0×868b7d4cfc30  \Windows\System32\drivers\UCPD.sys
0×868b7d4cfda0  \$Directory
0×868b7d4d0080  \$Directory
0×868b7d4d07b0  \Windows\System32\DriverStore\FileRepository\basicrender.inf_amd64_d3f5994a67770b50\BasicRender.sys
0×868b7d4d0a90  \Windows\System32\drivers\null.sys
0×868b7d4d0d70  \Windows\System32\drivers\watchdog.sys
0×868b7d4d11c0  \Windows\System32\drivers\vmrawdsk.sys
0×868b7d4d1330  \Windows\System32\drivers\tbs.sys
0×868b7d4d1eb0  $
0×868b7d4d2190  \Windows\System32\drivers\npfs.sys
0×868b7d4d2a30  \Windows\System32\drivers\tdx.sys
0×868b7d4d2ba0  \Windows\System32\drivers\cimfs.sys
0×868b7d4d2d10  \Windows\System32\drivers\msfs.sys
0×868b7d4e40c0  \Windows\System32\shell32.dll
0×868b7d4e4700  \Windows\System32\shlwapi.dll
0×868b7d4e4bb0  \Windows\System32\advapi32.dll
0×868b7d4e4ed0  \ProtectedPrefix
0×868b7d4e56a0  \Windows
0×868b7d4e5b50  \ProtectedPrefix\Administrators
0×868b7d4e5e70  \Windows\System32\oleaut32.dll
0×868b7d4f6390  \Windows\System32\drivers\netbt.sys
```

- Vol2 (dumpfiles), Vol3 (dumpfiles)

```
┌──(kali㉿kali)-[~/Desktop/volatility3]
└─$ python3 vol.py -f ~/Desktop/memdump/memdump.raw windows.filescan | grep -iE History
0×868b81b78510.0\Users\warlocksmurf\AppData\Local\Microsoft\Edge\User Data\Default\History-journal
0×868b81e6b160  \ProgramData\Microsoft\Windows Defender\Scans\History\CacheManager\14899E5E-0000-0000-0000-300300000000-0.bin
0×868b8308ec20  \Users\warlocksmurf\AppData\Local\Microsoft\Edge\User Data\Default\History
0×868b83467760  \Users\warlocksmurf\AppData\Local\Microsoft\Edge\User Data\Default\History-journal
0×868b8346c8a0  \Users\warlocksmurf\AppData\Local\Microsoft\Edge\User Data\Nurturing\campaign_history
0×868b8346f2d0  \Users\warlocksmurf\AppData\Local\Microsoft\Edge\User Data\Default\Nurturing\campaign_history
0×868b83497690  \Users\warlocksmurf\AppData\Local\Microsoft\Windows\History\desktop.ini
0×868b83b29c40  \ProgramData\Microsoft\Windows Defender\Scans\History\Store\EE96F36B015E7A95F496D63213BBBA5D
0×868b8465de80  \ProgramData\Microsoft\Windows Defender\Scans\History\Results\Resource\{E5512053-DA77-4D21-B893-0099ACEE1B7B}

┌──(kali㉿kali)-[~/Desktop/volatility3]
└─$ python3 vol.py -f ~/Desktop/memdump/memdump.raw -o ~/Desktop windows.dumpfiles --virtaddr 0×868b8308ec20
Volatility 3 Framework 2.10.0
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0×868b8308ec20  History file.0×868b8308ec20.0×868b8329b770.DataSectionObject.History.dat
SharedCacheMap  0×868b8308ec20  History file.0×868b8308ec20.0×868b82d868a0.SharedCacheMap.History.vacb
```

REGISTRY KEY

- Vol2 (hivelist, hivedump), Vol3 (registry.hivelist)

```
┌──(kali㉿kali)-[~/Desktop/volatility3]
└─$ python3 vol.py -f ~/Desktop/memdump/memdump.raw windows.registry.hivelist
Volatility 3 Framework 2.10.0
Progress:  100.00               PDB scanning finished
Offset  FileFullPath    File output

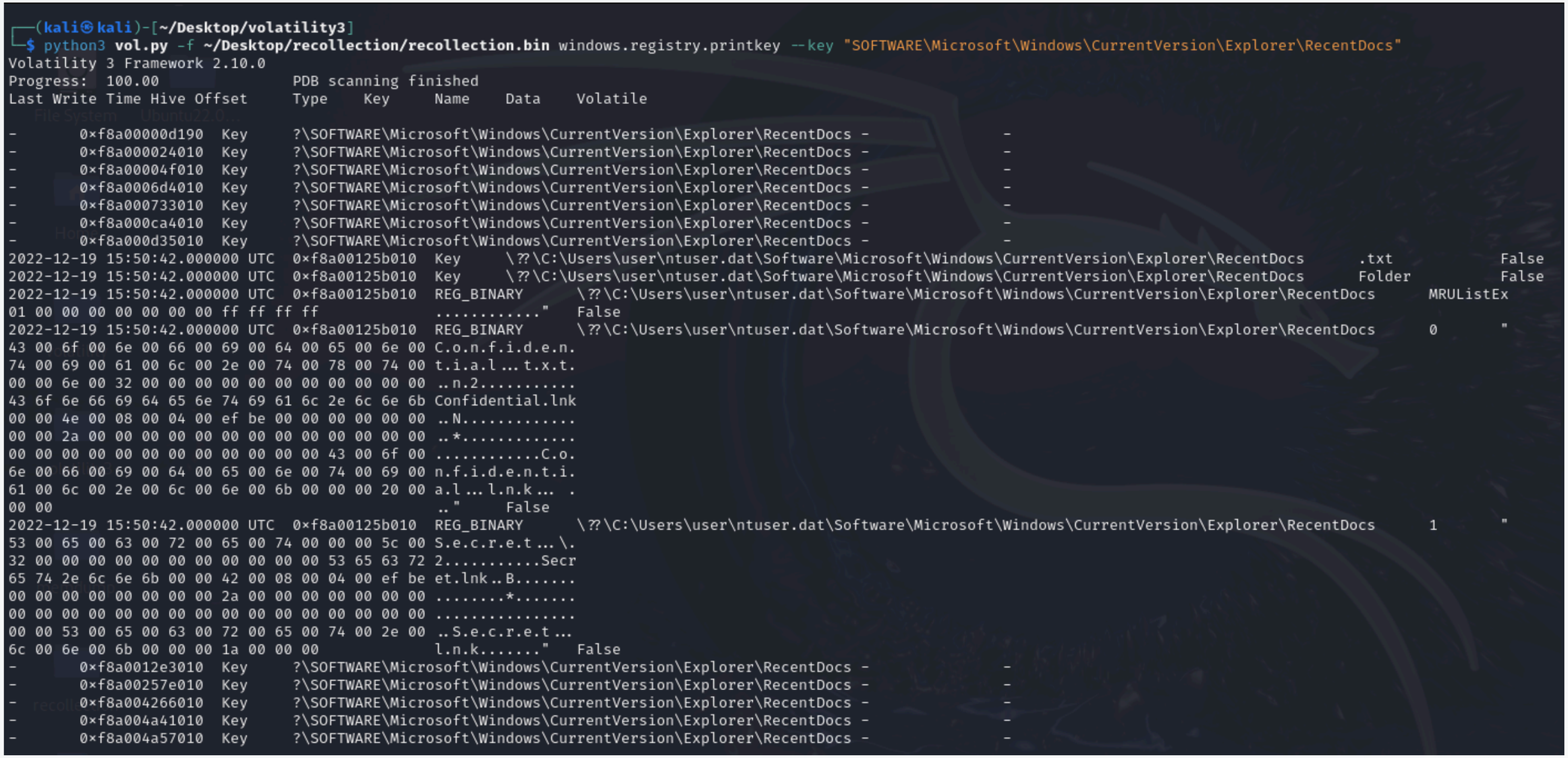
0×a0843cc52000          Disabled
0×a0843cc73000  \REGISTRY\MACHINE\SYSTEM        Disabled
0×a0843ccf0000  \REGISTRY\MACHINE\HARDWARE      Disabled
0×a0843e810000  \Device\HarddiskVolume1\Boot\BCD        Disabled
0×a0843e804000  \SystemRoot\System32\Config\SOFTWARE    Disabled
0×a0843e361000  \SystemRoot\System32\Config\DEFAULT     Disabled
0×a084404c8000  \SystemRoot\System32\Config\SECURITY    Disabled
0×a08440528000  \SystemRoot\System32\Config\SAM Disabled
0×a084406c6000  \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT        Disabled
0×a0844080e000  \SystemRoot\System32\Config\BBI Disabled
0×a0844085e000  \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  Disabled
0×a08440dc4000  \??\C:\Users\warlocksmurf\ntuser.dat    Disabled
0×a08440dc1000  \??\C:\Users\warlocksmurf\AppData\Local\Microsoft\Windows\UsrClass.dat  Disabled
0×a0844187a000  \SystemRoot\System32\config\DRIVERS     Disabled
0×a0844268b000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.StartMenuExperienceHost_10.0.19041.3636_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat Disabled
0×a084428a2000  \??\C:\Users\warlocksmurf\AppData\Local\Packages\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\Settings\settings.dat  Disabled
0×a08442698000  \??\C:\Windows\AppCompat\Programs\Amcache.hve   Disabled
0×a0844292d000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.Windows.Search_1.14.10.19041_neutral_neutral_cw5n1h2txyewy\ActivationStore.dat    Disabled
0×a08442a53000  \??\C:\Users\warlocksmurf\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\Settings\settings.dat   Disabled
0×a08442c5d000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\MicrosoftWindows.Client.CBS_1000.19053.1000.0_x64__cw5n1h2txyewy\ActivationStore.dat        Disabled
0×a0844314f000  \??\C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.SkypeApp_14.53.77.0_x64__kzf8qxf38zg5c\ActivationStore.dat        Disabled
0×a0844324b000  \??\C:\Users\warlocksmurf\AppData\Local\Packages\Microsoft.SkypeApp_kzf8qxf38zg5c\Settings\settings.dat Disabled
0×a0844314b000  \??\C:\Users\warlocksmurf\AppData\Local\Packages\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\Settings\settings.dat       Disabled
```

- Vol2 (hivedump), Vol3 (filedump)

```
┌──(kali㉿kali)-[~/Desktop/volatility]
└─$ python2 vol.py -f ~/Desktop/recollection/recollection.bin --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a004266010 0x000000009a90f010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a004a41010 0x000000009df13010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a004a57010 0x000000009ddb9010 \SystemRoot\System32\Config\SAM
0xfffff8a00000d190 0x00000000a9882190 [no name]
0xfffff8a000024010 0x00000000a96fa010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a00004f010 0x00000000a9725010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a0006d4010 0x0000000081300010 \SystemRoot\System32\Config\SECURITY
0xfffff8a000733010 0x00000000a1d49010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a000ca4010 0x000000009f5fb010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a000d35010 0x00000000976ff010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a00125b010 0x0000000083a0c010 \??\C:\Users\user\ntuser.dat
0xfffff8a0012e3010 0x000000007cb5d010 \??\C:\Users\user\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a00257e010 0x0000000106fd2010 \??\C:\System Volume Information\Syscache.hve

┌──(kali㉿kali)-[~/Desktop/volatility]
└─$ python2 vol.py -f ~/Desktop/recollection/recollection.bin --profile=Win7SP1x64 hivedump -o 0xfffff8a004a57010
Volatility Foundation Volatility Framework 2.6.1
Last Written         Key
2009-07-14 04:45:46 UTC+0000 \CMI-CreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7}
2011-12-20 13:01:01 UTC+0000 \CMI-CreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7}\SAM
2009-07-14 04:45:46 UTC+0000 \CMI-CreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7}\SAM\Domains
2022-12-10 09:49:53 UTC+0000 \CMI-CreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7}\SAM\Domains\Account
2022-12-10 09:49:52 UTC+0000 \CMI-CreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7}\SAM\Domains\Account\Aliases
2022-12-10 09:49:53 UTC+0000 \CMI-CreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7}\SAM\Domains\Account\Aliases\000003E8
2022-12-10 09:49:53 UTC+0000 \CMI-CreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7}\SAM\Domains\Account\Aliases\Members
2022-12-10 09:49:53 UTC+0000 \CMI-CreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7}\SAM\Domains\Account\Aliases\Members\S-1-5-21-3283867801-3593768392-30134530
2
2022-12-10 09:49:53 UTC+0000 \CMI-CreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7}\SAM\Domains\Account\Aliases\Members\S-1-5-21-3283867801-3593768392-30134530
2\000001F4
2022-12-10 09:49:53 UTC+0000 \CMI-CreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7}\SAM\Domains\Account\Aliases\Members\S-1-5-21-3283867801-3593768392-30134530
2\000003E9
2022-12-10 09:49:53 UTC+0000 \CMI-CreateHive{C4E7BA2B-68E8-499C-B1A1-371AC8D717C7}\SAM\Domains\Account\Aliases\Members\S-1-5-21-3283867801-3593768392-30134530
2\000003EA
```

- Vol2 (printkey), Vol3 (registry.printkey)

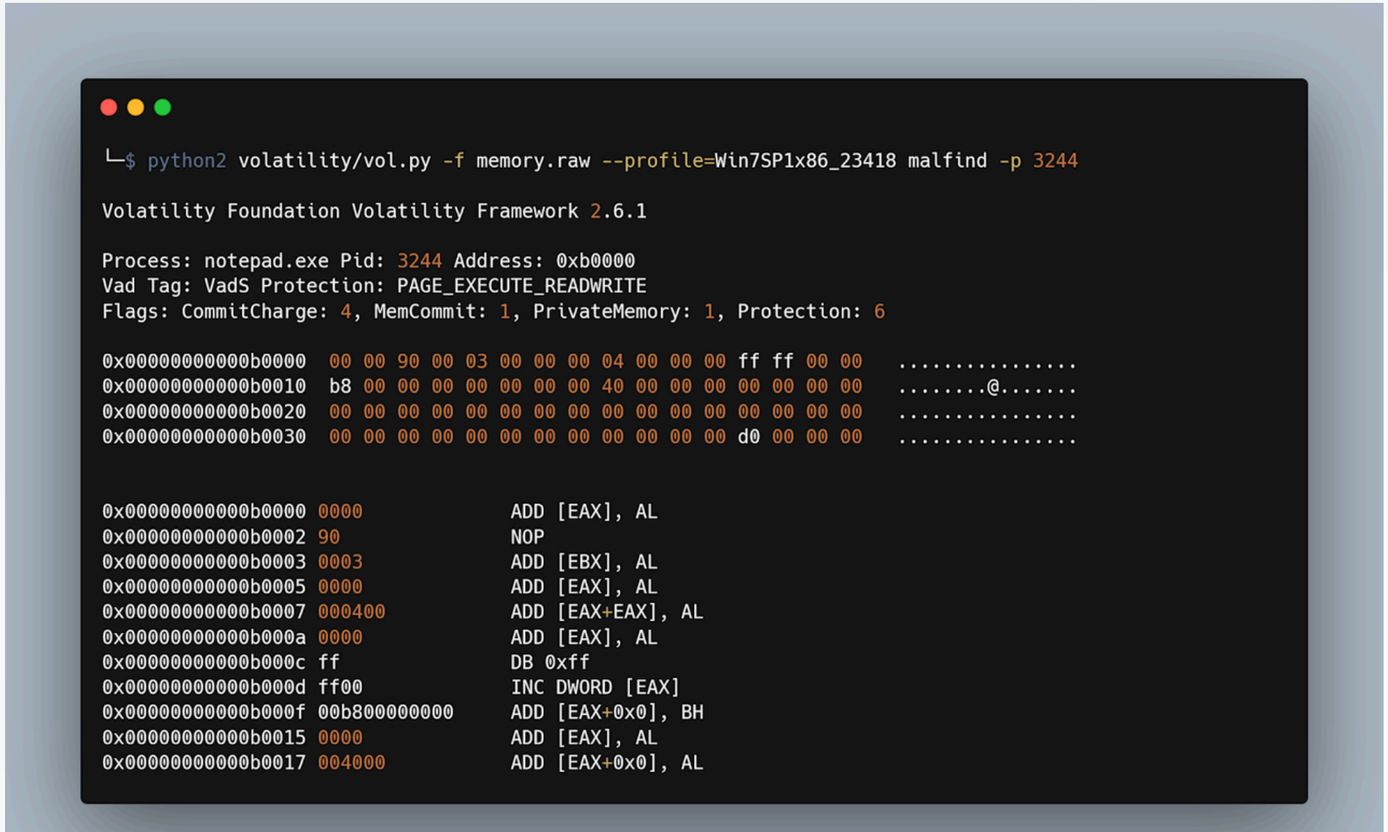


```
┌──(kali㉿kali)-[~/Desktop/volatility3]
└─$ python3 vol.py -f ~/Desktop/recollection/recollection.bin windows.registry.printkey --key "SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs"
Volatility 3 Framework 2.10.0
Progress:  100.00               PDB scanning finished
Last Write Time Hive Offset     Type    Key     Name    Data    Volatile

-       0×f8a00000d190  Key     ?\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs -               -
-       0×f8a000024010  Key     ?\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs -               -
-       0×f8a00004f010  Key     ?\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs -               -
-       0×f8a0006d4010  Key     ?\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs -               -
-       0×f8a000733010  Key     ?\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs -               -
-       0×f8a000ca4010  Key     ?\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs -               -
-       0×f8a000d35010  Key     ?\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs -               -
2022-12-19 15:50:42.000000 UTC  0×f8a00125b010  Key     \??\C:\Users\user\ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs      .txt            False
2022-12-19 15:50:42.000000 UTC  0×f8a00125b010  Key     \??\C:\Users\user\ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs      Folder          False
2022-12-19 15:50:42.000000 UTC  0×f8a00125b010  REG_BINARY      \??\C:\Users\user\ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs      MRUListEx
01 00 00 00 00 00 00 00 ff ff ff ff             ............"   False
2022-12-19 15:50:42.000000 UTC  0×f8a00125b010  REG_BINARY      \??\C:\Users\user\ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs      0       "
43 00 6f 00 6e 00 66 00 69 00 64 00 65 00 6e 00 C.o.n.f.i.d.e.n.
74 00 69 00 61 00 6c 00 2e 00 74 00 78 00 74 00 t.i.a.l ... t.x.t.
00 00 6e 00 32 00 00 00 00 00 00 00 00 00 00 00 ..n.2...........
43 6f 6e 66 69 64 65 6e 74 69 61 6c 2e 6c 6e 6b Confidential.lnk
00 00 4e 00 08 00 04 00 ef be 00 00 00 00 00 00 ..N.............
00 00 2a 00 00 00 00 00 00 00 00 00 00 00 00 00 ..*.............
00 00 00 00 00 00 00 00 00 00 00 00 43 00 6f 00 ............C.o.
6e 00 66 00 69 00 64 00 65 00 6e 00 74 00 69 00 n.f.i.d.e.n.t.i.
61 00 6c 00 2e 00 6c 00 6e 00 6b 00 00 00 20 00 a.l ... l.n.k ...  .
00 00                                           .."     False
2022-12-19 15:50:42.000000 UTC  0×f8a00125b010  REG_BINARY      \??\C:\Users\user\ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs      1       "
53 00 65 00 63 00 72 00 65 00 74 00 00 00 5c 00 S.e.c.r.e.t ... \.
32 00 00 00 00 00 00 00 00 00 00 00 53 65 63 72 2...........Secr
65 74 2e 6c 6e 6b 00 00 42 00 08 00 04 00 ef be et.lnk..B.......
00 00 00 00 00 00 00 00 2a 00 00 00 00 00 00 00 ........*.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 53 00 65 00 63 00 72 00 65 00 74 00 2e 00 ..S.e.c.r.e.t ...
6c 00 6e 00 6b 00 00 00 1a 00 00 00             l.n.k........"   False
-       0×f8a0012e3010  Key     ?\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs -               -
-       0×f8a00257e010  Key     ?\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs -               -
-       0×f8a004266010  Key     ?\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs -               -
-       0×f8a004a41010  Key     ?\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs -               -
-       0×f8a004a57010  Key     ?\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs -               -
```

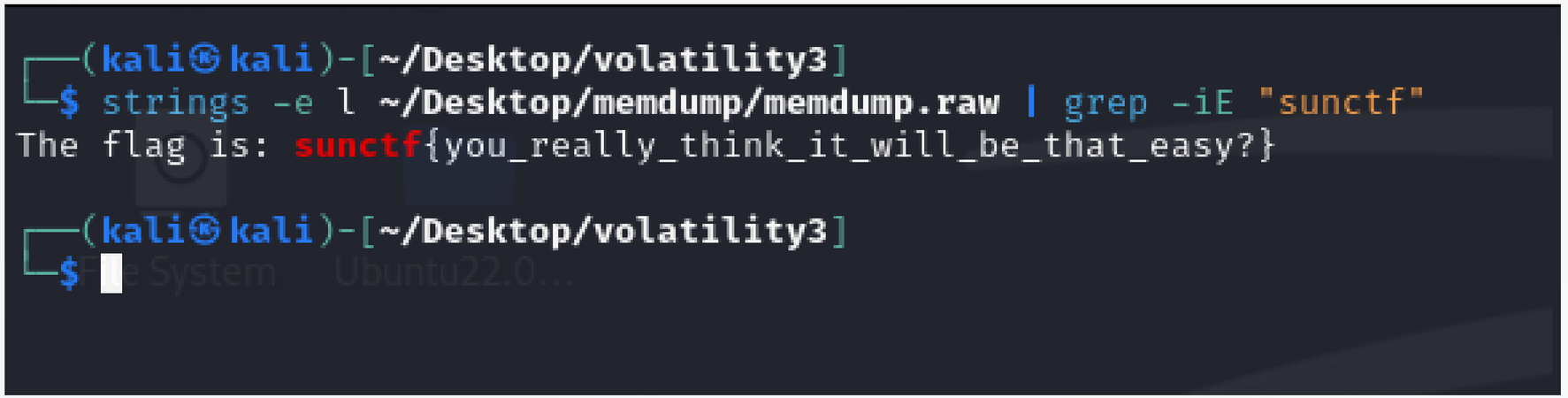
INJECTED CODE

- Vol2 (malfind), Vol3 (malfind)
- Find hidden or injected code/DLLs in user mode memory, based on characteristics such as VAD tag and page permissions.
- Suspicious if a memory page is marked for execution AND that don't have an associated file mapped to disk



REF: HTB CYBER APOCALYPSE CTF 2022

STRINGS/GREP



CONCLUSION

- So what is the conclusion, did you identify the malware? or did you identify the flag?



TRY IT!

CHALLENGE 1



- We managed to recover a memory dump from the compromised machine and require your analysis to obtain information about the attack. Can you identify when was the memory dump taken.

- The victim kept his study notes somewhere in the machine. Can you recover his study notes?

- The victim accidentally executed a malicious executable in the system. What was the malicious executable called, its process ID and parent process ID?

CHALLENGE 1



- The malicious executable injected the flag into its child process, can you retrieve the flag back?

- What is the password of the system user?

CHALLENGE 2



- What is the OS of the machine?
- What was the local IP address of the machine?
- A CMD command was executed to attempt to exfiltrate a file. What is the full command line?

CHALLENGE 2



- The attacker copied an obfuscated PowerShell command to the clipboard. What was the command?
- What is the Host Name of the machine?
- Attacker might have used an email address to login a social media. Can you tell us the email address?

WHAT ABOUT LINUX?



RESOURCES

- 13Cubed
- SANS
- Memory Forensics (Husam Shbib)
- fareedfauzi.github.io
- CyberDefenders
- Hack the Box
- CTFs
- warlocksmurf.github.io

THANKS!