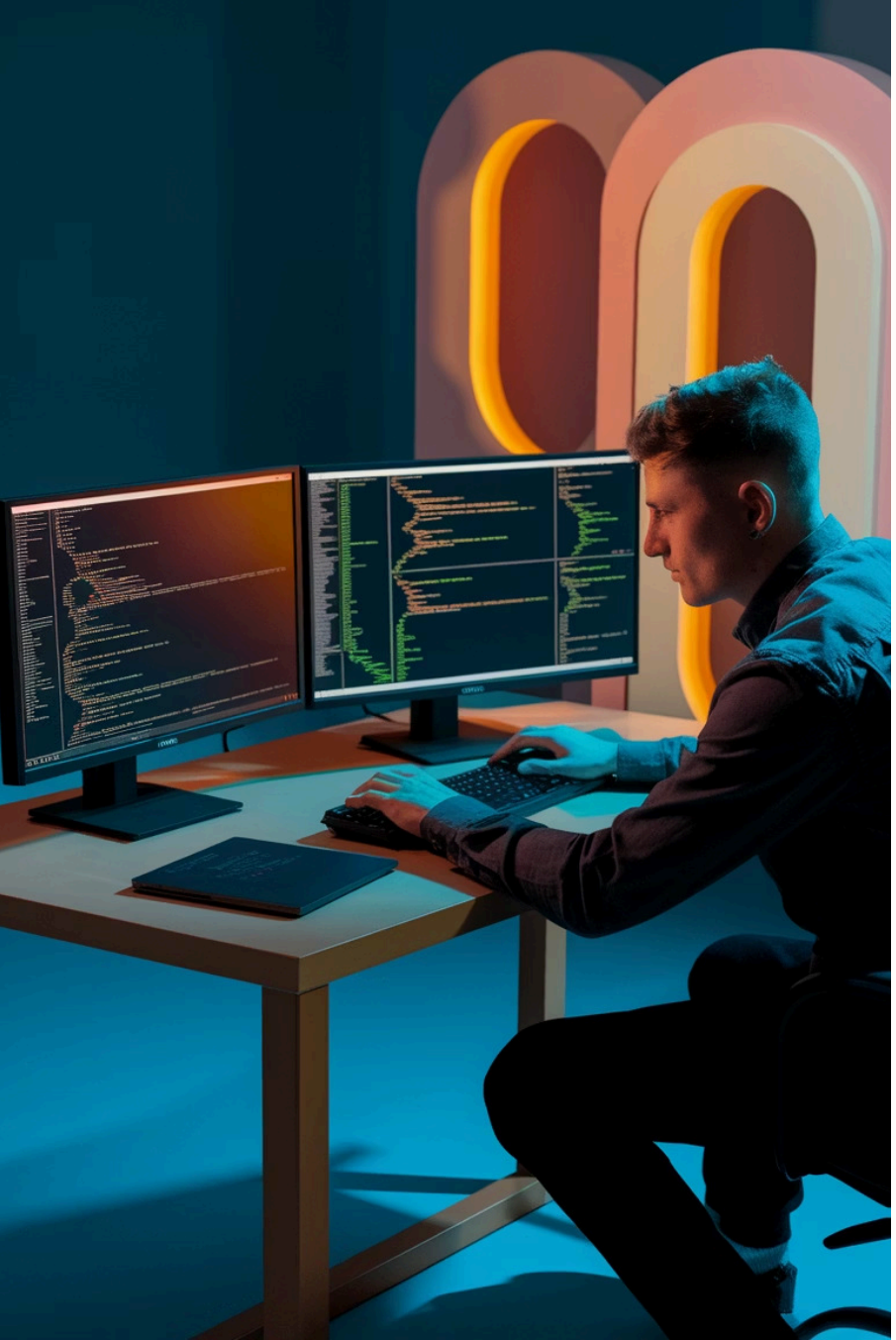
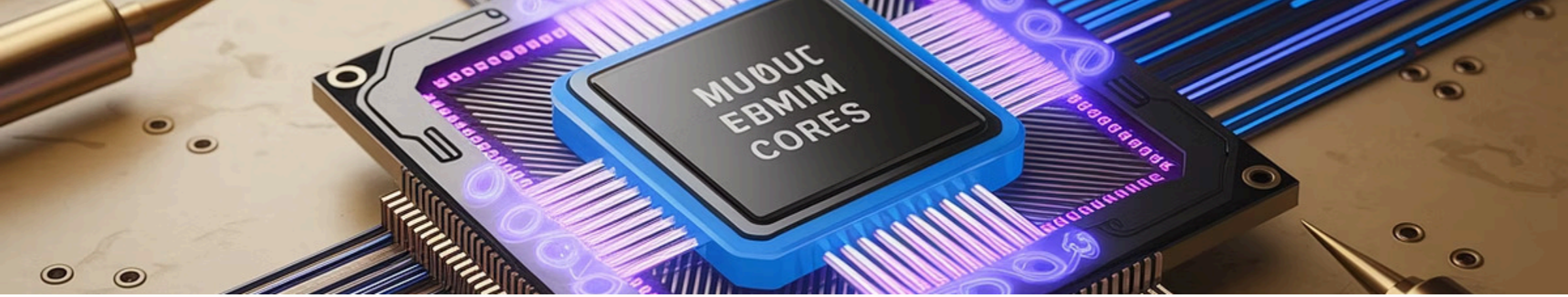


Volatility 3: Advanced Memory Forensics Framework

Volatility 3 represents the next generation of memory analysis frameworks for cybersecurity professionals. It builds upon its predecessor with enhanced capabilities for digital forensics and malware detection.

by Sean Sanders



Key Features

Python 3 Foundation

Built on modern Python 3 for improved performance and compatibility with current systems.

Modular Architecture

Plugin-based design enables custom extensions and specialized analysis tools.

Multi-core Processing

Leverages parallel processing capabilities for faster analysis of large memory dumps.

Advantages Over Volatility 2

Improved Scalability

Handles larger datasets with optimized memory usage and processing efficiency.

Performance scales linearly with available computing resources.

Cross-Platform Support

Enhanced compatibility across Windows, Linux, and macOS environments.

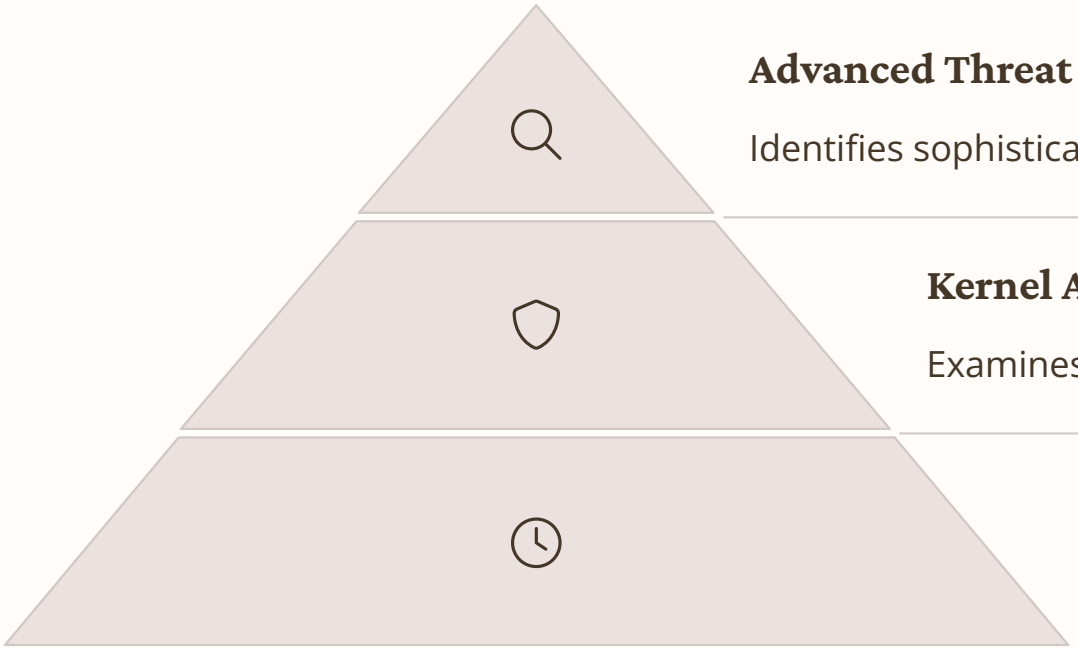
Unified analysis approach regardless of target operating system.

Simplified Codebase

Cleaner architecture with improved developer accessibility.

Reduced technical debt creates a more maintainable framework.

Applications in Cybersecurity



Advanced Threat Detection

Identifies sophisticated malware hiding in memory

Kernel Analysis

Examines kernel structures for signs of rootkits

Real-time Monitoring

Detects unauthorized processes and injections

Technical Architecture

Open-Source Core

Community-driven development with transparent code contributions

Plugin System

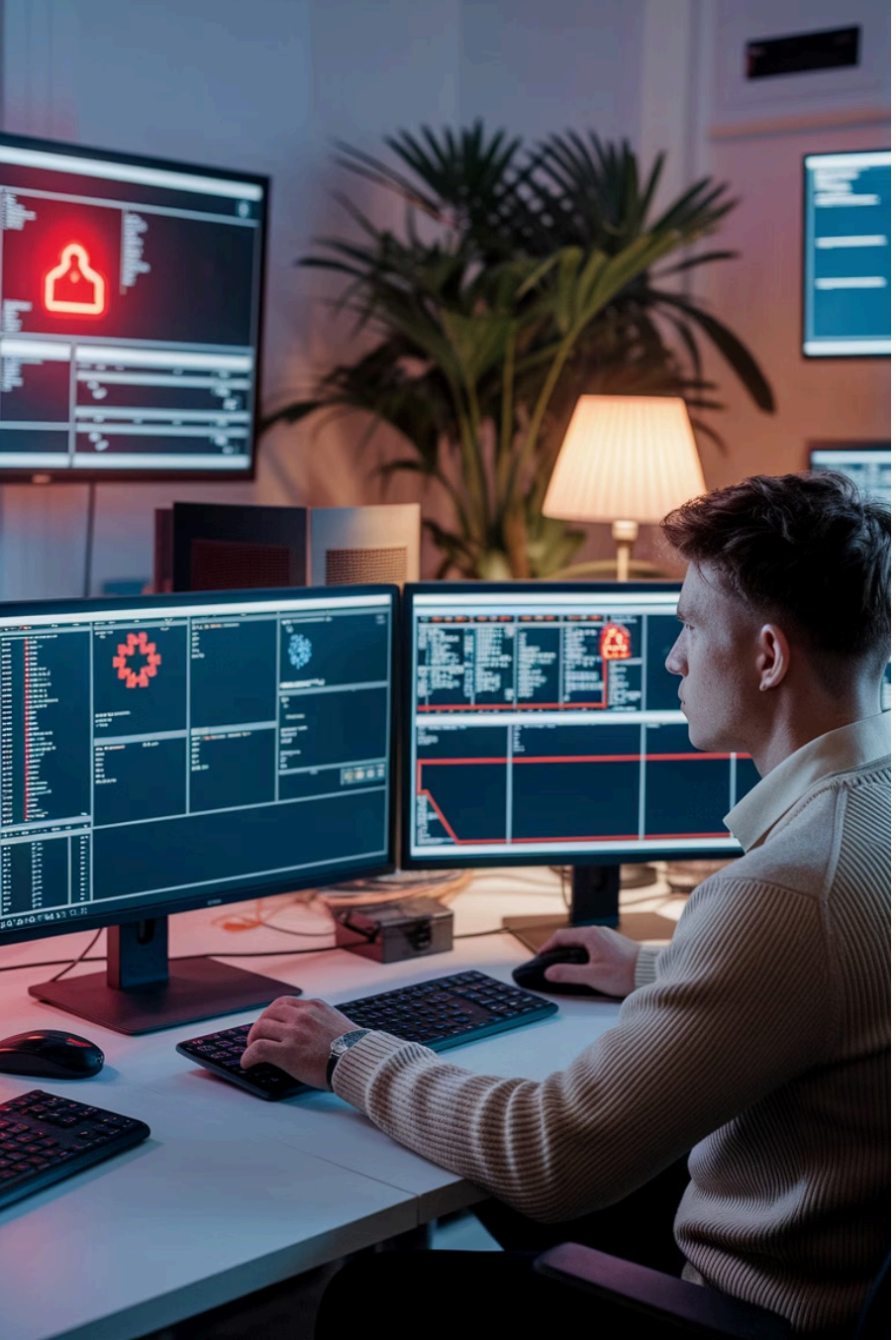
Separate plugins from core framework for better maintainability

Symbol Tables

Comprehensive memory mapping for accurate data interpretation

YAML Configuration

Flexible configuration files for customized analysis workflows



Real-World Use Cases

APT Investigation

Security teams use Volatility 3 to detect and analyze advanced persistent threats targeting critical infrastructure.

Post-Breach Analysis

Incident responders examine memory dumps to determine attack vectors and compromised systems.

Zero-Day Detection

Researchers identified previously unknown exploits by analyzing unusual memory patterns with Volatility 3.

Challenges and Limitations

Learning Curve

New users face a steep learning curve when mastering the tool's complex capabilities.

- Requires Python programming knowledge
- Deep understanding of OS internals needed

Memory Dump Quality

Analysis accuracy depends entirely on comprehensive memory captures.

- Partial dumps may miss critical evidence
- Acquisition errors can compromise results

Evolving Threats

Continuous updates needed to counter sophisticated evasion techniques.

- Anti-forensics tools target memory analysis
- New OS versions require profile updates

Volatility 3 Commands

OS Info

`vol.py -f “/path/to/file” windows.info`

Process Information

`vol.py -f “/path/to/file” windows.pslist`

`vol.py -f “/path/to/file” windows.psscan`

`vol.py -f “/path/to/file” windows.pstree`

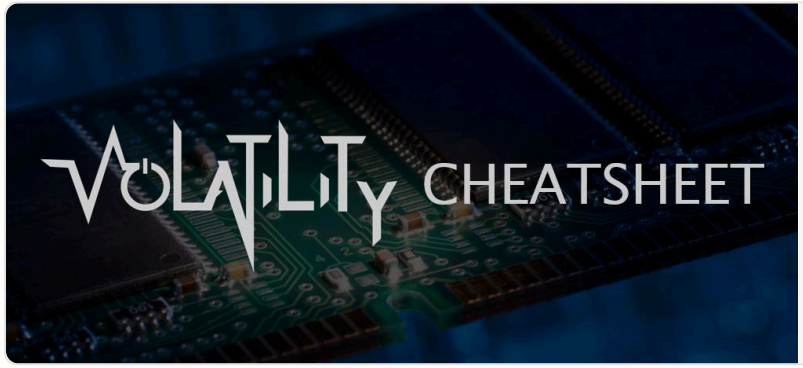
procdump

`vol.py -f “/path/to/file” -o “/path/to/dir” windows.dumpfiles --pid <PID>`

memdump

`vol.py -f “/path/to/file” -o “/path/to/dir” windows.memmap --dump --pid`

Cheat Sheet



onfvp

Volatility 3 CheatSheet

Comparing commands from Vol2 > Vol3

Exercise 1

Install volatility at **https://github.com/volatilityfoundation/volatility3**

Download Windows dump file from: **https://github.com/stuxnet999/MemLabs/tree/master/Lab%201**

Getting help info when stuck

Command: vol -h

```
(venv) ┌─[eu-dedivip-2]─[10.10.14.193]─[spsand1@htb-mdsyg0sz8x]─[~/Downloads]
└──╼ [★]$ vol -h
Volatility 3 Framework 2.26.2
usage: vol [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE]
           [--write-config] [--save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [--offline | -u URL] [--filters FILTERS] [--hide-columns [HIDE_COLUMNS ...]]
           [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]] [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
           PLUGIN ...

An open-source memory forensics framework

options:
  -h, --help            Show this help message and exit, for specific plugin options use 'vol <pluginname> --help'
  -c CONFIG, --config CONFIG
                        Load the configuration from a json file
  --parallelism [{processes,threads,off}]
                        Enables parallelism (defaults to off if no argument given)
  -e EXTEND, --extend EXTEND
                        Extend the configuration with a new (or changed) setting
  -p PLUGIN_DIRS, --plugin-dirs PLUGIN_DIRS
                        Semi-colon separated list of paths to find plugins
  -s SYMBOL_DIRS, --symbol-dirs SYMBOL_DIRS
                        Semi-colon separated list of paths to find symbols
  -v, --verbosity       Increase output verbosity
  -l LOG, --log LOG     Log output to a file as well as the console
  -o OUTPUT_DIR, --output-dir OUTPUT_DIR
                        Directory in which to output any generated files
  -q, --quiet           Remove progress feedback
  -r RENDERER, --renderer RENDERER
                        Determines how to render the output (quick, none, csv, pretty, json, jsonl)
```

Image Info

Command: vol -f MemoryDump_Lab1.raw windows.info

```
(venv) ┌─[eu-dedivip-2]─[10.10.14.193]─[spsand1@htb-mdsyg0sz8x]─[~/Downloads]
└──╼ [★]$ vol -f MemoryDump_Lab1.raw windows.info
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0xf8000261f000
DTB     0x187000
Symbols file:///home/spsand1/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/3844DBB920174967BE7AA4A2C20430FA-2.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdDebuggerDataBlock     0xf800028100a0
NTBuildLab      7601.17514.amd64fre.win7sp1_rtm.
CSDVersion      1
KdVersionBlock  0xf80002810068
Major/Minor     15.7601
MachineType     34404
KeNumberProcessors      1
SystemTime      2019-12-11 14:38:00+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  6
NtMinorVersion  1
PE MajorOperatingSystemVersion  6
PE MinorOperatingSystemVersion  1
PE Machine      34404
PE TimeDateStamp        Sat Nov 20 09:30:02 2010
```

Getting active processes

Command: vol -f MemoryDump_Lab1.raw windows.pslist

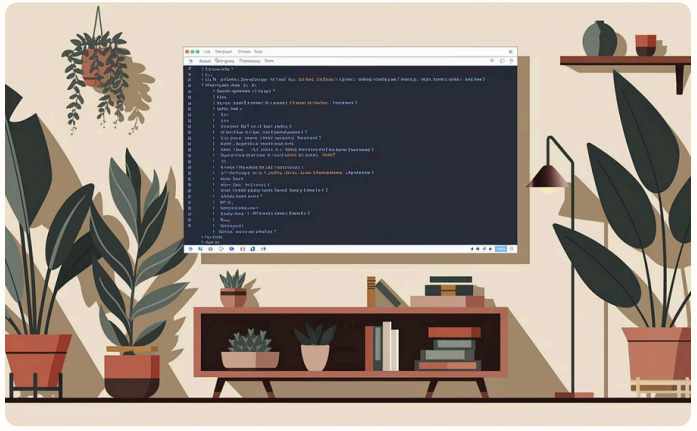
```
(venv) ┌─[eu-dedivip-2]─[10.10.14.193]─[spsand1@htb-mdsyg0sz8x]─[~/Downloads]
└──╼ [★]$ vol -f MemoryDump_Lab1.raw windows.pslist
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File outp

4       0       System  0xfa8000ca0040  80      570     N/A     False   2019-12-11 13:41:25.000000 UTC  N/A     Disabled
248     4       smss.exe        0xfa800148f040  3       37      N/A     False   2019-12-11 13:41:25.000000 UTC  N/A     Disabled
320     312     csrss.exe       0xfa800154f740  9       457     0       False   2019-12-11 13:41:32.000000 UTC  N/A     Disabled
368     360     csrss.exe       0xfa8000ca81e0  7       199     1       False   2019-12-11 13:41:33.000000 UTC  N/A     Disabled
376     248     psxss.exe       0xfa8001c45060  18      786     0       False   2019-12-11 13:41:33.000000 UTC  N/A     Disabled
416     360     winlogon.exe    0xfa8001c5f060  4       118     1       False   2019-12-11 13:41:34.000000 UTC  N/A     Disabled
424     312     wininit.exe     0xfa8001c5f630  3       75      0       False   2019-12-11 13:41:34.000000 UTC  N/A     Disabled
484     424     services.exe    0xfa8001c98530  13      219     0       False   2019-12-11 13:41:35.000000 UTC  N/A     Disabled
492     424     lsass.exe       0xfa8001ca0580  9       764     0       False   2019-12-11 13:41:35.000000 UTC  N/A     Disabled
500     424     lsm.exe 0xfa8001ca4b30  11      185     0       False   2019-12-11 13:41:35.000000 UTC  N/A     Disabled
588     484     svchost.exe     0xfa8001cf4b30  11      358     0       False   2019-12-11 13:41:39.000000 UTC  N/A     Disabled
652     484     VBoxService.ex  0xfa8001d327c0  13      137     0       False   2019-12-11 13:41:40.000000 UTC  N/A     Disabled
720     484     svchost.exe     0xfa8001d49b30  8       279     0       False   2019-12-11 13:41:41.000000 UTC  N/A     Disabled
816     484     svchost.exe     0xfa8001d8c420  23      569     0       False   2019-12-11 13:41:42.000000 UTC  N/A     Disabled
852     484     svchost.exe     0xfa8001da5b30  28      542     0       False   2019-12-11 13:41:43.000000 UTC  N/A     Disabled
876     484     svchost.exe     0xfa8001da96c0  32      941     0       False   2019-12-11 13:41:43.000000 UTC  N/A     Disabled
472     484     svchost.exe     0xfa8001e1bb30  19      476     0       False   2019-12-11 13:41:47.000000 UTC  N/A     Disabled
1044    484     svchost.exe     0xfa8001e50b30  14      366     0       False   2019-12-11 13:41:48.000000 UTC  N/A     Disabled
1208    484     spoolsv.exe     0xfa8001eba230  13      282     0       False   2019-12-11 13:41:51.000000 UTC  N/A     Disabled
1248    484     svchost.exe     0xfa8001eda060  19      313     0       False   2019-12-11 13:41:52.000000 UTC  N/A     Disabled
1372    484     svchost.exe     0xfa8001f58890  22      295     0       False   2019-12-11 13:41:54.000000 UTC  N/A     Disabled
1416    484     TCPSVCS.EXE     0xfa8001f91b30  4       97      0       False   2019-12-11 13:41:55.000000 UTC  N/A     Disabled
1508    484     sppsvc.exe      0xfa8000d3c400  4       141     0       False   2019-12-11 14:16:06.000000 UTC  N/A     Disabled
948     484     svchost.exe     0xfa8001c38580  13      322     0       False   2019-12-11 14:16:07.000000 UTC  N/A     Disabled
1856    484     wmpnetwk.exe    0xfa8002170630  16      451     0       False   2019-12-11 14:16:08.000000 UTC  N/A     Disabled
480     484     SearchIndexer.  0xfa8001d376f0  14      701     0       False   2019-12-11 14:16:09.000000 UTC  N/A     Disabled
```

```
296     484     taskhost.exe    0xfa8001eb47f0  8       151     1       False   2019-12-11 14:32:24.000000 UTC  N/A     Disabled
1988    852     dwm.exe 0xfa8001dfa910  5       72      1       False   2019-12-11 14:32:25.000000 UTC  N/A     Disabled
604     2016    explorer.exe    0xfa8002046960  33      927     1       False   2019-12-11 14:32:25.000000 UTC  N/A     Disabled
1844    604     VBoxTray.exe    0xfa80021c75d0  11      140     1       False   2019-12-11 14:32:35.000000 UTC  N/A     Disabled
2064    816     audiodg.exe     0xfa80021da060  6       131     0       False   2019-12-11 14:32:37.000000 UTC  N/A     Disabled
2368    484     svchost.exe     0xfa80022199e0  9       365     0       False   2019-12-11 14:32:51.000000 UTC  N/A     Disabled
1984    604     cmd.exe 0xfa8002222780  1       21      1       False   2019-12-11 14:34:54.000000 UTC  N/A     Disabled
2692    368     conhost.exe     0xfa8002227140  2       50      1       False   2019-12-11 14:34:54.000000 UTC  N/A     Disabled
2424    604     mspaint.exe     0xfa80022bab30  6       128     1       False   2019-12-11 14:35:14.000000 UTC  N/A     Disabled
2660    484     svchost.exe     0xfa8000eac770  6       100     0       False   2019-12-11 14:35:14.000000 UTC  N/A     Disabled
2760    2680    csrss.exe       0xfa8001e68060  7       172     2       False   2019-12-11 14:37:05.000000 UTC  N/A     Disabled
2808    2680    winlogon.exe    0xfa8000ecbb30  4       119     2       False   2019-12-11 14:37:05.000000 UTC  N/A     Disabled
2908    484     taskhost.exe    0xfa8000f3aab0  9       158     2       False   2019-12-11 14:37:13.000000 UTC  N/A     Disabled
3004    852     dwm.exe 0xfa8000f4db30  5       72      2       False   2019-12-11 14:37:14.000000 UTC  N/A     Disabled
2504    3000    explorer.exe    0xfa8000f4c670  34      825     2       False   2019-12-11 14:37:14.000000 UTC  N/A     Disabled
2304    2504    VBoxTray.exe    0xfa8000f9a4e0  14      144     2       False   2019-12-11 14:37:14.000000 UTC  N/A     Disabled
2524    480     SearchProtocol  0xfa8000fff630  7       226     2       False   2019-12-11 14:37:21.000000 UTC  N/A     Disabled
1720    480     SearchFilterHo  0xfa8000ecea60  5       90      0       False   2019-12-11 14:37:21.000000 UTC  N/A     Disabled
1512    2504    WinRAR.exe      0xfa8001010b30  6       207     2       False   2019-12-11 14:37:23.000000 UTC  N/A     Disabled
2868    480     SearchProtocol  0xfa8001020b30  8       279     0       False   2019-12-11 14:37:23.000000 UTC  N/A     Disabled
796     604     DumpIt.exe      0xfa8001048060  2       45      1       True    2019-12-11 14:37:54.000000 UTC  N/A     Disabled
2260    368     conhost.exe     0xfa800104a780  2       50      1       False   2019-12-11 14:37:54.000000 UTC  N/A     Disabled
```

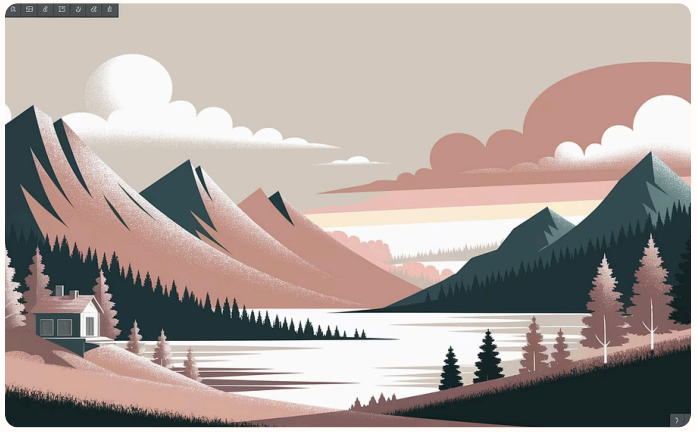
Getting active processes continued...

When analyzing suspicious activity, we need to identify processes that stand out based on user context.



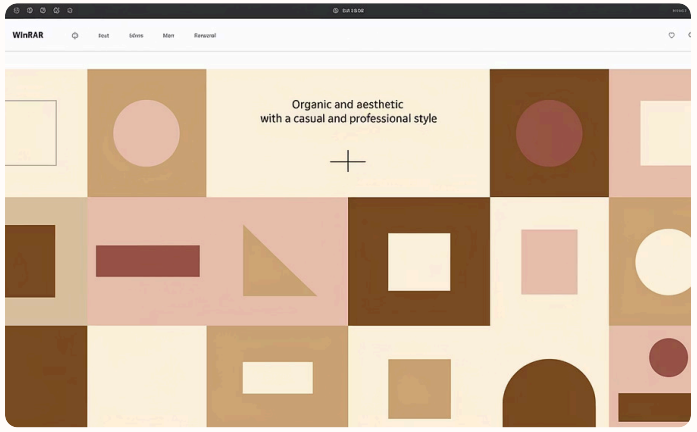
Command Prompt (cmd.exe)

The user reported a black window popup, which likely corresponds to this Command Prompt process in our memory dump



MS Paint (mspaint.exe)

The user mentioned they were drawing something, which explains the presence of the Paint application in our process list



WinRAR (WinRAR.exe)

This archive utility was also running during the incident and warrants further investigation in our memory forensics analysis

Let’s start with cmd.exe (PID 1984)

Command: vol -f MemoryDump_Lab1.raw windows.handles --pid 1984

```
(venv) ┌─[eu-dedivip-2]─[10.10.14.193]─[spsand1@htb-mdsyg0sz8x]─[~/Downloads]
└──╼ [★]$ vol -f MemoryDump_Lab1.raw windows.handles --pid 1984
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     Process Offset  HandleValue     Type    GrantedAccess   Name

1984    cmd.exe 0xf8a0021ae5b0  0x4     Key     0x9     MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS
1984    cmd.exe 0xf8a00027f360  0x8     Directory       0x3     KnownDlls
1984    cmd.exe 0xfa80021b5070  0xc     File    0x100020        \Device\HarddiskVolume2\Users\SmartNet
1984    cmd.exe 0xfa80021a11d0  0x10    Event   0x1f0003        -
1984    cmd.exe 0xf8a0020f68b0  0x14    Key     0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS
1984    cmd.exe 0xfa80022aa360  0x18    ALPC Port       0x1f0001        -
1984    cmd.exe 0xfa8002207c90  0x1c    ALPC Port       0x1f0001        -
1984    cmd.exe 0xf8a001f2a600  0x20    Key     0x1     MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER
1984    cmd.exe 0xfa800203e7e0  0x24    EtwRegistration 0x804   -
1984    cmd.exe 0xfa8001e6c850  0x28    Event   0x21f0003       -
1984    cmd.exe 0xfa8001c682f0  0x2c    WindowStation   0xf037f WinSta0
1984    cmd.exe 0xfa8001c86e90  0x30    Desktop 0xf01ff Default
1984    cmd.exe 0xfa8001c682f0  0x34    WindowStation   0xf037f WinSta0
1984    cmd.exe 0xf8a001ada120  0x38    Key     0x20019 MACHINE
1984    cmd.exe 0xfa80021e66a0  0x3c    Thread  0x1fffff        Tid 340 Pid 1984
1984    cmd.exe 0xf8a0021e2820  0x40    Key     0xf003f USER\S-1-5-21-3073570648-3149397540-2269648332-1001
1984    cmd.exe 0xf8a001ff4750  0x44    Key     0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE
1984    cmd.exe 0xf8a001fc41c0  0x48    Key     0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE\ALTERNATE SORTS
1984    cmd.exe 0xf8a0021095a0  0x4c    Key     0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LANGUAGE GROUPS
1984    cmd.exe 0xfa80022474c0  0x50    Mutant  0x1f0001        -
1984    cmd.exe 0xfa8001ee3c60  0x54    Event   0x1f0003        -
```

physical file that is linked with the process

Command: mkdir dump

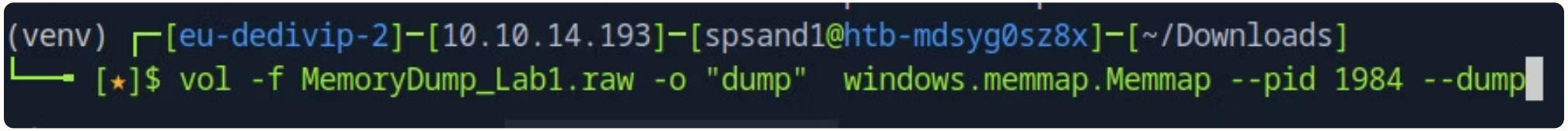
vol -f MemoryDump_Lab1.raw -o "dump" windows.dumpfile --pid 1984 --virtaddr 0xfa80021b5070

```
(venv) ┌─[eu-dedivip-2]─[10.10.14.193]─[spsand1@htb-mdsyg0sz8x]─[~/Downloads]
└──╼ [★]$ mkdir dump
(venv) ┌─[eu-dedivip-2]─[10.10.14.193]─[spsand1@htb-mdsyg0sz8x]─[~/Downloads]
└──╼ [★]$ vol -f MemoryDump_Lab1.raw -o "dump" windows.dumpfile --pid 1984 --virtaddr 0xfa80021b5070
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result
```

This will not work currnetly.

create a memory dump of cmd.exe

Command: vol -f MemoryDump_Lab1.raw -o "dump" windows.memmap.Memmap --pid 1984 --dump



Reading the dump file

Command: strings dump/pid.1984.dmp | grep St4G

```
(venv) ┌─[eu-dedivip-2]─[10.10.14.193]─[spsand1@htb-mdsyg0sz8x]─[~/Downloads]
└──╼ [★]$ strings -e l dump/pid.1984.dmp | grep St4G
C:\Windows\system32\cmd.exe - St4G3$1
m32\St4G
C:\Windows\system32\cmd.exe - St4G3$1
St4G3$1
St4G3$1
St4G3$1
C:\Windows\system32\St4G3$1.bat
St4G3$1
:\Windows\System32\St4G3$1.bat
\Device\HarddiskVolume2\Windows\System32\St4G3$1.bat
\Windows\System32\St4G3$1.bat
St4G3$1
St4G3$1
St4G3$1.bat
Microsoft Windows [Version 6.1.7601]Copyright (c) 2009 Microsoft Corporation.  All rights reserved.C:\Users\SmartNet>St4G3$1ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=Press any key to continue
. . .
St4G3$1
C:\Windows\system32\cmd.exe - St4G3$1
St4G3$1.bat
St4G3$1.bat
St4G3$1.bat
```

Extracted it using commands

Command: vol -f MemoryDump_Lab1.raw -o 'dump' windows.dumpfiles.DumpFiles --physaddr 0x3edcfc20

vol -f MemoryDump_Lab1.raw -o 'dump' windows.dumpfiles.DumpFiles --physaddr 0x3edcfc20

```
(venv) ┌─[eu-dedivip-2]─[10.10.14.193]─[spsand1@htb-mdsyg0sz8x]─[~/Downloads]
└──╼ [★]$ vol -f MemorDump_Lab1.raw -o "dump" windows.dumpfiles.DumpFiles --physaddr 0x3edcfc20
Volatility 3 Framework 2.26.2
usage: vol [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE]
           [--write-config] [--save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [--offline | -u URL] [--filters FILTERS] [--hide-columns [HIDE_COLUMNS ...]]
           [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]] [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
           PLUGIN ...
vol: error: File does not exist: /home/spsand1/Downloads/MemorDump_Lab1.raw
(venv) ┌─[eu-dedivip-2]─[10.10.14.193]─[spsand1@htb-mdsyg0sz8x]─[~/Downloads]
└──╼ [★]$ vol -f MemoryDump_Lab1.raw -o "dump" windows.dumpfiles.DumpFiles --physaddr 0x3edcfc20
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0x3edcfc20      St4G3$1.bat     file.0x3edcfc20.0xfa8000e9ac40.DataSectionObject.St4G3$1.bat.dat
```

Open file from the dump directory in a text editor

```
@ECHO OFF

ECHO ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=

PAUSE\00\00\00
```

mspaint.exe (PID 2424)

Command: vol -f MemoryDump_Lab1.raw -o "dump" windows.memmap.Memmap --pid 2424 --dump

cd dump

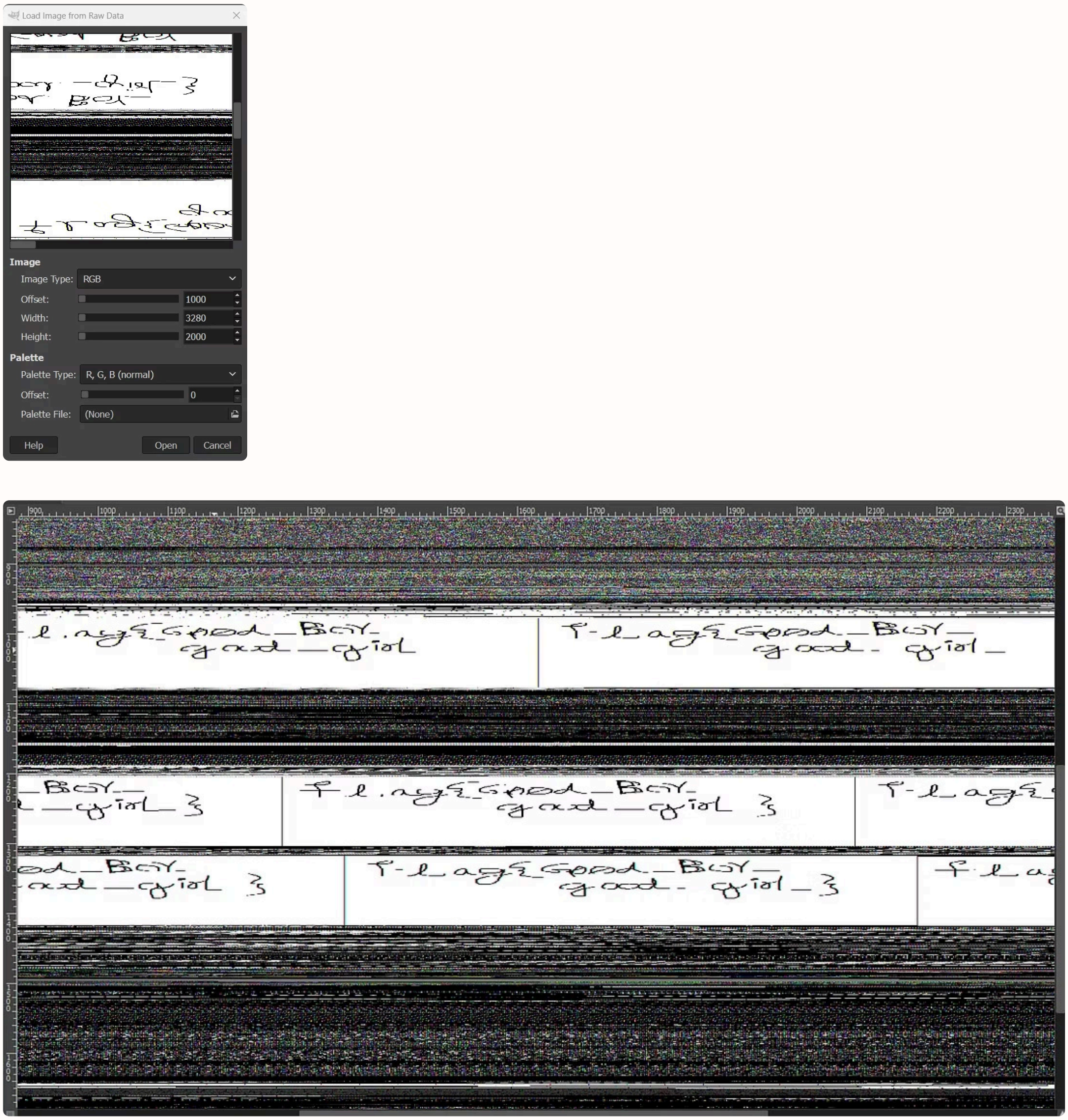
file pid.2424.dmp

mv pid.2424.dmp pid.2424.data

sudo apt-get install gimp

gimp pid.2424.data

```
(venv) ┌─[eu-dedivip-2]─[10.10.14.193]─[spsand1@htb-mdsyg0sz8x]─[~/Downloads]
└──╼ [★]$ vol -f MemoryDump_Lab1.raw -o "dump" windows.memmap.Memmap --pid 2424 --dump
```



winrar.exe (PID 1512)

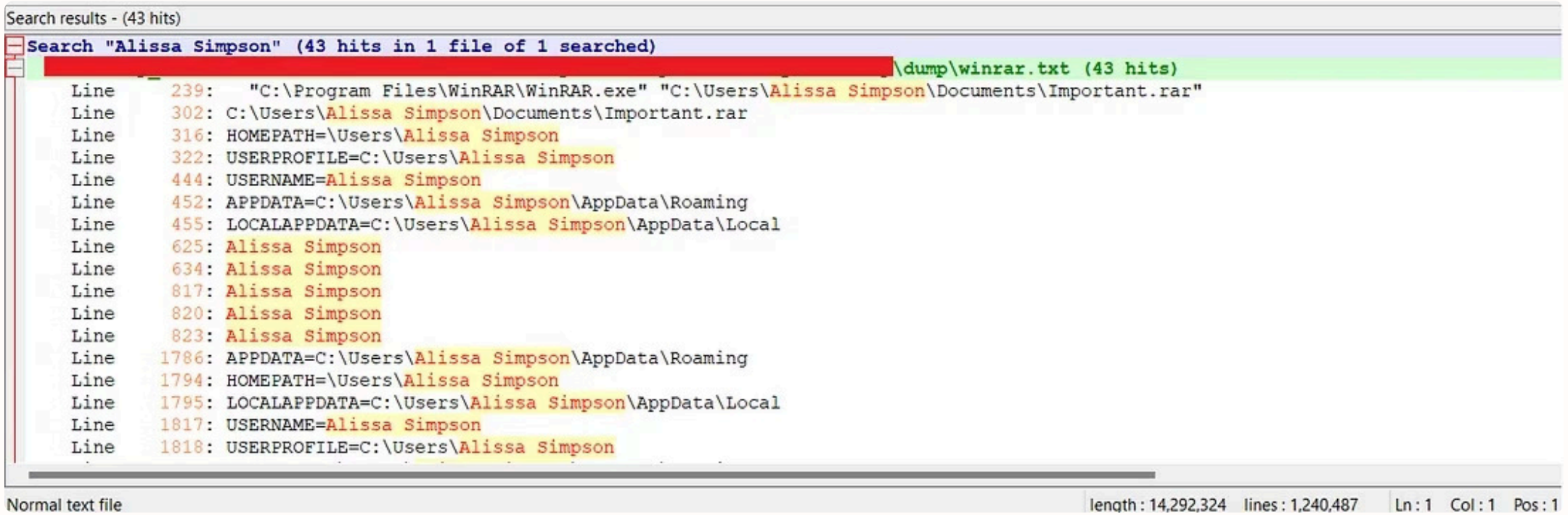
Command: vol -f MemoryDump_Lab1.raw windows.handles --pid 1512 | grep File

vol -f MemoryDump_Lab1.raw windows.handles --pid 1512 | grep Documents

```
(venv) ┌─[eu-dedivip-2]─[10.10.14.193]─[spsand1@htb-mdsyg0sz8x]─[~/Downloads]
└──╼ [★]$ vol -f MemoryDump_Lab1.raw windows.handles --pid 1512 | grep File
1512ressWinRAR.exe      0xfa8001004790an0xcg finFile    0x100020        \Device\HarddiskVolume2\Users\Alissa Simpson\Documents
1512    WinRAR.exe      0xfa800101d2d0  0x10    File    0x100020        \Device\HarddiskVolume2\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa
396087175ac9ac
1512    WinRAR.exe      0xfa800101d180  0x14    File    0x100020        \Device\HarddiskVolume2\Windows\winsxs\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71
ed437a
1512    WinRAR.exe      0xfa800102ae60  0xd8    File    0x100001        \Device\KsecDD
1512    WinRAR.exe      0xfa800102a840  0xdc    File    0x100020        \Device\HarddiskVolume2\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa
396087175ac9ac
1512    WinRAR.exe      0xfa800101b520  0x170   File    0x120089        \Device\HarddiskVolume2\Windows\Fonts\StaticCache.dat
1512    WinRAR.exe      0xfa8000ece4a0  0x178   File    0x120089        \Device\HarddiskVolume2\Windows\System32\en-US\KernelBase.dll.mui
1512    WinRAR.exe      0xfa8001012d10  0x17c   File    0x100020        \Device\HarddiskVolume2\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa
396087175ac9ac
1512    WinRAR.exe      0xfa8001013970  0x1d4   File    0x100020        \Device\HarddiskVolume2\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa
396087175ac9ac
1512    WinRAR.exe      0xfa8001edda20  0x27c   File    0x12019f        \Device\VBoxGuest
1512    WinRAR.exe      0xfa800100da00  0x2b0   File    0x12019f        \Device\NamedPipe\wkssvc
1512    WinRAR.exe      0xfa800102fa90  0x2c8   File    0x100020        \Device\HarddiskVolume2\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa
396087175ac9ac
(venv) ┌─[eu-dedivip-2]─[10.10.14.193]─[spsand1@htb-mdsyg0sz8x]─[~/Downloads]
└──╼ [★]$ vol -f MemoryDump_Lab1.raw windows.handles --pid 1512 | grep Documents
1512ressWinRAR.exe      0xfa8001004790an0xcg finFiled   0x100020        \Device\HarddiskVolume2\Users\Alissa Simpson\Documents
```

look for clues specifically for Alissa Simpson\Documents

Command: vol -f MemoryDump_Lab1.raw windows.filescan | grep Alissa



Dump files

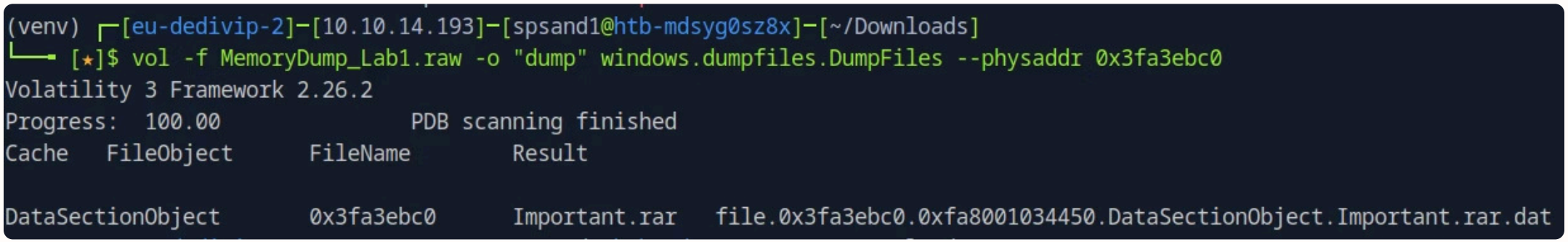
Command: vol -f MemoryDump_Lab1.raw -o "dump" windows.dumpfiles.DumpFiles --physaddr 0x3fa3ebc0

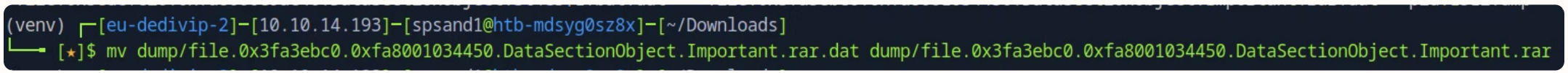
cd dump

file file.0x3fa3ebc0.0xfa8001034450.DataSectionObject.Important.rar.dat

mv file.0x3fa3ebc0.0xfa8001034450.DataSectionObject.Important.rar.dat
file.0x3fa3ebc0.0xfa8001034450.DataSectionObject.Important.rar

cd ../





Important.rar is password protected

Command: vol -f MemoryDump_Lab1.raw -o "dump" windows.hashdump

```
(venv) ┌─[eu-dedivip-2]─[10.10.14.193]─[spsand1@htb-mdsyg0sz8x]─[~/Downloads]
└──╼ [★]$ vol -f MemoryDump_Lab1.raw windows.hashdump
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
User    rid     lmhash  nthash
/home/spsand1/volatility3/volatility3/framework/deprecation.py:106: FutureWarning: This plugin (volatility3.plugins.windows.hashdump.Hashdump) has been renamed and will be removed in the fir
st release after 2025-09-25. Please ensure all method calls to this plugin are replaced with calls to volatility3.plugins.windows.registry.hashdump.Hashdump
  warnings.warn(

Administrator   500     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
Guest   501     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
SmartNet        1001    aad3b435b51404eeaad3b435b51404ee        4943abb39473a6f32c11301f4987e7e0
HomeGroupUser$  1002    aad3b435b51404eeaad3b435b51404ee        f0fc3d257814e08fea06e63c5762ebd5
Alissa Simpson  1003    aad3b435b51404eeaad3b435b51404ee        f4ff64c8baac57d22f22edc681055ba6
```

Crack the Hash

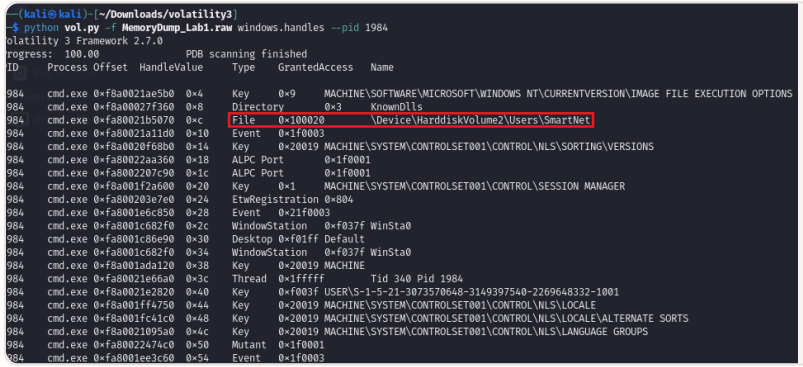
md5decrypt.net

Online NTLM Encrypt and Decrypt

Encrypt a word using ntlm hash generator, or decrypt your ntlm hash by comparing it with our free online ntlm database

f4ff64c8baac57d22f22edc681055ba6 : goodmorningindia

Full tutorial



```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ python vol.py -f MemoryDump_Lab1.raw windows.handles --pid 1984
olatility 3 Framework 2.7.0
rogress:  100.00               PDB scanning finished
ID     Process Offset  HandleValue     Type    GrantedAccess   Name

984    cmd.exe 0xf8a0021ae5b0  0x4     Key     0x9     MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS
984    cmd.exe 0xf8a00027f360  0x8     Directory       0x3     KnownDlls
984    cmd.exe 0xf8a0021b5070  0xc     File    0x100020        \Device\HarddiskVolume2\Users\SmartNet
984    cmd.exe 0xf8a0021a11d0  0x10    Event   0x1f0003
984    cmd.exe 0xf8a0020f68b0  0x14    Key     0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS
984    cmd.exe 0xf8a0022aa360  0x18    ALPC Port       0x1f0001
984    cmd.exe 0xfa8002207c90  0x1c    ALPC Port       0x1f0001
984    cmd.exe 0xf8a001f2a600  0x20    Key     0x1     MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER
984    cmd.exe 0xfa800203e7e0  0x24    EtwRegistration 0x804
984    cmd.exe 0xfa8001e6c850  0x28    Event   0x21f0003
984    cmd.exe 0xfa8001c682f0  0x2c    WindowStation   0xf037f WinSta0
984    cmd.exe 0xfa8001c86e90  0x30    Desktop 0xf01ff Default
984    cmd.exe 0xfa8001c682f0  0x34    WindowStation   0xf037f WinSta0
984    cmd.exe 0xf8a001ada120  0x38    Key     0x20019 MACHINE
984    cmd.exe 0xfa80021e66a0  0x3c    Thread  0x1fffff        Tid 340 Pid 1984
984    cmd.exe 0xf8a0021e2820  0x40    Key     0xf003f USER\S-1-5-21-3073570648-3149397540-2269648332-1001
984    cmd.exe 0xf8a001ff4750  0x44    Key     0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE
984    cmd.exe 0xf8a001fc41c0  0x48    Key     0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE\ALTERNATE SORTS
984    cmd.exe 0xf8a0021095a0  0x4c    Key     0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LANGUAGE GROUPS
984    cmd.exe 0xfa80022474c0  0x50    Mutant  0x1f0001
984    cmd.exe 0xfa8001ee3c60  0x54    Event   0x1f0003
```

Medium

Volatility3 Exercise—MemLabs Lab 1

Hi, this is an old challenge that was uploaded 4 years ago. There are already many writeups availabe in the internet regarding this. I...