WCSC CTF @ Hackabull 2023

Volatile Vault: Unlock the secrets hidden within.

Author: Kyd1ct

Contents

1 Introduction and Aims

Digital Forensics are a vital part of cybercrime prevention. While there may be numerous techniques and tools to identify various artefacts, some may remain hidden as they reside within the system's Random Access Memory. Considering this, forensic analysts should perform in-depth analysis of the hidden information inside the volatile RAM data.

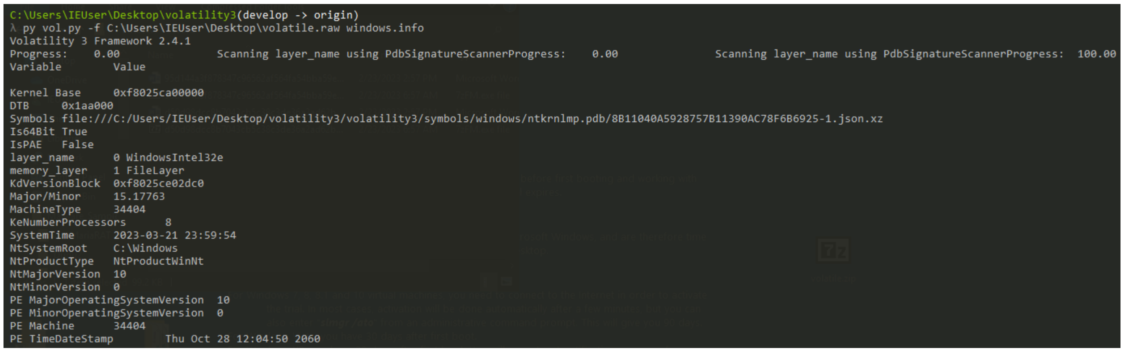
This paper aims to provide a detailed walkthrough of the Volatile Vault CTF challenge, giving security analysts an overview of the powerful RAM analysis tool called Volatility.

2 Methodology

2.1 OS Identification

The analysis of the provided memory dump will begin with the identification of the operating system. Knowing the type of OS is important as their architectures, file structures and processes differ. Failing to do so may result in inaccuracies when analysing the data.

The analyst identified the type of OS by using the **windows.info** Volatility plugin (**Figure 2.1**)



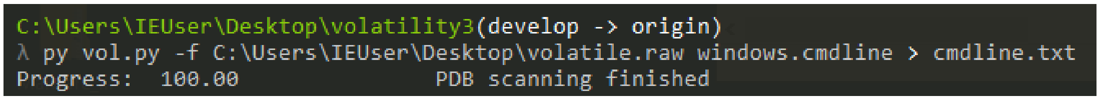
```
C:\Users\IEUser\Desktop\volatility3(develop -> origin)
λ py vol.py -f C:\Users\IEUser\Desktop\volatile.raw windows.info
Volatility 3 Framework 2.4.1
Progress:    0.00               Scanning layer_name using PdbSignatureScannerProgress:    0.00               Scanning layer_name using PdbSignatureScannerProgress:  100.00
Variable        Value

Kernel Base     0xf8025ca00000
DTB     0x1aa000
Symbols file:///C:/Users/IEUser/Desktop/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/8B11040A5928757B11390AC78F6B6925-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf8025ce02dc0
Major/Minor     15.17763
MachineType     34404
KeNumberProcessors      8
SystemTime      2023-03-21 23:59:54
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Thu Oct 28 12:04:50 2060
```

***Figure 2.1** – Windows.info results.*

The tool revealed a lot of information regarding the image and the OS. Based on the results, the analyst identified the OS, its version, system time during the RAM dump process, etc.

2.2 Analysis

After discovering the OS, the analyst continued with the investigation. As the description of the challenge mentioned hidden texts, the investigator forwarded their attention to the processes that were running during the time of the memory dump. Considering that data should be found in textual format, the analyst looked for artefacts from text editors such as word, text, vim, etc. This was achieved by using the **windows.cmdline** plugin. This plugin lists the process names, their PIDs and arguments used for their execution. (**Figure 2.2**) The full output can be found in Appendix A.



```
C:\Users\IEUser\Desktop\volatility3(develop -> origin)
λ py vol.py -f C:\Users\IEUser\Desktop\volatile.raw windows.cmdline > cmdline.txt
Progress:  100.00               PDB scanning finished
```

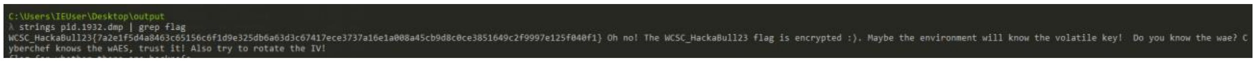
***Figure 2.2** – Windows.cmdline execution.*

The analyst piped the output onto a text file for easier analysis. Additionally, PowerShell can also be used to directly sort the output using cmdlets. After the analysis of the results, the investigator identified multiple processes related to text documents and editors:

- 412 notepad.exe "C:\Windows\system32\NOTEPAD.EXE" C:\Users\IEUser\Desktop\not_here.txt
- 6200 notepad.exe "C:\Windows\system32\NOTEPAD.EXE" C:\Users\IEUser\Desktop\definite_not_here.txt

- 5844 notepad++.exe "C:\Program Files\Notepad++\notepad++.exe" "C:\Users\IEUser\Desktop\base64_then_rot13"
- 5156 notepad.exe "C:\Windows\system32\NOTEPAD.EXE" C:\Users\IEUser\Desktop\aes_then_base64
- 1932 gvim.exe "C:\Program Files (x86)\Vim\vim81\gvim.exe" --literal "C:\Users\IEUser\Desktop\s@credt3xt"

The file created in Vim had a name hinting that it contains sacred texts. The analyst mapped and dumped the memory process using the following command: **py vol.py -f C:\Users\IEUser\Desktop\volatile.raw -o 'C:\Users\IEUser\Desktop\output\' windows.memmap --pid 1932 –dump**. After the dump was complete, the analyst used **strings** and **grep** to look for a potential flag. Looking for the "flag" string revealed a message with an encrypted flag and hints. (**Figure 2.3**)



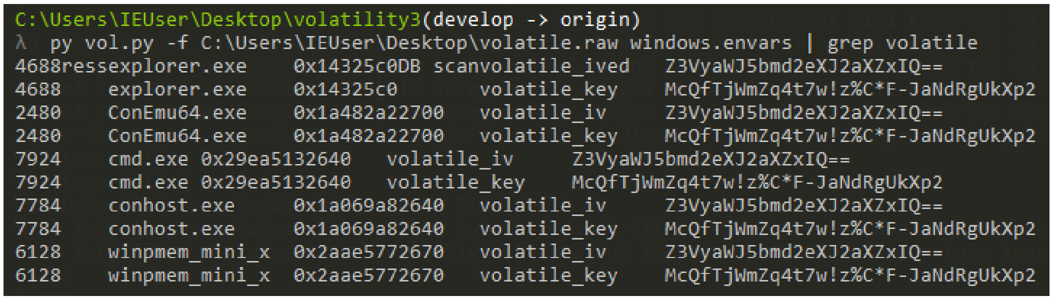
```
C:\Users\IEUser\Desktop\output
λ strings pid.1932.dmp | grep flag
WCSC_HackaBull23{7a2e1f5d4a8463c65156c6f1d9e325db6a63d3c67417ece3737a16e1a008a45cb9d8c0ce3851649c2f9997e125f040f1} Oh no! The WCSC_HackaBull23 flag is encrypted :). Maybe the environment will know the volatile key!  Do you know the wae? C
yberchef knows the wAES, trust it! Also try to rotate the IV!
```

***Figure 2.3** – Encrypted flag with hints.*

WCSC_HackaBull23{7a2e1f5d4a8463c65156c6f1d9e325db6a63d3c67417ece3737a16e1a008a45cb9d8c0ce3851649c2f9997e125f040f1} Oh no! The WCSC_HackaBull23 flag is encrypted :). Maybe the environment will know the volatile key! Do you know the wae? Cyberchef knows the wAES, trust it! Also try to rotate the IV!

The message hinted that the environment may know the key and the IV used in the encryption. Additionally, combining the previously discovered text files, the analyst identified that the flag was encrypted using AES (aes_then_base64) and that the IV should be "rotated" (base64_then_rot13).

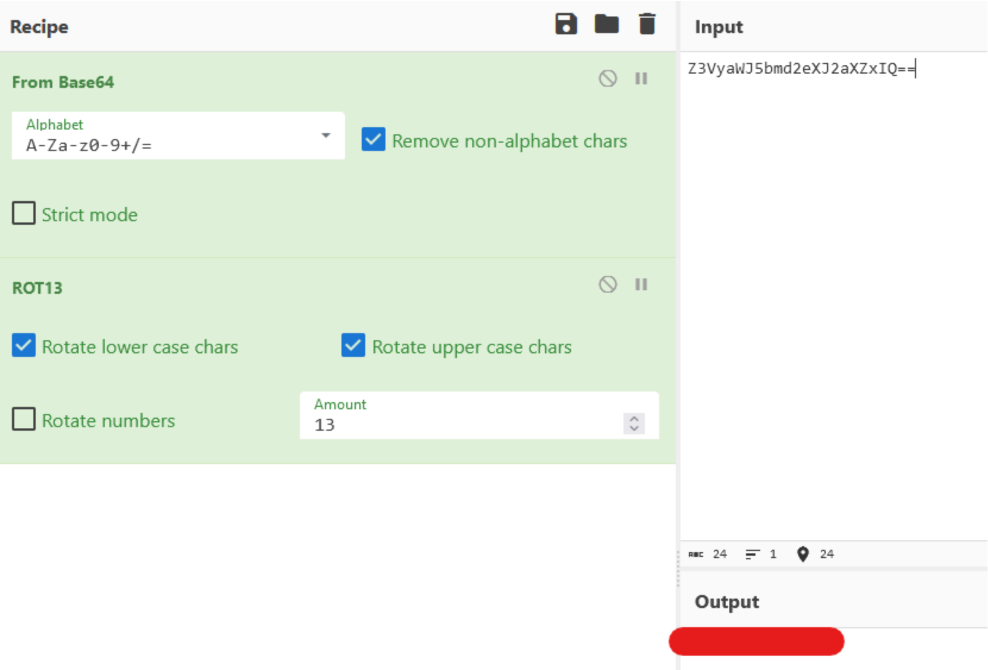
The investigator attempted to find the IV before decrypting the flag. This was achieved with the **windows.envars** plugin. They also tried sorting the data using the "volatile" keyword using **grep**. The results revealed both the key and the IV. (**Figure 2.4**)



```
C:\Users\IEUser\Desktop\volatility3(develop -> origin)
λ  py vol.py -f C:\Users\IEUser\Desktop\volatile.raw windows.envars | grep volatile
4688ressexplorer.exe    0x14325c0DB scanvolatile_ived   Z3VyaWJ5bmd2eXJ2aXZxIQ==
4688    explorer.exe    0x14325c0       volatile_key    McQfTjWmZq4t7w!z%C*F-JaNdRgUkXp2
2480    ConEmu64.exe    0x1a482a22700   volatile_iv     Z3VyaWJ5bmd2eXJ2aXZxIQ==
2480    ConEmu64.exe    0x1a482a22700   volatile_key    McQfTjWmZq4t7w!z%C*F-JaNdRgUkXp2
7924    cmd.exe 0x29ea5132640   volatile_iv     Z3VyaWJ5bmd2eXJ2aXZxIQ==
7924    cmd.exe 0x29ea5132640   volatile_key    McQfTjWmZq4t7w!z%C*F-JaNdRgUkXp2
7784    conhost.exe     0x1a069a82640   volatile_iv     Z3VyaWJ5bmd2eXJ2aXZxIQ==
7784    conhost.exe     0x1a069a82640   volatile_key    McQfTjWmZq4t7w!z%C*F-JaNdRgUkXp2
6128    winpmem_mini_x  0x2aae5772670   volatile_iv     Z3VyaWJ5bmd2eXJ2aXZxIQ==
6128    winpmem_mini_x  0x2aae5772670   volatile_key    McQfTjWmZq4t7w!z%C*F-JaNdRgUkXp2
```

***Figure 2.4** – Key and IV hidden as environmental variables.*

With the obtained data, the analyst opened CyberChef and attempted to decrypt the flag. The decryption process can be seen in the figures below:



From Base64

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

☑ Remove non-alphabet chars

☐ Strict mode

ROT13

☑ Rotate lower case chars

☑ Rotate upper case chars

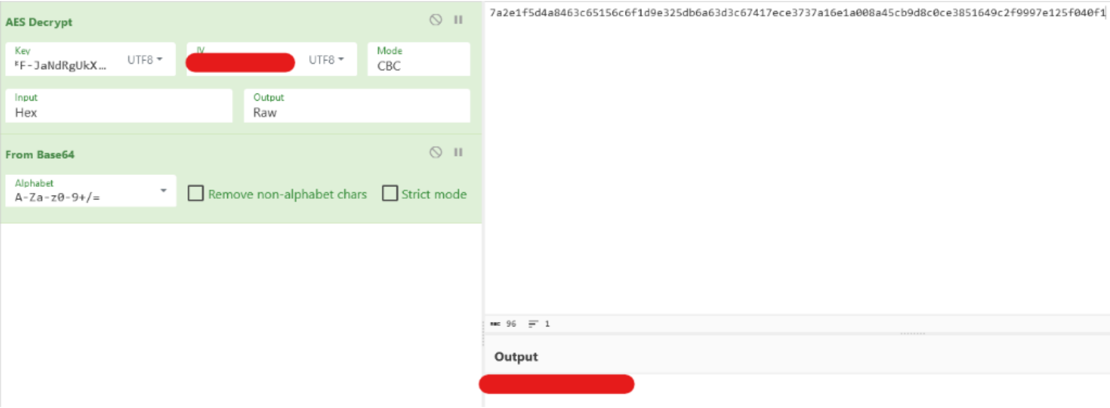
☐ Rotate numbers

Amount: 13

```
Z3VyaWJ5bmd2eXJ2aXZxIQ==
```

[redacted]

Figure 2.5 *– Decoding the IV.*



AES Decrypt

Key: F-JaNdRgUkX… UTF8

IV: [redacted] UTF8

Mode: CBC

Input: Hex

Output: Raw

From Base64

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

☐ Remove non-alphabet chars

☐ Strict mode

```
7a2e1f5d4a8463c65156c6f1d9e325db6a63d3c67417ece3737a16e1a008a45cb9d8c0ce3851649c2f9997e125f040f1
```

[redacted]

Figure 2.6 *– Decrypting the flag.*

3 Appendices

Appendix A

```
Volatility 3 Framework 2.4.1

PID     Process         Args

4       System  Required memory at 0x20 is not valid (process exited?)
136     Registry        Required memory at 0x20 is not valid (process exited?)
360     smss.exe        Required memory at 0xb94c1ef020 is inaccessible (swapped)
452     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1
ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off
MaxRequestThreads=16
528     wininit.exe     Required memory at 0xd87ebb3020 is inaccessible (swapped)
544     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1
ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off
MaxRequestThreads=16
628     winlogon.exe    winlogon.exe
672     services.exe    C:\Windows\system32\services.exe
680     lsass.exe       C:\Windows\system32\lsass.exe
816     svchost.exe     Required memory at 0x222c18038b8 is inaccessible (swapped)
840     fontdrvhost.ex  Required memory at 0x6621951020 is inaccessible (swapped)
848     fontdrvhost.ex  Required memory at 0x16b1eb11fe8 is inaccessible (swapped)
856     svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch -p
956     svchost.exe     C:\Windows\system32\svchost.exe -k RPCSS -p
1008    svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
408     dwm.exe         "dwm.exe"
836     svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s
lmhosts
1048    svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s
NcbService
1056    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s
TimeBrokerSvc
1164    svchost.exe     Required memory at 0x25bf5603938 is inaccessible (swapped)
1204    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
1288    svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s
EventLog
1376    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
1468    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
1496    VBoxService.ex          C:\Windows\System32\VBoxService.exe
1532    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s UserManager
1540    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s
Dhcp
1664    svchost.exe     C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s
SysMain
1680    svchost.exe     Required memory at 0x2657de038b8 is inaccessible (swapped)
```

```
1696    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
1780    svchost.exe     C:\Windows\System32\svchost.exe -k NetworkService -p -s NlaSvc
1808    MemCompression          Required memory at 0x20 is not valid (process exited?)
1896    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
1960    svchost.exe     Required memory at 0x1ebcb8038b8 is inaccessible (swapped)
1968    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s FontCache
1976    svchost.exe     C:\Windows\System32\svchost.exe -k LocalService -p -s netprofm
1636    svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
2072    svchost.exe     C:\Windows\system32\svchost.exe -k NetworkService -p -s Dnscache
2088    svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
2096    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
2164    svchost.exe     C:\Windows\System32\svchost.exe -k netsvcs -p -s ShellHWDetection
2228    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s
WinHttpAutoProxySvc
2360    spoolsv.exe     C:\Windows\System32\spoolsv.exe
2408    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
2444    svchost.exe     Required memory at 0x1c1d9c03938 is inaccessible (swapped)
2532    svchost.exe     Required memory at 0x20138e038b8 is inaccessible (swapped)
2540    svchost.exe     C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted -p -
s PolicyAgent
2676    ruby.exe        "C:\Program Files\Puppet Labs\Puppet\sys\ruby\bin\ruby.exe" -rubygems
"C:\Program Files\Puppet Labs\Puppet\service\daemon.rb"
2684    svchost.exe     C:\Windows\system32\svchost.exe -k NetworkService -p -s CryptSvc
2692    svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNoNetwork -p -s DPS
2700    svchost.exe     Required memory at 0x176ff8038b8 is inaccessible (swapped)
2708    wlms.exe        C:\Windows\system32\wlms\wlms.exe
2716    svchost.exe     Required memory at 0x1ef96803938 is inaccessible (swapped)
2724    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s Winmgmt
2732    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s WpnService
2784    OfficeClickToR  "C:\Program Files\Common Files\Microsoft
Shared\ClickToRun\OfficeClickToRun.exe" /service
2896    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s LanmanServer
2928    svchost.exe     C:\Windows\System32\svchost.exe -k NetSvcs -p -s iphlpsvc
3016    svchost.exe     Required memory at 0x1e1b3403938 is inaccessible (swapped)
3056    svchost.exe     C:\Windows\System32\svchost.exe -k netsvcs
4000    sihost.exe      sihost.exe
4028    svchost.exe     C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc
4068    svchost.exe     C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s WpnUserService
3684    taskhostw.exe   taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}
1036    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s TokenBroker
2188    svchost.exe     C:\Windows\system32\svchost.exe -k appmodel -p -s StateRepository
4168    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s CDPSvc
4292    svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s
TabletInputService
4336    ctfmon.exe      "ctfmon.exe"
4652    userinit.exe    Required memory at 0x422e23b020 is not valid (process exited?)
4688    explorer.exe    C:\Windows\Explorer.EXE
4848    svchost.exe     C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p -s cbdhsvc
5056    SearchIndexer.  C:\Windows\system32\SearchIndexer.exe /Embedding
```

```
4284    ShellExperienc Required memory at 0x203ce403f18 is inaccessible (swapped)
5148    SearchUI.exe   Required memory at 0x198e0e03ec8 is inaccessible (swapped)
5328    RuntimeBroker.         C:\Windows\System32\RuntimeBroker.exe -Embedding
5364    RuntimeBroker.         C:\Windows\System32\RuntimeBroker.exe -Embedding
5756    dllhost.exe    C:\Windows\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-
104DBCD66683}
6064    RuntimeBroker.         C:\Windows\System32\RuntimeBroker.exe -Embedding
3680    dllhost.exe    C:\Windows\system32\DllHost.exe /Processid:{973D20D7-562D-44B9-B70B-
5A0F49CCDF3F}
6336    VBoxTray.exe   "C:\Windows\System32\VBoxTray.exe"
6544    Teams.exe      Required memory at 0x7852d0a020 is not valid (process exited?)
7012    svchost.exe    C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
6300    cmd.exe        Required memory at 0x7357979020 is inaccessible (swapped)
3672    conhost.exe    \??\C:\Windows\system32\conhost.exe 0x4
6796    svchost.exe    C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s
PcaSvc
916     svchost.exe    C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p -s
SSDPSRV
5464    svchost.exe    C:\Windows\System32\svchost.exe -k NetworkService -p -s DoSvc
760     svchost.exe    C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s
StorSvc
4908    SgrmBroker.exe         C:\Windows\system32\SgrmBroker.exe
1092    svchost.exe    C:\Windows\system32\svchost.exe -k netsvcs -p -s UsoSvc
4176    cmd.exe        Required memory at 0x1f6275320a8 is inaccessible (swapped)
6548    conhost.exe    Required memory at 0x1dc495d20a8 is inaccessible (swapped)
2812    svchost.exe    C:\Windows\System32\svchost.exe -k NetworkService -p -s WinRM
6016    svchost.exe    C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s
wscsvc
4304    svchost.exe    C:\Windows\system32\svchost.exe -k UnistackSvcGroup
5068    svchost.exe    Required memory at 0x5be1799020 is not valid (process exited?)
2960    WindowsInterna         Required memory at 0xbda70f1020 is inaccessible (swapped)
5516    SecurityHealth C:\Windows\system32\SecurityHealthService.exe
4608    svchost.exe    C:\Windows\system32\svchost.exe -k LocalService -p -s fdPHost
2424    svchost.exe    C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p -s
FDResPub
1524    svchost.exe    C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s
Netman
1528    dllhost.exe    C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-
B78D-A8F59079A8D5}
2428    svchost.exe    C:\Windows\system32\svchost.exe -k LocalService -s W32Time
3928    ApplicationFra C:\Windows\system32\ApplicationFrameHost.exe -Embedding
640     MicrosoftEdge. Required memory at 0x28af2f6020 is not valid (process exited?)
5680    svchost.exe    C:\Windows\system32\svchost.exe -k LocalService -p -s BthAvctpSvc
3036    svchost.exe    C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
3528    dllhost.exe    C:\Windows\system32\DllHost.exe /Processid:{3AD05575-8857-4850-9277-
11B85BDB8E09}
5444    SearchProtocol"C:\Windows\system32\SearchProtocolHost.exe"
Global\UsGthrFltPipeMssGthrPipe5_ Global\UsGthrCtrlFltPipeMssGthrPipe5 1 -2147483646
```

```
"Software\Microsoft\Windows Search" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT; MS Search
4.0 Robot)" "C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc" "DownLevelDaemon"
5872    GoogleUpdate.e          Required memory at 0x9e20a8 is inaccessible (swapped)
5072    OneDriveStanda          "C:\Program Files (x86)\Microsoft
OneDrive\OneDriveStandaloneUpdater.exe"
6108    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s wuauserv
6028    svchost.exe     C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
1932    gvim.exe        "C:\Program Files (x86)\Vim\vim81\gvim.exe" --literal
"C:\Users\IEUser\Desktop\s@credt3xt"
2792    PDFStreamDumpe          "C:\PDFStreamDumper\PDFStreamDumper.exe"
6284    Wireshark.exe  "C:\Program Files\Wireshark\Wireshark.exe"
1412    dumpcap.exe    Required memory at 0xeae3090020 is not valid (process exited?)
5936    dumpcap.exe    "C:\Program Files\Wireshark\dumpcap.exe" -S -Z 6284.dummy
6720    conhost.exe     \??\C:\Windows\system32\conhost.exe 0x4
1660    autopsy64.exe "C:\Program Files\Autopsy-4.18.0\bin\autopsy64.exe"
412     notepad.exe     "C:\Windows\system32\NOTEPAD.EXE"
C:\Users\IEUser\Desktop\not_here.txt
4696    cmd.exe         Required memory at 0xd70718b020 is not valid (process exited?)
400     conhost.exe     \??\C:\Windows\system32\conhost.exe 0x4
1512    java.exe        "C:\Program Files\Autopsy-4.18.0\jre\bin\java.exe"  -server -Xmx2048m -
Duser.timezone=UTC -XX:+UseG1GC     -XX:+PerfDisableSharedMem     -
XX:+ParallelRefProcEnabled     -XX:MaxGCPauseMillis=250     -XX:+UseLargePages     -
XX:+AlwaysPreTouch -verbose:gc      -XX:+PrintHeapAtGC      -XX:+PrintGCDetails      -
XX:+PrintGCDateStamps      -XX:+PrintGCTimeStamps      -XX:+PrintTenuringDistribution      -
XX:+PrintGCApplicationStoppedTime "-
Xloggc:C:\Users\IEUser\AppData\Roaming\autopsy\var\log\solr\solr_gc.log" -
XX:+UseGCLogFileRotation -XX:NumberOfGCLogFiles=9 -XX:GCLogFileSize=20M -Xss256k  -
Dbootstrap_confdir=../solr/configsets/AutopsyConfig/conf -Dcollection.configName=AutopsyConfig -
Dsolr.default.confdir=../solr/configsets/AutopsyConfig/conf  -
Dsolr.log.dir="C:\Users\IEUser\AppData\Roaming\autopsy\var\log\solr"     -
Dlog4j.configurationFile="file:///C:\Program Files\Autopsy-
4.18.0\autopsy\solr\server\resources\log4j2.xml" -DSTOP.PORT=8079 -DSTOP.KEY=jjk#09s     -
Dsolr.log.muteconsole     -Dsolr.solr.home="C:\Users\IEUser\AppData\Roaming\autopsy\solr" -
Dsolr.install.dir="C:\Program Files\Autopsy-4.18.0\autopsy\solr" -Dsolr.default.confdir="C:\Program
Files\Autopsy-4.18.0\autopsy\solr\server\solr\configsets\_default\conf"     -Djetty.host=0.0.0.0 -
Djetty.port=23232 -Djetty.home="C:\Program Files\Autopsy-4.18.0\autopsy\solr\server"     -
Djava.io.tmpdir="C:\Users\IEUser\AppData\Roaming\autopsy\var\log\solr\tmp" -jar start.jar --
module=http ""
3308    chrome.exe      "C:\Program Files\Google\Chrome\Application\chrome.exe"
6936    chrome.exe      "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=crashpad-
handler "--user-data-dir=C:\Users\IEUser\AppData\Local\Google\Chrome\User Data" /prefetch:7 --
monitor-self-annotation=ptype=crashpad-handler "--
database=C:\Users\IEUser\AppData\Local\Google\Chrome\User Data\Crashpad" --
url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win64 --
annotation=prod=Chrome --annotation=ver=110.0.5481.104 --initial-client-
data=0xdc,0xe0,0xe4,0xb8,0xe8,0x7ffc3162ab58,0x7ffc3162ab68,0x7ffc3162ab78
3956    chrome.exe      "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=gpu-
process --gpu-
preferences=UAAAAAAAAADgAAAYAAAAAAAAAAAAAAAAAABgAAAAAAAwAAAAAAAAAAAAA
```

```
AQAAAAAAAAAAAAAAAAAAAAAAAAAEgAAAAAAAAASAAAAAAAAAAYAAAAAgAAABAAAAAA
AAAAGAAAAAAAAAAQAAAAAAAAAAAAAAAOAAAAEAAAAAAAAAABAAAADgAAAAgAAAAAAA
AACAAAAAAAAAA= --mojo-platform-channel-handle=1812 --field-trial-
handle=1924,i,6473459410547971157,15783263393177205349,131072 /prefetch:2
1744    chrome.exe      "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --
utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-
platform-channel-handle=2264 --field-trial-
handle=1924,i,6473459410547971157,15783263393177205349,131072 /prefetch:8
6276    chrome.exe      "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --
utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --
mojo-platform-channel-handle=2332 --field-trial-
handle=1924,i,6473459410547971157,15783263393177205349,131072 /prefetch:8
5708    chrome.exe      "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer -
-first-renderer-process --lang=en-US --device-scale-factor=1 --num-raster-threads=4 --enable-main-
frame-before-activation --renderer-client-id=6 --time-ticks-at-unix-epoch=-1679440730578448 --
launch-time-ticks=2175230828 --mojo-platform-channel-handle=3136 --field-trial-
handle=1924,i,6473459410547971157,15783263393177205349,131072 /prefetch:1
5572    chrome.exe      "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer -
-lang=en-US --device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-before-activation -
-renderer-client-id=5 --time-ticks-at-unix-epoch=-1679440730578448 --launch-time-
ticks=2175240784 --mojo-platform-channel-handle=3144 --field-trial-
handle=1924,i,6473459410547971157,15783263393177205349,131072 /prefetch:1
4604    chrome.exe      "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer -
-disable-gpu-compositing --lang=en-US --device-scale-factor=1 --num-raster-threads=4 --enable-
main-frame-before-activation --renderer-client-id=7 --time-ticks-at-unix-epoch=-1679440730578448 -
-launch-time-ticks=2175554658 --mojo-platform-channel-handle=4340 --field-trial-
handle=1924,i,6473459410547971157,15783263393177205349,131072 /prefetch:1
6200    notepad.exe     "C:\Windows\system32\NOTEPAD.EXE"
C:\Users\IEUser\Desktop\definite_not_here.txt
1880    x32dbg.exe      "C:\Program Files\x64dbg\release\x32\x32dbg.exe"
1504    cutter.exe      "C:\ProgramData\chocolatey\lib\cutter.flare\tools\cutter\cutter.exe"
6220    conhost.exe     \??\C:\Windows\system32\conhost.exe 0x4
6856    HxD.exe         "C:\Program Files\HxD\HxD.exe"
6600    ida64.exe       "C:\Program Files\IDA Freeware 7.0\ida64.exe"
5844    notepad++.exe "C:\Program Files\Notepad++\notepad++.exe"
"C:\Users\IEUser\Desktop\base64_then_rot13"
6472    svchost.exe     C:\Windows\system32\svchost.exe -k appmodel -p -s camsvc
2112    MicrosoftEdge. Required memory at 0x18e20c03eb8 is inaccessible (swapped)
7204    browser_broker          C:\Windows\system32\browser_broker.exe -Embedding
7284    svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
7440    RuntimeBroker.          C:\Windows\System32\RuntimeBroker.exe -Embedding
7512    MicrosoftEdgeS          Required memory at 0x9bf501020 is inaccessible (swapped)
7520    svchost.exe     C:\Windows\system32\svchost.exe -k wsappx -p -s AppXSvc
7576    MicrosoftEdgeC          Required memory at 0x29c68603ee8 is inaccessible (swapped)
7756    Windows.WARP.J          C:\Windows\system32\Windows.WARP.JITService.exe 01c3c47c-
5e53-44bf-865e-3f365cf4fc56 S-1-15-2-3624051433-2125758914-1423191267-1740899205-
1073925389-3782572162-737981194-3513710562-3729412521-1863153555-1462103995 S-1-5-
21-3461203602-4096304019-2269080069-1000 700
```

```
8008    WmiPrvSE.exe Process 8008: Required memory at 0x61006c0000 is not valid (incomplete
layer memory_layer?)
944     MicrosoftEdgeC          Required memory at 0x1b7ef403ee8 is inaccessible (swapped)
1068    Windows.WARP.J          C:\Windows\system32\Windows.WARP.JITService.exe 01c3c47d-
5e53-44bf-865e-3f365cf4fc56 S-1-15-2-3624051433-2125758914-1423191267-1740899205-
1073925389-3782572162-737981194 S-1-5-21-3461203602-4096304019-2269080069-1000 468
7932    Windows.WARP.J          C:\Windows\system32\Windows.WARP.JITService.exe 01c3c47e-
5e53-44bf-865e-3f365cf4fc56 S-1-15-2-3624051433-2125758914-1423191267-1740899205-
1073925389-3782572162-737981194-2385269614-3243675-834220592-3047885450 S-1-5-21-
3461203602-4096304019-2269080069-1000 556
8252    MicrosoftPdfReRequired memory at 0x1ac15e03ee8 is inaccessible (swapped)
8284    SearchFilterHo "C:\Windows\system32\SearchFilterHost.exe" 0 772 776 784 8192 780
8392    Windows.WARP.J          C:\Windows\system32\Windows.WARP.JITService.exe 01c3c47f-
5e53-44bf-865e-3f365cf4fc56 S-1-15-2-3624051433-2125758914-1423191267-1740899205-
1073925389-3782572162-737981194-2385269614-3243675-834220592-3047885450 S-1-5-21-
3461203602-4096304019-2269080069-1000 724
8708    MicrosoftEdgeC          Required memory at 0x9d340da020 is not valid (process exited?)
8844    MicrosoftEdgeC          Required memory at 0xe56084a020 is inaccessible (swapped)
8948    MicrosoftEdgeC          Required memory at 0x894800171194 is not valid (process exited?)
4956    software_repor "C:\Users\IEUser\AppData\Local\Google\Chrome\User
Data\SwReporter\107.294.200\software_reporter_tool.exe" --engine=2 --scan-
locations=1,2,3,4,5,6,7,8,10 --disabled-locations=9,11 --session-
id=aP8c6yEWnCqg+Y1zAvjcxFJdjSxNmoZ6DMYyr5R4 --registry-suffix=ESET
84      software_repor "c:\users\ieuser\appdata\local\google\chrome\user
data\swreporter\107.294.200\software_reporter_tool.exe" --crash-handler "--
database=c:\users\ieuser\appdata\local\Google\Software Reporter Tool" --
url=https://clients2.google.com/cr/report --annotation=plat=Win32 --annotation=prod=ChromeFoil --
annotation=ver=107.294.200 --initial-client-
data=0x278,0x27c,0x280,0x254,0x284,0x7ff77c995960,0x7ff77c995970,0x7ff77c995980
2968    software_repor "c:\users\ieuser\appdata\local\google\chrome\user
data\swreporter\107.294.200\software_reporter_tool.exe" --use-crash-handler-with-
id="\\.\pipe\crashpad_4956_PWSVEMOUDDSVPIJO" --sandboxed-process-id=2 --init-done-
notifier=788 --sandbox-mojo-pipe-token=2949342779102371989 --mojo-platform-channel-
handle=764 --engine=2
9200    software_repor "c:\users\ieuser\appdata\local\google\chrome\user
data\swreporter\107.294.200\software_reporter_tool.exe" --use-crash-handler-with-
id="\\.\pipe\crashpad_4956_PWSVEMOUDDSVPIJO" --sandboxed-process-id=3 --init-done-
notifier=960 --sandbox-mojo-pipe-token=1475416946335677024 --mojo-platform-channel-
handle=964
9028    MicrosoftEdgeC          Required memory at 0x21a12203ee8 is inaccessible (swapped)
5156    notepad.exe     "C:\Windows\system32\NOTEPAD.EXE"
C:\Users\IEUser\Desktop\aes_then_base64
2480    ConEmu64.exe            /Icon "C:\Tools\Cmder\icons\cmder.ico" /Title Cmder
8568    ConEmuC64.exe           "C:\Tools\Cmder\vendor\conemu-
maximus5\ConEmu\ConEmuC64.exe"  /CINMODE=600020 /AID=9204 /GID=2480
/GHWND=000807DC /BW=117 /BH=56 /BZ=1000 "/FN=Lucida Console" /FW=3 /FH=5
/TA=10100007 /HIDE /ROOT cmd /k ""%ConEmuDir%\..\init.bat" "
8552    conhost.exe     \??\C:\Windows\system32\conhost.exe 0x4
7604    cmd.exe         cmd /k ""C:\Tools\Cmder\vendor\conemu-maximus5\..\init.bat" "
```

```
9168    svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s
WdiSystemHost
8432    taskhostw.exe   taskhostw.exe
8912    ILSpy.exe       "C:\ProgramData\chocolatey\lib\ilspy\tools\ILSpy.exe"
7924    cmd.exe         "cmd.exe" /s /k pushd "C:\Users\IEUser\Desktop"
7784    conhost.exe     \??\C:\Windows\system32\conhost.exe 0x4
6128    winpmem_mini_x          winpmem_mini_x64_rc2.exe  volatile.raw
```