School of Computing

[KH5036CMD]

[Digital Forensics]

[Milestone 4: Memory Dump Analysis Report]

[Hala Ahmed Sayed] / [202300277] / [14762750]

Ethical Hacking and Cybersecurity

School of Computing

Coventry University – The Knowledge Hub Universities

[Thursday, 14th of December 2025]

Module ML/ [Haitham Ghalwash]

Module AL(s)/ [Kareem El Debassy]

Contents

Objective

This report aims to portray the technical digital forensics analysis of a raw memory image, highlighting any hidden artifacts found and the tools used. In addition to, it reports the whole analysis, summarizes the investigator's analysis flow, and identifies the hidden data: password and the secret text.

Deliverables

As mentioned previously, this report aims to perform a deep analysis of the given memory image. Therefore, the deliverables of this part (milestone 4) consist of a technical report and two python scripts for specific cryptography usages mentioned thoroughly in the report.

Abstract

This project is a technical based project, where a memory image is taken from a user. The image goes under a strict digital forensics analysis to investigate the hidden data and behavior done on the user's pc. After investigating, a technical, detailed, documentation highlighting cryptographical and stenographical procedures is provided along with the tools, flow, evidence, and methodology used.

Introduction

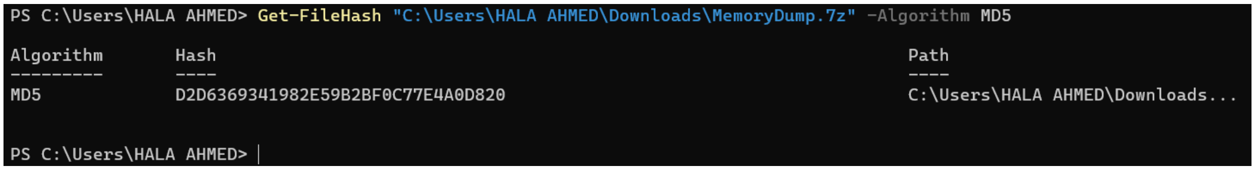
As studied, digital forensics is the process of digitally investigating a specific case to reach an outcome: either for incident response processes or court processes (Badman & Forrest, 2025). Therefore, any suspicious activity leads to a case; where the investigator follows some standard procedures to transform found artifacts into well trusted evidence. Consequently, this project previously tackled the process of a suspicious case, highlighted through the user's suspicious behavior on the pc. In this section, a new forensics aspect is used which is memory analysis. A raw memory image is taken from a user who is assumed to be using cryptography and steganography procedures to hide or make data unreadable. By following the digital forensics procedures, python scripts and the help of forensics tools: volatility and steghide, this report investigates the memory image thoroughly, analyzing multiple areas such as operating system, architecture, processes, network and finally files and decoding.

Part 1: Memory Analysis Tasks and Required Data

• Hash Verification

In this section, the first step taken was to download the memory image folder and verify it. The verification process was done to ensure that no errors or tampering occurred to the image during the downloading process. The MD5 Hash verification process was implemented through power shell using the Get-FileHash command and the algorithm given. The output of the given hash and the PowerShell generated hash was the same, ensuring accuracy; therefore, after verification, the image got extracted highlighting that the given memory image is called MemoryDump with a raw extension and size of 1,023,936KB.

Hash: D2D6369341982E59B2BF0C77E4A0D820

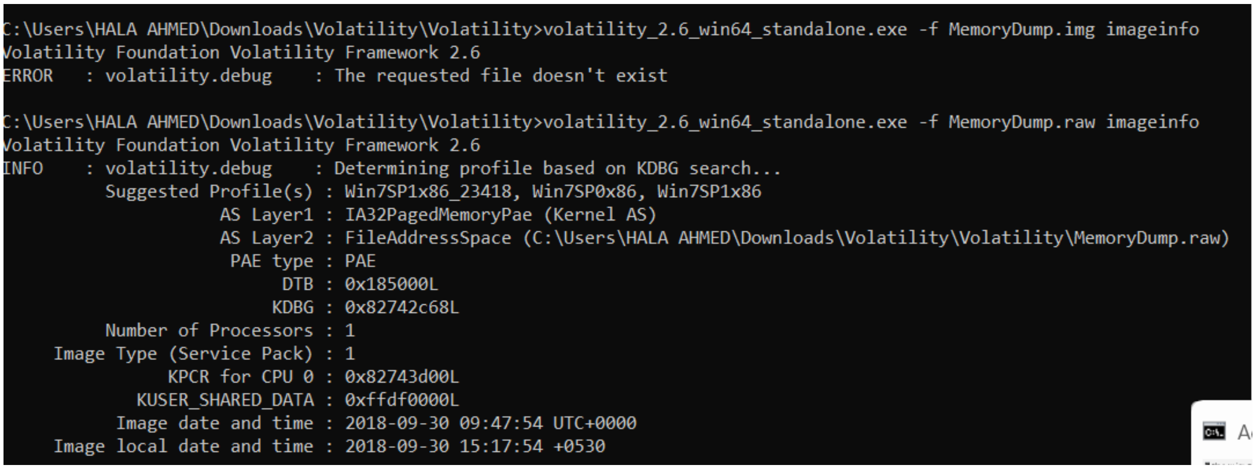


```
PS C:\Users\HALA AHMED> Get-FileHash "C:\Users\HALA AHMED\Downloads\MemoryDump.7z" -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             D2D6369341982E59B2BF0C77E4A0D820                                       C:\Users\HALA AHMED\Downloads...


PS C:\Users\HALA AHMED> |
```

Illustration 1: showcases the matched, verified hashes

• Operating System and Architecture

In this section, volatility was used. Volatility is a memory analysis forensics tool used through the cmd. The volatility folder was downloaded and extracted. The memory image was also downloaded and extracted. The memory dump file was then copied to the volatility folder to ensure a smooth-running process between the memory image and the tool. To know the operating system and architecture, the image info command inside volatility was used. The command extracted the operating system, which is windows 7, the architecture, which is x86, the number of processors which is one and finally the image data and time.



```
C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.img imageinfo
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : The requested file doesn't exist

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\HALA AHMED\Downloads\Volatility\Volatility\MemoryDump.raw)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82742c68L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82743d00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2018-09-30 09:47:54 UTC+0000
     Image local date and time : 2018-09-30 15:17:54 +0530
```

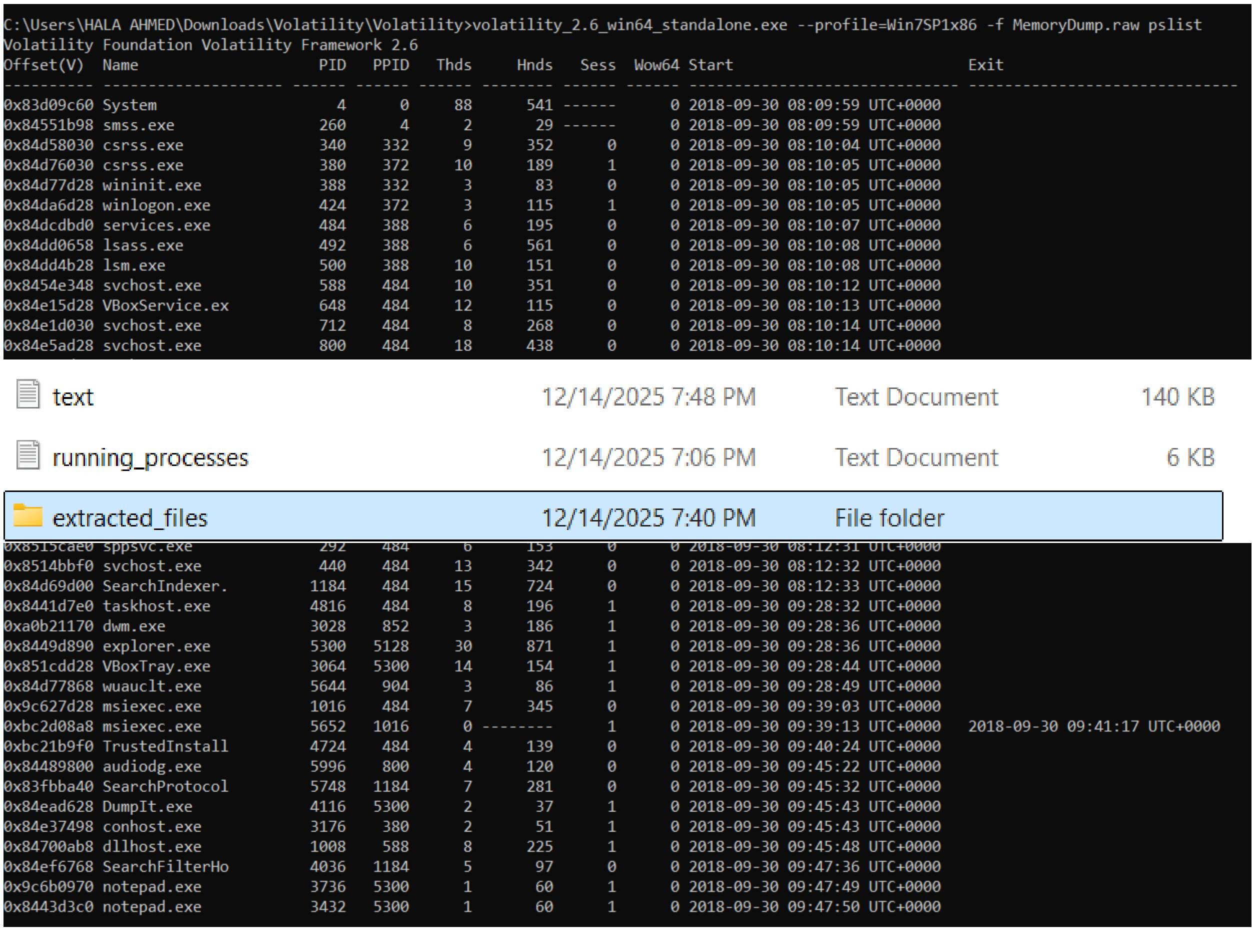
Illustration 2: showcases the imageinfo command output: system information

- Memory Time and User logon info

As mentioned earlier the memory time was already done through the imageinfo. The image date and time was 2018-09-30 09:47:54 and locally 2018-09-30 15:17:54.

- ## Running Processes

The Running Processes were done through the pslist command also through volatility. This command lists all the running processes on the memory image. The output contains two main elements which are the PID and PPID which stands for process ID and Parent process ID.



```
C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe --profile=Win7SP1x86 -f MemoryDump.raw pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x83d09c60 System                    4      0     88      541 ------      0 2018-09-30 08:09:59 UTC+0000
0x84551b98 smss.exe                260      4      2       29 ------      0 2018-09-30 08:09:59 UTC+0000
0x84d58030 csrss.exe               340    332      9      352      0      0 2018-09-30 08:10:04 UTC+0000
0x84d76030 csrss.exe               380    372     10      189      1      0 2018-09-30 08:10:05 UTC+0000
0x84d77d28 wininit.exe             388    332      3       83      0      0 2018-09-30 08:10:05 UTC+0000
0x84da6d28 winlogon.exe            424    372      3      115      1      0 2018-09-30 08:10:05 UTC+0000
0x84dcdbd0 services.exe            484    388      6      195      0      0 2018-09-30 08:10:07 UTC+0000
0x84dd0658 lsass.exe               492    388      6      561      0      0 2018-09-30 08:10:08 UTC+0000
0x84dd4b28 lsm.exe                 500    388     10      151      0      0 2018-09-30 08:10:08 UTC+0000
0x8454e348 svchost.exe             588    484     10      351      0      0 2018-09-30 08:10:12 UTC+0000
0x84e15d28 VBoxService.ex          648    484     12      115      0      0 2018-09-30 08:10:13 UTC+0000
0x84e1d030 svchost.exe             712    484      8      268      0      0 2018-09-30 08:10:14 UTC+0000
0x84e5ad28 svchost.exe             800    484     18      438      0      0 2018-09-30 08:10:14 UTC+0000
```

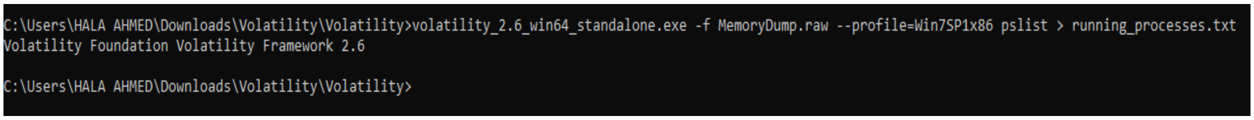
text	12/14/2025 7:48 PM	Text Document	140 KB
running_processes	12/14/2025 7:06 PM	Text Document	6 KB
extracted_files	12/14/2025 7:40 PM	File folder	

```
0x8515cae0 sppsvc.exe              292    484      6      153      0      0 2018-09-30 08:12:31 UTC+0000
0x8514bbf0 svchost.exe             440    484     13      342      0      0 2018-09-30 08:12:32 UTC+0000
0x84d69d00 SearchIndexer.         1184    484     15      724      0      0 2018-09-30 08:12:33 UTC+0000
0x8441d7e0 taskhost.exe           4816    484      8      196      1      0 2018-09-30 09:28:32 UTC+0000
0xa0b21170 dwm.exe                3028    852      3      186      1      0 2018-09-30 09:28:36 UTC+0000
0x8449d890 explorer.exe           5300   5128     30      871      1      0 2018-09-30 09:28:36 UTC+0000
0x851cdd28 VBoxTray.exe           3064   5300     14      154      1      0 2018-09-30 09:28:44 UTC+0000
0x84d77868 wuauclt.exe            5644    904      3       86      1      0 2018-09-30 09:28:49 UTC+0000
0x9c627d28 msiexec.exe            1016    484      7      345      0      0 2018-09-30 09:39:03 UTC+0000
0xbc2d08a8 msiexec.exe            5652   1016      0 --------      1      0 2018-09-30 09:39:13 UTC+0000   2018-09-30 09:41:17 UTC+0000
0xbc21b9f0 TrustedInstall         4724    484      4      139      0      0 2018-09-30 09:40:24 UTC+0000
0x84489800 audiodg.exe            5996    800      4      120      0      0 2018-09-30 09:45:22 UTC+0000
0x83fbba40 SearchProtocol         5748   1184      7      281      0      0 2018-09-30 09:45:32 UTC+0000
0x84ead628 DumpIt.exe             4116   5300      2       37      1      0 2018-09-30 09:45:43 UTC+0000
0x84e37498 conhost.exe            3176    380      2       51      1      0 2018-09-30 09:45:43 UTC+0000
0x84700ab8 dllhost.exe            1008    588      8      225      1      0 2018-09-30 09:45:48 UTC+0000
0x84ef6768 SearchFilterHo         4036   1184      5       97      0      0 2018-09-30 09:47:36 UTC+0000
0x9c6b0970 notepad.exe            3736   5300      1       60      1      0 2018-09-30 09:47:49 UTC+0000
0x8443d3c0 notepad.exe            3432   5300      1       60      1      0 2018-09-30 09:47:50 UTC+0000
```

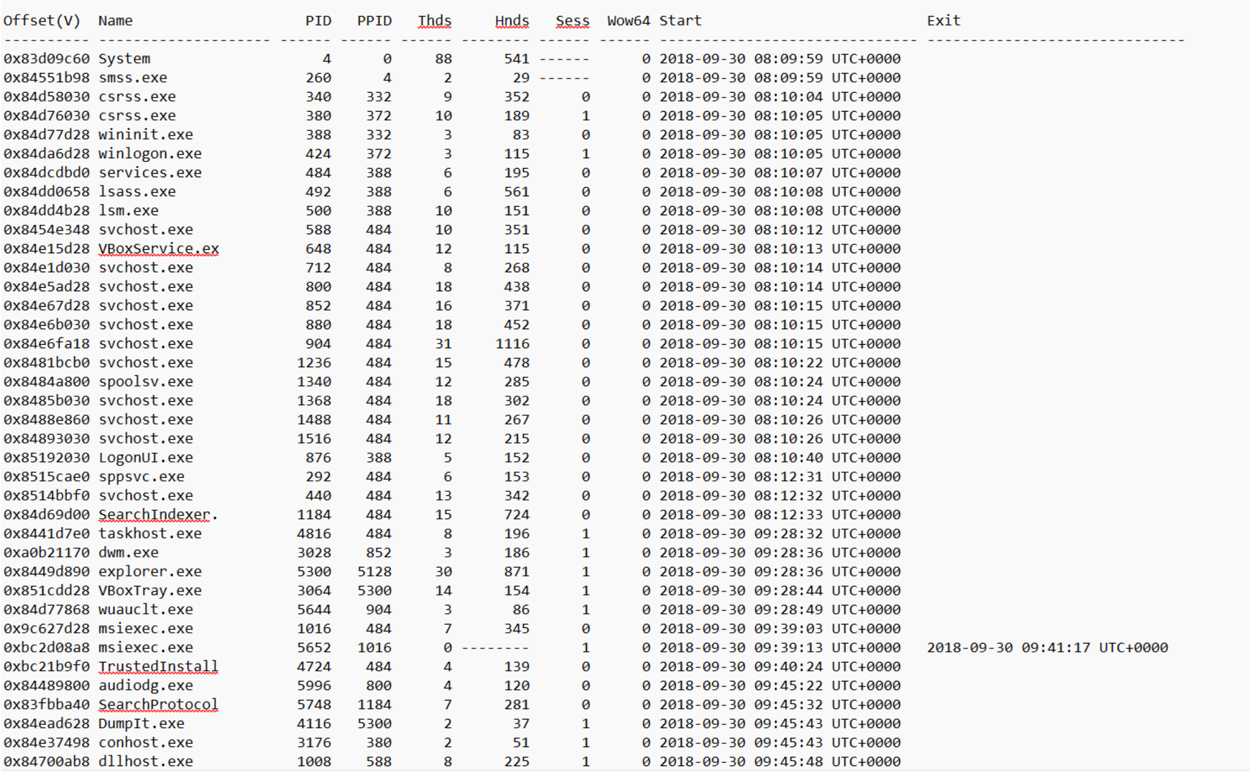
Illustration 4: showcases the running processes on the image

- ## Running Processes File Extraction

As the running processes are a main component of memory analysis, the running processes were extracted on the investigator's disk for future analysis or usages. This was done through the same volatility pslist command however a file with a .txt extension was added to serve as the storage of the processes.



```
C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 pslist > running_processes.txt
Volatility Foundation Volatility Framework 2.6

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>
```



```
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x83d09c60 System                    4      0     88      541 ------      0 2018-09-30 08:09:59 UTC+0000
0x84551b98 smss.exe                260      4      2       29 ------      0 2018-09-30 08:09:59 UTC+0000
0x84d58030 csrss.exe               340    332      9      352      0      0 2018-09-30 08:10:04 UTC+0000
0x84d76030 csrss.exe               380    372     10      189      1      0 2018-09-30 08:10:05 UTC+0000
0x84d77d28 wininit.exe             388    332      3       83      0      0 2018-09-30 08:10:05 UTC+0000
0x84da6d28 winlogon.exe            424    372      3      115      1      0 2018-09-30 08:10:05 UTC+0000
0x84dcdbd0 services.exe            484    388      6      195      0      0 2018-09-30 08:10:07 UTC+0000
0x84dd0658 lsass.exe               492    388      6      561      0      0 2018-09-30 08:10:08 UTC+0000
0x84dd4b28 lsm.exe                 500    388     10      151      0      0 2018-09-30 08:10:08 UTC+0000
0x8454e348 svchost.exe             588    484     10      351      0      0 2018-09-30 08:10:12 UTC+0000
0x84e15d28 VBoxService.ex          648    484     12      115      0      0 2018-09-30 08:10:13 UTC+0000
0x84e1d030 svchost.exe             712    484      8      268      0      0 2018-09-30 08:10:14 UTC+0000
0x84e5ad28 svchost.exe             800    484     18      438      0      0 2018-09-30 08:10:14 UTC+0000
0x84e67d28 svchost.exe             852    484     16      371      0      0 2018-09-30 08:10:15 UTC+0000
0x84e6b030 svchost.exe             880    484     18      452      0      0 2018-09-30 08:10:15 UTC+0000
0x84e6fa18 svchost.exe             904    484     31     1116      0      0 2018-09-30 08:10:15 UTC+0000
0x8481bcb0 svchost.exe            1236    484     15      478      0      0 2018-09-30 08:10:22 UTC+0000
0x8484a800 spoolsv.exe            1340    484     12      285      0      0 2018-09-30 08:10:24 UTC+0000
0x8485b030 svchost.exe            1368    484     18      302      0      0 2018-09-30 08:10:24 UTC+0000
0x8488e860 svchost.exe            1488    484     11      267      0      0 2018-09-30 08:10:26 UTC+0000
0x84893030 svchost.exe            1516    484     12      215      0      0 2018-09-30 08:10:26 UTC+0000
0x85192030 LogonUI.exe             876    388      5      152      0      0 2018-09-30 08:10:40 UTC+0000
0x8515cae0 sppsvc.exe              292    484      6      153      0      0 2018-09-30 08:12:31 UTC+0000
0x8514bbf0 svchost.exe             440    484     13      342      0      0 2018-09-30 08:12:32 UTC+0000
0x84d69d00 SearchIndexer.         1184    484     15      724      0      0 2018-09-30 08:12:33 UTC+0000
0x8441d7e0 taskhost.exe           4816    484      8      196      1      0 2018-09-30 09:28:32 UTC+0000
0xa0b21170 dwm.exe                3028    852      3      186      1      0 2018-09-30 09:28:36 UTC+0000
0x8449d890 explorer.exe           5300   5128     30      871      1      0 2018-09-30 09:28:36 UTC+0000
0x851cdd28 VBoxTray.exe           3064   5300     14      154      1      0 2018-09-30 09:28:44 UTC+0000
0x84d77868 wuauclt.exe            5644    904      3       86      1      0 2018-09-30 09:28:49 UTC+0000
0x9c627d28 msiexec.exe            1016    484      7      345      0      0 2018-09-30 09:39:03 UTC+0000
0xbc2d08a8 msiexec.exe            5652   1016      0 --------      1      0 2018-09-30 09:39:13 UTC+0000   2018-09-30 09:41:17 UTC+0000
0xbc21b9f0 TrustedInstall         4724    484      4      139      0      0 2018-09-30 09:40:24 UTC+0000
0x84489800 audiodg.exe            5996    800      4      120      0      0 2018-09-30 09:45:22 UTC+0000
0x83fbba40 SearchProtocol         5748   1184      7      281      0      0 2018-09-30 09:45:32 UTC+0000
0x84ead628 DumpIt.exe             4116   5300      2       37      1      0 2018-09-30 09:45:43 UTC+0000
0x84e37498 conhost.exe            3176    380      2       51      1      0 2018-09-30 09:45:43 UTC+0000
0x84700ab8 dllhost.exe            1008    588      8      225      1      0 2018-09-30 09:45:48 UTC+0000
```

<u>Illustration 5,6:</u> showcases the running processes extraction process

- Memory Acquisition tool

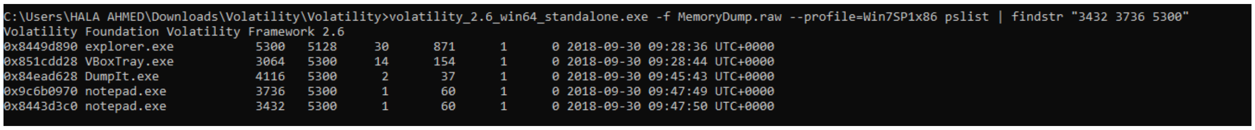
  As highlighted through the running processes, Dump.it with a process id of 4116 and ppid of 5300 was used for the memory acquisition method.

- Processes 3432, 3736 and 5300

3432: notepad

3736: notepad

5300: explorer.exe

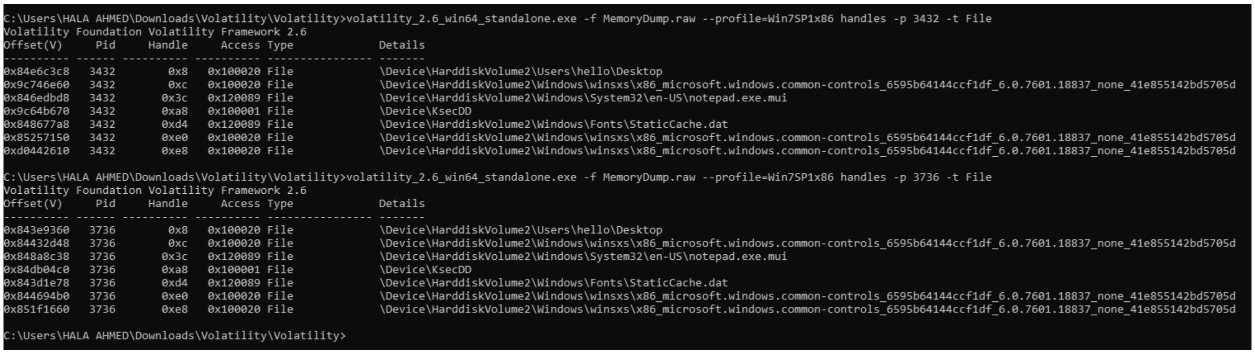


```
C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 pslist | findstr "3432 3736 5300"
Volatility Foundation Volatility Framework 2.6
0x8449d890 explorer.exe           5300   5128     30      871      1      0 2018-09-30 09:28:36 UTC+0000
0x851cdd28 VBoxTray.exe           3064   5300     14      154      1      0 2018-09-30 09:28:44 UTC+0000
0x84ead628 DumpIt.exe             4116   5300      2       37      1      0 2018-09-30 09:45:43 UTC+0000
0x9c6b0970 notepad.exe            3736   5300      1       60      1      0 2018-09-30 09:47:49 UTC+0000
0x8443d3c0 notepad.exe            3432   5300      1       60      1      0 2018-09-30 09:47:50 UTC+0000
```

Illustration 7*:* showcases the processes with their PID, PPID and date and time

The 3xxx processes are notepad processes, indicating .txt files. The 5300 file is an explorer.exe file which is a browser. Regardless of the app's differences, the notepad processes have the parent processes id of the browser which means the browser opened it. Moreover, the dumpit.exe is also launched from the browser but before the opening of the notepad files. Therefore, it is almost concluded that the browser was opened, dumpit got downloaded and the notepad files contains the taken data.

In addition to, processes 3432 and 3736 were used to open certain files. Therefore, the volatility tool was used to identify the opened files through the processes ID. In each process ID, it was found that notepad , static cache and other multiple files were all opened through these process.

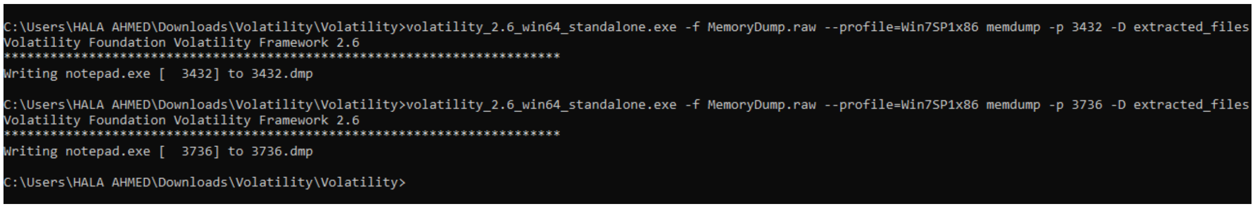


```
C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 handles -p 3432 -t File
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0x84e6c3c8   3432        0x8   0x100020 File             \Device\HarddiskVolume2\Users\hello\Desktop
0x9c746e60   3432        0xc   0x100020 File             \Device\HarddiskVolume2\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d
0x846edbd8   3432       0x3c   0x120089 File             \Device\HarddiskVolume2\Windows\System32\en-US\notepad.exe.mui
0x9c64b670   3432       0xa8   0x100001 File             \Device\KsecDD
0x848677a8   3432       0xd4   0x120089 File             \Device\HarddiskVolume2\Windows\Fonts\StaticCache.dat
0x85257150   3432       0xe0   0x100020 File             \Device\HarddiskVolume2\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d
0xd0442610   3432       0xe8   0x100020 File             \Device\HarddiskVolume2\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 handles -p 3736 -t File
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0x843e9360   3736        0x8   0x100020 File             \Device\HarddiskVolume2\Users\hello\Desktop
0x84432d48   3736        0xc   0x100020 File             \Device\HarddiskVolume2\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d
0x848a8c38   3736       0x3c   0x120089 File             \Device\HarddiskVolume2\Windows\System32\en-US\notepad.exe.mui
0x84db04c0   3736       0xa8   0x100001 File             \Device\KsecDD
0x843d1e78   3736       0xd4   0x120089 File             \Device\HarddiskVolume2\Windows\Fonts\StaticCache.dat
0x844694b0   3736       0xe0   0x100020 File             \Device\HarddiskVolume2\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d
0x851f1660   3736       0xe8   0x100020 File             \Device\HarddiskVolume2\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>
```

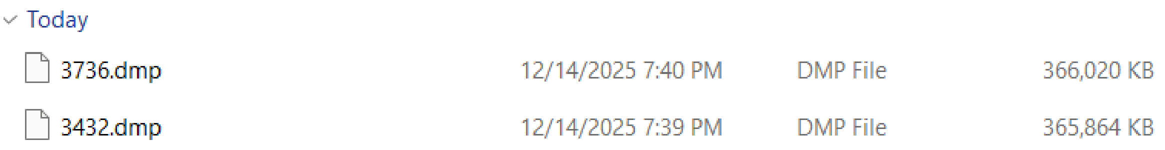
Illustration 8*:* showcases the processes open files

Files Extraction:

In this step, volatility was also used to extract the files found opened by the processes. These files were not opening on my disk even when exported. This is because their extension and the concept of having a huge part of a memory.



```
C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 memdump -p 3432 -D extracted_files
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing notepad.exe [  3432] to 3432.dmp

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 memdump -p 3736 -D extracted_files
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing notepad.exe [  3736] to 3736.dmp

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>
```

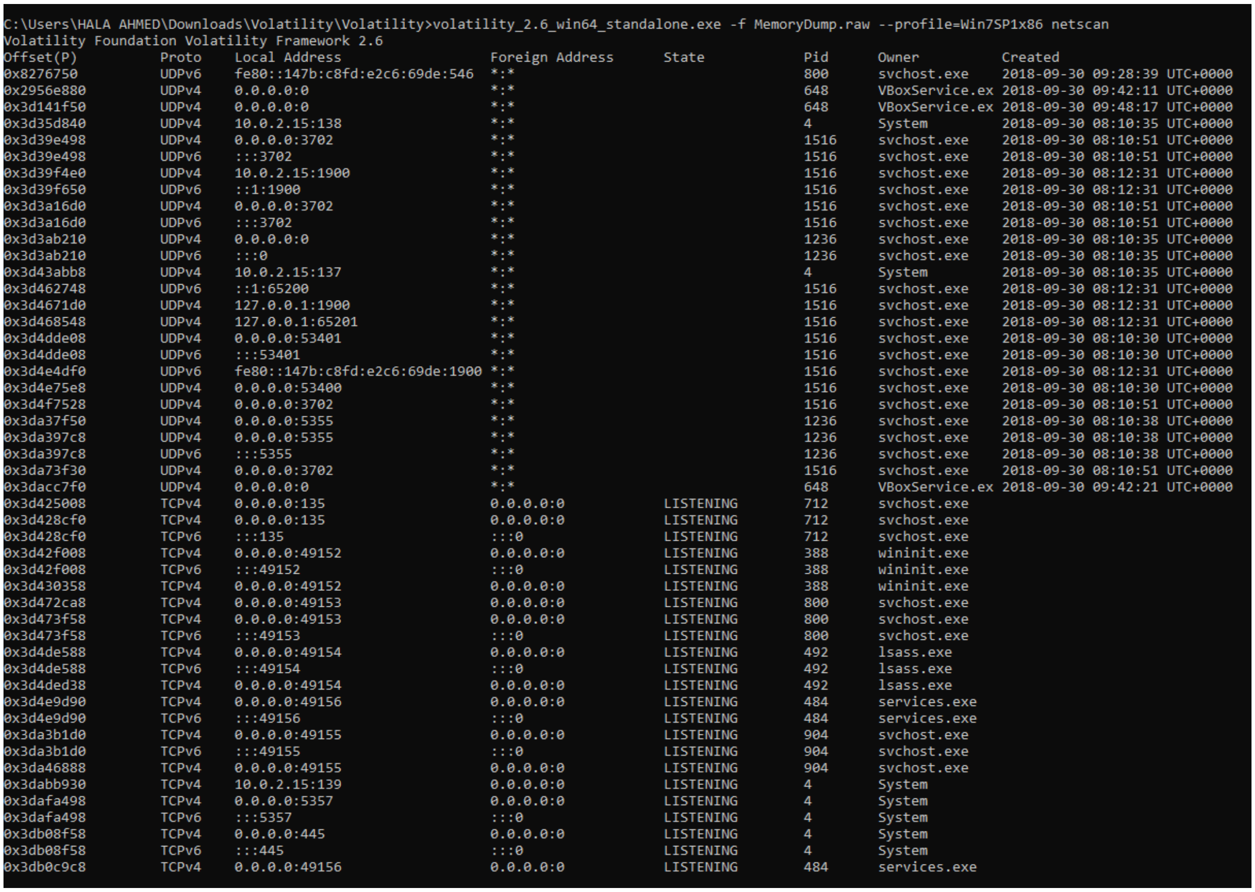


3736.dmp	12/14/2025 7:40 PM	DMP File	366,020 KB
3432.dmp	12/14/2025 7:39 PM	DMP File	365,864 KB

Illustration 9,10*:* showcases the files extraction processes

- ### Network Connections and Machine’s IP

As mentioned previously, explorer.exe was used which indicates that network connections occurred. Therefore, a small network analysis was done. As expected, there were internet and networks connections as highlighted below through the netscan command done through volatility, highlighting the Ip machine of the memory acquired: 10.0.2.15**.**



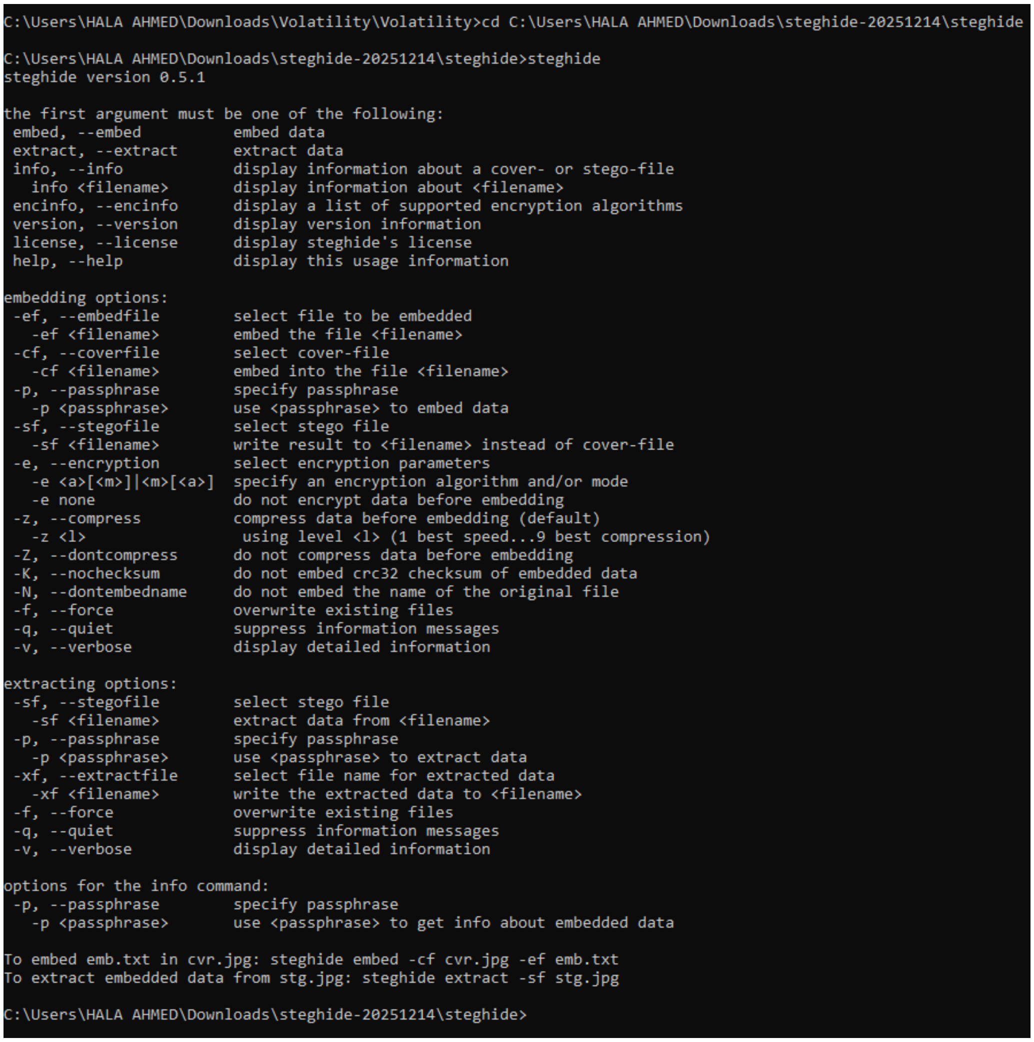
```
C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x8276750          UDPv6    fe80::147b:c8fd:e2c6:69de:546  *:*                                   800      svchost.exe    2018-09-30 09:28:39 UTC+0000
0x2956e880         UDPv4    0.0.0.0:0                      *:*                                   648      VBoxService.ex 2018-09-30 09:42:11 UTC+0000
0x3d141f50         UDPv4    0.0.0.0:0                      *:*                                   648      VBoxService.ex 2018-09-30 09:48:17 UTC+0000
0x3d35d840         UDPv4    10.0.2.15:138                  *:*                                   4        System         2018-09-30 08:10:35 UTC+0000
0x3d39e498         UDPv4    0.0.0.0:3702                   *:*                                   1516     svchost.exe    2018-09-30 08:10:51 UTC+0000
0x3d39e498         UDPv6    :::3702                        *:*                                   1516     svchost.exe    2018-09-30 08:10:51 UTC+0000
0x3d39f4e0         UDPv4    10.0.2.15:1900                 *:*                                   1516     svchost.exe    2018-09-30 08:12:31 UTC+0000
0x3d39f650         UDPv6    ::1:1900                       *:*                                   1516     svchost.exe    2018-09-30 08:12:31 UTC+0000
0x3d3a16d0         UDPv4    0.0.0.0:3702                   *:*                                   1516     svchost.exe    2018-09-30 08:10:51 UTC+0000
0x3d3a16d0         UDPv6    :::3702                        *:*                                   1516     svchost.exe    2018-09-30 08:10:51 UTC+0000
0x3d3ab210         UDPv4    0.0.0.0:0                      *:*                                   1236     svchost.exe    2018-09-30 08:10:35 UTC+0000
0x3d3ab210         UDPv6    :::0                           *:*                                   1236     svchost.exe    2018-09-30 08:10:35 UTC+0000
0x3d43abb8         UDPv4    10.0.2.15:137                  *:*                                   4        System         2018-09-30 08:10:35 UTC+0000
0x3d462748         UDPv6    ::1:65200                      *:*                                   1516     svchost.exe    2018-09-30 08:12:31 UTC+0000
0x3d4671d0         UDPv4    127.0.0.1:1900                 *:*                                   1516     svchost.exe    2018-09-30 08:12:31 UTC+0000
0x3d468548         UDPv4    127.0.0.1:65201                *:*                                   1516     svchost.exe    2018-09-30 08:12:31 UTC+0000
0x3d4dde08         UDPv4    0.0.0.0:53401                  *:*                                   1516     svchost.exe    2018-09-30 08:10:30 UTC+0000
0x3d4dde08         UDPv6    :::53401                       *:*                                   1516     svchost.exe    2018-09-30 08:10:30 UTC+0000
0x3d4e4df0         UDPv6    fe80::147b:c8fd:e2c6:69de:1900 *:*                                   1516     svchost.exe    2018-09-30 08:12:31 UTC+0000
0x3d4e75e8         UDPv4    0.0.0.0:53400                  *:*                                   1516     svchost.exe    2018-09-30 08:10:30 UTC+0000
0x3d4f7528         UDPv4    0.0.0.0:3702                   *:*                                   1516     svchost.exe    2018-09-30 08:10:51 UTC+0000
0x3da37f50         UDPv4    0.0.0.0:5355                   *:*                                   1236     svchost.exe    2018-09-30 08:10:38 UTC+0000
0x3da397c8         UDPv4    0.0.0.0:5355                   *:*                                   1236     svchost.exe    2018-09-30 08:10:38 UTC+0000
0x3da397c8         UDPv6    :::5355                        *:*                                   1236     svchost.exe    2018-09-30 08:10:38 UTC+0000
0x3da73f30         UDPv4    0.0.0.0:3702                   *:*                                   1516     svchost.exe    2018-09-30 08:10:51 UTC+0000
0x3dacc7f0         UDPv4    0.0.0.0:0                      *:*                                   648      VBoxService.ex 2018-09-30 09:42:21 UTC+0000
0x3d425008         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        712      svchost.exe
0x3d428cf0         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        712      svchost.exe
0x3d428cf0         TCPv6    :::135                         :::0                 LISTENING        712      svchost.exe
0x3d42f008         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        388      wininit.exe
0x3d42f008         TCPv6    :::49152                       :::0                 LISTENING        388      wininit.exe
0x3d430358         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        388      wininit.exe
0x3d472ca8         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        800      svchost.exe
0x3d473f58         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        800      svchost.exe
0x3d473f58         TCPv6    :::49153                       :::0                 LISTENING        800      svchost.exe
0x3d4de588         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        492      lsass.exe
0x3d4de588         TCPv6    :::49154                       :::0                 LISTENING        492      lsass.exe
0x3d4ded38         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        492      lsass.exe
0x3d4e9d90         TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING        484      services.exe
0x3d4e9d90         TCPv6    :::49156                       :::0                 LISTENING        484      services.exe
0x3da3b1d0         TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING        904      svchost.exe
0x3da3b1d0         TCPv6    :::49155                       :::0                 LISTENING        904      svchost.exe
0x3da46888         TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING        904      svchost.exe
0x3dabb930         TCPv4    10.0.2.15:139                  0.0.0.0:0            LISTENING        4        System
0x3dafa498         TCPv4    0.0.0.0:5357                   0.0.0.0:0            LISTENING        4        System
0x3dafa498         TCPv6    :::5357                        :::0                 LISTENING        4        System
0x3db08f58         TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING        4        System
0x3db08f58         TCPv6    :::445                         :::0                 LISTENING        4        System
0x3db0c9c8         TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING        484      services.exe
```

Illustration 11*:* showcases the netscan output and the machine’s IP

Part 2: File Extraction and decoding

- ### Brief and Steghide introduction

In this section, steganography and cryptography procedures are implemented. Therefore, volatility and steghide which is a steganography forensics tool will both be used to extract any hidden or encrypted data. The steghide folder was downloaded, extracted and used through the cmd within its path and through its commands. In this section, there's a picture where investigation is done on it and done on 2 more files; the aim is to know if the photo contains any message and if it does, then the message should be found. In addition to, the sections aim to retrieve the password, so the photo could be retrieved.



```
C:\Users\HALA AHMED\Downloads\Volatility\Volatility>cd C:\Users\HALA AHMED\Downloads\steghide-20251214\steghide

C:\Users\HALA AHMED\Downloads\steghide-20251214\steghide>steghide
steghide version 0.5.1

the first argument must be one of the following:
 embed, --embed          embed data
 extract, --extract      extract data
 info, --info            display information about a cover- or stego-file
   info <filename>       display information about <filename>
 encinfo, --encinfo      display a list of supported encryption algorithms
 version, --version      display version information
 license, --license      display steghide's license
 help, --help            display this usage information

embedding options:
 -ef, --embedfile        select file to be embedded
   -ef <filename>        embed the file <filename>
 -cf, --coverfile        select cover-file
   -cf <filename>        embed into the file <filename>
 -p, --passphrase        specify passphrase
   -p <passphrase>       use <passphrase> to embed data
 -sf, --stegofile        select stego file
   -sf <filename>        write result to <filename> instead of cover-file
 -e, --encryption        select encryption parameters
   -e <a>[<m>]|<m>[<a>]  specify an encryption algorithm and/or mode
   -e none               do not encrypt data before embedding
 -z, --compress          compress data before embedding (default)
   -z <l>                 using level <l> (1 best speed...9 best compression)
 -Z, --dontcompress      do not compress data before embedding
 -K, --nochecksum        do not embed crc32 checksum of embedded data
 -N, --dontembedname     do not embed the name of the original file
 -f, --force             overwrite existing files
 -q, --quiet             suppress information messages
 -v, --verbose           display detailed information

extracting options:
 -sf, --stegofile        select stego file
   -sf <filename>        extract data from <filename>
 -p, --passphrase        specify passphrase
   -p <passphrase>       use <passphrase> to extract data
 -xf, --extractfile      select file name for extracted data
   -xf <filename>        write the extracted data to <filename>
 -f, --force             overwrite existing files
 -q, --quiet             suppress information messages
 -v, --verbose           display detailed information

options for the info command:
 -p, --passphrase        specify passphrase
   -p <passphrase>       use <passphrase> to get info about embedded data

To embed emb.txt in cvr.jpg: steghide embed -cf cvr.jpg -ef emb.txt
To extract embedded data from stg.jpg: steghide extract -sf stg.jpg

C:\Users\HALA AHMED\Downloads\steghide-20251214\steghide>
```

Illustration 12: showcases the steghide verification and information

- Password Extraction

The investigation began with Volatility analysis of the memory dump to find running processes in the system. Two suspicious notepad.exe processes have been identified and their command line arguments indicated that the processes were used to open the files vip.txt and evilscript.py. As these files were actively utilized by the executing processes, it was searched in memory with the help of the filescan plugin and with the dumpfiles command, it was extracted. Then, the contents of evilscript.py were extracted and exposed after where an encryption algorithm was found. The script did a basic XOR operation on the input data with a key of 3 which was fixed and then coded the output using Base64 and then wrote it to vip.txt. This was done in reverse with the purpose of retrieving the original password consuming the following steps: First the Base64 string was decoded followed by the same XOR operation which then made the hidden password that was required in the next step of the analysis.

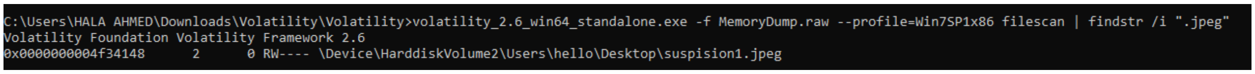
- Secret Text Extraction

In the memory analysis, it was also found that one suspicious JPEG image was present in the memory and extracted in memory under name of suspision1.jpeg. This file was examined with Steghide which proved that this file had hidden information with the help of passphrase. Because Steghide needs the right password to unlock a hidden content, the former password that was stolen in vip.txt was entered. Steghide was able to extract the hidden file of the image when the proper passphrase was given. The content extracted showed a hidden text message, which finished the hidden message hidden in the JPEG file and proved the existence of steganography as a data-hiding method used in the present case.

- Results and Steps

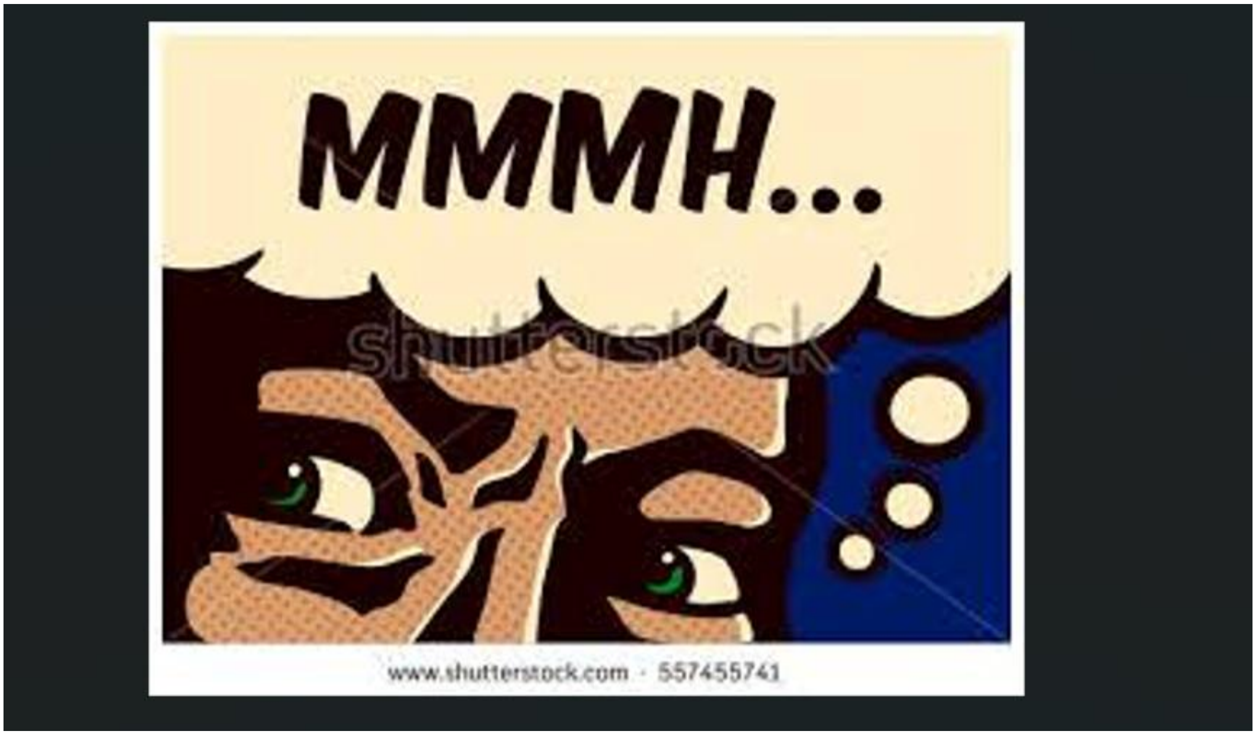
The password extracted is "inctf{0n3_h4lf"and the secret test extracted is 1s_n0t_3n0ugh}". Combining both together would be " inctf{0n3_h4lf is 1s_n0t_3n0ugh}".

- Jpeg extraction

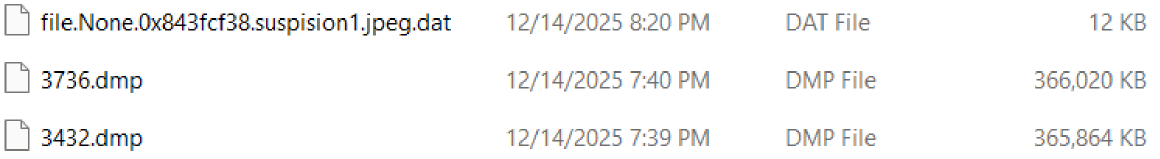


```
C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 filescan | findstr /i ".jpeg"
Volatility Foundation Volatility Framework 2.6
0x0000000004f34148      2      0 RW---- \Device\HarddiskVolume2\Users\hello\Desktop\suspision1.jpeg
```

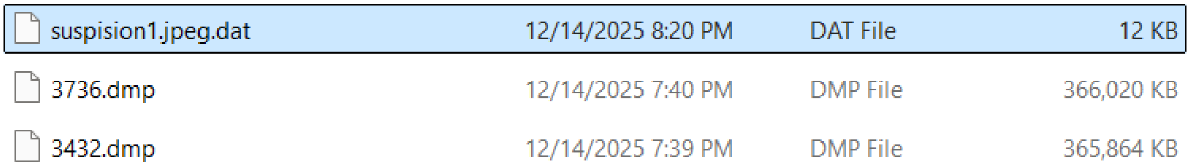
- Image



- Extracted the jpg from the memory and exported it to my disk

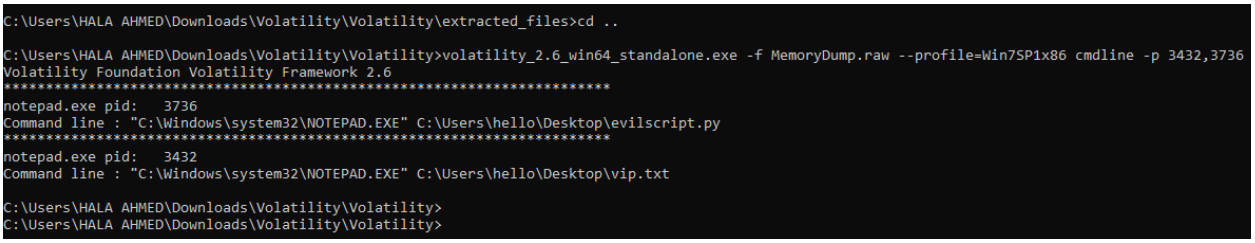


file.None.0x843fcf38.suspision1.jpeg.dat	12/14/2025 8:20 PM	DAT File	12 KB
3736.dmp	12/14/2025 7:40 PM	DMP File	366,020 KB
3432.dmp	12/14/2025 7:39 PM	DMP File	365,864 KB



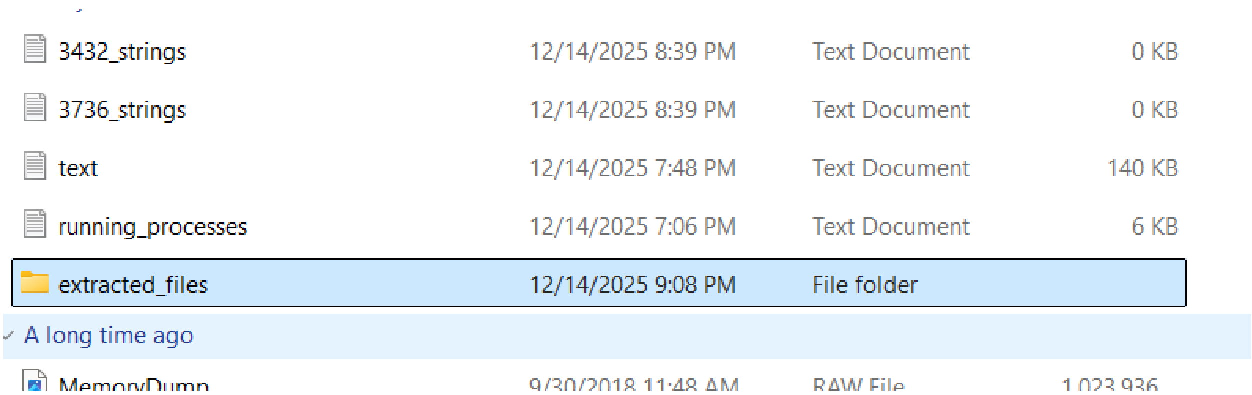
suspision1.jpeg.dat	12/14/2025 8:20 PM	DAT File	12 KB
3736.dmp	12/14/2025 7:40 PM	DMP File	366,020 KB
3432.dmp	12/14/2025 7:39 PM	DMP File	365,864 KB

- Files done for extraction



```
C:\Users\HALA AHMED\Downloads\Volatility\Volatility\extracted_files>cd ..

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 cmdline -p 3432,3736
Volatility Foundation Volatility Framework 2.6
************************************************************************
notepad.exe pid:   3736
Command line : "C:\Windows\system32\NOTEPAD.EXE" C:\Users\hello\Desktop\evilscript.py
************************************************************************
notepad.exe pid:   3432
Command line : "C:\Windows\system32\NOTEPAD.EXE" C:\Users\hello\Desktop\vip.txt

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>
C:\Users\HALA AHMED\Downloads\Volatility\Volatility>
```

- Extracted files



3432_strings	12/14/2025 8:39 PM	Text Document	0 KB
3736_strings	12/14/2025 8:39 PM	Text Document	0 KB
text	12/14/2025 7:48 PM	Text Document	140 KB
running_processes	12/14/2025 7:06 PM	Text Document	6 KB
extracted_files	12/14/2025 9:08 PM	File folder	

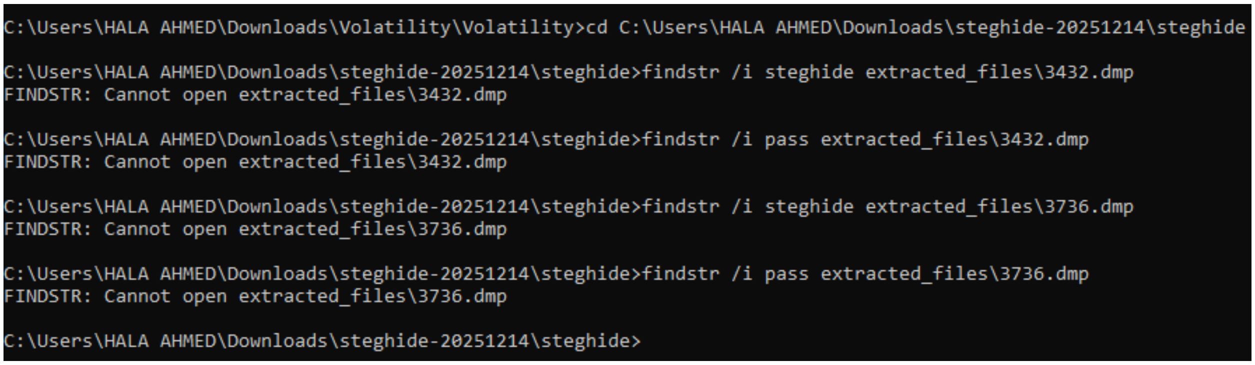
A long time ago

MemoryDump	9/30/2018 11:48 AM	RAW File	1,023,936

- errors faced

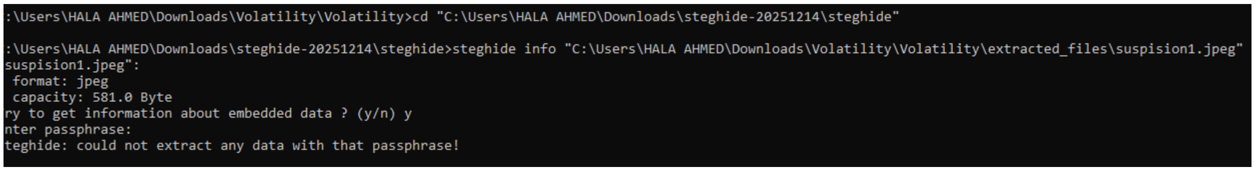
```
#define ISCSI_LOGIN_OPTIONS_PASSWORD            0x00000040
```

Founded Paths

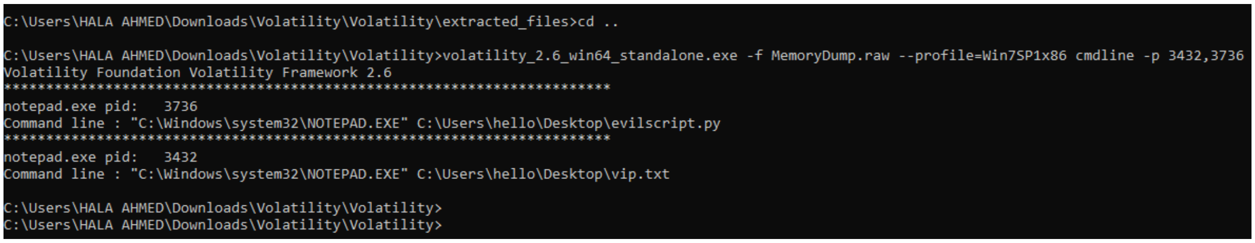


```
C:\Users\HALA AHMED\Downloads\Volatility\Volatility>cd C:\Users\HALA AHMED\Downloads\steghide-20251214\steghide

C:\Users\HALA AHMED\Downloads\steghide-20251214\steghide>findstr /i steghide extracted_files\3432.dmp
FINDSTR: Cannot open extracted_files\3432.dmp

C:\Users\HALA AHMED\Downloads\steghide-20251214\steghide>findstr /i pass extracted_files\3432.dmp
FINDSTR: Cannot open extracted_files\3432.dmp

C:\Users\HALA AHMED\Downloads\steghide-20251214\steghide>findstr /i steghide extracted_files\3736.dmp
FINDSTR: Cannot open extracted_files\3736.dmp

C:\Users\HALA AHMED\Downloads\steghide-20251214\steghide>findstr /i pass extracted_files\3736.dmp
FINDSTR: Cannot open extracted_files\3736.dmp

C:\Users\HALA AHMED\Downloads\steghide-20251214\steghide>
```

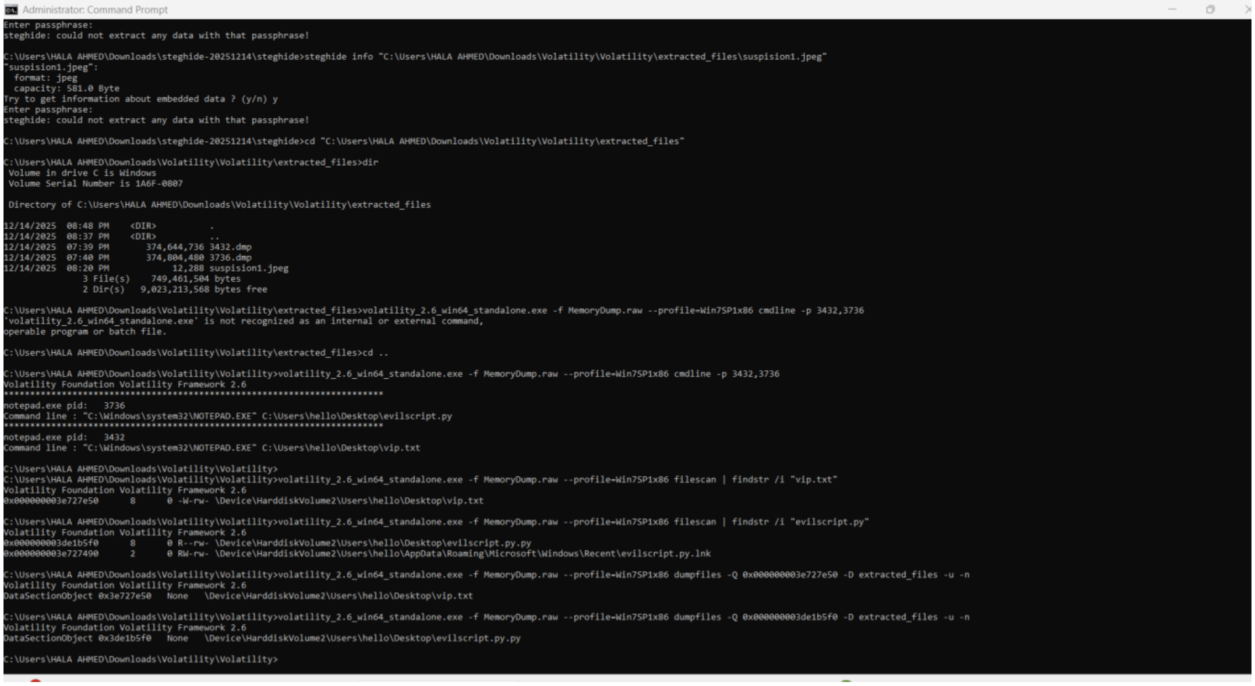
Founded Paths



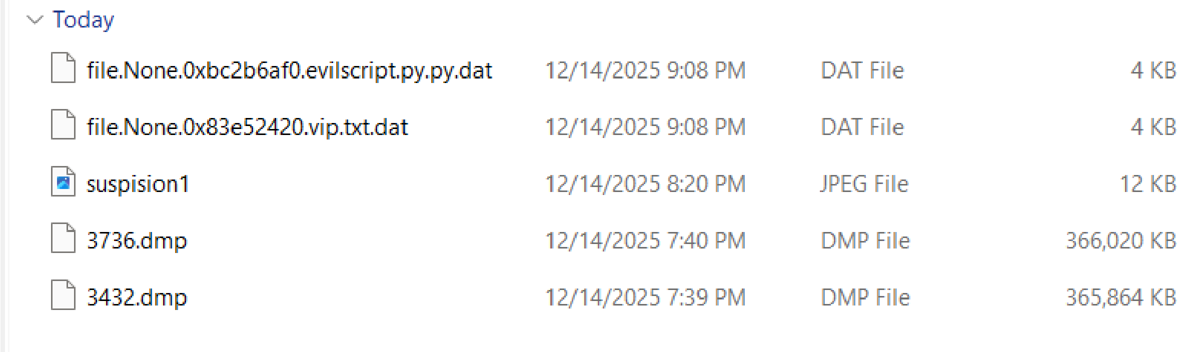
```
:\Users\HALA AHMED\Downloads\Volatility\Volatility>cd "C:\Users\HALA AHMED\Downloads\steghide-20251214\steghide"

:\Users\HALA AHMED\Downloads\steghide-20251214\steghide>steghide info "C:\Users\HALA AHMED\Downloads\Volatility\Volatility\extracted_files\suspision1.jpeg"
suspision1.jpeg":
 format: jpeg
 capacity: 581.0 Byte
ry to get information about embedded data ? (y/n) y
nter passphrase:
teghide: could not extract any data with that passphrase!
```



```
C:\Users\HALA AHMED\Downloads\Volatility\Volatility\extracted_files>cd ..

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 cmdline -p 3432,3736
Volatility Foundation Volatility Framework 2.6
************************************************************************
notepad.exe pid:   3736
Command line : "C:\Windows\system32\NOTEPAD.EXE" C:\Users\hello\Desktop\evilscript.py
************************************************************************
notepad.exe pid:   3432
Command line : "C:\Windows\system32\NOTEPAD.EXE" C:\Users\hello\Desktop\vip.txt

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>
C:\Users\HALA AHMED\Downloads\Volatility\Volatility>
```

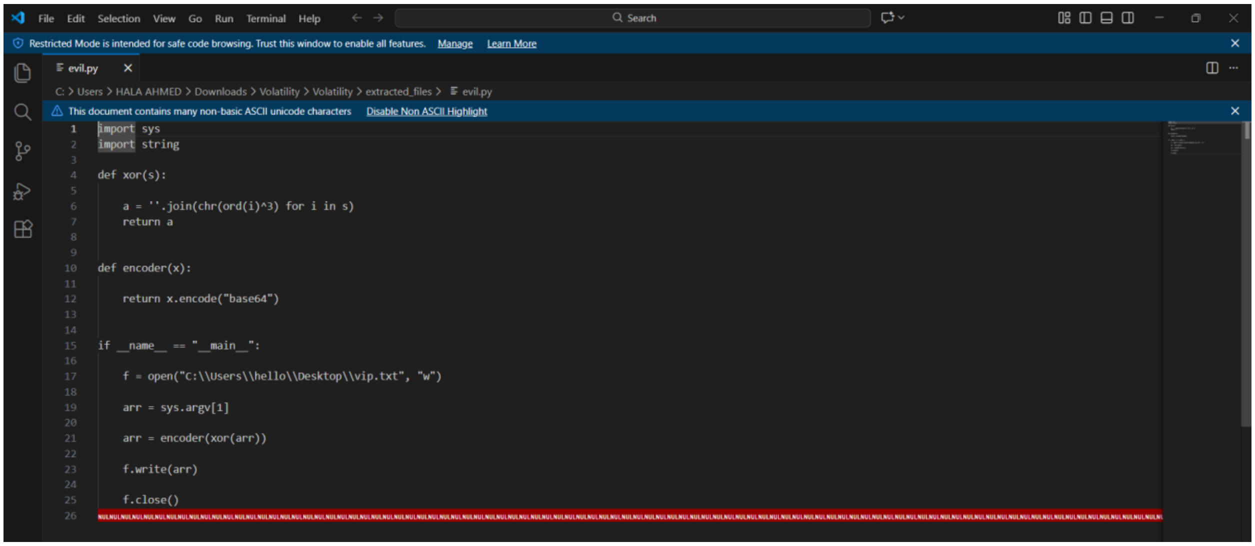


```
Enter passphrase:
steghide: could not extract any data with that passphrase!

C:\Users\HALA AHMED\Downloads\steghide-20251214\steghide>steghide info "C:\Users\HALA AHMED\Downloads\Volatility\Volatility\extracted_files\suspision1.jpeg"
"suspision1.jpeg":
  format: jpeg
  capacity: 581.0 Byte
Try to get information about embedded data ? (y/n) y
Enter passphrase:
steghide: could not extract any data with that passphrase!

C:\Users\HALA AHMED\Downloads\steghide-20251214\steghide>cd "C:\Users\HALA AHMED\Downloads\Volatility\Volatility\extracted_files"

C:\Users\HALA AHMED\Downloads\Volatility\Volatility\extracted_files>dir
 Volume in drive C is Windows
 Volume Serial Number is 1A6F-0807

 Directory of C:\Users\HALA AHMED\Downloads\Volatility\Volatility\extracted_files

12/14/2025  08:48 PM    <DIR>          .
12/14/2025  08:37 PM    <DIR>          ..
12/14/2025  07:39 PM       374,644,736 3432.dmp
12/14/2025  07:40 PM       374,804,480 3736.dmp
12/14/2025  08:20 PM            12,288 suspision1.jpeg
               3 File(s)    749,461,504 bytes
               2 Dir(s)   9,023,213,568 bytes free

C:\Users\HALA AHMED\Downloads\Volatility\Volatility\extracted_files>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 cmdline -p 3432,3736
'volatility_2.6_win64_standalone.exe' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\HALA AHMED\Downloads\Volatility\Volatility\extracted_files>cd ..

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 cmdline -p 3432,3736
Volatility Foundation Volatility Framework 2.6
************************************************************************
notepad.exe pid:   3736
Command line : "C:\Windows\system32\NOTEPAD.EXE" C:\Users\hello\Desktop\evilscript.py
************************************************************************
notepad.exe pid:   3432
Command line : "C:\Windows\system32\NOTEPAD.EXE" C:\Users\hello\Desktop\vip.txt

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>
C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 filescan | findstr /i "vip.txt"
Volatility Foundation Volatility Framework 2.6
0x000000003e727e50      8      0 -W-rw- \Device\HarddiskVolume2\Users\hello\Desktop\vip.txt

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 filescan | findstr /i "evilscript.py"
Volatility Foundation Volatility Framework 2.6
0x000000003de1b5f0      8      0 R--rw- \Device\HarddiskVolume2\Users\hello\Desktop\evilscript.py.py
0x000000003e727490      2      0 RW-rw- \Device\HarddiskVolume2\Users\hello\AppData\Roaming\Microsoft\Windows\Recent\evilscript.py.lnk

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 dumpfiles -Q 0x000000003e727e50 -D extracted_files -u -n
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x3e727e50   None   \Device\HarddiskVolume2\Users\hello\Desktop\vip.txt

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 dumpfiles -Q 0x000000003de1b5f0 -D extracted_files -u -n
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x3de1b5f0   None   \Device\HarddiskVolume2\Users\hello\Desktop\evilscript.py.py

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>
```



Today

file.None.0xbc2b6af0.evilscript.py.py.dat	12/14/2025 9:08 PM	DAT File	4 KB
file.None.0x83e52420.vip.txt.dat	12/14/2025 9:08 PM	DAT File	4 KB
suspision1	12/14/2025 8:20 PM	JPEG File	12 KB
3736.dmp	12/14/2025 7:40 PM	DMP File	366,020 KB
3432.dmp	12/14/2025 7:39 PM	DMP File	365,864 KB

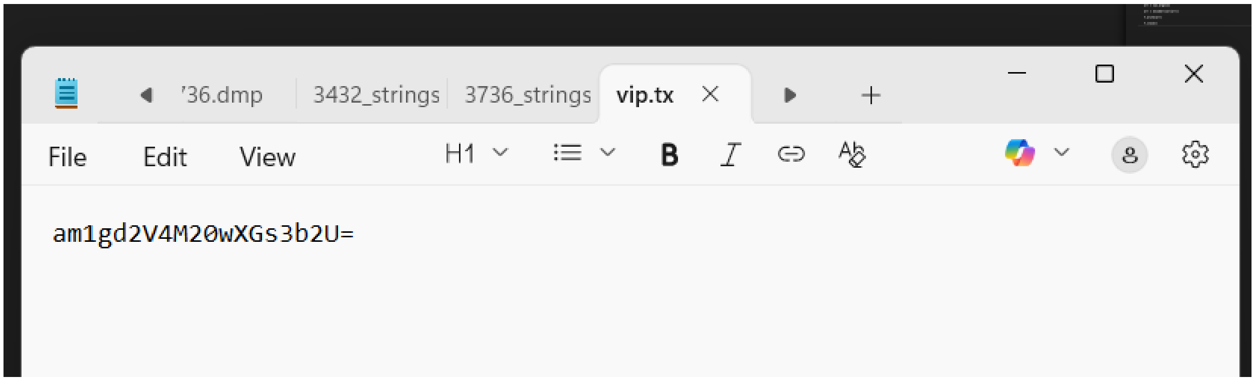


Restricted Mode is intended for safe code browsing. Trust this window to enable all features.

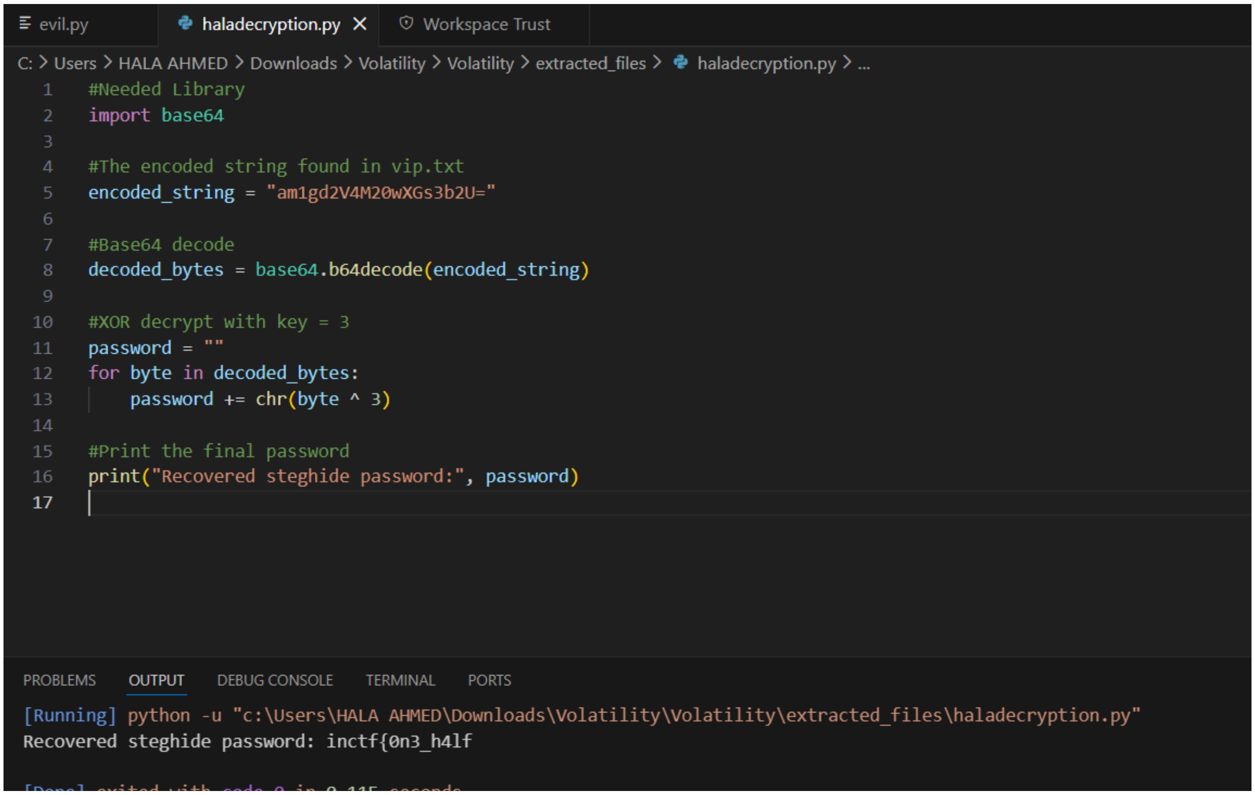
C: > Users > HALA AHMED > Downloads > Volatility > Volatility > extracted_files > evil.py

This document contains many non-basic ASCII unicode characters

```
import sys
import string

def xor(s):

    a = ''.join(chr(ord(i)^3) for i in s)
    return a


def encoder(x):

    return x.encode("base64")


if __name__ == "__main__":

    f = open("C:\\Users\\hello\\Desktop\\vip.txt", "w")

    arr = sys.argv[1]

    arr = encoder(xor(arr))

    f.write(arr)

    f.close()
```



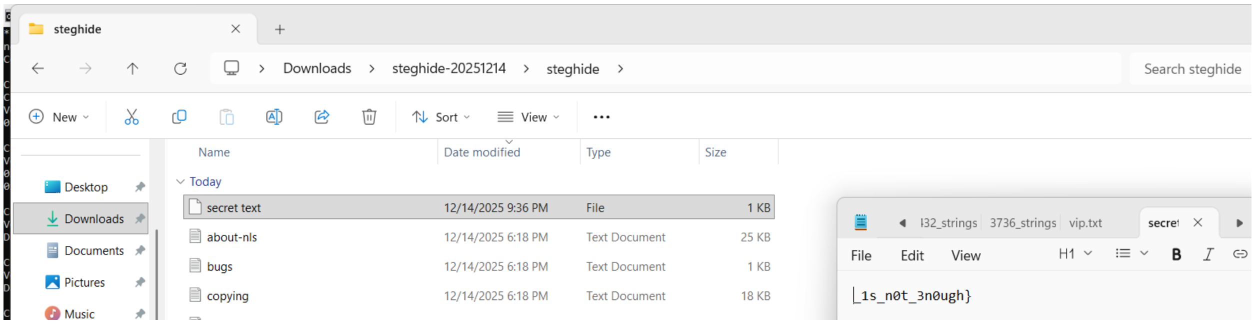
```
am1gd2V4M20wXGs3b2U=
```



C: > Users > HALA AHMED > Downloads > Volatility > Volatility > extracted_files > haladecryption.py > ...

```python
#Needed Library
import base64

#The encoded string found in vip.txt
encoded_string = "am1gd2V4M20wXGs3b2U="

#Base64 decode
decoded_bytes = base64.b64decode(encoded_string)

#XOR decrypt with key = 3
password = ""
for byte in decoded_bytes:
    password += chr(byte ^ 3)

#Print the final password
print("Recovered steghide password:", password)

```

```
[Running] python -u "c:\Users\HALA AHMED\Downloads\Volatility\Volatility\extracted_files\haladecryption.py"
Recovered steghide password: inctf{0n3_h4lf

[Done] exited with code 0 in 0.115 seconds
```

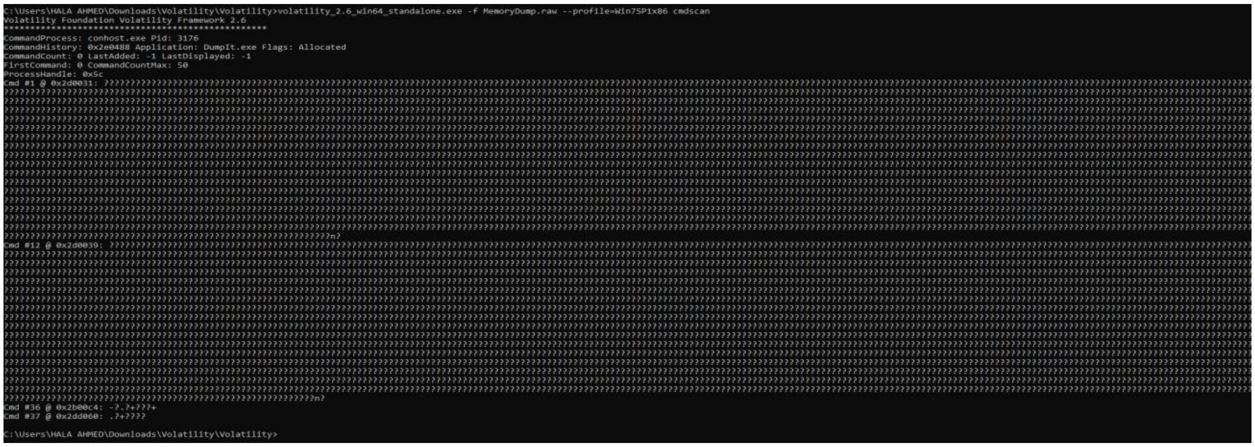


Name	Date modified	Type	Size
Today			
secret text	12/14/2025 9:36 PM	File	1 KB
about-nls	12/14/2025 6:18 PM	Text Document	25 KB
bugs	12/14/2025 6:18 PM	Text Document	1 KB
copying	12/14/2025 6:18 PM	Text Document	18 KB

```
_1s_n0t_3n0ugh}
```

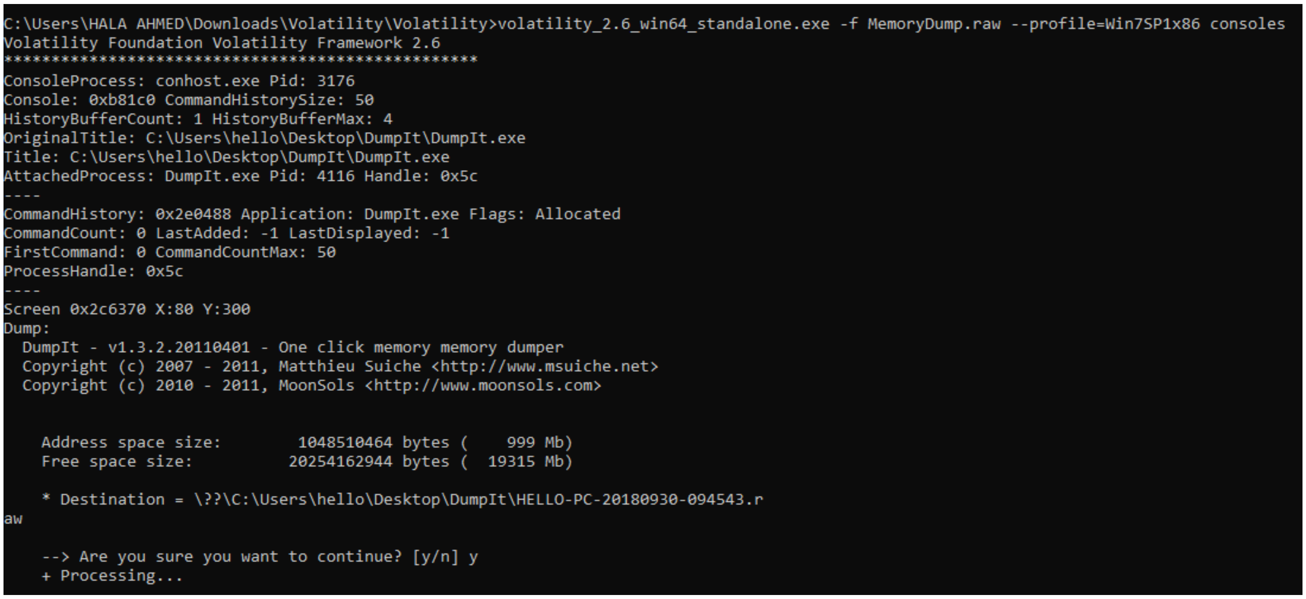
Part 3: Additional Memory Analysis Features

- Cmd scan



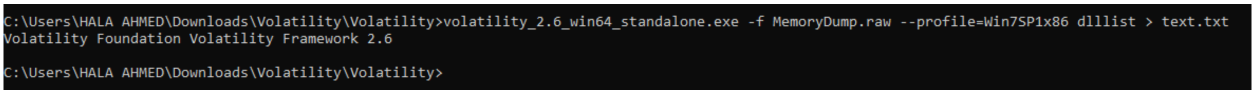
```
C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 cmdscan
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: conhost.exe Pid: 3176
CommandHistory: 0x2e0488 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #1 @ 0x2d0031: ?????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
?????????????????????????????????????????????????????????????????????n?
Cmd #12 @ 0x2d0039: ????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????
?????????????????????????????????????????????????????????????????n?
Cmd #36 @ 0x2b00c4: -?.?+???+
Cmd #37 @ 0x2dd060: .?+????

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>
```

- Console Buffer:



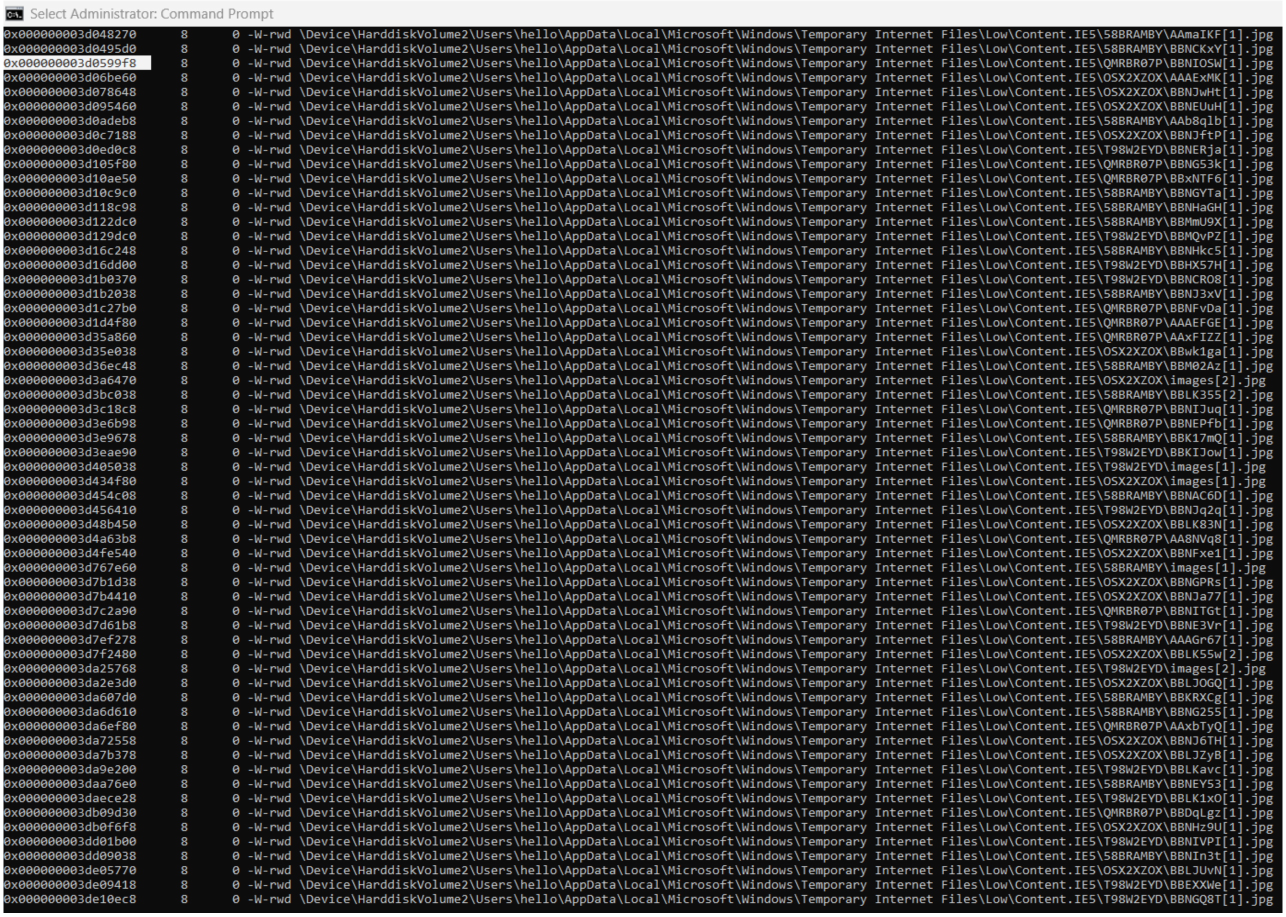
```
C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 consoles
Volatility Foundation Volatility Framework 2.6
**************************************************
ConsoleProcess: conhost.exe Pid: 3176
Console: 0xb81c0 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: C:\Users\hello\Desktop\DumpIt\DumpIt.exe
Title: C:\Users\hello\Desktop\DumpIt\DumpIt.exe
AttachedProcess: DumpIt.exe Pid: 4116 Handle: 0x5c
----
CommandHistory: 0x2e0488 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
----
Screen 0x2c6370 X:80 Y:300
Dump:
  DumpIt - v1.3.2.20110401 - One click memory memory dumper
  Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
  Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>


    Address space size:        1048510464 bytes (    999 Mb)
    Free space size:          20254162944 bytes (  19315 Mb)

    * Destination = \??\C:\Users\hello\Desktop\DumpIt\HELLO-PC-20180930-094543.r
aw

    --> Are you sure you want to continue? [y/n] y
    + Processing...
```

- DLLs

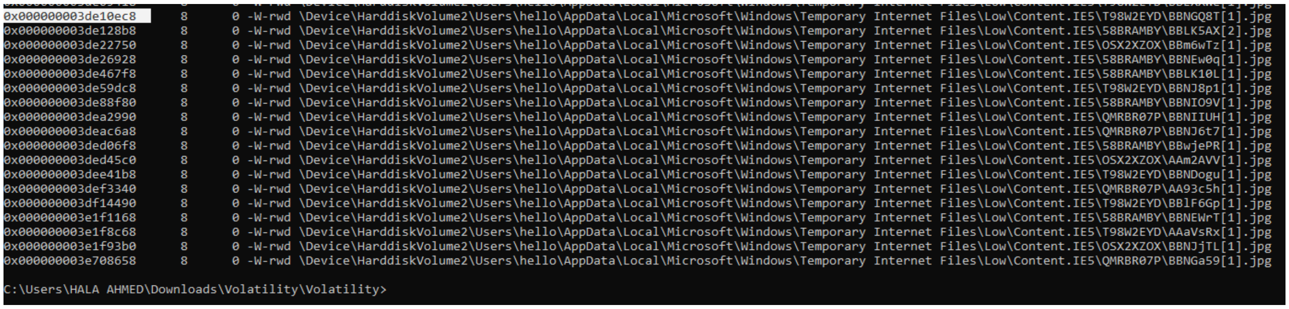


```
C:\Users\HALA AHMED\Downloads\Volatility\Volatility>volatility_2.6_win64_standalone.exe -f MemoryDump.raw --profile=Win7SP1x86 dlllist > text.txt
Volatility Foundation Volatility Framework 2.6

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>
```

- JPG extraction



```
0x000000003d048270      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\AAmaIKF[1].jpg
0x000000003d0495d0      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBNCKxY[1].jpg
0x000000003d0599f8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\BBNIOSW[1].jpg
0x000000003d06be60      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\AAAExMK[1].jpg
0x000000003d078648      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBNJwHt[1].jpg
0x000000003d095460      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBNEUuH[1].jpg
0x000000003d0adeb8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\AAb8qlb[1].jpg
0x000000003d0c7188      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBNJftP[1].jpg
0x000000003d0ed0c8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBNERja[1].jpg
0x000000003d105f80      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\BBNG53k[1].jpg
0x000000003d10ae50      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\BBxNTF6[1].jpg
0x000000003d10c9c0      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBNGYTa[1].jpg
0x000000003d118c98      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBNHaGH[1].jpg
0x000000003d122dc0      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBMmU9X[1].jpg
0x000000003d129dc0      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBMQvPZ[1].jpg
0x000000003d16c248      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBNHkc5[1].jpg
0x000000003d16dd00      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBHX57H[1].jpg
0x000000003d1b0370      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBNCRO8[1].jpg
0x000000003d1b2038      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBNJ3xV[1].jpg
0x000000003d1c27b0      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\BBNFvDa[1].jpg
0x000000003d1d4f80      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\AAAEFGE[1].jpg
0x000000003d35a860      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\AAxFIZZ[1].jpg
0x000000003d35e038      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBwk1ga[1].jpg
0x000000003d36ec48      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBM02Az[1].jpg
0x000000003d3a6470      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\images[2].jpg
0x000000003d3bc038      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBLK355[2].jpg
0x000000003d3c18c8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\BBNIJuq[1].jpg
0x000000003d3e6b98      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\BBNEPfb[1].jpg
0x000000003d3e9678      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBK17mQ[1].jpg
0x000000003d3eae90      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBKIJow[1].jpg
0x000000003d405038      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\images[1].jpg
0x000000003d434f80      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\images[1].jpg
0x000000003d454c08      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBNAC6D[1].jpg
0x000000003d456410      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBNJq2q[1].jpg
0x000000003d48b450      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBLK83N[1].jpg
0x000000003d4a63b8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\AA8NVq8[1].jpg
0x000000003d4fe540      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBNFxe1[1].jpg
0x000000003d767e60      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\images[1].jpg
0x000000003d7b1d38      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBNGPRs[1].jpg
0x000000003d7b4410      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBNJa77[1].jpg
0x000000003d7c2a90      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\BBNITGt[1].jpg
0x000000003d7d61b8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBNE3Vr[1].jpg
0x000000003d7ef278      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\AAAGr67[1].jpg
0x000000003d7f2480      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBLK55w[2].jpg
0x000000003da25768      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\images[2].jpg
0x000000003da2e3d0      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBLJOGQ[1].jpg
0x000000003da607d0      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBKRXCg[1].jpg
0x000000003da6d610      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBNG255[1].jpg
0x000000003da6ef80      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\AAxbTyQ[1].jpg
0x000000003da72558      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBNJ6TH[1].jpg
0x000000003da7b378      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBLJZyB[1].jpg
0x000000003da9e200      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBLKavc[1].jpg
0x000000003daa76e0      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBNEY53[1].jpg
0x000000003daece28      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBLK1xO[1].jpg
0x000000003db09d30      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\BBDqLgz[1].jpg
0x000000003db0f6f8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBNHz9U[1].jpg
0x000000003dd01b00      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBNIVPI[1].jpg
0x000000003dd09038      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBNIn3t[1].jpg
0x000000003de05770      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBLJUvN[1].jpg
0x000000003de09418      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBEXXWe[1].jpg
0x000000003de10ec8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBNGQ8T[1].jpg
```



```
0x000000003de10ec8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBNGQ8T[1].jpg
0x000000003de128b8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBLK5AX[2].jpg
0x000000003de22750      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBm6wTz[1].jpg
0x000000003de26928      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBNEw0q[1].jpg
0x000000003de467f8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBLK10L[1].jpg
0x000000003de59dc8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBNJ8p1[1].jpg
0x000000003de88f80      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBNIO9V[1].jpg
0x000000003dea2990      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\BBNIIUH[1].jpg
0x000000003deac6a8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\BBNJ6t7[1].jpg
0x000000003ded06f8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBwjePR[1].jpg
0x000000003ded45c0      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\AAm2AVV[1].jpg
0x000000003dee41b8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBNDogu[1].jpg
0x000000003def3340      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\AA93c5h[1].jpg
0x000000003df14490      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBlF6Gp[1].jpg
0x000000003e1f1168      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\BBNEWrT[1].jpg
0x000000003e1f8c68      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\AAaVsRx[1].jpg
0x000000003e1f93b0      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBNJjTL[1].jpg
0x000000003e708658      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\BBNGa59[1].jpg

C:\Users\HALA AHMED\Downloads\Volatility\Volatility>
```

Tools Used

1. Volatility
2. Steghide
3. PowerShell
4. Word Document

Conclusion

In this section, the memory analysis was done through 2 main apps: volatility and steghide. It also used python scripts for encoding and decoding the password. The analysis process went through multiple steps; however, the last step of cryptography and steganography highlighted everything that was needed. The password extracted is "inctf{0n3_h4lf"and the secret test extracted is 1s_n0t_3n0ugh}”. Combining both together would be “ inctf{0n3_h4lf is 1s_n0t_3n0ugh}”.

References

Week 9-11 Labs