

# Writeup :

## Challenge Overview – Memory Forensics Objective

The objective of this challenge is to analyze a Windows memory dump in order to recover sensitive user data belonging to a well-known environmental activist who lost access to his system due to an unknown error.

The investigation focuses on extracting:

- Environment variables
- Browser / password manager artifacts
- KeePass database credentials stored in memory

---

### Q1 – Environment Variable Analysis

#### Investigation Context

During the memory analysis, it was noted that the victim frequently uses:

- Web browsers
- Password managers (KeePass)

Given the hint that the victim is an **environmental activist**, environment variables may contain **user-specific or suspicious values** that provide an initial clue.

---

### Tool Used

- **Volatility 3 Framework (CLI , GUI )**
  - **Windows memory dump (.raw)**
-

# 1) Initial Analysis – Process Enumeration

## First Step in the Analysis

The first step in the memory forensic analysis was to enumerate all running processes in the memory dump.

This step is critical to understand what applications were active on the victim's system at the time the memory was captured.

```
"C:\Users\NVIDIA PLUS\Desktop\vol.exe" -f "C:\Users\NVIDIA PLUS\Desktop\New folder\MemoryDump_Lab2.raw" windows.pslist.PsList

Please wait, this may take a few minutes.

Volatility 3 Framework 2.26.2
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime File output
4 0 System 0xfa8000ca0040 80 541 N/A False 2019-12-14 10:35:21.000000 UTC N/A Disabled
248 4 smss.exe 0xfa80014976c0 3 37 N/A False 2019-12-14 10:35:21.000000 UTC N/A Disabled
320 312 csrss.exe 0xfa80014fdb30 10 446 0 False 2019-12-14 10:35:27.000000 UTC N/A Disabled
368 360 csrss.exe 0xfa8001c40060 8 237 1 False 2019-12-14 10:35:28.000000 UTC N/A Disabled
376 248 pcsss.exe 0xfa8000ca8840 18 786 0 False 2019-12-14 10:35:28.000000 UTC N/A Disabled
416 360 winlogon.exe 0xfa8001c5a700 6 112 1 False 2019-12-14 10:35:30.000000 UTC N/A Disabled
424 312 wininit.exe 0xfa8001c5b2b0 3 75 0 False 2019-12-14 10:35:30.000000 UTC N/A Disabled
484 424 services.exe 0xfa8001c95320 8 206 0 False 2019-12-14 10:35:31.000000 UTC N/A Disabled
492 424 lsass.exe 0xfa8001c9d910 8 546 0 False 2019-12-14 10:35:31.000000 UTC N/A Disabled
500 424 lsm.exe 0xfa8001c9e2d0 10 181 0 False 2019-12-14 10:35:31.000000 UTC N/A Disabled
588 484 svchost.exe 0xfa8001cec790 12 354 0 False 2019-12-14 10:35:35.000000 UTC N/A Disabled
652 484 VBoxService.exe 0xfa8001d13060 14 135 0 False 2019-12-14 10:35:36.000000 UTC N/A Disabled
720 484 svchost.exe 0xfa8001d4ab30 7 275 0 False 2019-12-14 10:35:37.000000 UTC N/A Disabled
812 484 svchost.exe 0xfa8001d76320 21 474 0 False 2019-12-14 10:35:38.000000 UTC N/A Disabled
```

## 2) Command Line Analysis

identifying the suspicious processes, the next step was to analyze how these processes were launched and whether any sensitive information was passed to them at runtime.

Volatility Plugin Used : windows.cmdline.CmdLine

```
Time Stamp: Thu Dec 25 20:27:16 2025
"C:\Users\NVIDIA PLUS\Desktop\vol.exe" -f "C:\Users\NVIDIA PLUS\Desktop\New folder\MemoryDump_Lab2.raw" windows.cmdline.CmdLine

Please wait, this may take a few minutes.

Volatility 3 Framework 2.26.2
PID Process Args
4 System -
248 smss.exe \SystemRoot\System32\smss.exe
320 csrss.exe %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=baf
368 csrss.exe %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=baf
376 pcsss.exe %SystemRoot%\system32\pcssss.exe
416 winlogon.exe winlogon.exe
424 wininit.exe wininit.exe
484 services.exe C:\Windows\system32\services.exe
492 lsass.exe C:\Windows\system32\lsass.exe
```

## Suspicious Processes Identified

The results revealed three suspicious processes that were of high forensic value. These processes were directly related to the challenge context (browsing activity, password management, and user data handling):

### Google Chrome

- **Process Name:** chrome.exe
- **PID:** (2296 , 2304 , 2479 , 2964 , 2575)
- **Reason for Suspicion:**
  - Active web browser

```

2096 cmd.exe "C:\Windows\system32\cmd.exe"
2068 conhost.exe ??\C:\Windows\system32\conhost.exe
2296 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
3304 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=crashpad-handler "--user-data-dir=C:\Users\SmartNet\AppData\Local\Google\Chrome\User Da
3476 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=watcher --main-thread-id=2312 --on-initialized-event-handle=12 --parent-handle=164 /pre
3944 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utility --field-trial-handle=920,18321715965689748971,11882971420757355211,131072 --lan
3572 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=gpu-process --field-trial-handle=920,18321715965689748971,11882971420757355211,131072 -
2636 WmiPrvSE.exe C:\Windows\system32\wbem\WmiPrvse.exe
2004 WmiApSrv.exe C:\Windows\system32\wbem\WmiApSrv.exe
3452 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=920,18321715965689748971,11882971420757355211,131072 --di
2376 dllhost.exe C:\Windows\system32\DllHost.exe /ProcessId:{76D0CB12-7604-4048-B83C-1005C7DDC503}
3008 KeePass.exe "C:\Program Files (x86)\KeePass Password Safe 2\KeePass.exe" "C:\Users\SmartNet\Secrets\Hidden.kdbx"
...

```

---

## Notepad

- **Process Name:** notepad.exe
- **PID:** (3260)
- **Reason for Suspicion:**
  - Often used to temporarily store passwords, notes, or copied text

```

2764 sppsvc.exe C:\Windows\system32\sppsvc.exe
1076 svchost.exe C:\Windows\System32\svchost.exe -k secsvcs
928 wmpnetwk.exe "C:\Program Files\Windows Media Player\wmpnetwk.exe"
3260 notepad.exe "C:\Windows\system32\NOTEPAD.EXE" C:\Users\SmartNet\Secrets\Hidden.kdbx
3844 DumpIt.exe "C:\Users\SmartNet\Downloads\DumpIt\DumpIt.exe"
3852 conhost.exe ??\C:\Windows\system32\conhost.exe
4004 WmiPrvSE.exe -
Time Stamp: Thu Dec 25 20:27:27 2025

```

---

## KeePass

- **Process Name:** KeePass.exe
- **PID:** 3008
- **Reason for Suspicion:**
  - Password manager
  - High-value target in memory for:
    - Database paths

```

2004 WmiApSrv.exe C:\Windows\system32\wbem\WmiApSrv.exe
1632 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=920,18321715965689748971,11882971420757355211,131072 --lan
2376 dllhost.exe C:\Windows\system32\DllHost.exe /ProcessId:{76D0CB12-7604-4048-B83C-1005C7DDC503}
3008 KeePass.exe "C:\Program Files (x86)\KeePass Password Safe 2\KeePass.exe" "C:\Users\SmartNet\Secrets\Hidden.kdbx"
2764 sppsvc.exe C:\Windows\system32\sppsvc.exe
1076 svchost.exe C:\Windows\System32\svchost.exe -k secsvcs
928 wmpnetwk.exe "C:\Program Files\Windows Media Player\wmpnetwk.exe"
3260 notepad.exe "C:\Windows\system32\NOTEPAD.EXE" C:\Users\SmartNet\Secrets\Hidden.kdbx
...

```

## 3- Environment Variable Analysis

Since the challenge explicitly mentions that the victim is an “environmental activist”, this strongly suggests that environment variables may contain relevant clues or hidden information.

The windows.envars.Envars plugin was used because it directly aligns with the challenge hint (“environmental activist”) and provided critical insight into sensitive data stored in environment variables, leading to the next phase of the investigation.

```
"C:\Users\NVIDIA PLUS\Desktop\vol.exe" -f "C:\Users\NVIDIA PLUS\Desktop\New folder\MemoryDump_Lab2.raw" windows.envars.Envars

Please wait, this may take a few minutes.
Volatility 3 Framework 2.26.2
PID  Process Block  Variable          Value
248   smss.exe    0x2d1430    Path      C:\Windows\System32
248   smss.exe    0x2d1430    SystemDrive  C:
248   smss.exe    0x2d1430    SystemRoot  C:\Windows
320   csrss.exe   0x481970    ComSpec   C:\Windows\system32\cmd.exe
320   csrss.exe   0x481970    FP NO HOST CHECK  NO
320   csrss.exe   0x481970    NEW_TMR C:\Windows\ZmxhZ3t3M2xjMG0zX1QwXyRUNGczXyFft2ZfTDRCXzJ9
320   csrss.exe   0x481970    NUMBER OF PROCESSORS 1
320   csrss.exe   0x481970    OS        Windows NT
```

## 4- Encoded Data Discovery & Flag Extraction

During further memory analysis, multiple Base64-encoded strings were identified across different memory regions and file paths.

The repetition of the same encoded content strongly indicated that it was intentionally stored, rather than being random memory noise.

### ■ Notepad Memory Dump Analysis

Given that Notepad is commonly used to temporarily store sensitive information in plain text, its memory was dumped and analyzed.

### ■ Decoding Process

The extracted Base64 string was then analyzed using CyberChef, a well-known forensic and decoding tool

The screenshot shows the CyberChef interface. The top section is labeled "Input" and contains the Base64 string: ZmxhZ3t3M2xjMG0zX1QwXyRUNGczXyFft2ZfTDRCXzJ9. The bottom section is labeled "Output" and contains the decoded flag: flag{w3lc0m3\_T0\_\$T4g3\_!\_Of\_L4B\_2}. The interface includes various buttons and options for file operations and encoding/decoding modes.

## Q2- Overview – KeePass Database Recovery

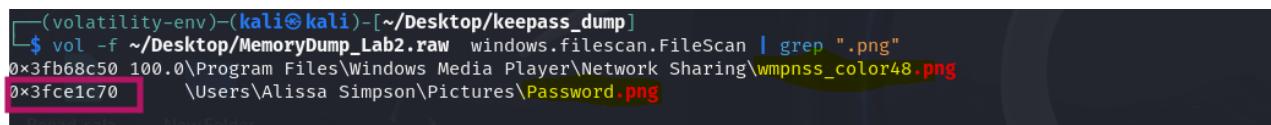
This task focuses on memory forensics to recover sensitive user data from a system memory dump.

During the investigation, it was discovered that the victim relies heavily on:

- Web browsers
- Password managers (specifically KeePass)
- Simple applications for storing information (Notepad)

While analyzing the memory dump, a reference to an image file named **Password.png** was found.

This image contained a **password**, which was crucial because it was used as the **master password** to unlock a **KeePass database** that also existed in memor



```
(volatility-env)–(kali㉿kali)–[~/Desktop/keepass_dump]
$ vol -f ~/Desktop/MemoryDump_Lab2.raw windows.filescan.Filescan | grep ".png"
0x3fb68c50 100.0\Program Files\Windows Media Player\Network Sharing\wmpnss_color48.png
0x3fce1c70   \Users\Alissa Simpson\Pictures\Password.png
```

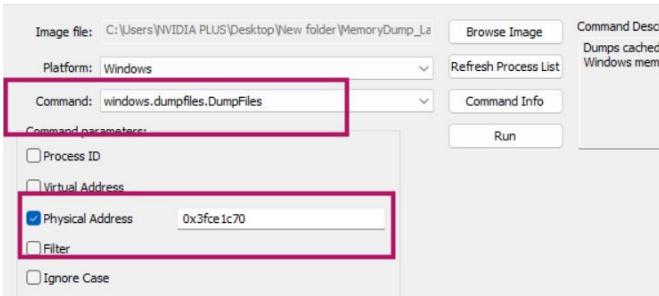


Image file: C:\Users\NVIDIA PLUS\Desktop\New folder\MemoryDump\_Lab2.raw  
Platform: Windows  
Command: windows.dumpfiles.DumpFiles  
Command parameters:  
 Process ID  
 Virtual Address  
 Physical Address 0x3fce1c70  
 Filter  
 Ignore Case

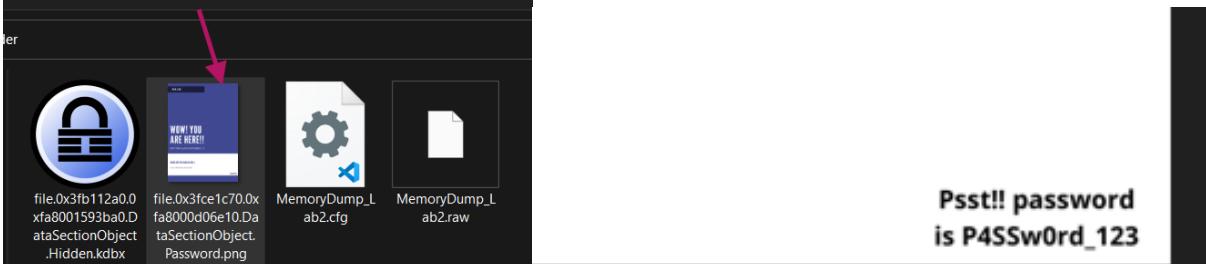
Run

Command Description: Dumps cached Windows memo



Please wait, this may take a few minutes.  
Volatility 3 Framework 2.26.2  
Cache FileObject File Name: 0x3fce1c70  
DataSectionObject DataSectionObject 0x3fce1c70  
Time Stamp: Thu Dec 21 20:50:50 2005

Result: Password.png  
file.0x3fce1c70.0xfa8000d06e10.DataSectionObject.Password.png.dat



file.0x3fb112a00.xfa8001593ba0.D ataSectionObject.Hidden.kdbx

file.0x3fce1c70.0xfa8000d06e10.D ataSectionObject.Password.png

MemoryDump\_L ab2.cfg

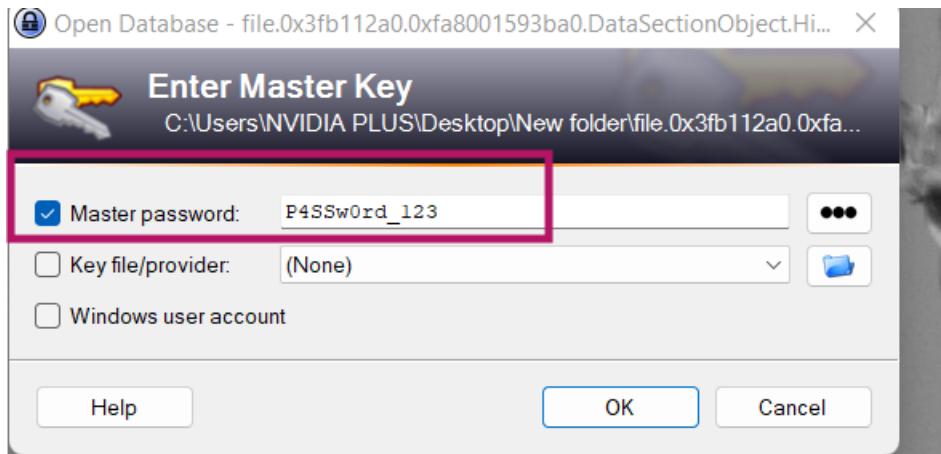
MemoryDump\_L ab2.raw

Psst!! password  
is P4SSw0rd\_123

## Using the Recovered Password to Unlock KeePass

After dumping the image file **Password.png** from memory and analyzing its contents, the password was successfully recovered.

The next step was to use this password as the **master password** for the **KeePass database** that was also found in the memory dump.



The screenshot shows the main KeePass interface with a toolbar at the top and a menu bar. The left sidebar shows a tree view with a 'Hidden' node expanded, containing categories like General, Windows, Network, Internet, eMail, Homebanking, and Recycle Bin. The main pane displays a table of entries:

Title	User Name	Password	URL	Notes
Sample Entry	User Name	*****	https://keepass.info/	Notes
Sample Entr...	Michael321	*****	https://keepass.info/hel...	
Sabka Baap	Flag	*****		

Right click on username “flag”

