

Họ và tên: Tiên Phú Huy

Mã học viên: 250104009

### Bài Tập 3 – Memory Analysis

#### **I. Chuẩn Bị Môi Trường Phân Tích**

(Nội dung: kiểm tra cấu hình hệ thống, tải công cụ, chuẩn bị thư mục lab)

#### **II. Thu Thập Thông Tin Cơ Bản Từ RAM Dump**

(Nội dung: imageinfo, profile, pstree, consoles, giải mã flag stage 1)

#### **III. Khôi Phục Dữ Liệu Ảnh Từ Vùng Nhớ Tiền Trình**

(Nội dung: memdump tiền trình PID 2424 → xử lý raw pixel → tạo ảnh → lấy flag stage 2)

#### **IV. Truy Vết và Phục Hồi Tập Tin Bị Ẩn Trong RAM**

(Nội dung: filescan → dumpfile → đổi dat → rar → hashdump phá mật khẩu → xem flag stage 3)

#### **V. Tổng Hợp Các Flag Thu Được**

(Nội dung: liệt kê stage 1–3)

## **I. Chuẩn Bị Môi Trường Phân Tích**

### **Kiểm tra môi trường thực hành**

Nhấn tổ hợp phím Windows + R để mở hộp thoại Run.

Gõ msinfo32 vào ô và Enter.

Một cửa sổ Thông tin hệ thống sẽ hiện ra, cung cấp chi tiết về phần cứng, phần mềm và các cấu hình khác của máy.

System Information	
File	Edit
<b>System Summary</b>	
Hardware Resources	
Components	
Software Environment	
Item	Value
OS Name	Microsoft Windows 11 Home Single Language
Version	10.0.26200 Build 26200
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	AURORA
System Manufacturer	Dell Inc.
System Model	G3 3590
System SKU	x64-based PC
Processor	Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 2400 Mhz, 4 Core(s), 8 Logical ...
BIOS Version/Date	Dell Inc. 1.21.0, 4/10/2023
SMBIOS Version	3.2
Embedded Controller Version	255.255
BIOS Mode	UEFI
BaseBoard Manufacturer	Dell Inc.
BaseBoard Product	0VFVNR
BaseBoard Version	A00
Platform Role	Mobile
Secure Boot State	On
PCR7 Configuration	Elevation Required to View
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	Version = "10.0.26100.1"
User Name	Aurora\tpphy

Thông tin này giúp xác định RAM dump thuộc hệ điều hành nào (ví dụ Win7SP1x64).

## Download Tools

+ Tải Volatility từ Github: <https://github.com/volatilityfoundation/volatility/releases>

Vì Github có cập nhật một số tính năng và sửa lỗi cho bản 2.6

+ Tải memory dump sẵn:

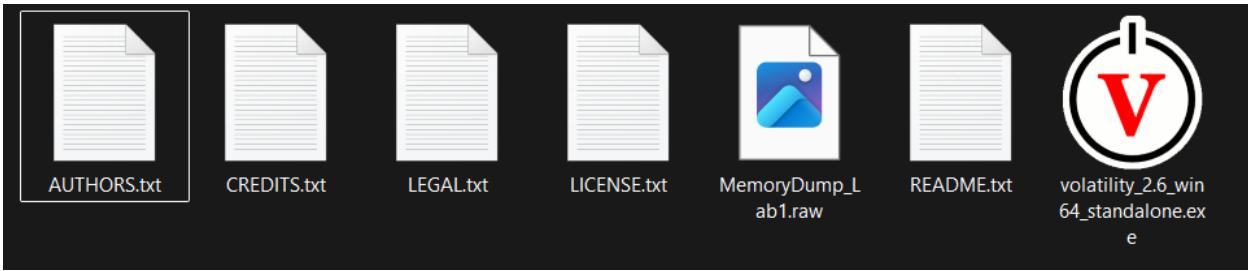
<https://drive.google.com/file/d/1sfvCHSWTFRuRsmh787XfOMt5xKCHgVcW>

▼ Assets 7			
	<a href="#">hashes.txt</a>	671 Bytes	Apr 10, 2024
	<a href="#">volatility-2.6.zip</a>	3.99 MB	Apr 10, 2024
	<a href="#">volatility_2.6_lin64_standalone.zip</a>	14.1 MB	Apr 10, 2024
	<a href="#">volatility_2.6_mac64_standalone.zip</a>	18.9 MB	Apr 10, 2024
	<a href="#">volatility_2.6_win64_standalone.zip</a>	14.8 MB	Apr 10, 2024
	<a href="#">Source code (zip)</a>		Dec 19, 2018
	<a href="#">Source code (tar.gz)</a>		Dec 19, 2018

## Tạo thư mục MemoryForensicLab01:

+ Giải nén tất cả MemoryForensicLab01.rar có tệp MemoryDump\_Lab1.raw

+ Volatility đã tải về từ Github



```
PS C:\Users\tphuy\OneDrive\Desktop\ANBMTT\MemoryForensicLab01> ls

Directory: C:\Users\tphuy\OneDrive\Desktop\ANBMTT\MemoryForensicLab01

Mode                LastWriteTime         Length Name
----                -              ----- 
-a---        12/27/2016 10:44 PM          778 AUTHORS.txt
-a---        12/27/2016 10:52 PM        3917 CREDITS.txt
-a---         7/7/2016 9:16 AM          698 LEGAL.txt
-a---         7/7/2016 9:16 AM        15127 LICENSE.txt
-a---        12/11/2019 9:38 PM      1073676288 MemoryDump_Lab1.raw
-a---        12/24/2016 9:13 PM        31879 README.txt
-a---        12/27/2016 11:02 PM      15794079 volatility_2.6_win64_standalone.exe
```

## II. Thu Thập Thông Tin Cơ Bản Từ RAM Dump

### imageinfo

```
volatility_2.6_win64_standalone.exe imageinfo -f .\MemoryDump_Lab1.raw
```

```
PS C:\Users\tphuy\OneDrive\Desktop\ANBMTT\MemoryForensicLab01> .\volatility_2.6_win64_standalone.exe imageinfo -f .\MemoryDump_Lab1.raw
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
INFO    :                         Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
INFO    :                         AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
INFO    :                         AS Layer2 : FileAddressSpace (C:\Users\tphuy\OneDrive\Desktop\ANBMTT\MemoryForensicLab01\MemoryDump_Lab1.raw)
INFO    :                         PAE type : No PAE
INFO    :                         DTB : 0x187000L
INFO    :                         KDBG : 0xf800028100a0L
INFO    :                         Number of Processors : 1
INFO    :                         Image Type (Service Pack) : 1
INFO    :                           KPCR for CPU 0 : 0xfffff80002811d00L
INFO    :                           KUSER_SHARED_DATA : 0xfffff78000000000L
INFO    :                         Image date and time : 2019-12-11 14:38:00 UTC+0000
INFO    :                         Image local date and time : 2019-12-11 20:08:00 +0530
```

Dùng imageinfo để tìm profile phù hợp.

Volatility cần profile đúng thì mới phân tích chính xác.

Kết quả cho thấy dùng profile: **Win7SP1x64**.

### profile

```
.\volatility_2.6_win64_standalone.exe -f .\MemoryDump_Lab1.raw --profile Win7SP1x64 pstree
```

Name	Pid	PPid	Thds	Hnds	Time
0xfffffa8000f4c670:explorer.exe	2504	3000	34	825	2019-12-11 14:37:14 UTC+0000
. 0xfffffa8000f9a4e0:VBoxTray.exe	2304	2504	14	144	2019-12-11 14:37:14 UTC+0000
. 0xfffffa8001010b30:WinRAR.exe	1512	2504	6	207	2019-12-11 14:37:23 UTC+0000
0xfffffa8001c5f630:wininit.exe	424	312	3	75	2019-12-11 13:41:34 UTC+0000
. 0xfffffa8001c98530:services.exe	484	424	13	219	2019-12-11 13:41:35 UTC+0000
.. 0xfffffa8002170630:wmpnetwk.exe	1856	484	16	451	2019-12-11 14:16:08 UTC+0000
.. 0xfffffa8001f91b30:TCPSPVCS.EXE	1416	484	4	97	2019-12-11 13:41:55 UTC+0000
.. 0xfffffa8001da96c0:svchost.exe	876	484	32	941	2019-12-11 13:41:43 UTC+0000
.. 0xfffffa8001d327c0:VBoxService.exe	652	484	13	137	2019-12-11 13:41:40 UTC+0000
.. 0xfffffa8000eac770:svchost.exe	2660	484	6	100	2019-12-11 14:35:14 UTC+0000
.. 0xfffffa80022199e0:svchost.exe	2368	484	9	365	2019-12-11 14:32:51 UTC+0000
.. 0xfffffa8001e50b30:svchost.exe	1044	484	14	366	2019-12-11 13:41:48 UTC+0000
.. 0xfffffa8001d8c420:svchost.exe	816	484	23	569	2019-12-11 13:41:42 UTC+0000
.. . 0xfffffa80021da060:audiodg.exe	2064	816	6	131	2019-12-11 14:32:37 UTC+0000
.. 0xfffffa8001c38580:svchost.exe	948	484	13	322	2019-12-11 14:16:07 UTC+0000
.. 0xfffffa8001leba230:spoolsv.exe	1208	484	13	282	2019-12-11 13:41:51 UTC+0000
.. 0xfffffa8001d376f0:SearchIndexer.	480	484	14	701	2019-12-11 14:16:09 UTC+0000
.. . 0xfffffa8000ffff630:SearchProtocol	2524	480	7	226	2019-12-11 14:37:21 UTC+0000
.. . 0xfffffa8001020b30:SearchProtocol	2868	480	8	279	2019-12-11 14:37:23 UTC+0000
.. . 0xfffffa8000ecea60:SearchFilterHo	1720	480	5	90	2019-12-11 14:37:21 UTC+0000
.. 0xfffffa8000f3aab0:taskhost.exe	2908	484	9	158	2019-12-11 14:37:13 UTC+0000
.. 0xfffffa8001cf4b30:svchost.exe	588	484	11	358	2019-12-11 13:41:39 UTC+0000
.. 0xfffffa8001d49b30:svchost.exe	720	484	8	279	2019-12-11 13:41:41 UTC+0000
.. 0xfffffa8001da5b30:svchost.exe	852	484	28	542	2019-12-11 13:41:43 UTC+0000
.. . 0xfffffa8000f4db30:dwm.exe	3004	852	5	72	2019-12-11 14:37:14 UTC+0000
.. . 0xfffffa8001dfa910:dwm.exe	1988	852	5	72	2019-12-11 14:32:25 UTC+0000
.. 0xfffffa8001e1bb30:svchost.exe	472	484	19	476	2019-12-11 13:41:47 UTC+0000
.. 0xfffffa8000d3c400:sppsvc.exe	1508	484	4	141	2019-12-11 14:16:06 UTC+0000
.. 0xfffffa8001f58890:svchost.exe	1372	484	22	295	2019-12-11 13:41:54 UTC+0000
.. . 0xfffffa8001eda060:svchost.exe	1248	484	19	313	2019-12-11 13:41:52 UTC+0000
.. . 0xfffffa8001eb47f0:taskhost.exe	296	484	8	151	2019-12-11 14:32:24 UTC+0000
.. 0xfffffa8001ca0580:lsass.exe	492	424	9	764	2019-12-11 13:41:35 UTC+0000
.. 0xfffffa8001ca4b30:lsm.exe	500	424	11	185	2019-12-11 13:41:35 UTC+0000
0xfffffa800154f740:csrss.exe	320	312	9	457	2019-12-11 13:41:32 UTC+0000
0xfffffa8000ca0040:System	4	0	80	570	2019-12-11 13:41:25 UTC+0000
. 0xfffffa800148f040:smss.exe	248	4	3	37	2019-12-11 13:41:25 UTC+0000
.. 0xfffffa8001c45060:psxss.exe	376	248	18	786	2019-12-11 13:41:33 UTC+0000
0xfffffa8001c5f060:winlogon.exe	416	360	4	118	2019-12-11 13:41:34 UTC+0000
0xfffffa8000ca81e0:csrss.exe	368	360	7	199	2019-12-11 13:41:33 UTC+0000
. 0xfffffa8002227140:conhost.exe	2692	368	2	50	2019-12-11 14:34:54 UTC+0000
. 0xfffffa800104a780:conhost.exe	2260	368	2	50	2019-12-11 14:37:54 UTC+0000
0xfffffa8002046960:explorer.exe	604	2016	33	927	2019-12-11 14:32:25 UTC+0000
. 0xfffffa80021c75d0:VBoxTray.exe	1844	604	11	140	2019-12-11 14:32:35 UTC+0000
. 0xfffffa8002222780:cmd.exe	1984	604	1	21	2019-12-11 14:34:54 UTC+0000
. 0xfffffa80022bab30:mspaint.exe	2424	604	6	128	2019-12-11 14:35:14 UTC+0000
. 0xfffffa8001048060:DumpIt.exe	796	604	2	45	2019-12-11 14:37:54 UTC+0000
0xfffffa8001e68060:csrss.exe	2760	2680	7	172	2019-12-11 14:37:05 UTC+0000
0xfffffa8000ecbb30:winlogon.exe	2808	2680	4	119	2019-12-11 14:37:05 UTC+0000

Những lệnh này giúp quan sát tiến trình, cây tiến trình, và dòng lệnh mà các tiến trình đã chạy.

### pstree

```
\volatility_2.6_win64_standalone.exe -f .\MemoryDump_Lab1.raw --profile Win7SP1x64
cmdline -p 2504,2304,1512,1984,2424
```

```
PS C:\Users\tphuy\OneDrive\Desktop\ANBMTT\MemoryForensicLab01> .\volatility_2.6_win64_standalone.exe -V
Volatility Foundation Volatility Framework 2.6
*****
cmd.exe pid: 1984
Command line : "C:\Windows\system32\cmd.exe"
*****
mspaint.exe pid: 2424
Command line : "C:\Windows\system32\mspaint.exe"
*****
explorer.exe pid: 2504
Command line : C:\Windows\Explorer.EXE
*****
VBoxTray.exe pid: 2304
Command line : "C:\Windows\System32\VBoxTray.exe"
*****
WinRAR.exe pid: 1512
Command line : "C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\Alissa Simpson\Documents\Important.rar"
```

Đây là nơi nhìn ra được tiến trình lạ, tiến trình nghi ngờ, và hành vi khả nghi.

### consoles

```
.\volatility_2.6_win64_standalone.exe -f .\MemoryDump_Lab1.raw --profile Win7SP1x64
consoles
```

```

PS C:\Users\tphuy\OneDrive\Desktop\ANBMTT\MemoryForensicLab01> .\volatility_2.6_1
Volatility Foundation Volatility Framework 2.6
*****
ConsoleProcess: conhost.exe Pid: 2692
Console: 0xffff756200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe - St4G3$1
AttachedProcess: cmd.exe Pid: 1984 Handle: 0x60
----
CommandHistory: 0x1fe9c0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 at 0x1de3c0: St4G3$1
----
Screen 0x1e0f70 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\SmartNet>St4G3$1
ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=
Press any key to continue . .
*****
ConsoleProcess: conhost.exe Pid: 2260
Console: 0xffff756200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: C:\Users\SmartNet\Downloads\DumpIt\DumpIt.exe
Title: C:\Users\SmartNet\Downloads\DumpIt\DumpIt.exe
AttachedProcess: DumpIt.exe Pid: 796 Handle: 0x60
----
CommandHistory: 0x38ea90 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
----
Screen 0x371050 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: 1073676288 bytes ( 1023 Mb)
Free space size: 24185389056 bytes ( 23064 Mb)

* Destination = \??\C:\Users\SmartNet\Downloads\DumpIt\SMARTNET-PC-20191211-
143755.raw

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

```

Lệnh consoles dùng để lấy nội dung terminal trong bộ nhớ

Em phát hiện được đoạn mã: **ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=**

## CyberChef

<https://gchq.github.io/CyberChef/>

The screenshot shows the CyberChef interface. In the 'Operations' sidebar, 'From Base64' is selected. The 'Input' field contains the base64 encoded string: ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZZhIX0. The 'Output' field displays the decoded text: flag{th1s\_1s\_th3\_1st\_st4g3!!}. The 'BAKE!' button is highlighted.

Đã dịch đoạn mã từ base64 sang text và lấy được chuỗi: **flag{th1s\_1s\_th3\_1st\_st4g3!!}**

### III. Khôi Phục Dữ Liệu Ảnh Từ Vùng Nhớ Tiến Trình

#### **memdump**

```
.\\volatility_2.6_win64_standalone.exe -f .\\MemoryDump_Lab1.raw --profile Win7SP1x64
memdump -p 2424 -D .
```

```
PS C:\\Users\\tphuy\\OneDrive\\Desktop\\ANBMTT\\MemoryForensicLab01> .\\volatil
Volatility Foundation Volatility Framework 2.6
*****
Writing mspaint.exe [ 2424] to 2424.dmp
```

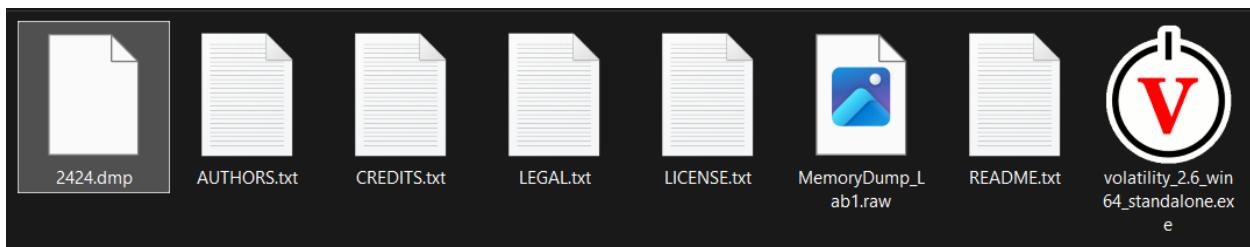
Trước đó ở phần cmdline, pstree thấy tiến trình 2424 này khả nghi — thường bài lab sẽ giàu dữ liệu trong tiến trình lạ.

Dùng memdump để trích toàn bộ vùng nhớ của tiến trình 2424.

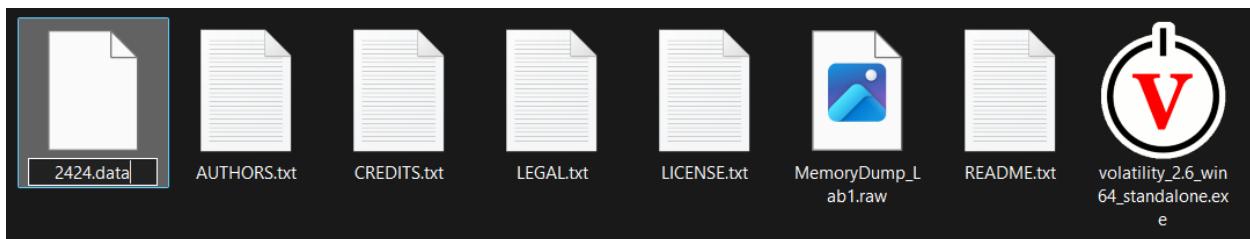
File tạo ra không phải ảnh, không có header, chỉ là raw pixel data.

#### **2424.dmp**

Sinh ra tệp tin 2424.dmp



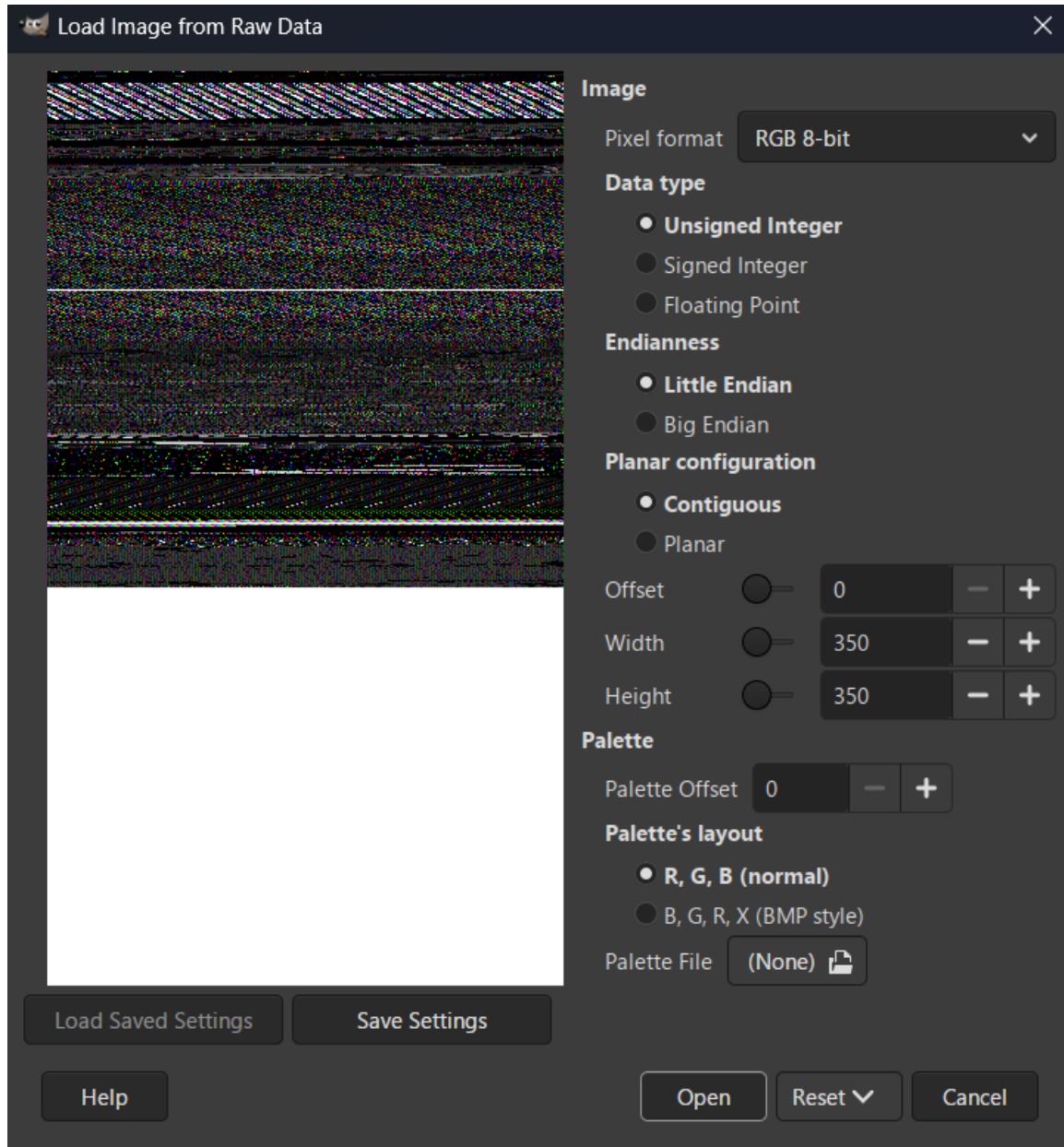
Đổi tên tệp tin 2424.data



## Gimp

<https://www.gimp.org/downloads/>

Mở 2424.data từ Gimp

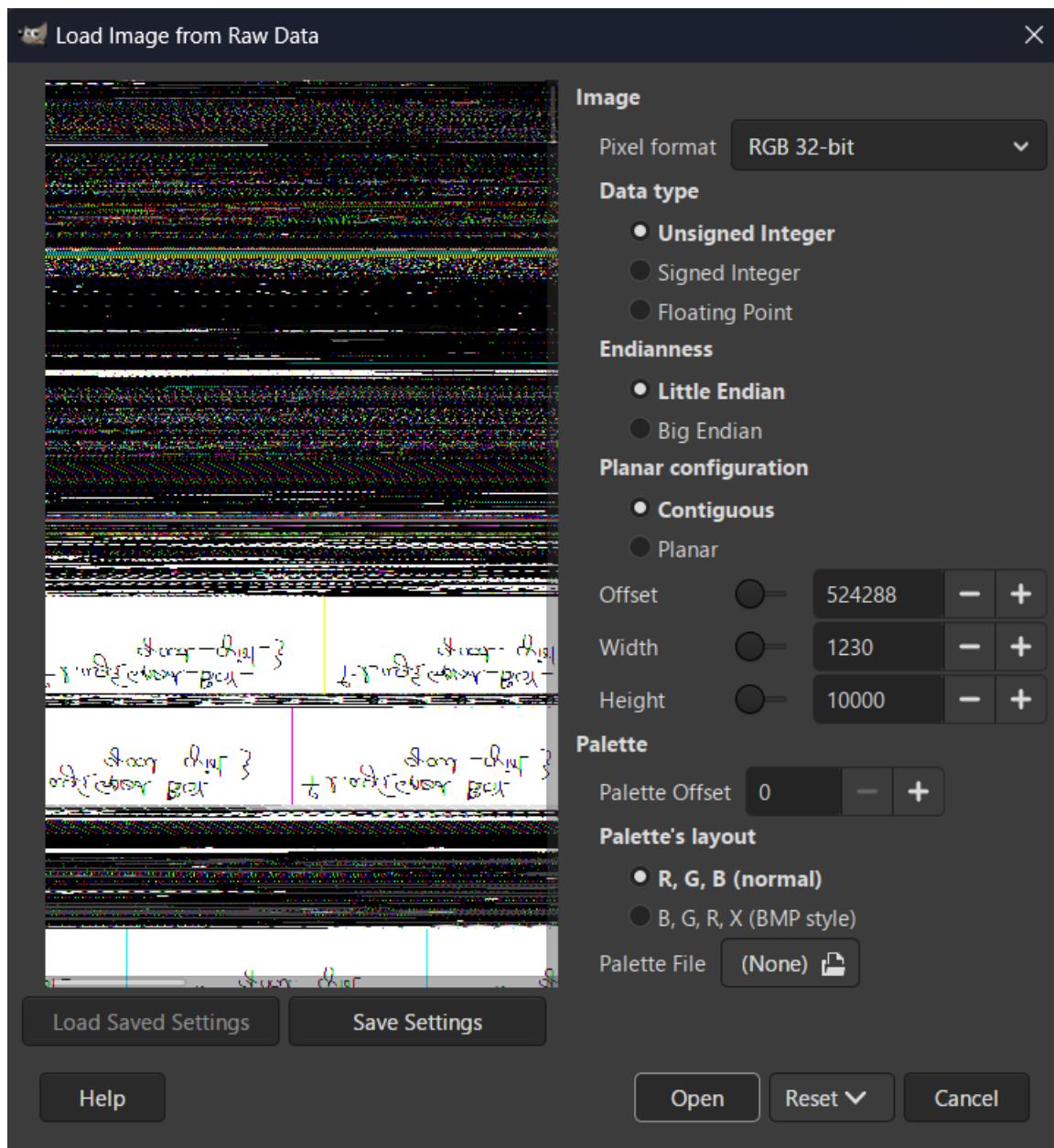


Khi mở file, GIMP hỏi:

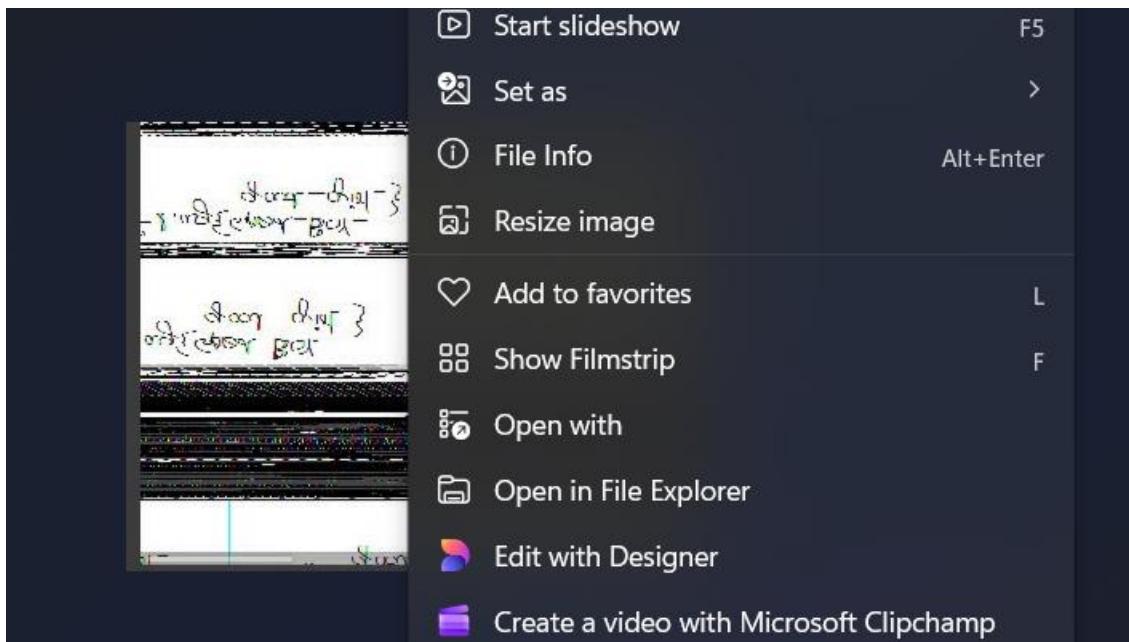
Pixel Format, Offset, Width và Height

Đây chính là trò “khóa hình”: ảnh được nhúng trong bộ nhớ nhưng bị xóa header, phải tự đoán thông số để khôi phục.

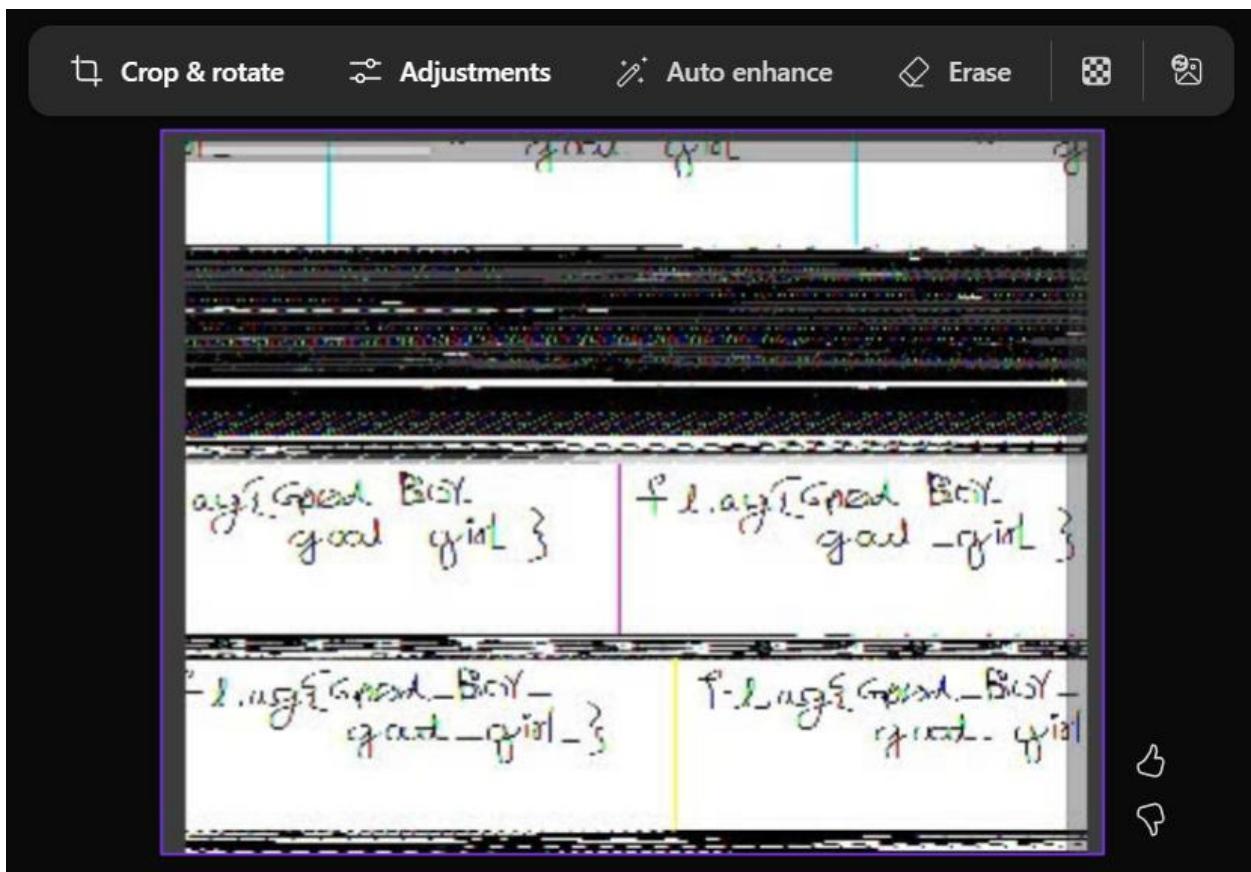
Trong lab này, chỉ cần chỉnh đúng format (thường là RGB) + chỉnh width, height + offset -> ảnh xuất hiện.



Lưu ảnh lại và sử dụng Designer



Lật ảnh để lấy chuỗi



Sau khi lật ảnh lấy được chuỗi là: **flag{Good\_BoY\_good\_girl}**

# IV. Truy Vết và Phục Hồi Tập Tin Bị Ẩn Trong RAM

## profile

```
.\volatility_2.6_win64_standalone.exe -f .\MemoryDump_Lab1.raw --profile Win7SP1x64  
cmdline -p 2504,2304,1512,1984,2424
```

```
PS C:\Users\tphuy\OneDrive\Desktop\ANBMTT\MemoryForensicLab01> .\volatility_2.6_win64_standalone.exe  
Volatility Foundation Volatility Framework 2.6  
*****  
cmd.exe pid: 1984  
Command line : "C:\Windows\system32\cmd.exe"  
*****  
mspaint.exe pid: 2424  
Command line : "C:\Windows\system32\mspaint.exe"  
*****  
explorer.exe pid: 2504  
Command line : C:\Windows\Explorer.EXE  
*****  
VBoxTray.exe pid: 2304  
Command line : "C:\Windows\System32\VBoxTray.exe"  
*****  
WinRAR.exe pid: 1512  
Command line : "C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\Alissa Simpson\Documents\Important.rar"
```

Thấy dấu vết Important.rar từ cmdline.

Điều này gợi ý file từng tồn tại trong bộ nhớ.

Khi quét profile ta thấy có Important.rar có vẻ khả nghi ở cuối.

## filescan

```
.\volatility_2.6_win64_standalone.exe -f .\MemoryDump_Lab1.raw --profile Win7SP1x64  
filescan | FINDSTR Important.rar
```

```
PS C:\Users\tphuy\OneDrive\Desktop\ANBMTT\MemoryForensicLab01> .\volatility_2.6_win64_standalone.exe -f .\MemoryDump_Lab1.raw  
Volatility Foundation Volatility Framework 2.6  
0x000000003fa3ebc0 1 0 R--- \Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar  
0x000000003fac3bc0 1 0 R--- \Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar  
0x000000003fb48bc0 1 0 R--- \Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar
```

Dùng filescan để tìm đúng một vị trí offset trong bộ nhớ 0x000000003fa3ebc0

=> đây là nơi hệ điều hành lưu metadata của file.

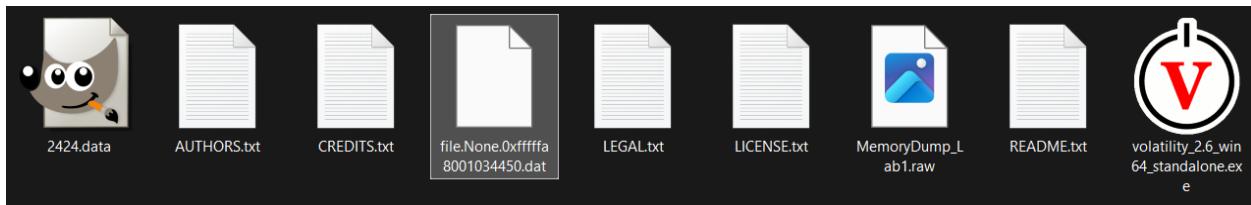
## dumpfile

```
.\volatility_2.6_win64_standalone.exe -f .\MemoryDump_Lab1.raw --profile Win7SP1x64  
dumpfiles -Q 0x000000003fa3ebc0 -D .
```

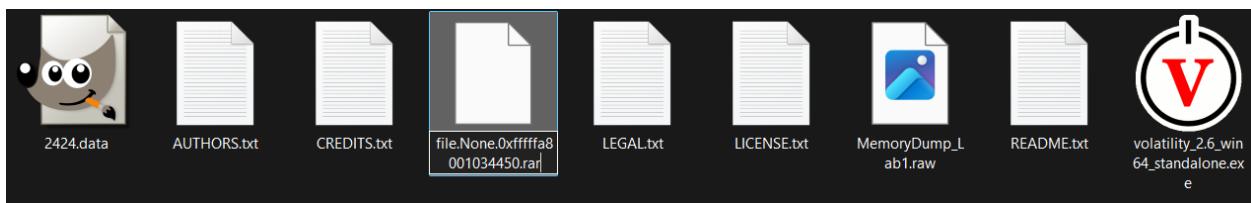
```
PS C:\Users\tphuy\OneDrive\Desktop\ANBMTT\MemoryForensicLab01> .\volatility_2.6_win64_standalone.exe -f .\MemoryDump_Lab1.raw  
Volatility Foundation Volatility Framework 2.6  
DataSectionObject 0x3fa3ebc0 None \Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar
```

Dùng dumpfiles để trích xuất file RAR từ RAM.

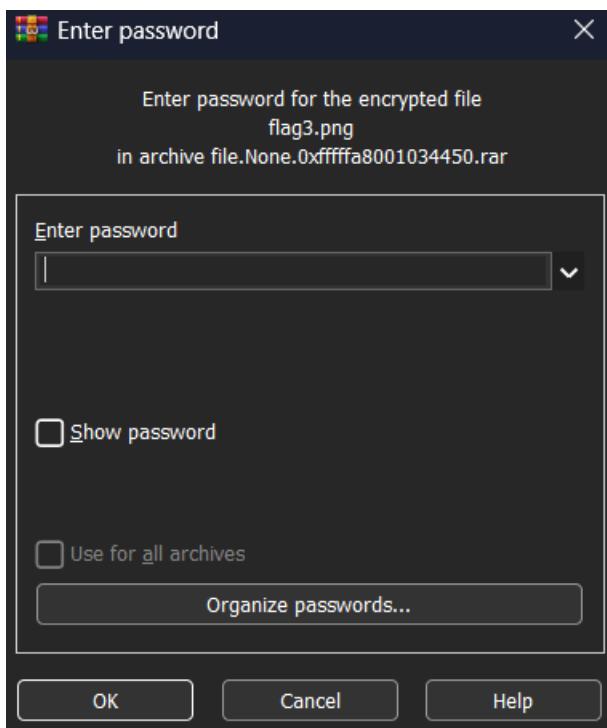
Kết quả là file .dat nên đổi lại thành .rar.



Khi kéo file ra khỏi bộ nhớ sinh ra thư mục .dat



Đổi đuôi .dat thành .rar



Phải cần password khi giải nén

file.None.0xfffffa8001034450.rar - RAR archive, unpacked size 46,045 bytes						Password is NTLM hash(in uppercase) of Alissa's account passwd.
Name	Size	Packed	Type	Modified	Checksum	
..			File folder			
flag3.png *	46,045	41,856	PNG File	12/11/2019 8:3...	997C37CD	

Kiểm tra thông tin thì thấy có một ảnh flag3.png và password gợi ý là viết hoa khi hash

## hashdump

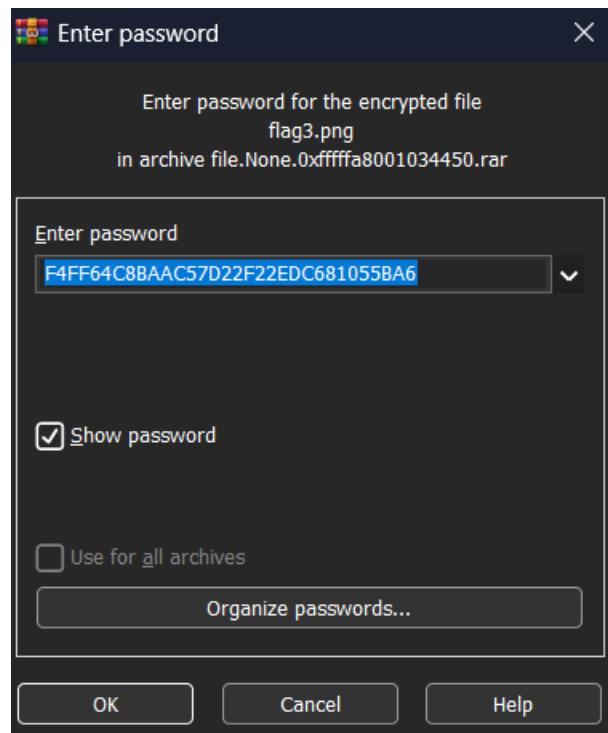
```
.\\volatility_2.6_win64_standalone.exe -f .\\MemoryDump_Lab1.raw --profile Win7SP1x64  
hashdump
```

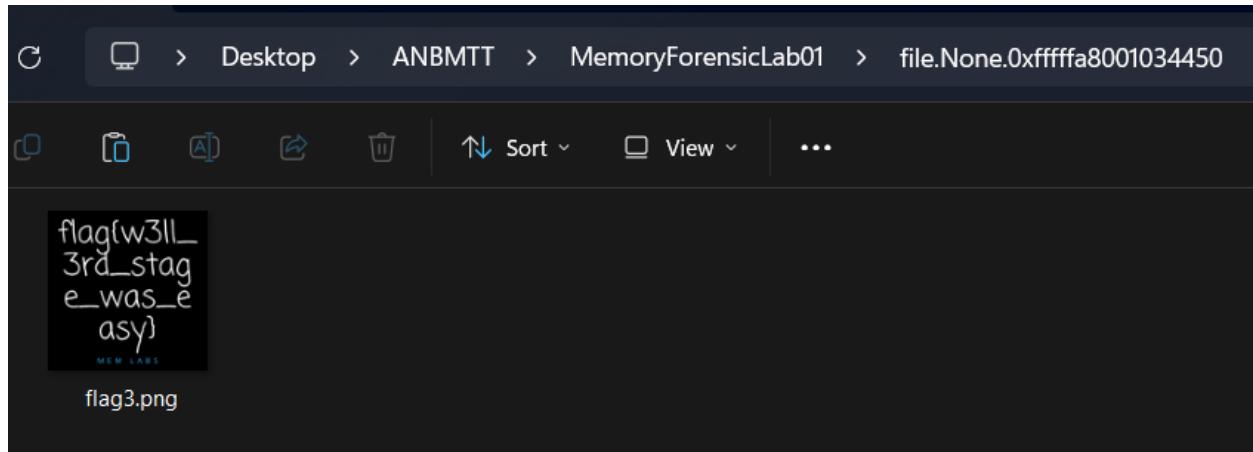
```
PS C:\\Users\\tphuy\\OneDrive\\Desktop\\ANBMTT\\MemoryForensicLab01> .\\volatility_2.6_win64_standalone.exe -f .\\MemoryDump_Lab1.raw --profile Win7SP1x64 hashdump  
Volatility Foundation Volatility Framework 2.6  
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
SmartNet:1001:aad3b435b51404eeaad3b435b51404ee:4943abb39473a6f32c11301f4987e7e0:::  
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f0fc3d257814e08fea06e63c5762ebd5:::  
Alissa Simpson:1003:aad3b435b51404eeaad3b435b51404ee:f4ff64c8baac57d22f22edc681055ba6:::
```

Sinh ra được chuỗi: f4ff64c8baac57d22f22edc681055ba6

In hoa lên: F4FF64C8BAAC57D22F22EDC681055BA6

Và nhập password





Giải nén thành công và xem flag3.png lấy được chuỗi: **flag{w3ll\_3rd\_stage\_was\_easy}**

## V. Tổng Hợp Các Flag Thu Được

Từ (1), (2) và (3) lấy được:

(1): **flag{th1s\_1s\_th3\_1st\_st4g3!!}**

(2): **flag{Good\_BoY\_good\_girl}**

(3): **flag{w3ll\_3rd\_stage\_was\_easy}**