BÁO CÁO BÀI TẬP

Môn học: Pháp chứng kĩ thuật số

Tên chủ đề: MEMLABS

GVHD: Nghi Hoàng Khoa

1. **THÔNG TIN CHUNG:**

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.O21.ANTN

STT	Họ và tên	MSSV	Email
1	Hà Thị Thu Hiền	21522056	21522056@gm.uit.edu.vn
2	Phạm Ngọc Thơ	21522641	21522641@gm.uit.edu.vn
3	Nguyễn Ngọc Nhung	21521248	21521248@gm.uit.edu.vn

2. **NỘI DUNG THỰC HIỆN:**[1]

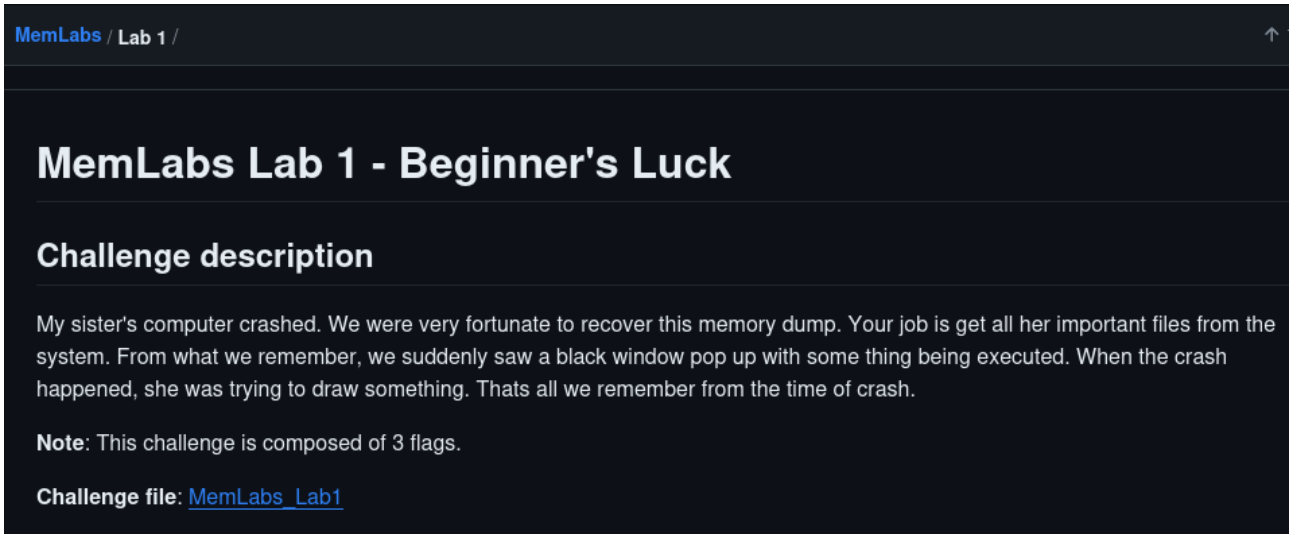
STT	Công việc	Kết quả tự đánh giá
1	MemLabs Lab 1	100%
2	MemLabs Lab 2	100%
3	MemLabs Lab 3	100%
4	MemLabs Lab 4	100%
5	MemLabs Lab 5	100%
6	MemLabs Lab 6	

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

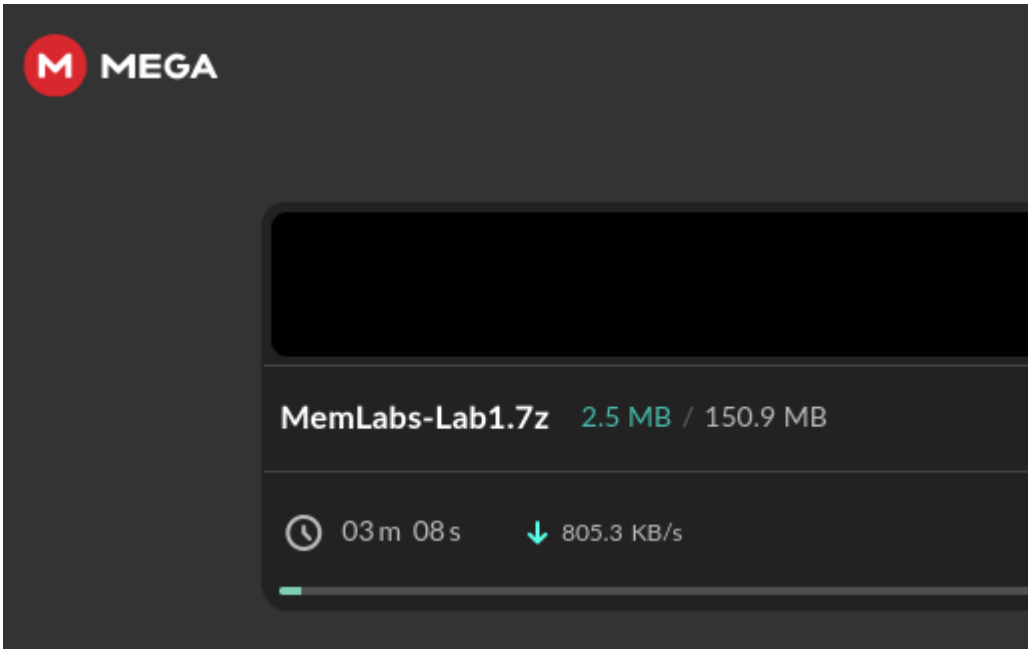
[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

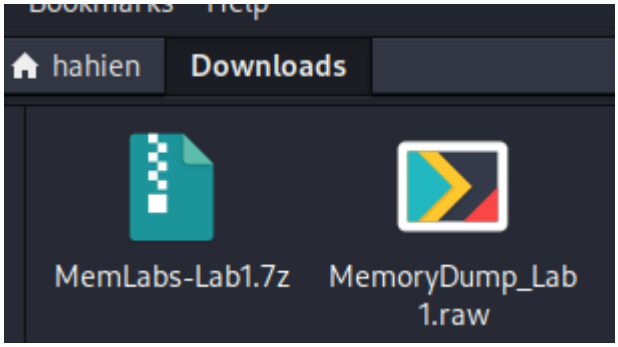
1. Lab 1 - Beginner's Luck



- Đầu tiên, ta hãy tải challenge file về máy kali:



- Sau khi tải file thành công, chúng ta sử dụng volatility với plugin là imageinfo để xem thông tin:




```
┌──(root㉿kali)-[~/volatility]
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab1.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000,
3418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/hahien/Downloads/MemoryDump_Lab1.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800028100a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002811d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2019-12-11 14:38:00 UTC+0000
     Image local date and time : 2019-12-11 20:08:00 +0530
```

➔ Profile được điều tra là Win7SP1x64.

- Theo mô tả **"we suddenly saw a black window pop up with some thing being executed."** Có thể là màn hình cmd ➔ thử kiểm tra các tiến trình được chạy với plugin pslist:

```
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab1.raw --profile Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8000ca0040 System                    4      0     80      570 ------      0 2019-12-11 13:41:25 UTC+0000
0xfffffa800148f040 smss.exe                248      4      3       37 ------      0 2019-12-11 13:41:25 UTC+0000
0xfffffa800154f740 csrss.exe               320    312      9      457      0      0 2019-12-11 13:41:32 UTC+0000
0xfffffa8000ca81e0 csrss.exe               368    360      7      199      1      0 2019-12-11 13:41:33 UTC+0000
0xfffffa8001c45060 psxss.exe               376    248     18      786      0      0 2019-12-11 13:41:33 UTC+0000
0xfffffa8001c5f060 winlogon.exe            416    360      4      118      1      0 2019-12-11 13:41:34 UTC+0000
0xfffffa8001c5f630 wininit.exe             424    312      3       75      0      0 2019-12-11 13:41:34 UTC+0000
0xfffffa8001c98530 services.exe            484    424     13      219      0      0 2019-12-11 13:41:35 UTC+0000
0xfffffa8001ca0580 lsass.exe               492    424      9      764      0      0 2019-12-11 13:41:35 UTC+0000
0xfffffa8001ca4b30 lsm.exe                 500    424     11      185      0      0 2019-12-11 13:41:35 UTC+0000
0xfffffa8001cf4b30 svchost.exe             588    484     11      358      0      0 2019-12-11 13:41:39 UTC+0000
0xfffffa8001d327c0 VBoxService.ex          652    484     13      137      0      0 2019-12-11 13:41:40 UTC+0000
0xfffffa8001d49b30 svchost.exe             720    484      8      279      0      0 2019-12-11 13:41:41 UTC+0000
0xfffffa8001d8c420 svchost.exe             816    484     23      569      0      0 2019-12-11 13:41:42 UTC+0000
0xfffffa8001da5b30 svchost.exe             852    484     28      542      0      0 2019-12-11 13:41:43 UTC+0000
0xfffffa8001da96c0 svchost.exe             876    484     32      941      0      0 2019-12-11 13:41:43 UTC+0000
0xfffffa8001e1bb30 svchost.exe             472    484     19      476      0      0 2019-12-11 13:41:47 UTC+0000
0xfffffa8001e50b30 svchost.exe            1044    484     14      366      0      0 2019-12-11 13:41:48 UTC+0000
0xfffffa8001eba230 spoolsv.exe            1208    484     13      282      0      0 2019-12-11 13:41:51 UTC+0000
0xfffffa8001eda060 svchost.exe            1248    484     19      313      0      0 2019-12-11 13:41:52 UTC+0000
0xfffffa8001f58890 svchost.exe            1372    484     22      295      0      0 2019-12-11 13:41:54 UTC+0000
0xfffffa8001f91b30 TCPSVCS.EXE            1416    484      4       97      0      0 2019-12-11 13:41:55 UTC+0000
0xfffffa8000d3c400 sppsvc.exe             1508    484      4      141      0      0 2019-12-11 14:16:06 UTC+0000
0xfffffa8001c38580 svchost.exe             948    484     13      322      0      0 2019-12-11 14:16:07 UTC+0000
0xfffffa8002170630 wmpnetwk.exe           1856    484     16      451      0      0 2019-12-11 14:16:08 UTC+0000
0xfffffa8001d376f0 SearchIndexer.          480    484     14      701      0      0 2019-12-11 14:16:09 UTC+0000
0xfffffa8001eb47f0 taskhost.exe            296    484      8      151      1      0 2019-12-11 14:32:24 UTC+0000
0xfffffa8001f58890 svchost.exe            1372    484     22      295      0      0 2019-12-11 13:41:54 UTC+0000
0xfffffa8001f91b30 TCPSVCS.EXE            1416    484      4       97      0      0 2019-12-11 13:41:55 UTC+0000
0xfffffa8000d3c400 sppsvc.exe             1508    484      4      141      0      0 2019-12-11 14:16:06 UTC+0000
0xfffffa8001c38580 svchost.exe             948    484     13      322      0      0 2019-12-11 14:16:07 UTC+0000
0xfffffa8002170630 wmpnetwk.exe           1856    484     16      451      0      0 2019-12-11 14:16:08 UTC+0000
0xfffffa8001d376f0 SearchIndexer.          480    484     14      701      0      0 2019-12-11 14:16:09 UTC+0000
0xfffffa8001eb47f0 taskhost.exe            296    484      8      151      1      0 2019-12-11 14:32:24 UTC+0000
0xfffffa8001dfa910 dwm.exe                1988    852      5       72      1      0 2019-12-11 14:32:25 UTC+0000
0xfffffa8002046960 explorer.exe            604   2016     33      927      1      0 2019-12-11 14:32:25 UTC+0000
0xfffffa80021c75d0 VBoxTray.exe           1844    604     11      140      1      0 2019-12-11 14:32:35 UTC+0000
0xfffffa80021da060 audiodg.exe            2064    816      6      131      0      0 2019-12-11 14:32:37 UTC+0000
0xfffffa80022199e0 svchost.exe            2368    484      9      365      0      0 2019-12-11 14:32:51 UTC+0000
0xfffffa8002222780 cmd.exe                1984    604      1       21      1      0 2019-12-11 14:34:54 UTC+0000
0xfffffa8002227140 conhost.exe            2692    368      2       50      1      0 2019-12-11 14:34:54 UTC+0000
0xfffffa80022bab30 mspaint.exe            2424    604      6      128      1      0 2019-12-11 14:35:14 UTC+0000
0xfffffa8000eac770 svchost.exe            2660    484      6      100      0      0 2019-12-11 14:35:14 UTC+0000
0xfffffa8001e68060 csrss.exe              2760   2680      7      172      2      0 2019-12-11 14:37:05 UTC+0000
0xfffffa8000ecbb30 winlogon.exe           2808   2680      4      119      2      0 2019-12-11 14:37:05 UTC+0000
0xfffffa8000f3aab0 taskhost.exe           2908    484      9      158      2      0 2019-12-11 14:37:13 UTC+0000
0xfffffa8000f4db30 dwm.exe                3004    852      5       72      2      0 2019-12-11 14:37:14 UTC+0000
0xfffffa8000f4c670 explorer.exe           2504   3000     34      825      2      0 2019-12-11 14:37:14 UTC+0000
0xfffffa8000f9a4e0 VBoxTray.exe           2304   2504     14      144      2      0 2019-12-11 14:37:14 UTC+0000
0xfffffa8000fff630 SearchProtocol         2524    480      7      226      2      0 2019-12-11 14:37:21 UTC+0000
0xfffffa8000ecea60 SearchFilterHo         1720    480      5       90      0      0 2019-12-11 14:37:21 UTC+0000
0xfffffa8001010b30 WinRAR.exe             1512   2504      6      207      2      0 2019-12-11 14:37:23 UTC+0000
0xfffffa8001020b30 SearchProtocol         2868    480      8      279      0      0 2019-12-11 14:37:23 UTC+0000
0xfffffa8001048060 DumpIt.exe              796    604      2       45      1      1 2019-12-11 14:37:54 UTC+0000
0xfffffa800104a780 conhost.exe            2260    368      2       50      1      0 2019-12-11 14:37:54 UTC+0000

┌──(root㉿kali)-[~/volatility]
└─#
```

- Ta thấy tiến trình cmd.exe ➔ dùng plugin cmdscan để kiểm tra:

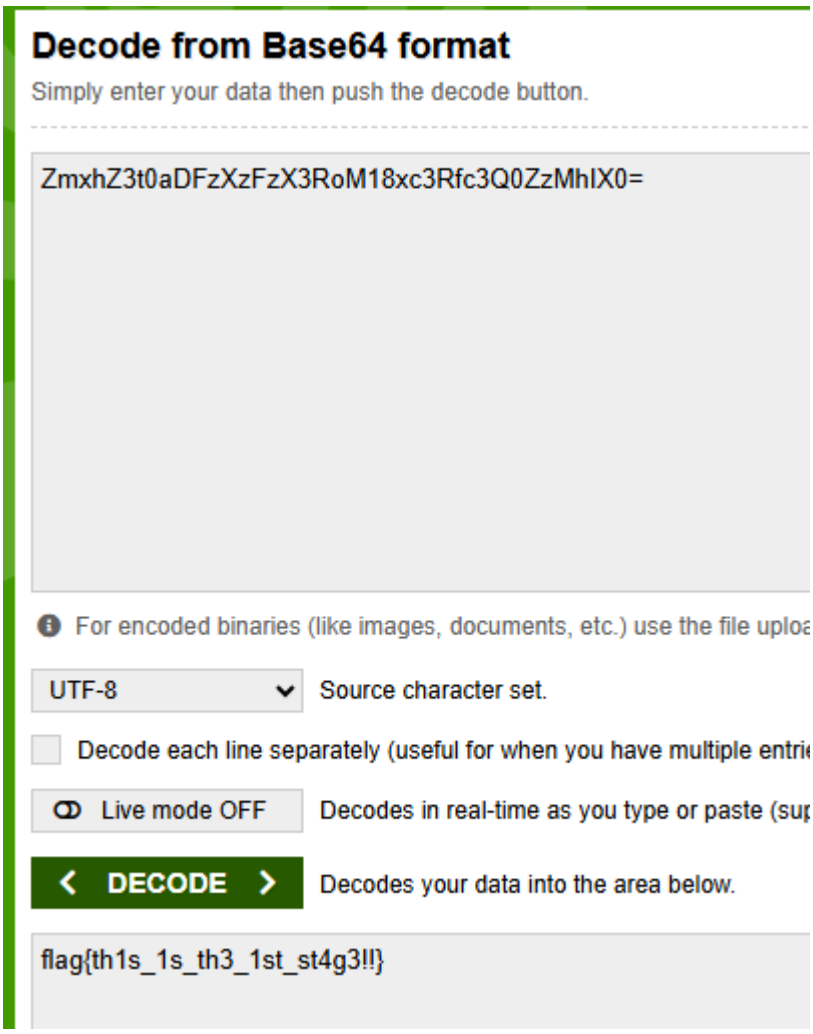
```
┌──(root㉿kali)-[~/volatility]
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab1.raw --profile Win7SP1x64 cmdscan
Volatility Foundation Volatility Framework 2.6.1
**************************************************
CommandProcess: conhost.exe Pid: 2692
CommandHistory: 0x1fe9c0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0x1de3c0: St4G3$1
Cmd #15 @ 0x1c0158:
Cmd #16 @ 0x1fdb30:
**************************************************
CommandProcess: conhost.exe Pid: 2260
CommandHistory: 0x38ea90 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #15 @ 0x350158: 8
Cmd #16 @ 0x38dc00: 8
```

- Phát hiện được 1 chuỗi: **St4G3$1**
- Dùng plugin consoles để kiểm tra rõ hơn về chuỗi này:

```
┌──(root㉿kali)-[~/volatility]
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab1.raw --profile Win7SP1x64 consoles
Volatility Foundation Volatility Framework 2.6.1
**************************************************
ConsoleProcess: conhost.exe Pid: 2692
Console: 0xff756200 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: 0xff756200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
```

➔ Ta phát hiện 1 chuỗi base64 encoded:
ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=

- Giải mã base64 ta được:



➔ **STAGE 1: flag{th1s_1s_th3_1st_st4g3!!}**

- Để tìm flag 2 thì ta tiếp tục dựa vào thông tin mô tả sau: **"When the crash happened, she was trying to draw something."** Tiếp tục nhìn vào thông tin sau, ta thấy:

```
0xfffffa8001f58890 svchost.exe        1372    484     22      295     0      0 2019-12-11 13:41:54 UTC+0000
0xfffffa8001f91b30 TCPSVCS.EXE        1416    484      4       97     0      0 2019-12-11 13:41:55 UTC+0000
0xfffffa8000d3c400 sppsvc.exe         1508    484      4      141     0      0 2019-12-11 14:16:06 UTC+0000
0xfffffa8001c38580 svchost.exe         948    484     13      322     0      0 2019-12-11 14:16:07 UTC+0000
0xfffffa8002170630 wmpnetwk.exe       1856    484     16      451     0      0 2019-12-11 14:16:08 UTC+0000
0xfffffa8001d376f0 SearchIndexer.      480    484     14      701     0      0 2019-12-11 14:16:09 UTC+0000
0xfffffa8001eb47f0 taskhost.exe        296    484      8      151     1      0 2019-12-11 14:32:24 UTC+0000
0xfffffa8001dfa910 dwm.exe            1988    852      5       72     1      0 2019-12-11 14:32:25 UTC+0000
0xfffffa8002046960 explorer.exe        604   2016     33      927     1      0 2019-12-11 14:32:25 UTC+0000
0xfffffa80021c75d0 VBoxTray.exe       1844    604     11      140     1      0 2019-12-11 14:32:35 UTC+0000
0xfffffa80021da060 audiodg.exe        2064    816      6      131     0      0 2019-12-11 14:32:37 UTC+0000
0xfffffa80022199e0 svchost.exe        2368    484      9      365     0      0 2019-12-11 14:32:51 UTC+0000
0xfffffa8002222780 cmd.exe            1984    604      1       21     1      0 2019-12-11 14:34:54 UTC+0000
0xfffffa8002227140 conhost.exe        2692    368      2       50     1      0 2019-12-11 14:34:54 UTC+0000
0xfffffa80022bab30 mspaint.exe        2424    604      6      128     1      0 2019-12-11 14:35:14 UTC+0000
0xfffffa8000eac770 svchost.exe        2660    484      6      100     0      0 2019-12-11 14:35:14 UTC+0000
0xfffffa8001e68060 csrss.exe          2760   2680      7      172     2      0 2019-12-11 14:37:05 UTC+0000
0xfffffa8000ecbb30 winlogon.exe       2808   2680      4      119     2      0 2019-12-11 14:37:05 UTC+0000
0xfffffa8000f3aab0 taskhost.exe       2908    484      9      158     2      0 2019-12-11 14:37:13 UTC+0000
0xfffffa8000f4db30 dwm.exe            3004    852      5       72     2      0 2019-12-11 14:37:14 UTC+0000
0xfffffa8000f4c670 explorer.exe       2504   3000     34      825     2      0 2019-12-11 14:37:14 UTC+0000
0xfffffa8000f9a4e0 VBoxTray.exe       2304   2504     14      144     2      0 2019-12-11 14:37:14 UTC+0000
0xfffffa8000fff630 SearchProtocol     2524    480      7      226     2      0 2019-12-11 14:37:21 UTC+0000
0xfffffa8000ecea60 SearchFilterHo     1720    480      5       90     0      0 2019-12-11 14:37:21 UTC+0000
0xfffffa8001010b30 WinRAR.exe         1512   2504      6      207     2      0 2019-12-11 14:37:23 UTC+0000
0xfffffa8001020b30 SearchProtocol     2868    480      8      279     0      0 2019-12-11 14:37:23 UTC+0000
0xfffffa8001048060 DumpIt.exe          796    604      2       45     1      1 2019-12-11 14:37:54 UTC+0000
0xfffffa800104a780 conhost.exe        2260    368      2       50     1      0 2019-12-11 14:37:54 UTC+0000

┌──(root㉿kali)-[~/volatility]
└─#
```

➔ Tiến trình PID=2424 mspaint.exe đang run.

- Thực hiện dump tiến trình này với plugin là memdump

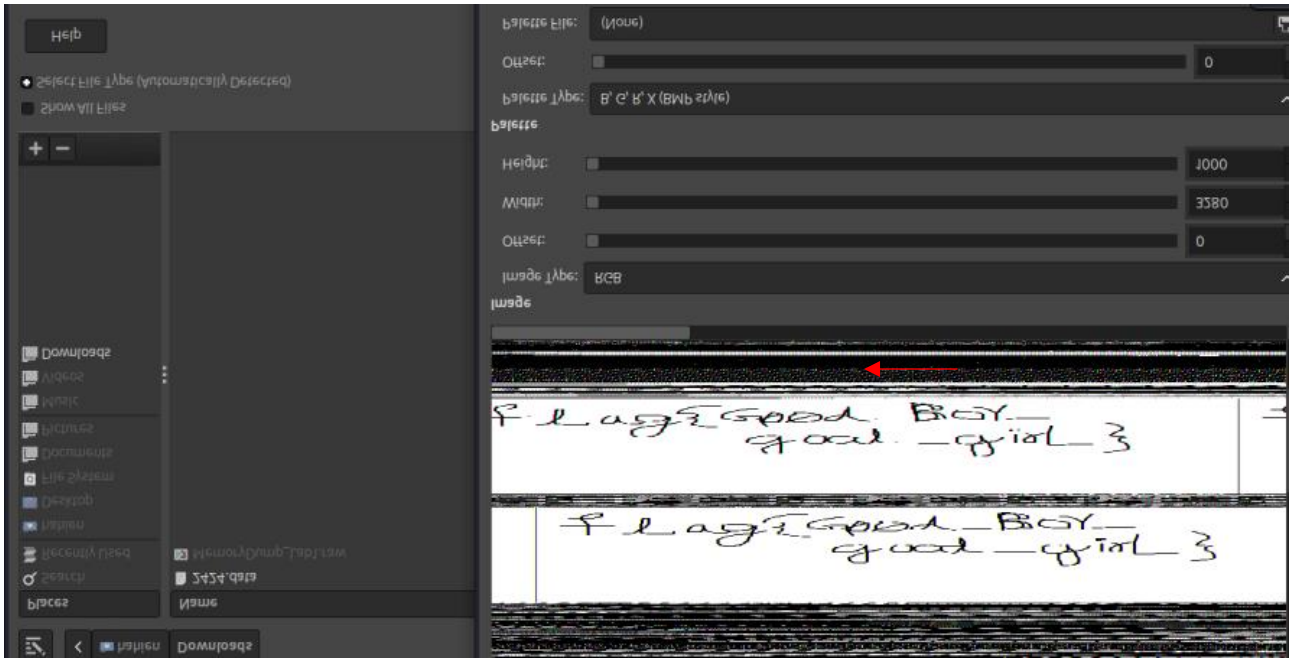
```
┌──(root㉿kali)-[~/volatility]
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab1.raw --profile Win7SP1x64 memdump -p 2424 -D .
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
Writing mspaint.exe [  2424] to 2424.dmp
```

- Thực đổi tên file từ 2424.dmp thành 2424.data

```
┌──(root㉿kali)-[~/volatility]
└─# mv 2424.dmp 2424.data
```

```
┌──(root㉿kali)-[~/volatility]
└─# cp 2424.data /home/hahien/Downloads/2424.data
```

- Mở file 2424.data với GIMP tool chỉnh thông số Width, Height của RGB image ➔ cho tăng dần width đến khi thấy rõ được chữ gì đó, sau đó lật ngược ảnh ta có như sau:



➔ **STAGE 2: flag{G00d_BoY_good_girl_}**

- Tiếp tục tìm kiếm flag của STAGE 3 ➔ Quay lại plugin pslist để thăm dò thêm các tiến trình đáng nghi:

```
0×fffffa8001f58890 svchost.exe         1372    484     22      295     0      0 2019-12-11 13:41:54 UTC+0000
0×fffffa8001f91b30 TCPSVCS.EXE         1416    484      4       97     0      0 2019-12-11 13:41:55 UTC+0000
0×fffffa8000d3c400 sppsvc.exe          1508    484      4      141     0      0 2019-12-11 14:16:06 UTC+0000
0×fffffa8001c38580 svchost.exe          948    484     13      322     0      0 2019-12-11 14:16:07 UTC+0000
0×fffffa8002170630 wmpnetwk.exe        1856    484     16      451     0      0 2019-12-11 14:16:08 UTC+0000
0×fffffa8001d376f0 SearchIndexer.       480    484     14      701     0      0 2019-12-11 14:16:09 UTC+0000
0×fffffa8001eb47f0 taskhost.exe         296    484      8      151     1      0 2019-12-11 14:32:24 UTC+0000
0×fffffa8001dfa910 dwm.exe             1988    852      5       72     1      0 2019-12-11 14:32:25 UTC+0000
0×fffffa8002046960 explorer.exe         604   2016     33      927     1      0 2019-12-11 14:32:25 UTC+0000
0×fffffa80021c75d0 VBoxTray.exe        1844    604     11      140     1      0 2019-12-11 14:32:35 UTC+0000
0×fffffa80021da060 audiodg.exe         2064    816      6      131     0      0 2019-12-11 14:32:37 UTC+0000
0×fffffa80022199e0 svchost.exe         2368    484      9      365     0      0 2019-12-11 14:32:51 UTC+0000
0×fffffa8002222780 cmd.exe             1984    604      1       21     1      0 2019-12-11 14:34:54 UTC+0000
0×fffffa8002227140 conhost.exe         2692    368      2       50     1      0 2019-12-11 14:34:54 UTC+0000
0×fffffa80022bab30 mspaint.exe         2424    604      6      128     1      0 2019-12-11 14:35:14 UTC+0000
0×fffffa8000eac770 svchost.exe         2660    484      6      100     0      0 2019-12-11 14:35:14 UTC+0000
0×fffffa8001e68060 csrss.exe           2760   2680      7      172     2      0 2019-12-11 14:37:05 UTC+0000
0×fffffa8000ecbb30 winlogon.exe        2808   2680      4      119     2      0 2019-12-11 14:37:05 UTC+0000
0×fffffa8000f3aab0 taskhost.exe        2908    484      9      158     2      0 2019-12-11 14:37:13 UTC+0000
0×fffffa8000f4db30 dwm.exe             3004    852      5       72     2      0 2019-12-11 14:37:14 UTC+0000
0×fffffa8000f4c670 explorer.exe        2504   3000     34      825     2      0 2019-12-11 14:37:14 UTC+0000
0×fffffa8000f9a4e0 VBoxTray.exe        2304   2504     14      144     2      0 2019-12-11 14:37:14 UTC+0000
0×fffffa8000fff630 SearchProtocol      2524    480      7      226     2      0 2019-12-11 14:37:21 UTC+0000
0×fffffa8000ecea60 SearchFilterHo      1720    480      5       90     0      0 2019-12-11 14:37:21 UTC+0000
0×fffffa8001010b30 WinRAR.exe          1512   2504      6      207     2      0 2019-12-11 14:37:23 UTC+0000
0×fffffa8001020b30 SearchProtocol      2868    480      8      279     0      0 2019-12-11 14:37:23 UTC+0000
0×fffffa8001048060 DumpIt.exe           796    604      2       45     1      1 2019-12-11 14:37:54 UTC+0000
0×fffffa800104a780 conhost.exe         2260    368      2       50     1      0 2019-12-11 14:37:54 UTC+0000

┌──(root㉿kali)-[~/volatility]
└─#
```

➔ Có 1 tiến trình của WinRAR.exe khá nghi ngờ, với WinRAR thì thường có các file .rar, tiến hành kiểm tra xem:

```
┌──(root㉿kali)-[~/volatility]
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab1.raw --profile Win7SP1×64 filescan | grep "\.rar"
Volatility Foundation Volatility Framework 2.6.1
0×000000003fa3ebc0      1      0 R--r-- \Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar
0×000000003fac3bc0      1      0 R--r-- \Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar
0×000000003fb48bc0      1      0 R--r-- \Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar
```

- Dùng plugin dumpfiles với Offset tìm thấy, file sau khi dump thu được:

```
┌──(root㉿kali)-[~/volatility]
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab1.raw --profile Win7SP1x64 dumpfiles -D . -Q 0x000000003fb48bc0

Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3fb48bc0   None   \Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar

┌──(root㉿kali)-[~/volatility]
└─# ls
2424.data          CHANGELOG.txt                  file.None.0xfffffa801a4ec470.vacb  flag.txt      PKG-INFO          setup.py
3720.dmp           chrome-history.splite          file.None.0xfffffa801a5193d0.dat   get-pip.py    pwdhashes.txt     tools
3720.dmp.strings   contrib                        file.None.0xfffffa801af10010.dat   LEGAL.txt     pyinstaller       volatility
708.dmp            CREDITS.txt                    file.None.0xfffffa801b0532e0.dat   LICENSE.txt   pyinstaller.spec  vol.py
708.dmp.strings    distorm                        file.None.0xfffffa801b2def10.dat   Makefile      README.txt
AUTHORS.txt        file.None.0xfffffa8001034450.dat  file.None.0xfffffa801b42c9e0.dat  MANIFEST.in   resources

┌──(root㉿kali)-[~/volatility]
└─# file file.None.0xfffffa8001034450.dat
file.None.0xfffffa8001034450.dat: RAR archive data, v5
```

- Đổi định dạng file đã dump về dạng ".rar" để thực hiện được unrar

```
┌──(root㉿kali)-[~/volatility]
└─# mv file.None.0xfffffa8001034450.dat Important.rar

┌──(root㉿kali)-[~/volatility]
└─# ls
2424.data          CHANGELOG.txt                  file.None.0xfffffa801a5193d0.dat  get-pip.py
3720.dmp           chrome-history.splite          file.None.0xfffffa801af10010.dat  Important.rar
3720.dmp.strings   contrib                        file.None.0xfffffa801b0532e0.dat  LEGAL.txt
708.dmp            CREDITS.txt                    file.None.0xfffffa801b2def10.dat  LICENSE.txt
708.dmp.strings    distorm                        file.None.0xfffffa801b42c9e0.dat  Makefile
AUTHORS.txt        file.None.0xfffffa801a4ec470.vacb  flag.txt                      MANIFEST.in
```

- Nhưng khi unrar thì file này cần nhập password và được gợi ý là NTLM hash in uppercase password tài khoản của Alissa

```
┌──(root㉿kali)-[~/volatility]
└─# unrar e Important.rar

UNRAR 7.00 beta 2 freeware      Copyright (c) 1993-2023 Alexander Roshal

Password is NTLM hash(in uppercase) of Alissa's account passwd.


Extracting from Important.rar

Enter password (will not be echoed) for flag3.png:
```

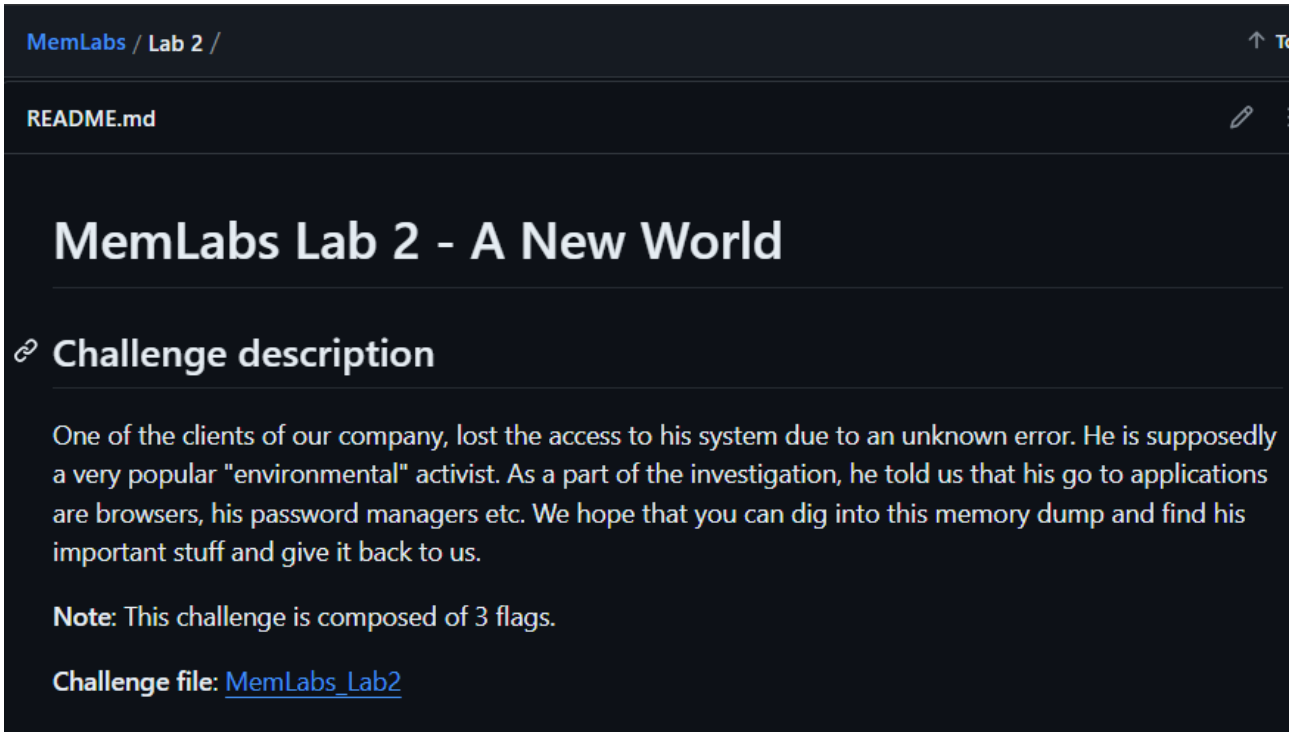
- Để xem được NTLM hash nên dùng plugin hashdump -> sau đó chuyển về dạng in hoa

```
┌──(root㉿kali)-[~/volatility]
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab1.raw --profile Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SmartNet:1001:aad3b435b51404eeaad3b435b51404ee:4943abb39473a6f32c11301f4987e7e0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f0fc3d257814e08fea06e63c5762ebd5:::
Alissa Simpson:1003:aad3b435b51404eeaad3b435b51404ee:f4ff64c8baac57d22f22edc681055ba6:::

┌──(root㉿kali)-[~/volatility]
└─# echo "f4ff64c8baac57d22f22edc681055ba6"
f4ff64c8baac57d22f22edc681055ba6

┌──(root㉿kali)-[~/volatility]
└─# echo "f4ff64c8baac57d22f22edc681055ba6" | tr '[:lower:]' '[:upper:]'
F4FF64C8BAAC57D22F22EDC681055BA6

┌──(root㉿kali)-[~/volatility]
└─# unrar e Important.rar

UNRAR 7.00 beta 2 freeware      Copyright (c) 1993-2023 Alexander Roshal

Password is NTLM hash(in uppercase) of Alissa's account passwd.


Extracting from Important.rar

Enter password (will not be echoed) for flag3.png:

Extracting  flag3.png                                                 OK
All OK
```

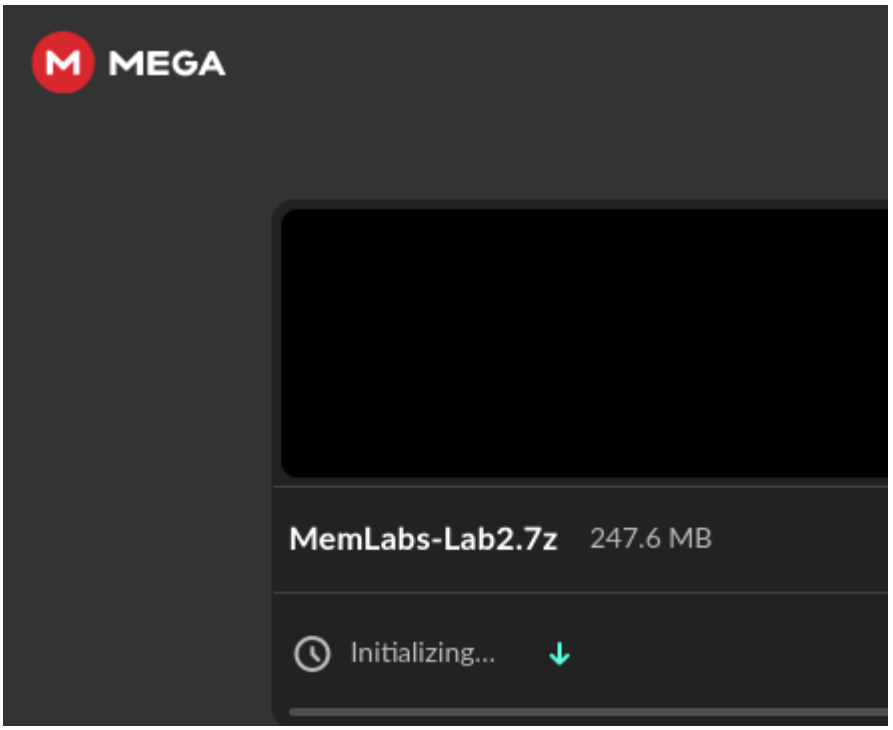
- Mở ảnh flag3.png để xem nội dung

➔ **STAGE 3: flag{w3lL_3rd_stage_was_easy}**

2. Lab 2 - A New World



- Đầu tiên, ta hãy tải challenge file về máy kali:



- Xem thông tin với plugin imageinfo:

```
┌──(root㉿kali)-[~/volatility]
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab2.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/hahien/Downloads/MemoryDump_Lab2.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800027f20a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff800027f3d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2019-12-14 10:38:46 UTC+0000
     Image local date and time : 2019-12-14 16:08:46 +0530
```

- Với profile Win7SP1x64, thực hiện kiểm tra các tiến trình với plugin pslist:

```
┌──(root㉿kali)-[~/volatility]
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab2.raw --profile Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8000ca0040 System                    4      0     80      541 ------      0 2019-12-14 10:35:21 UTC+0000
0xfffffa80014976c0 smss.exe                248      4      3       37 ------      0 2019-12-14 10:35:21 UTC+0000
0xfffffa80014fdb30 csrss.exe               320    312     10      446      0      0 2019-12-14 10:35:27 UTC+0000
0xfffffa8001c40060 csrss.exe               368    360      8      237      1      0 2019-12-14 10:35:28 UTC+0000
0xfffffa8000ca8840 psxss.exe               376    248     18      786      0      0 2019-12-14 10:35:28 UTC+0000
0xfffffa8001c5a700 winlogon.exe            416    360      6      112      1      0 2019-12-14 10:35:30 UTC+0000
0xfffffa8001c5b2b0 wininit.exe             424    312      3       75      0      0 2019-12-14 10:35:30 UTC+0000
0xfffffa8001c95320 services.exe            484    424      8      206      0      0 2019-12-14 10:35:31 UTC+0000
0xfffffa8001c9d910 lsass.exe               492    424      8      546      0      0 2019-12-14 10:35:31 UTC+0000
0xfffffa8001c9e2d0 lsm.exe                 500    424     10      181      0      0 2019-12-14 10:35:31 UTC+0000
0xfffffa8001cec790 svchost.exe             588    484     12      354      0      0 2019-12-14 10:35:35 UTC+0000
0xfffffa8001d13060 VBoxService.ex          652    484     14      135      0      0 2019-12-14 10:35:36 UTC+0000
0xfffffa8001d4ab30 svchost.exe             720    484      7      275      0      0 2019-12-14 10:35:37 UTC+0000
0xfffffa8001d76320 svchost.exe             812    484     21      474      0      0 2019-12-14 10:35:38 UTC+0000
0xfffffa8001da6930 svchost.exe             852    484     20      417      0      0 2019-12-14 10:35:38 UTC+0000
0xfffffa8001dacb30 svchost.exe             876    484     39      962      0      0 2019-12-14 10:35:38 UTC+0000
0xfffffa8001df65f0 audiodg.exe             268    812      7      131      0      0 2019-12-14 10:35:41 UTC+0000
0xfffffa8001e1eb30 svchost.exe             472    484     12      301      0      0 2019-12-14 10:35:42 UTC+0000
0xfffffa8001e47740 svchost.exe            1044    484     16      361      0      0 2019-12-14 10:35:43 UTC+0000
0xfffffa8000cf9220 spoolsv.exe            1208    484     13      279      0      0 2019-12-14 10:35:47 UTC+0000
0xfffffa8001ed8b30 svchost.exe            1248    484     18      303      0      0 2019-12-14 10:35:49 UTC+0000
0xfffffa8001f4eb30 svchost.exe            1368    484     23      314      0      0 2019-12-14 10:35:51 UTC+0000
0xfffffa8001f7c060 TCPSVCS.EXE            1412    484      4       97      0      0 2019-12-14 10:35:53 UTC+0000
0xfffffa80020f2b30 taskhost.exe           1928    484      9      154      1      0 2019-12-14 10:36:04 UTC+0000
0xfffffa8002105b30 taskeng.exe            1996    876      5       79      0      0 2019-12-14 10:36:04 UTC+0000
0xfffffa800211e7c0 dwm.exe                2012    852      4       72      1      0 2019-12-14 10:36:04 UTC+0000
```

```
0xfffffa8002131340 explorer.exe          1064   2004     37      989      1      0 2019-12-14 10:36:05 UTC+0000
0xfffffa80021bb240 SearchIndexer.        1836    484     12      628      0      0 2019-12-14 10:36:11 UTC+0000
0xfffffa80021c0b30 VBoxTray.exe          1896   1064     13      138      1      0 2019-12-14 10:36:13 UTC+0000
0xfffffa80022a3b30 csrss.exe             2308   2300      9      246      2      0 2019-12-14 10:36:24 UTC+0000
0xfffffa80022a73e0 winlogon.exe          2336   2300      4      109      2      0 2019-12-14 10:36:24 UTC+0000
0xfffffa8000e76060 taskhost.exe          2604    484      9      154      2      0 2019-12-14 10:36:29 UTC+0000
0xfffffa8000e95060 dwm.exe               2652    852      3       71      2      0 2019-12-14 10:36:29 UTC+0000
0xfffffa8000e9a110 explorer.exe          2664   2632     19      632      2      0 2019-12-14 10:36:29 UTC+0000
0xfffffa8000edcb30 VBoxTray.exe          2792   2664     12      139      2      0 2019-12-14 10:36:30 UTC+0000
0xfffffa80022e5950 cmd.exe               2096   2664      1       19      2      0 2019-12-14 10:36:35 UTC+0000
0xfffffa8000e63060 conhost.exe           2068   2308      2       50      2      0 2019-12-14 10:36:35 UTC+0000
0xfffffa8002109b30 chrome.exe            2296   2664     27      658      2      0 2019-12-14 10:36:45 UTC+0000
0xfffffa8001cc7a90 chrome.exe            2304   2296      8       71      2      0 2019-12-14 10:36:45 UTC+0000
0xfffffa8000eea7a0 chrome.exe            2476   2296      2       55      2      0 2019-12-14 10:36:46 UTC+0000
0xfffffa8000ea2b30 chrome.exe            2964   2296     13      295      2      0 2019-12-14 10:36:47 UTC+0000
0xfffffa8000fae6a0 chrome.exe            2572   2296      8      177      2      0 2019-12-14 10:36:56 UTC+0000
0xfffffa800105c060 WmiPrvSE.exe          2636    588     12      293      0      0 2019-12-14 10:37:02 UTC+0000
0xfffffa800100c060 WmiApSrv.exe          2004    484      6      115      0      0 2019-12-14 10:37:05 UTC+0000
0xfffffa800230eb30 chrome.exe            1632   2296     14      219      2      0 2019-12-14 10:37:12 UTC+0000
0xfffffa800101e640 dllhost.exe           2376    588      9      250      1      0 2019-12-14 10:37:40 UTC+0000
0xfffffa800224a8c0 KeePass.exe           3008   1064     12      316      1      0 2019-12-14 10:37:56 UTC+0000
0xfffffa8002230b30 sppsvc.exe            2764    484      5      151      0      0 2019-12-14 10:38:00 UTC+0000
0xfffffa80010e5b30 svchost.exe           1076    484     17      337      0      0 2019-12-14 10:38:02 UTC+0000
0xfffffa80010f44a0 wmpnetwk.exe           928    484     18      523      0      0 2019-12-14 10:38:03 UTC+0000
0xfffffa80011956a0 notepad.exe           3260   3180      1       61      1      0 2019-12-14 10:38:20 UTC+0000
0xfffffa80011aa060 DumpIt.exe            3844   1064      2       45      1      1 2019-12-14 10:38:43 UTC+0000
0xfffffa8001194570 conhost.exe           3852    368      2       52      1      0 2019-12-14 10:38:43 UTC+0000
0xfffffa8001189b30 WmiPrvSE.exe          4004    588      9  1572864 ------      0 2019-12-14 10:39:00 UTC+0000

┌──(root㉿kali)-[~/volatility]
```

- Có 3 điểm cần chú ý như sau:
  - He is supposedly a very popular "**environmental**" activist. (envars)
  - go to applications are **browsers**, his **password managers**.

➔ Tiến trình cmd.exe, chrome.exe, KeePass.exe khả nghi

- Tiến trình cmd.exe run ➔ thử với plugin cmdscan:

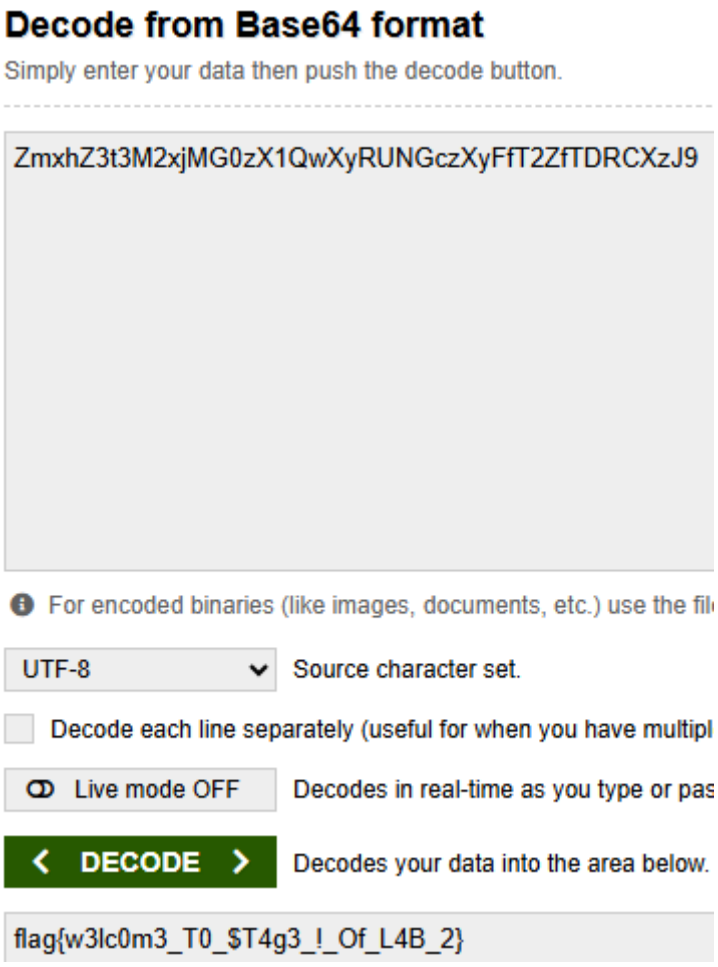
```
┌──(root㉿kali)-[~/volatility]
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab2.raw --profile Win7SP1x64 cmdscan

Volatility Foundation Volatility Framework 2.6.1
**************************************************
CommandProcess: conhost.exe Pid: 2068
CommandHistory: 0x3deb10 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0x3db330: Nothing here kids :)
Cmd #15 @ 0x3a0158: =
Cmd #16 @ 0x3ddc80: >
**************************************************
CommandProcess: conhost.exe Pid: 3852
CommandHistory: 0x16eba0 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #15 @ 0x130158:
Cmd #16 @ 0x16dd00:
```

➔ Ở PID 2068 có chuỗi: Nothing here kids :)

- Sử dụng envars kiểm tra biến môi trường cho tiến trình 2068:

```
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab2.raw --profile Win7SP1x64 envars -p 2068
Volatility Foundation Volatility Framework 2.6.1
Pid      Process          Block              Variable                       Value
-------- ---------------- ------------------ ------------------------------ -----
    2068 conhost.exe      0x00000000003bd810 CommonProgramFiles             C:\Program Files\Common Files
    2068 conhost.exe      0x00000000003bd810 CommonProgramFiles(x86)        C:\Program Files (x86)\Common Files
    2068 conhost.exe      0x00000000003bd810 CommonProgramW6432             C:\Program Files\Common Files
    2068 conhost.exe      0x00000000003bd810 ComSpec                        C:\Windows\system32\cmd.exe
    2068 conhost.exe      0x00000000003bd810 FP_NO_HOST_CHECK               NO
    2068 conhost.exe      0x00000000003bd810 NEW_TMP                        C:\Windows\ZmxhZ3t3M2xjMG0zX1QwXyRUNGczXyFfT2ZfTDRCXzJ9
    2068 conhost.exe      0x00000000003bd810 NUMBER_OF_PROCESSORS           1
    2068 conhost.exe      0x00000000003bd810 OS                             Windows_NT
    2068 conhost.exe      0x00000000003bd810 Path                           C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\W
indows\System32\WindowsPowerShell\v1.0\
    2068 conhost.exe      0x00000000003bd810 PATHEXT                        .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
    2068 conhost.exe      0x00000000003bd810 PROCESSOR_ARCHITECTURE         AMD64
    2068 conhost.exe      0x00000000003bd810 PROCESSOR_IDENTIFIER           Intel64 Family 6 Model 142 Stepping 9, GenuineIntel
    2068 conhost.exe      0x00000000003bd810 PROCESSOR_LEVEL                6
    2068 conhost.exe      0x00000000003bd810 PROCESSOR_REVISION             8e09
    2068 conhost.exe      0x00000000003bd810 ProgramFiles                   C:\Program Files
    2068 conhost.exe      0x00000000003bd810 ProgramFiles(x86)              C:\Program Files (x86)
    2068 conhost.exe      0x00000000003bd810 ProgramW6432                   C:\Program Files
    2068 conhost.exe      0x00000000003bd810 PSModulePath                   C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
    2068 conhost.exe      0x00000000003bd810 SystemDrive                    C:
    2068 conhost.exe      0x00000000003bd810 SystemRoot                     C:\Windows
    2068 conhost.exe      0x00000000003bd810 TEMP                           C:\Windows\TEMP
    2068 conhost.exe      0x00000000003bd810 TMP                            C:\Windows\TEMP
    2068 conhost.exe      0x00000000003bd810 USERNAME                       SYSTEM
    2068 conhost.exe      0x00000000003bd810 windir                         C:\Windows
    2068 conhost.exe      0x00000000003bd810 windows_tracing_flags          3
    2068 conhost.exe      0x00000000003bd810 windows_tracing_logfile        C:\BVTBin\Tests\installpackage\csilogfile.log
```

- Decode Base64 mã này xem sao:
  ZmxhZ3t3M2xjMG0zX1QwXyRUNGczXyFfT2ZfTDRCXzJ9



➔ **STAGE 1: flag{w3lc0m3_T0_$T4g3_!_Of_L4B_2}**

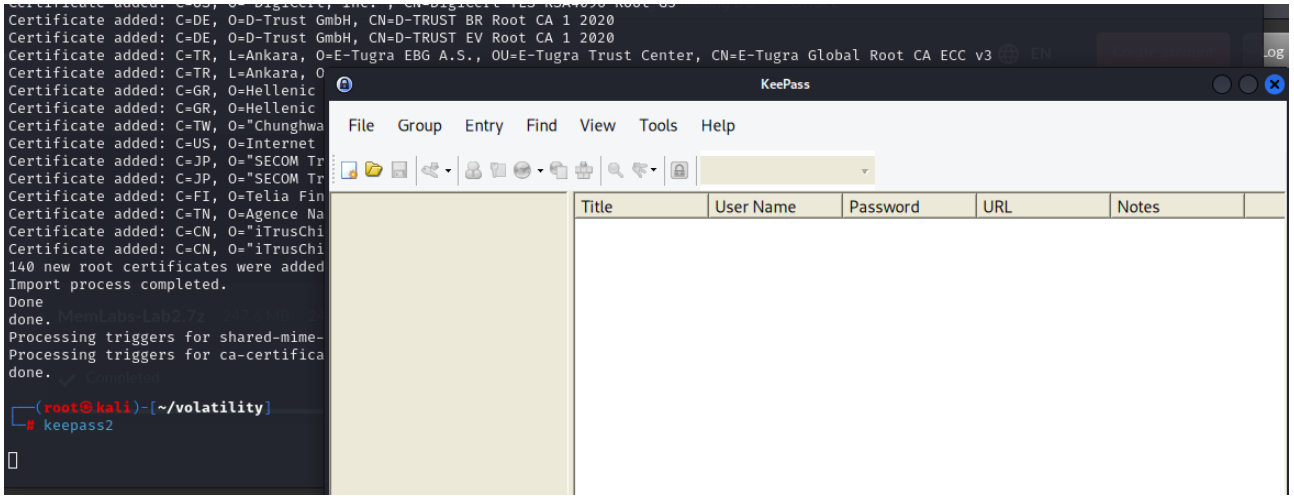
- Để tìm ra flag tiếp theo thử kiểm tra tiến trình KeePass.exe (ứng dụng để lưu tài khoản và mật khẩu với định dạng là ".kdbx")
- Sử dụng plugin filescan và tìm tất cả file chứa từ khóa "kdbx":

```
┌──(root㉿kali)-[~/volatility]
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab2.raw --profile Win7SP1x64 filescan | grep "kdbx"
Volatility Foundation Volatility Framework 2.6.1
0x000000003fb112a0     16      0 R--r-- \Device\HarddiskVolume2\Users\SmartNet\Secrets\Hidden.kdbx
```

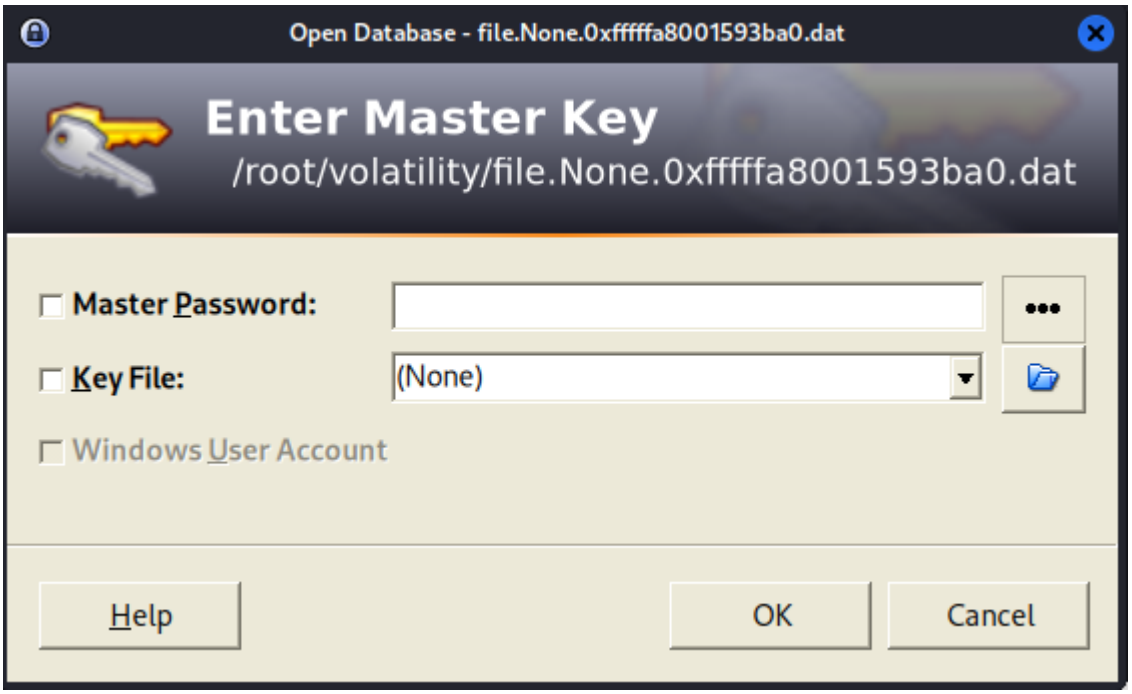
- Với file Hidden.kdbx, thực hiện dumpfile để đọc được nội dung:

```
┌──(root㉿kali)-[~/volatility]
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab2.raw --profile Win7SP1x64 dumpfiles -D . -Q 0x000000003fb112a0
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3fb112a0   None   \Device\HarddiskVolume2\Users\SmartNet\Secrets\Hidden.kdbx

┌──(root㉿kali)-[~/volatility]
└─# ls
2424.data          CHANGELOG.txt                 file.None.0xfffffa801a4ec470.vacb  flag3.png      Makefile          README.txt
3720.dmp           chrome-history.splite         file.None.0xfffffa801a5193d0.dat   flag.txt       MANIFEST.in       resources
3720.dmp.strings   contrib                       file.None.0xfffffa801af10010.dat   get-pip.py     PKG-INFO          setup.py
708.dmp            CREDITS.txt                   file.None.0xfffffa801b0532e0.dat   Important.rar  pwdhashes.txt     tools
708.dmp.strings    distorm                       file.None.0xfffffa801b2def10.dat   LEGAL.txt      pyinstaller       volatility
AUTHORS.txt        file.None.0xfffffa8001593ba0.dat  file.None.0xfffffa801b42c9e0.dat   LICENSE.txt    pyinstaller.spec  vol.py

┌──(root㉿kali)-[~/volatility]
└─#
```

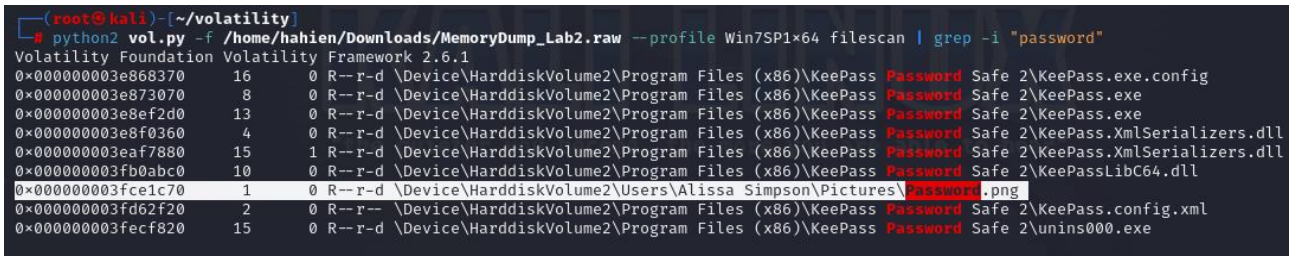
- Cài KeePass để có thể mở file:



- Mở ứng dụng KeePass và chọn mở file đã dump được ở trên thì nó yêu cầu 1 password



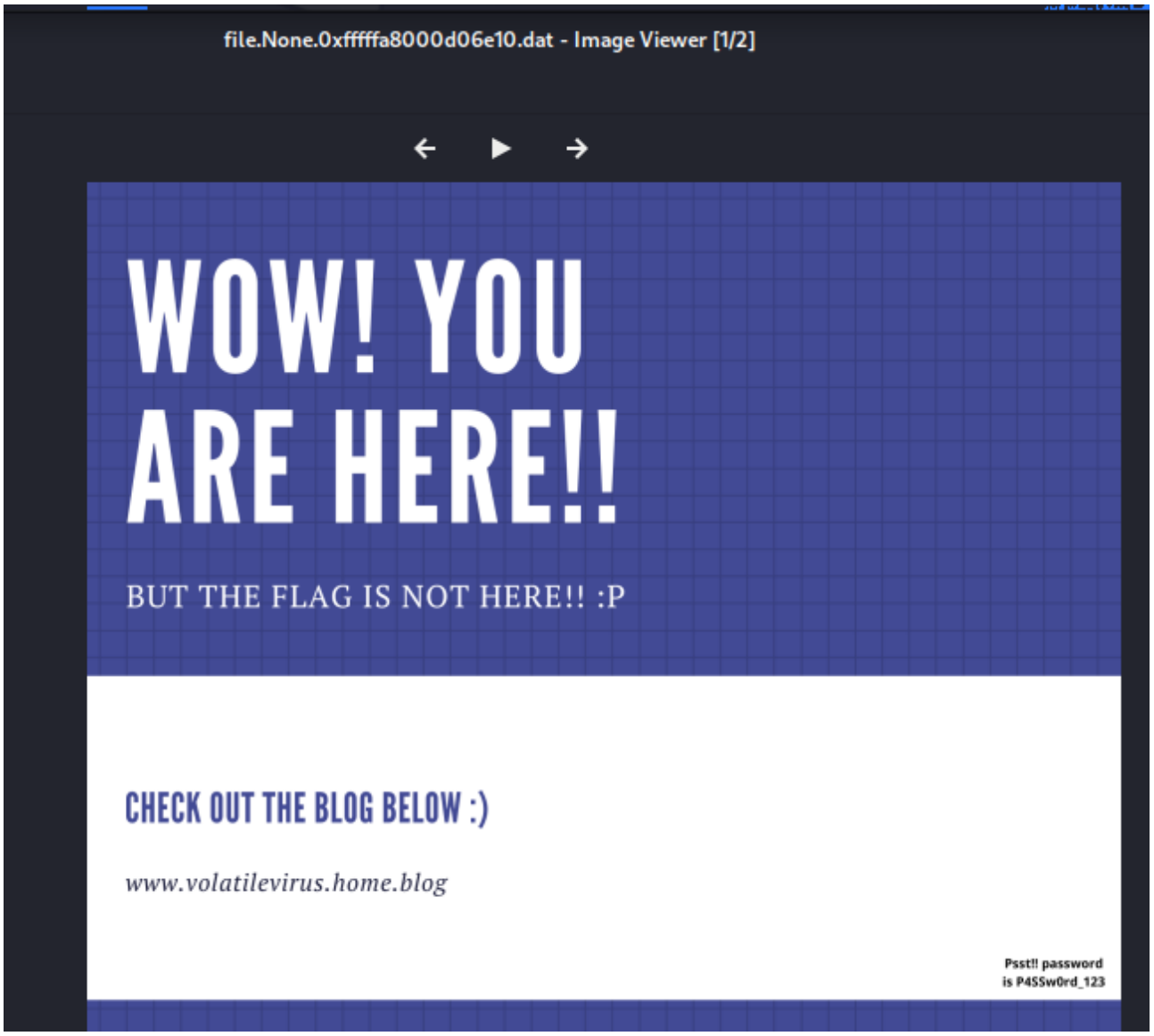
- Sử dụng plugin filescan và tìm với từ khóa “password” thì phát hiện 1 file Password.png ➔ thực hiện dumpfile với offset đó.



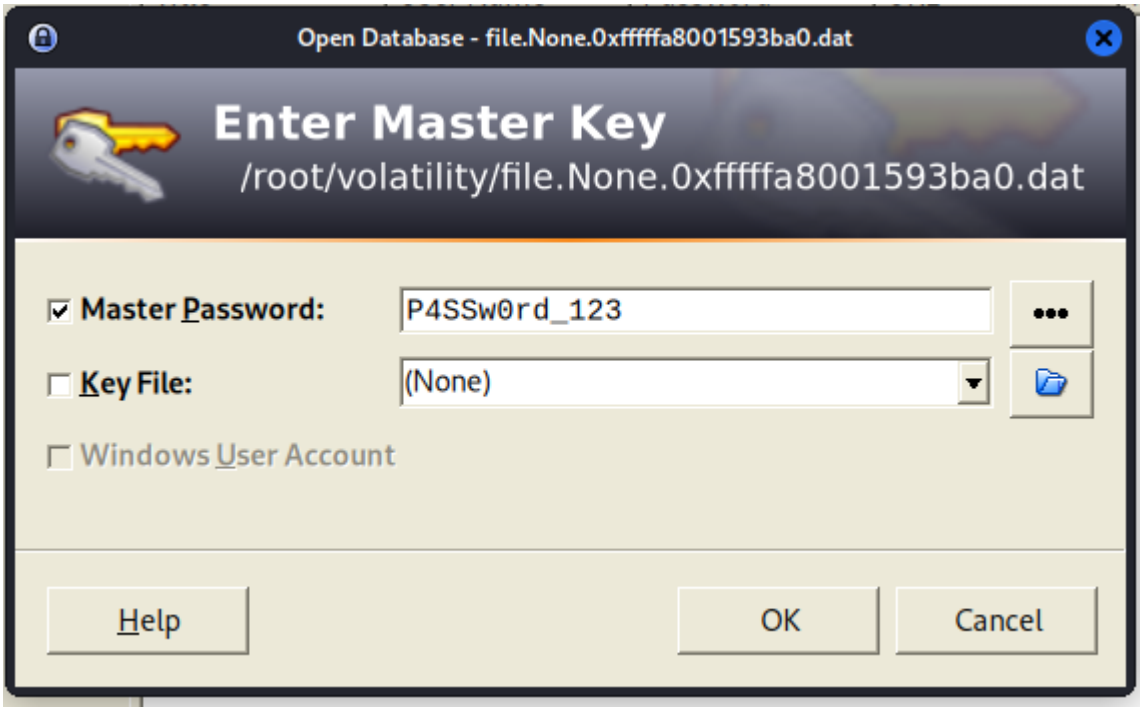
```
┌──(root㉿kali)-[~/volatility]
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab2.raw --profile Win7SP1x64 dumpfiles -D . -Q 0x000000003fce1c70
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3fce1c70   None   \Device\HarddiskVolume2\Users\Alissa Simpson\Pictures\Password.png
```

```
┌──(root㉿kali)-[~/volatility]
└─# ls
2424.data           chrome-history.splite
3720.dmp            contrib
3720.dmp.strings    CREDITS.txt
708.dmp             distorm
708.dmp.strings     file.None.0xfffffa8000d06e10.dat
AUTHORS.txt         file.None.0xfffffa8001593ba0.dat
CHANGELOG.txt       file.None.0xfffffa801a4ec470.vacb
```

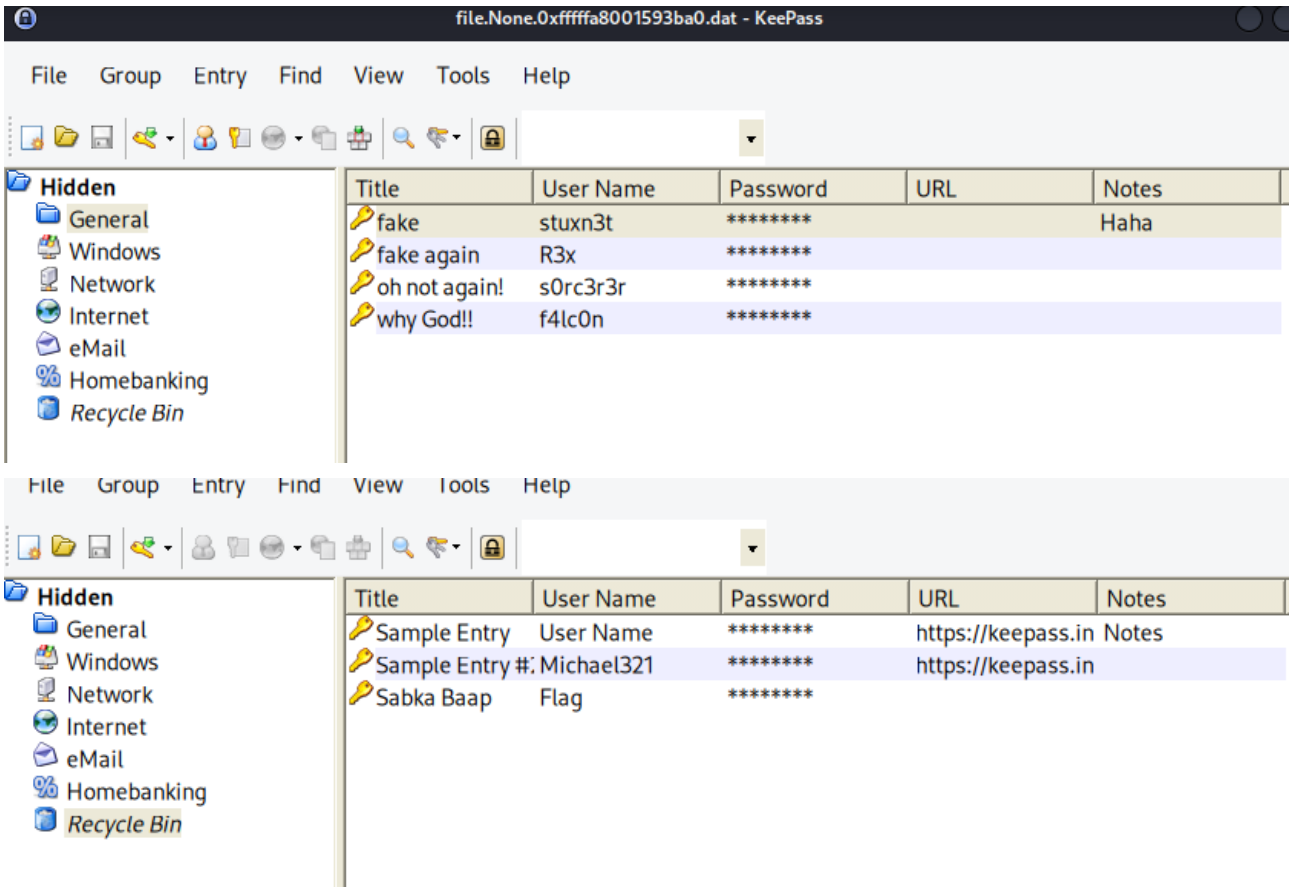
- Mở file .dat, phía góc cuối bên phải có 1 dòng Psst!! password is **P4SSw0rd_123**

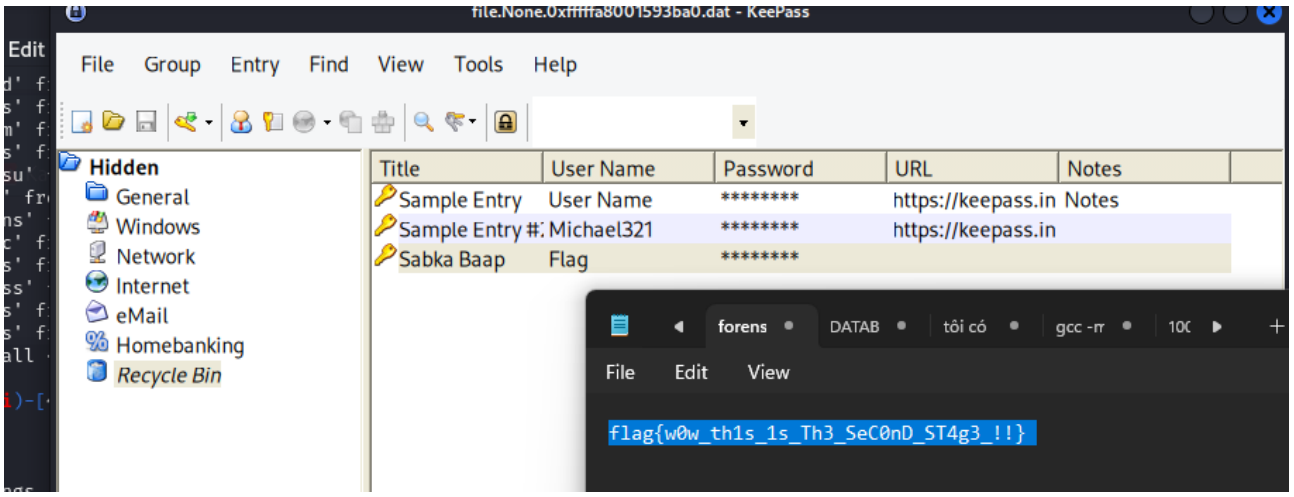


- Nhập **P4SSw0rd_123** vào để mở được file .kdbx



- Xem các file trên KeePass để tìm kiếm các file chứa flag cần tìm:





➔ **STAGE 2: flag{w0w_th1s_1s_Th3_SeC0nD_ST4g3_!!}**

- Để tìm kiếm flag cuối cùng ➔ thử xem xét về trình duyệt với các tiến trình chrome.exe ➔ duyệt các file với filescan và tìm lịch sử duyệt web với 2 từ khóa là "Chrome" và "History":

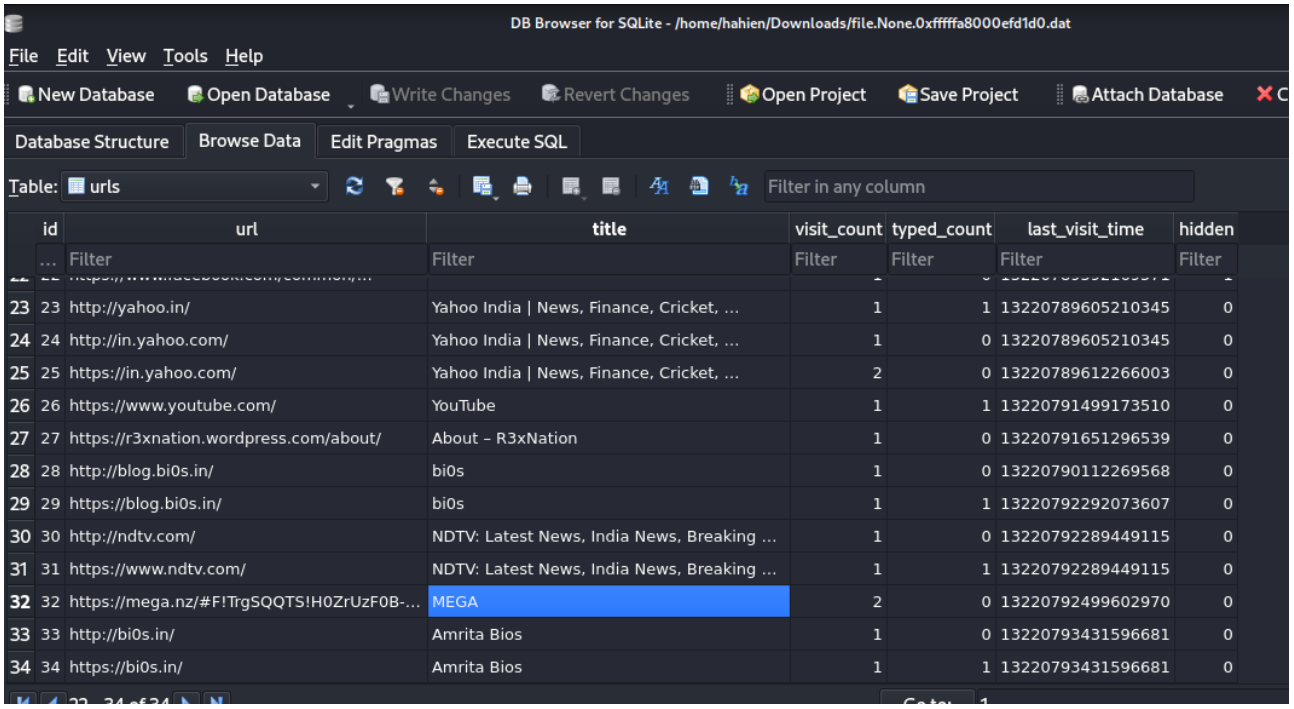
```
┌──(root㉿kali)-[~/volatility]
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab2.raw --profile Win7SP1x64 filescan | grep "Chrome" | grep "History"
Volatility Foundation Volatility Framework 2.6.1
0x000000003fa3e430     17      1 RW-rw- \Device\HarddiskVolume2\Users\SmartNet\AppData\Local\Google\Chrome\User Data\Default\History-journal
0x000000003fcfb1d0     18      1 RW-rw- \Device\HarddiskVolume2\Users\SmartNet\AppData\Local\Google\Chrome\User Data\Default\History
0x000000003fd4a670     16      0 R--rw- \Device\HarddiskVolume2\Users\SmartNet\AppData\Local\Google\Chrome\User Data\Default\History-journal
```

- Lịch sử duyệt web thường được lưu ở đường dẫn **AppData\Local\Google\Chrome\User Data\Default\History**
- Thực hiện dump thư mục trên với plugin là dumpfiles:

```
┌──(root㉿kali)-[~/volatility]
└─# python2 vol.py -f /home/hahien/Downloads/MemoryDump_Lab2.raw --profile Win7SP1x64 dumpfiles -D . -Q 0x000000003fcfb1d0
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3fcfb1d0   None   \Device\HarddiskVolume2\Users\SmartNet\AppData\Local\Google\Chrome\User Data\Default\History
SharedCacheMap 0x3fcfb1d0   None   \Device\HarddiskVolume2\Users\SmartNet\AppData\Local\Google\Chrome\User Data\Default\History

┌──(root㉿kali)-[~/volatility]
└─# ls
2424.data          chrome-history.splite              file.None.0xfffffa8001593ba0.dat  flag3.png        MANIFEST.in       setup.py
3720.dmp           contrib                            file.None.0xfffffa801a4ec470.vacb  flag.txt         PKG-INFO          tools
3720.dmp.strings   CREDITS.txt                       file.None.0xfffffa801a5193d0.dat  get-pip.py       pwdhashes.txt     volatility
708.dmp            distorm                            file.None.0xfffffa801af10010.dat  Important.rar    pyinstaller       vol.py
708.dmp.strings    file.None.0xfffffa8000d06e10.dat   file.None.0xfffffa801b0532e0.dat  LEGAL.txt        pyinstaller.spec
AUTHORS.txt        file.None.0xfffffa8000efd1d0.dat   file.None.0xfffffa801b2def10.dat  LICENSE.txt      README.txt
CHANGELOG.txt      file.None.0xfffffa8000efde00.vacb  file.None.0xfffffa801b42c9e0.dat  Makefile         resources
```

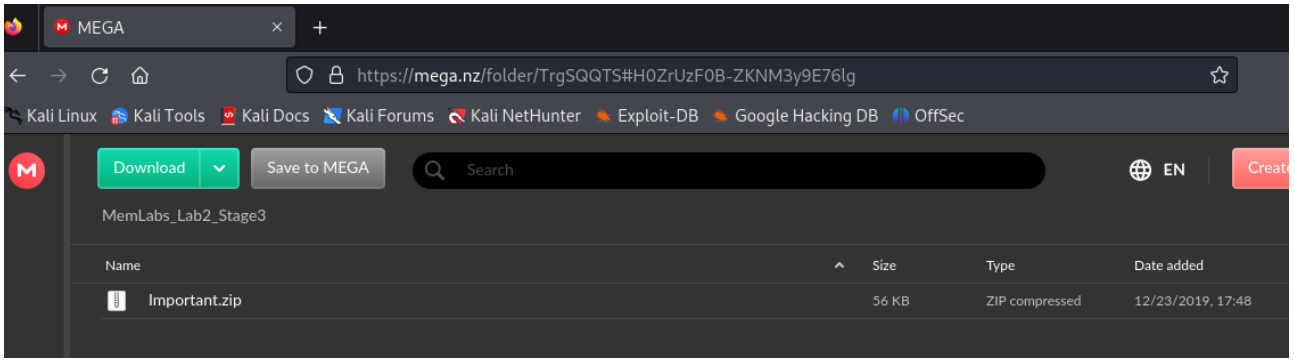
- Mở file đã dump với DB Browser for SQLite để xem thông tin:

```
┌──(root㉿kali)-[~/volatility]
└─# cp file.None.0xfffffa8000efd1d0.dat /home/hahien/Downloads/file.None.0xfffffa8000efd1d0.dat
```



id	url	title	visit_count	typed_count	last_visit_time	hidden
23	http://yahoo.in/	Yahoo India | News, Finance, Cricket, ...	1	1	13220789605210345	0
24	http://in.yahoo.com/	Yahoo India | News, Finance, Cricket, ...	1	0	13220789605210345	0
25	https://in.yahoo.com/	Yahoo India | News, Finance, Cricket, ...	2	0	13220789612266003	0
26	https://www.youtube.com/	YouTube	1	1	13220791499173510	0
27	https://r3xnation.wordpress.com/about/	About – R3xNation	1	0	13220791651296539	0
28	http://blog.bi0s.in/	bi0s	1	0	13220790112269568	0
29	https://blog.bi0s.in/	bi0s	1	1	13220792292073607	0
30	http://ndtv.com/	NDTV: Latest News, India News, Breaking ...	1	0	13220792289449115	0
31	https://www.ndtv.com/	NDTV: Latest News, India News, Breaking ...	1	1	13220792289449115	0
32	https://mega.nz/#F!TrgSQQTS!H0ZrUzF0B-...	MEGA	2	0	13220792499602970	0
33	http://bi0s.in/	Amrita Bios	1	0	13220793431596681	0
34	https://bi0s.in/	Amrita Bios	1	1	13220793431596681	0

- Tại table urls, phát hiện 1 đường dẫn của mege.nz (nơi chia sẻ file trên internet)
- Copy đường dẫn và tìm kiếm:

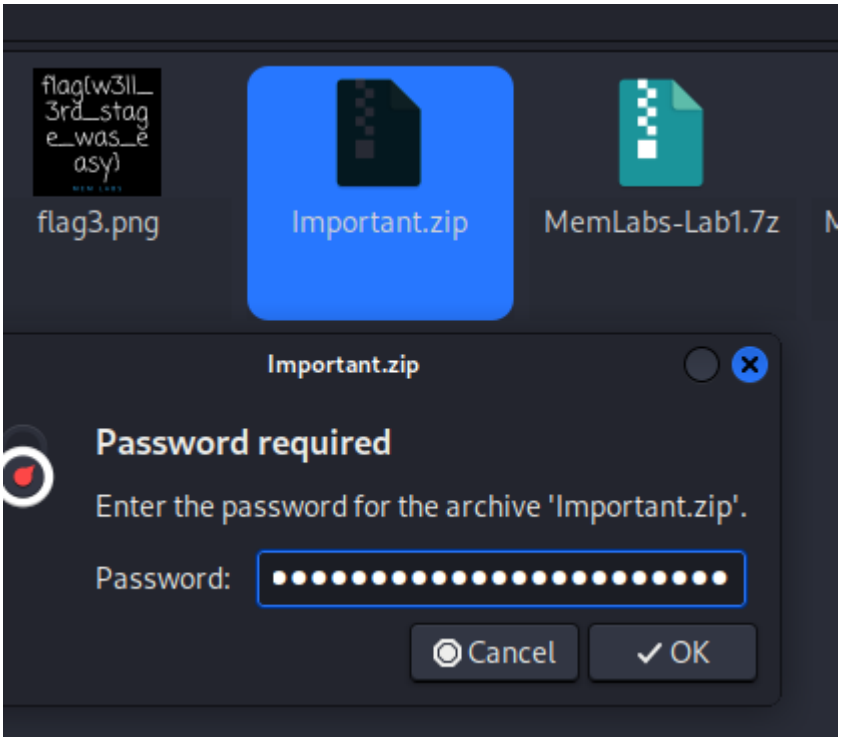


- Giải nén và unzip file Important.zip nhưng nhận được gợi ý về password là SHA1 flag tìm được ở stage3 Lab1 dạng lowercase

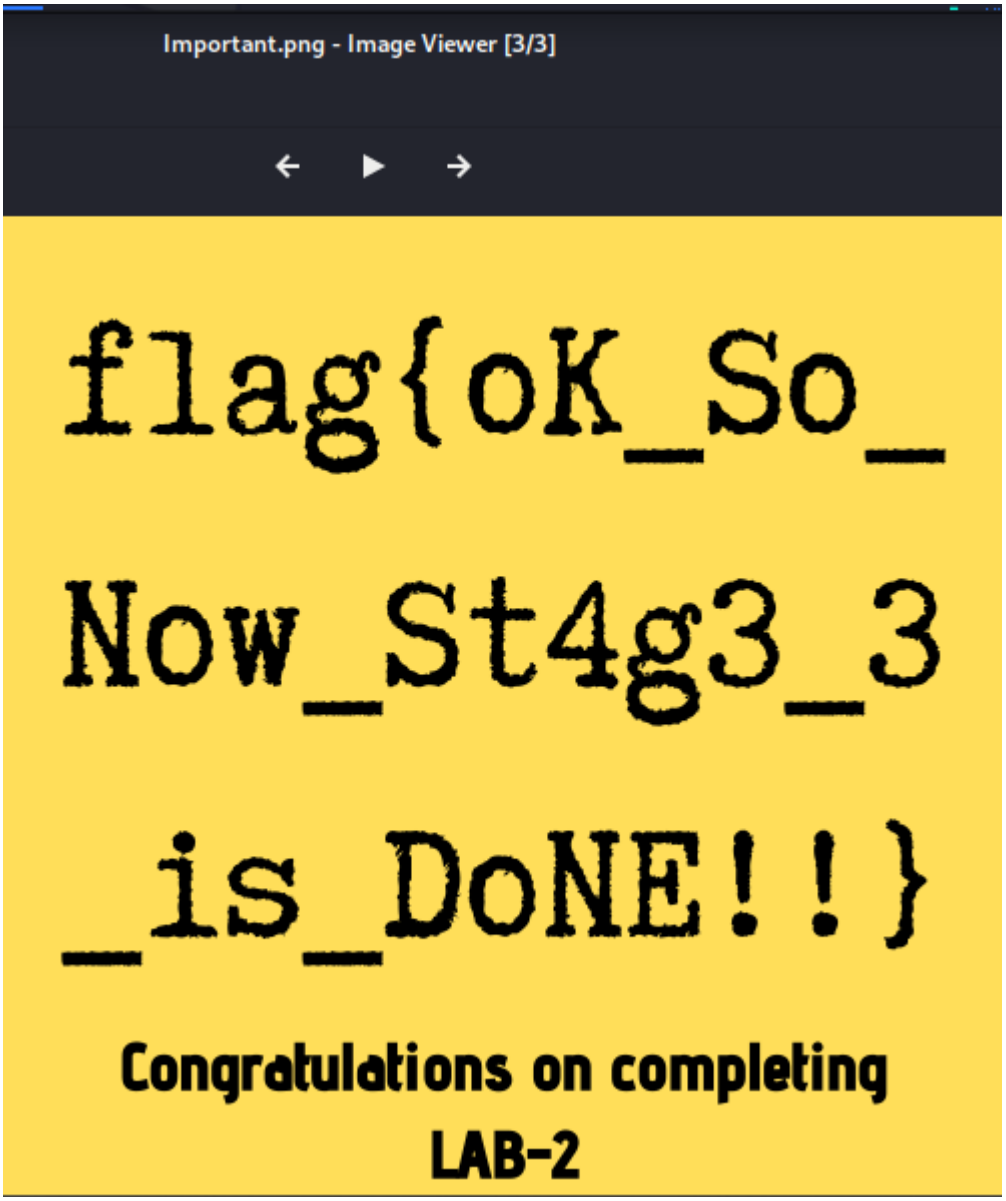
```
┌──(root㉿kali)-[~/volatility]
└─# unzip /home/hahien/Downloads/Important.zip
Archive:  /home/hahien/Downloads/Important.zip
Password is SHA1(stage-3-FLAG) from Lab-1. Password is in lowercase.
   skipping: Important.png           unsupported compression method 99

┌──(root㉿kali)-[~/volatility]
└─#
```

- Với flag{w3lL_3rd_stage_was_easy} sử dụng sha1sum để hash và copy nhập vào password khi extract Important.zip:

```
┌──(root㉿kali)-[~/volatility]
└─# echo -n "flag{w3ll_3rd_stage_was_easy}" | sha1sum
6045dd90029719a039fd2d2ebcca718439dd100a  -
```



- Đọc nội dung của file Important.png:



➔ **STAGE 3: flag{oK_So_Now_St4g3_3_is_DoNE!!}**

3. Lab 3: The Evil's Den

Challenge Description

A malicious script encrypted a very secret piece of information I had on my system. Can you recover the information for me please?

Note-1: This challenge is composed of only 1 flag. The flag split into 2 parts.

Note-2: You'll need the first half of the flag to get the second.

You will need this additional tool to solve the challenge,

```
$ sudo apt install steghide
```

The flag format for this lab is: **inctf{s0me_l33t_Str1ng}**

- Xem thông tin file dump.

```
born21@VM-Ubuntu:~/volatility$ python2 vol.py -f ~/Downloads/MemLabs-Lab3/Memory
Dump_Lab3.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000,
 Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/born21/Downloads/MemLab
s-Lab3/MemoryDump_Lab3.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
```

- Đầu tiên, kiểm tra các tiến trình đang chạy bằng plugin pstree.

```
born21@VM-Ubuntu:~/volatility$ python2 vol.py -f ~/Downloads/MemLabs-Lab3/MemoryDump_Lab3.raw --profile=Win7SP1x86 pslist
Volatility Foundation Volatility Framework 2.6.1
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
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
```

- Hiện có hai quy trình của chương trình notepad.exe đang chạy trên máy tính với các ID quy trình (Pid) là 3736 và 3432. Bằng cách sử dụng plugin cmdline, có thể xem được các tập tin cụ thể đã được mở bằng các phiên bản của chương trình notepad.exe này.

```
born21@VM-Ubuntu:~/volatility$ python2 vol.py -f ~/Downloads/MemLabs-Lab3/MemoryDump_Lab3.raw --profile=Win7SP1x86
cmdline -p 3736,3432
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
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
```

- Notepad đang mở 2 tệp evilscript.py và vip.txt. Để xem nội dung của 2 file, trước tiên, sử dụng plugin filescan để quét thông tin 2 file này.

```
born21@VM-Ubuntu:~/volatility$ python2 vol.py -f ~/Downloads/MemLabs-Lab3/MemoryDump_Lab3.raw --profile=Win7SP1x86
filescan > filescan.txt
Volatility Foundation Volatility Framework 2.6.1
born21@VM-Ubuntu:~/volatility$ grep -E '\\Desktop\\evilscript.py|\\Desktop\\vip.txt' filescan.txt
0x000000003de1b5f0      8      0 R--rw- \Device\HarddiskVolume2\Users\hello\Desktop\evilscript.py.py
0x000000003e727e50      8      0 -W-rw- \Device\HarddiskVolume2\Users\hello\Desktop\vip.txt
```

- Biết được offset của 2 file, ta tiến hành dumpfiles.

```
born21@VM-Ubuntu:~/volatility$ python2 vol.py -f ~/Downloads/MemLabs-Lab3/MemoryDump_Lab3.raw --profile=Win7SP1x86
dumpfiles -Q 0x000000003de1b5f0 -D . -n
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3de1b5f0   None   \Device\HarddiskVolume2\Users\hello\Desktop\evilscript.py.py
born21@VM-Ubuntu:~/volatility$ python2 vol.py -f ~/Downloads/MemLabs-Lab3/MemoryDump_Lab3.raw --profile=Win7SP1x86
dumpfiles -Q 0x000000003e727e50 -D . -n
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3e727e50   None   \Device\HarddiskVolume2\Users\hello\Desktop\vip.txt
```

- Đọc nội dung 2 file vừa dump.

```
born21@VM-Ubuntu:~/volatility$ cat file.None.0xbc2b6af0.evilscript.py.py.dat
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()
born21@VM-Ubuntu:~/volatility$ cat file.None.0x83e52420.vip.txt.dat
am1gd2V4M20wXGs3b2U=
```

- Đoạn code trong file evilscript.py thực hiện mã hoá một chuỗi input bằng cách xor mỗi kí tự trong chuỗi với 3, sau đó mã hoá base64 và ghi vào tệp vip.txt
- Để biết được chuỗi input ban đầu, ta tiến hành đảo ngược quá trình trên.

```
solve.py > ...
1   import base64
2
3   base64_string = "am1gd2V4M20wXGs3b2U="
4   decoded_string = base64.b64decode(base64_string).decode('utf-8')
5   a = ''.join(chr(ord(i)^3) for i in decoded_string)
6   print(a)

PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS  Code

PS D:\PCKTS> python -u "d:\PCKTS\solve.py"
inctf{0n3_h4lf
PS D:\PCKTS>
```

- Ta có được 1 phần của flag: inctf{0n3_h4lf
- Từ gợi ý steghide của đề bài, chúng ta sẽ scan những định dạng tệp hình ảnh phổ biến.

```
born21@VM-Ubuntu:~/volatility$ grep -E '.jpg$|.jpeg$' filescan.txt | head
0x0000000001163f80      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\58BRAMBY\th[1].jpg
0x000000000308df80      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\BBNIP4D[1].jpg
0x0000000004155470      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\AAAtDTI[1].jpg
0x0000000004f34148      2      0 RW---- \Device\HarddiskVolume2\Users\hello\Desktop\suspision1.jpeg
0x00000000068610e8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\QMRBR07P\BBMWckP[1].jpg
0x000000006a4dad8      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBND2yV[1].jpg
0x000000006d02228      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBNGYH1[1].jpg
0x0000000007a89f80      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\T98W2EYD\BBKbPoW[1].jpg
0x0000000007f26c08      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBNJkfh[1].jpg
0x0000000008596cb0      8      0 -W-rwd \Device\HarddiskVolume2\Users\hello\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\OSX2XZOX\BBNHoac[1].jpg
```

- Trong kết quả trả về có 1 tệp khá đặc biệt nên chúng ta sẽ dump file này để xem nội dung.

```
born21@VM-Ubuntu:~/volatility$ python2 vol.py -f ~/Downloads/MemLabs-Lab3/MemoryDump_Lab3.raw --profile=Win7SP1x86
dumpfiles -Q 0x0000000004f34148 -D . -n
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x04f34148   None   \Device\HarddiskVolume2\Users\hello\Desktop\suspision1.jpeg
```

- File thu được:

- Không có thông tin gì ở đây, chúng ta có thể dùng steghide để kiểm tra xem có nội dung nào được ẩn hay không.

```
born21@VM-Ubuntu:~/volatility$ steghide extract -sf file.None.0x843fcf38.suspision1.jpeg.dat
Enter passphrase:
wrote extracted data to "secret text".
born21@VM-Ubuntu:~/volatility$ cat secret\ text
_1s_n0t_3n0ugh}
born21@VM-Ubuntu:~/volatility$
```

- Password là 1 phần của flag đã giải trước đó. Ta biết được phần còn lại của flag.
- Flag: inctf{0n3_h4lf _1s_n0t_3n0ugh}

4. Lab 4: Obsession

Challenge Description

My system was recently compromised. The Hacker stole a lot of information but he also deleted a very important file of mine. I have no idea on how to recover it. The only evidence we have, at this point of time is this memory dump. Please help me.

Note: This challenge is composed of only 1 flag.

The flag format for this lab is: **inctf{s0me_l33t_Str1ng}**

- Xem thông tin file dump.

```
born21@VM-Ubuntu:~/volatility$ python2 vol.py -f ~/Downloads/MemLabs-Lab4/MemoryDump_Lab4.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23
418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/born21/Downloads/MemLabs-Lab4/MemoryDump_Lab4.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800027f60a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff800027f7d00L
             KUSER_SHARED_DATA : 0xffffff78000000000L
           Image date and time : 2019-06-29 07:30:00 UTC+0000
     Image local date and time : 2019-06-29 13:00:00 +0530
```

- Kiểm tra các tiến trình đang chạy.

```
born21@VM-Ubuntu:~/volatility$ python2 vol.py -f ~/Downloads/MemLabs-Lab4/MemoryDump_Lab4.raw --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ----------
0xfffffa8000ca0040 System                    4      0     79      509 ------      0 2019-06-29 07:28:07 UTC+0000
0xfffffa80014af950 smss.exe                256      4      3       32 ------      0 2019-06-29 07:28:07 UTC+0000
0xfffffa8001c57b30 csrss.exe               328    320     11      385      0      0 2019-06-29 07:28:14 UTC+0000
0xfffffa8000ca8960 csrss.exe               376    368      7      200      1      0 2019-06-29 07:28:15 UTC+0000
0xfffffa8001c6f760 wininit.exe             384    320      3       75      0      0 2019-06-29 07:28:15 UTC+0000
0xfffffa8001c751f0 winlogon.exe            412    368      6      119      1      0 2019-06-29 07:28:15 UTC+0000
0xfffffa8001bc1b30 services.exe            472    384     13      193      0      0 2019-06-29 07:28:17 UTC+0000
0xfffffa8001cb5940 lsass.exe               480    384      8      582      0      0 2019-06-29 07:28:17 UTC+0000
0xfffffa8001cc1b30 lsm.exe                 488    384     12      187      0      0 2019-06-29 07:28:17 UTC+0000
0xfffffa8001d02b30 svchost.exe             580    472     11      358      0      0 2019-06-29 07:28:21 UTC+0000
0xfffffa8001d30b30 VBoxService.ex          640    472     14      137      0      0 2019-06-29 07:28:21 UTC+0000
0xfffffa8001d43a70 svchost.exe             708    472      7      260      0      0 2019-06-29 07:28:22 UTC+0000
0xfffffa8001dacb30 svchost.exe             804    472     19      393      0      0 2019-06-29 07:28:23 UTC+0000
0xfffffa8001db9b30 svchost.exe             840    472     21      431      0      0 2019-06-29 07:28:24 UTC+0000
0xfffffa8001dc6850 svchost.exe             864    472     37      917      0      0 2019-06-29 07:28:24 UTC+0000
0xfffffa8001df1060 audiodg.exe             952    804      7      131      0      0 2019-06-29 07:28:26 UTC+0000
0xfffffa8001e1b890 svchost.exe             220    472     16      323      0      0 2019-06-29 07:28:27 UTC+0000
0xfffffa8001e45630 svchost.exe             484    472     18      376      0      0 2019-06-29 07:28:29 UTC+0000
0xfffffa8001eaab30 spoolsv.exe            1132    472     15      286      0      0 2019-06-29 07:28:32 UTC+0000
0xfffffa8001ed7b30 svchost.exe            1176    472     21      307      0      0 2019-06-29 07:28:33 UTC+0000
0xfffffa8001f452e0 svchost.exe            1276    472     14      220      0      0 2019-06-29 07:28:34 UTC+0000
0xfffffa8001f81b30 taskhost.exe           1804    472     10      161      1      0 2019-06-29 07:28:42 UTC+0000
0xfffffa8001ff9630 taskeng.exe            1824    864      6       82      0      0 2019-06-29 07:28:42 UTC+0000
0xfffffa80020bbb30 dwm.exe                1908    840      5       77      1      0 2019-06-29 07:28:43 UTC+0000
0xfffffa80020f7b30 explorer.exe           1944   1872     37      854      1      0 2019-06-29 07:28:44 UTC+0000
0xfffffa80021abab0 VBoxTray.exe           1592   1944     13      141      1      0 2019-06-29 07:28:53 UTC+0000
0xfffffa8002201ab0 SearchIndexer.         1068    472     13      710      0      0 2019-06-29 07:28:58 UTC+0000
0xfffffa800226e910 SearchProtocol         1696   1068      7      225      1      0 2019-06-29 07:29:02 UTC+0000
0xfffffa8002279890 SearchFilterHo         1688   1068      5       78      0      0 2019-06-29 07:29:02 UTC+0000
0xfffffa8002292b30 dllhost.exe            2076    580     13      260      1      0 2019-06-29 07:29:02 UTC+0000
0xfffffa80022f0610 GoogleCrashHan         2272   2008      7       99      0      1 2019-06-29 07:29:08 UTC+0000
0xfffffa80022f6b30 GoogleCrashHan         2284   2008      7       93      0      0 2019-06-29 07:29:08 UTC+0000
0xfffffa80020a4420 DumpIt.exe             2624   1944      3       45      1      1 2019-06-29 07:29:25 UTC+0000
0xfffffa8002320350 conhost.exe            2636    376      3       50      1      0 2019-06-29 07:29:25 UTC+0000
0xfffffa8001cac460 csrss.exe              2700   2692      7      164      2      0 2019-06-29 07:29:30 UTC+0000
0xfffffa8002330060 winlogon.exe           2728   2692      6      121      2      0 2019-06-29 07:29:30 UTC+0000
0xfffffa8000e54b30 taskhost.exe           2976    472      9      160      2      0 2019-06-29 07:29:36 UTC+0000
0xfffffa8000e62b30 dwm.exe                3000    840      5       76      2      0 2019-06-29 07:29:36 UTC+0000
0xfffffa8000eaeb30 explorer.exe           3012   2992     28      677      2      0 2019-06-29 07:29:36 UTC+0000
0xfffffa8000eeeb30 VBoxTray.exe           2384   3012     14      144      2      0 2019-06-29 07:29:37 UTC+0000
```

- Không khai thác được thông tin gì từ các tiến trình. Từ gợi ý đề bài là file đã bị xoá, chúng ta hãy thử filescan. File rất quan trọng đối với người dùng có thể sẽ được lưu trong thư mục User nên sẽ lọc ra các tệp ở trong thư mục này.

```
born21@VM-Ubuntu:~/volatility$ python2 vol.py -f ~/Downloads/MemLabs-Lab4/MemoryDump_Lab4.raw --profile=Win7SP1x64 filescan > filescan.txt
Volatility Foundation Volatility Framework 2.6.1
born21@VM-Ubuntu:~/volatility$ grep '\\Users\\' filescan.txt
0x000000003e839710      2      2 RW-rwd \Device\HarddiskVolume2\Users\eminem\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
0x000000003e83b2d0      2      0 R--rwd \Device\HarddiskVolume2\Users\eminem\Videos\desktop.ini
0x000000003e88a8c0      1      1 -W-rw- \Device\HarddiskVolume2\Users\eminem\AppData\Local\Temp\FXSAPIDebugLogFile.txt
0x000000003e88ba20      2      0 R--rwd \Device\HarddiskVolume2\Users\eminem\AppData\Roaming\Microsoft\Windows\Themes\slideshow.ini
0x000000003e89b070     15      0 RW-rw- \Device\HarddiskVolume2\Users\eminem\AppData\Local\GDIPFONTCACHEV1.DAT
0x000000003e8a85b0      2      0 RW-rw- \Device\HarddiskVolume2\Users\eminem\AppData\Roaming\Microsoft\Windows\Recent\Flag not here.lnk
0x000000003e8a9610     16      0 RW-r-- \Device\HarddiskVolume2\Users\eminem\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd
automaticDestinations-ms
0x000000003e8aa6f0      2      0 R--rwd \Device\HarddiskVolume2\Users\eminem\AppData\Roaming\Microsoft\Windows\Recent\desktop.ini
0x000000003e8ab250      1      1 RW-rwd \Device\HarddiskVolume2\Users\eminem\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
0x000000003e8acc40     17      1 RW-rw- \Device\HarddiskVolume2\Users\eminem\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
0x000000003e8ad250     14      0 R--r-- \Device\HarddiskVolume2\Users\eminem\Desktop\galf.jpeg
0x000000003e8af4a0     17      1 RW-rw- \Device\HarddiskVolume2\Users\eminem\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
0x000000003e8b04e0     15      0 RW-rw- \Device\HarddiskVolume2\Users\eminem\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x000000003e8b1a50      2      0 R--rwd \Device\HarddiskVolume2\Users\eminem\AppData\Local\Microsoft\Windows\History\desktop.ini
```

- Chú ý vào file sau:

```
0x000000003f9ccf20      1      1 RW-rwd \Device\HarddiskVolume2\Users\eminem\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db
0x000000003f9ce930      1      1 RW-rwd \Device\HarddiskVolume2\Users\eminem\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1024.db
0x000000003f9cea80      1      1 RW-rwd \Device\HarddiskVolume2\Users\eminem\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
0x000000003f9cebd0      1      1 RW-rwd \Device\HarddiskVolume2\Users\eminem\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db
0x000000003f9ff6d0      1      1 RW---- \Device\HarddiskVolume2\Users\SlimShady\NTUSER.DAT
0x000000003f9ff8e0      2      1 RW-r-- \Device\HarddiskVolume2\Users\SlimShady\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
0x000000003f9ffcb0      1      1 R--rw- \Device\HarddiskVolume2\Users\eminem\Desktop\DumpIt
0x000000003fc398d0     16      0 R--rw- \Device\HarddiskVolume2\Users\SlimShady\Desktop\Important.txt
0x000000003fc39a20     17      1 RW-rw- \Device\HarddiskVolume2\Users\SlimShady\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x000000003fc39cd0      2      1 RW-r-- \Device\HarddiskVolume2\Users\SlimShady\AppData\Local\Microsoft\Windows\UsrClass.dat{8381e871-9808-11e
```

- Thử dumpfile để xem nội dung nhưng không có ou

Đoan

5. Lab 5: Black Tuesday

- Mô tả challenge:

We received this memory dump from our client recently. Someone accessed his system when he was not there and he found some rather strange files being accessed. Find those files and they might be useful. I quote his exact statement,

> The names were not readable. They were composed of alphabets and numbers but I wasn't able to make out what exactly it was.

Also, he noticed his most loved application that he always used crashed every time he ran it. Was it a virus?

Note-1: This challenge is composed of 3 flags. If you think 2nd flag is the end, it isn't!! :P

Note-2: There was a small mistake when making this challenge. If you find any string which has the string "***L4B_3_D0n3!!***" in it, please change it to "***L4B_5_D0n3!!***" and then proceed.

Note-3: You'll get the stage 2 flag only when you have the stage 1 flag.

Gần đây chúng tôi đã nhận được kết xuất bộ nhớ này từ khách hàng của mình. Ai đó đã truy cập vào hệ thống của anh ấy khi anh ấy không có ở đó và anh ấy phát hiện thấy một số tệp khá lạ đang được truy cập. Tìm những tập tin đó và chúng có thể hữu ích. Tôi trích dẫn chính xác tuyên bố của anh ấy, Những cái tên không thể đọc được. Chúng bao gồm các bảng chữ cái và số nhưng tôi không thể biết chính xác nó là gì. Ngoài ra, anh ấy còn nhận thấy ứng dụng yêu thích nhất mà anh ấy luôn sử dụng bị lỗi mỗi khi chạy nó. Đó có phải là virus không?

Lab 5 có 3 flags.

- Sau khi tải và giải nén, được 1 tập tin raw. Em sử dụng plugin imageinfo để kiểm tra thông tin của file dump:

```
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418,
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/MemoryDump_Lab5.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800028460a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002847d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2019-12-20 03:47:57 UTC+0000
     Image local date and time : 2019-12-20 09:17:57 +0530
```

- Dùng *psscan* để kiểm tra các process đang chạy:

```
┌──(kali㉿kali)-[~/volatility]
└─$ python2 vol.py -f /home/kali/MemoryDump_Lab5.raw --profile=Win7SP1x64 psscan
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
Offset(P)          Name                PID   PPID PDB                Time created                   Time exited
------------------ ---------------- ------ ------ ------------------ ------------------------------ ------------------------------
0x000000003e806890 VBoxTray.exe        528   1396 0x000000000d90f000 2019-12-20 03:43:25 UTC+0000
0x000000003e81ab30 NOTEPAD.EXE        1388   1580 0x0000000345fd000 2019-12-20 03:48:00 UTC+0000
0x000000003e82d7a0 SearchIndexer.     1800    484 0x0000000009b1a000 2019-12-20 03:43:36 UTC+0000
0x000000003e8a9b30 wmpnetwk.exe       1928    484 0x00000000081ec000 2019-12-20 03:43:40 UTC+0000
0x000000003ea9b760 sppsvc.exe         2940    484 0x000000003a542000 2019-12-20 03:44:24 UTC+0000
0x000000003eb17b30 taskeng.exe        1140    880 0x0000000018615000 2019-12-20 03:43:19 UTC+0000
0x000000003eb70b30 dwm.exe            1172    856 0x000000000fd0b000 2019-12-20 03:43:19 UTC+0000
0x000000003eb98b30 explorer.exe       1396   1180 0x000000000f786000 2019-12-20 03:43:19 UTC+0000
0x000000003ec1cb30 svchost.exe         340    484 0x000000001aec7000 2019-12-20 03:42:03 UTC+0000
0x000000003ec6c700 svchost.exe        1044    484 0x000000001a410000 2019-12-20 03:42:04 UTC+0000
0x000000003ecc57c0 svchost.exe        2296    484 0x0000000006371000 2019-12-20 03:43:45 UTC+0000
0x000000003ece1060 spoolsv.exe        1232    484 0x000000001722d000 2019-12-20 03:42:09 UTC+0000
0x000000003ecfbb30 svchost.exe        1272    484 0x000000000148bd000 2019-12-20 03:42:10 UTC+0000
0x000000003ed775f0 svchost.exe        1372    484 0x0000000013f75000 2019-12-20 03:42:12 UTC+0000
```

Do em cài lại máy ảo nên lỗi Crypto.Hash em chưa kịp fix, để dễ quan sát thì em sẽ chỉ chụp kết quả sau khi chạy plugin chứ không chụp lại câu lệnh ạ.

Lướt xuống phía dưới, em tìm thấy 2 ứng dụng quen thuộc là NOTEPAD và WinRAR:

```
0x000000003fa8cb30 NOTEPAD.EXE       2724   1580 0x0000000035622000 2019-12-20 03:47:53 UTC+0000
0x000000003fa9f060 svchost.exe       2632    484 0x00000000354f8000 2019-12-20 03:47:54 UTC+0000
0x000000003fab8060 notepad.exe       2744   1580 0x0000000016395000 2019-12-20 03:47:21 UTC+0000
0x000000003fafd3d0 explorer.exe      1580   2256 0x0000000031b88000 2019-12-20 03:46:49 UTC+0000
0x000000003fb36b30 VBoxTray.exe      2144   1580 0x000000002bdd2000 2019-12-20 03:46:50 UTC+0000
0x000000003fb68b30 NOTEPAD.EXE       2724   1580 0x0000000035622000 2019-12-20 03:47:53 UTC+0000
0x000000003fb7b060 svchost.exe       2632    484 0x00000000354f8000 2019-12-20 03:47:54 UTC+0000
0x000000003fb94060 notepad.exe       2744   1580 0x0000000016395000 2019-12-20 03:47:21 UTC+0000
0x000000003fbd93d0 explorer.exe      1580   2256 0x0000000031b88000 2019-12-20 03:46:49 UTC+0000
0x000000003fca7b30 SearchProtocol     628   1800 0x000000000ccfb000 2019-12-20 03:46:41 UTC+0000
0x000000003fcab790 conhost.exe       2612   1988 0x0000000039385000 2019-12-20 03:47:40 UTC+0000
0x000000003fce8060 WerFault.exe      2716   2632 0x0000000033753000 2019-12-20 03:47:54 UTC+0000
0x000000003fceb060 DumpIt.exe        2208   1580 0x000000000af3f000 2019-12-20 03:47:39 UTC+0000
0x000000003fcfbb30 WerFault.exe       780   2632 0x000000003431b000 2019-12-20 03:48:01 UTC+0000
0x000000003fd02b30 NOTEPAD.EXE       2056   1580 0x000000000a85a000 2019-12-20 03:48:15 UTC+0000
0x000000003fd05b30 WerFault.exe      2168   2632 0x0000000033a60000 2019-12-20 03:48:15 UTC+0000
0x000000003fd27b30 dllhost.exe        668    588 0x000000000b951000 2019-12-20 03:46:37 UTC+0000
0x000000003fd63060 SearchFilterHo    2608   1800 0x000000000bcdb000 2019-12-20 03:46:41 UTC+0000
0x000000003fd7a630 csrss.exe         1988    364 0x0000000010809000 2019-12-20 03:46:42 UTC+0000
0x000000003fd82060 winlogon.exe      2120    364 0x0000000014bce000 2019-12-20 03:46:42 UTC+0000
0x000000003fd97a20 WinRAR.exe        2924   1580 0x0000000023174000 2019-12-20 03:47:13 UTC+0000
```

- Do đó, em sẽ tìm file .rar bằng *filescan | grep .rar*:

```
┌──(kali㉿kali)-[~/volatility]
└─$ python2 vol.py -f /home/kali/MemoryDump_Lab5.raw --profile=Win7SP1×64 filescan | grep .rar
Volatility Foundation Volatility Framework 2.6.1
0×000000003e81c650      2      0 R--rwd \Device\HarddiskVolume2\Users\Alissa Simpson\AppData\Roaming\Microsoft\Wind
0×000000003e81e390      2      0 R--rwd \Device\HarddiskVolume2\Users\Alissa Simpson\AppData\Roaming\Microsoft\Wind
0×000000003e81ff20     16      0 R--rwd \Device\HarddiskVolume2\Users\Alissa Simpson\AppData\Roaming\Microsoft\Wind
0×000000003e8259a0     16      0 R--rwd \Device\HarddiskVolume2\Users\Alissa Simpson\AppData\Roaming\Microsoft\Wind
0×000000003eb10930      2      0 R--rwd \Device\HarddiskVolume2\Users\SmartNet\AppData\Roaming\Microsoft\Windows\Li
0×000000003eb11c80      2      0 R--rwd \Device\HarddiskVolume2\Users\SmartNet\AppData\Roaming\Microsoft\Windows\Li
0×000000003eb12dd0      3      1 R--rwd \Device\HarddiskVolume2\Users\SmartNet\AppData\Roaming\Microsoft\Windows\Li
0×000000003eb12f20      2      0 R--rwd \Device\HarddiskVolume2\Users\Public\Libraries\RecordedTV.library-ms
0×000000003eb13ae0      3      1 R--rwd \Device\HarddiskVolume2\Users\Public\Libraries
0×000000003eb13cb0      3      1 R--rwd \Device\HarddiskVolume2\Users\Alissa Simpson\AppData\Roaming\Microsoft\Wind
0×000000003eb13e00      3      1 R--rwd \Device\HarddiskVolume2\Users\Public\Libraries
0×000000003eb7c460      2      0 R--rwd \Device\HarddiskVolume2\Users\Public\Libraries\desktop.ini
0×000000003eb7c5b0      2      0 R--rwd \Device\HarddiskVolume2\Users\SmartNet\AppData\Roaming\Microsoft\Windows\Li
0×000000003eb90160      2      0 R--rwd \Device\HarddiskVolume2\Users\Alissa Simpson\AppData\Roaming\Microsoft\Wind
0×000000003ebffc80      2      1 R--rwd \Device\HarddiskVolume2\Users\Alissa Simpson\AppData\Roaming\Microsoft\Wind
0×000000003ebffdd0      2      1 R--rwd \Device\HarddiskVolume2\Users\Alissa Simpson\AppData\Roaming\Microsoft\Wind
0×000000003ecf1d10      2      0 R--rw- \Device\HarddiskVolume2\Program Files\Windows Media Player\Network Sharing\
0×000000003ed3be20      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\Tasks\Microsoft\Windows\Windows Me
0×000000003eed56f0      1      0 R--r-- \Device\HarddiskVolume2\Users\SmartNet\Documents\SW1wb3J0YW50.rar
0×000000003f6a85d0     16      0 RW-rw- \Device\HarddiskVolume2\Windows\ServiceProfiles\LocalService\AppData\Local\
```

Có một file với tên kỳ lạ, đọc vào không hiểu rõ đó là file gì.

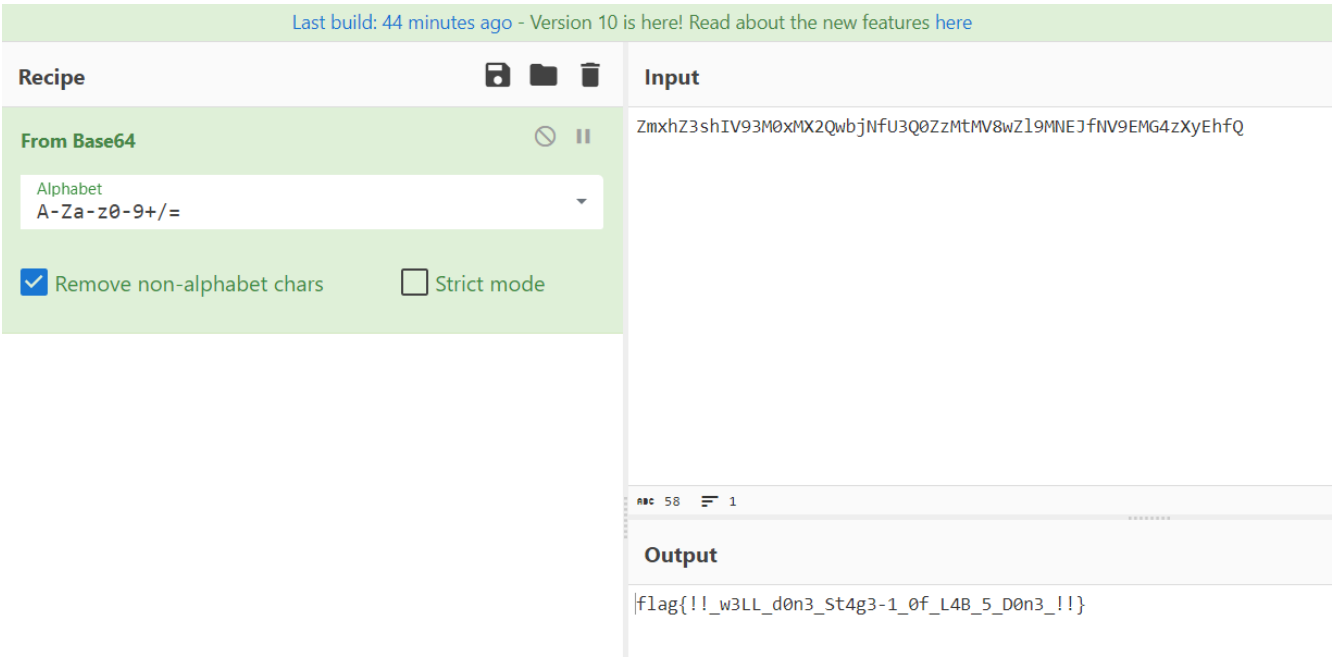
- Để xem rõ về file .rar trên, em sẽ dùng *dumpfile:*

```
┌──(kali㉿kali)-[~/volatility]
└─$ python2 vol.py -f /home/kali/MemoryDump_Lab5.raw --profile=Win7SP1×64 dumpfiles -Q 0×000000003eed56f0 -D .
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
DataSectionObject 0×3eed56f0   None   \Device\HarddiskVolume2\Users\SmartNet\Documents\SW1wb3J0YW50.rar
```

- Sau khi dump thì được 1 file nén. Tuy nhiên nó cần password để mở. Em thực hiện tiếp để tìm password đầu tiên.
- Kiểm tra lịch sử duyệt web bằng *iehistory*, em tìm được đoạn mã đang ngờ:

```
**************************************************
Process: 1396 explorer.exe
Cache type "URL " at 0×2955200
Record length: 0×100
Location: :2019122020191221: Alissa Simpson@file:///C:/Users/Alissa%20Simpson/Pictures/ZmxhZ3shIV93M0xMX2QwbjNfU3Q0ZzMtMV8wZl9MNEJfNV9EMG4zXyEhfQ.bmp
Last modified: 2019-12-20 09:16:09 UTC+0000
Last accessed: 2019-12-20 03:46:09 UTC+0000
File Offset: 0×100, Data Offset: 0×0, Data Length: 0×0
**************************************************
```

- Em decode đoạn mã trên bằng CyberChef, thành công tìm được cờ đầu tiên:



flag{!!_w3LL_d0n3_St4g3-1_0f_L4B_5_D0n3_!!}

- Flag trên chính là password cần tìm, nhập vào thì đã extract được 1 file ảnh png:

```
┌──(kali㉿kali)-[~/volatility]
└─$ ls
AUTHORS.txt    contrib      file.None.0xfffffa80010b44f0.dat
CHANGELOG.txt  CREDITS.txt  file.None.0xfffffa80010b44f0.SW1wb3J0YW50.rar.dat

┌──(kali㉿kali)-[~/volatility]
└─$ unrar e file.None.0xfffffa80010b44f0.SW1wb3J0YW50.rar.dat

UNRAR 7.00 beta 4 freeware      Copyright (c) 1993-2024 Alexander Roshal


Extracting from file.None.0xfffffa80010b44f0.SW1wb3J0YW50.rar.dat

Enter password (will not be echoed) for Stage2.png:

The specified password is incorrect.
Enter password (will not be echoed) for Stage2.png:

Extracting  Stage2.png                                                OK
All OK
```

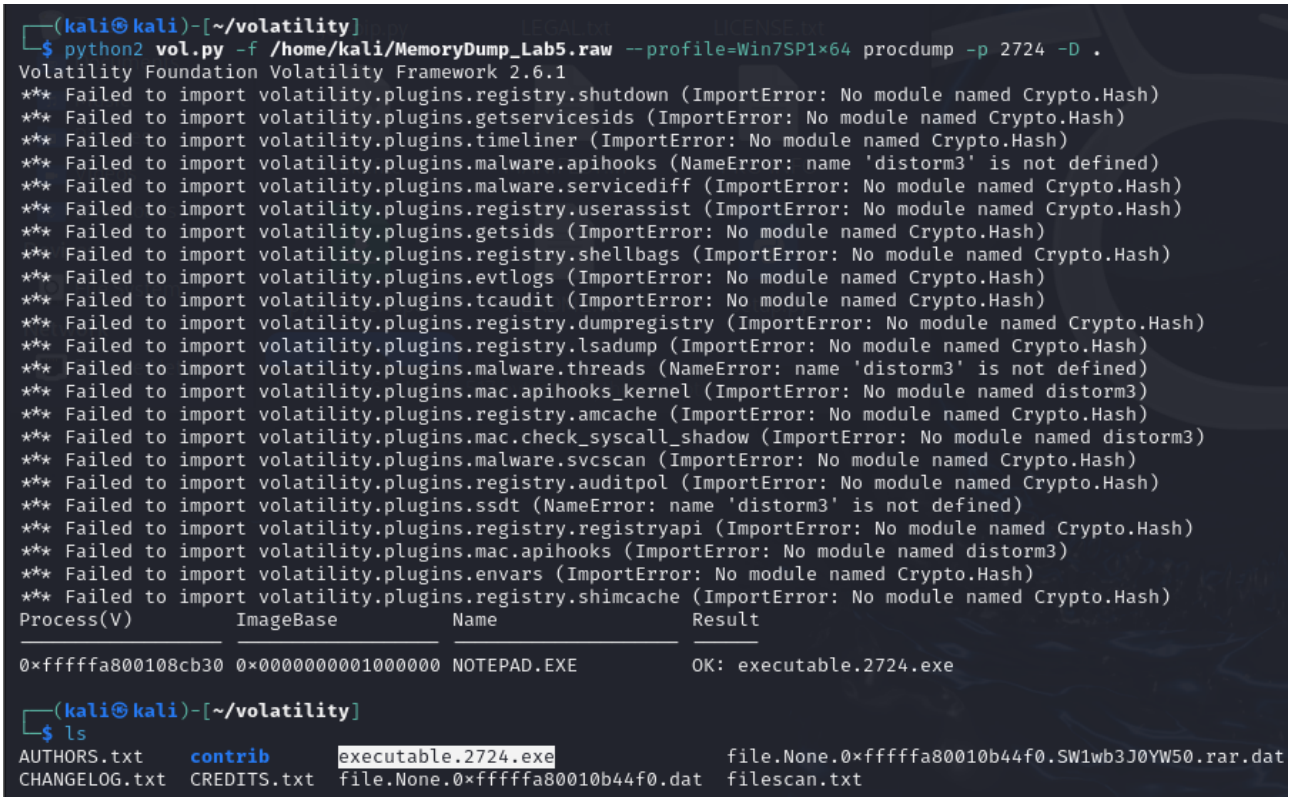
Và flag thứ 2 là

- Tuy nhiên, đề yêu cầu 3 flag, nên tìm tiếp flag cuối cùng, em sẽ xử lý tiếp NODEPAD.exe. Dùng psxview để xem các quá trình ẩn trên hệ thống:

```
0×000000003fd05b30 WerFault.exe          2168 True   True   True     False  False True    False
0×000000003fafd3d0 explorer.exe          1580 False  True   False    False  False False   False
0×000000003fb36b30 VBoxTray.exe          2144 False  True   False    False  False False   False
0×000000003fb68b30 NOTEPAD.EXE           2724 False  True   False    False  False False   False
0×000000003fb94060 notepad.exe           2744 False  True   False    False  False False   False
0×000000003fb7b060 svchost.exe           2632 False  True   False    False  False False   False
0×000000003fbd93d0 explorer.exe          1580 False  True   False    False  False False   False
```

NODEPAD có nhiều tiến trình, tuy nhiên do đề có nói truy cập nhưng không sử dụng được, nên em sẽ chọn tiến trình bị false nhiều nhất có PID là 2724.

- Sử dụng procdump:



6. Lab 6: The Reckoning

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

  *Ví dụ: [*NT101.K11.ANTT*]-Exe01_Group03.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT