

# BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Kỳ báo cáo: Buổi 1

Tên chủ đề: Memory Forensics

GVHD: Lê Đức Thịnh

Ngày báo cáo: 3/4/2023

Nhóm: 7

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Nguyễn Bùi Kim Ngân	20520648	20520648@gm.uit.edu.vn
2	Nguyễn Bình Thực Trâm	20520815	20520815@gm.uit.edu.vn
3	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Công việc	Thực hiện	Thành viên thực hiện	Kết quả tự đánh giá
1	Kịch bản 01	Đã hoàn thành tại lớp	Võ Anh Kiệt	100%
2	Kịch bản 02	Đã hoàn thành tại lớp	Nguyễn Bùi Kim Ngân	100%
3	Kịch bản 03	Đã hoàn thành tại lớp	Võ Anh Kiệt	100%
4	Kịch bản 04	Tìm flag của 5 challenge root me, Command & Control 2 3 4 5 6: Hoàn thành	Nguyễn Bình Thực Trâm Nguyễn Bùi Kim Ngân	100%
5	Kịch bản 05	11 yêu cầu thực hiện phân tích, điều tra: Hoàn thành Tìm flag trong file bị mã hóa: Hoàn thành	Võ Anh Kiệt	100%

**Lưu ý:** Chỉ ghi Kịch bản thực hành được GVTH chỉ định phải làm báo cáo

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

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

*(Xem trang kế tiếp)*

# BÁO CÁO CHI TIẾT

## 1. Kịch bản 01

Đã hoàn thành tại lớp.

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

Từ file dump ta có thể có được một số thông tin nhạy cảm hữu ích như hive, reg, các tiến trình đang chạy, network, socket đang chạy. Việc này giống giám nghiệm và theo dõi hoạt động người dùng đang thực hiện thao tác trên máy tại thời điểm.

Thủ nghiệm lấy password

Xem danh sách hive:

```
./volatility_2.6_lin64_standalone -f find-me.bin --profile=Win7SP1x86 hivelist
```

Lấy thông tin hash của password bằng cách dump file sam với 0x87a1a250 là địa chỉ system và là địa chỉ của sam

```
./volatility_2.6_lin64_standalone -f find-me.bin --profile=Win7SP1x86 hashdump -y 0x87a1a250 -s 0x882ea460 > hashedPass.txt
```

Ta có được thông tin hash sau (không thể dịch ngược thành plaintext)

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Black

Eagle:1000:aad3b435b51404eeaad3b435b51404ee:a39b211d0441a8380ec21a97e88531ff:::

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ ./volatility_2.6_lin64_standalone -f find-me.bin --profile=Win7SP1x86 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual Physical Name
_____
0x87a0c420 0x27d12420 [no name]
0x87a1a250 0x27dde250 \REGISTRY\MACHINE\SYSTEM
0x87a449d0 0x27bca9d0 \REGISTRY\MACHINE\HARDWARE
0x88273008 0x1ff6c008 \SystemRoot\System32\Config\SECURITY
0x8828b9d0 0x1ff269d0 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x882ea460 0x24869460 \SystemRoot\System32\Config\SAM
0x8a47f008 0x24286008 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8bbc39d0 0x258df9d0 \Device\HarddiskVolume1\Boot\BCD
0x8bbde008 0x25970008 \SystemRoot\System32\Config\SOFTWARE
0x8e9b19d0 0x2538a9d0 \SystemRoot\System32\Config\DEFAULT
0x906af9d0 0x1a6ab9d0 \??\C:\Users\Black Eagle\ntuser.dat
0x906f39d0 0x2bb679d0 \??\C:\Users\Black Eagle\AppData\Local\Microsoft\Windows\UsrClass.dat
0x957579d0 0x0a3d79d0 \??\C:\System Volume Information\Syscache.hve

(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ ./volatility_2.6_lin64_standalone -f find-me.bin --profile=Win7SP1x86 hashdump -y 0x87a1a250 -s 0x882ea460 > hashedPas
s.txt
Volatility Foundation Volatility Framework 2.6

(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ cat hashedPass.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Black Eagle:1000:aad3b435b51404eeaad3b435b51404ee:a39b211d0441a8380ec21a97e88531ff:::

(kali㉿kali)-[~/Downloads/nhombay_lab1]
$
```

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

Việc xem lịch sử giúp nắm các thao tác attacker, nắm được hành động và có thể truy vết. Thông tin cho thấy attacker sử dụng backdoor để gọi shell nhằm phá hoại và lấy thông tin.

Tham khảo: <https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#consoles>

### Cmdscan

Plugin cmdscan: tìm kiếm bộ nhớ của csrss trên XP / 2003 / Vista / 2008 và conhost trên Windows 7 để tìm các lệnh attacker đã nhập thông qua giao diện điều khiển. Đây là một trong những lệnh mạnh mẽ nhất mà ta có thể sử dụng để có được khả năng hiển thị các hành động của kẻ tấn công trên hệ thống nạn nhân, cho dù chúng đã mở cmd.exe thông qua phiên RDP hoặc đầu vào / đầu ra được ủy quyền cho một trình bao lệnh từ một cửa hậu được nối mạng.

Ngắn gọn thông tin đầu ra, cmdscan show lệnh từ dump csrss.exe và conhost.exe

Hiển thị lệnh nhập lên shell

```
(kali㉿kali)-[~/Downloads/nhombay_lab1] volcans -books - vol-cheatsheet - find
$ ./volatility_2.6_lin64_standalone -f find-me.bin --profile=Win7SP1x86 cmdscan
Volatility Foundation Volatility Framework 2.6
*****
CommandProcess: conhost.exe Pid: 2284
CommandHistory: 0x200338 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 2 LastAdded: 1 LastDisplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 @ 0x1fdb30: cd Desktop
Cmd #1 @ 0x204570: sdelete.exe -p 3 -s Th1s_is_Fl4g_f0r_100.pdf
Cmd #8 @ 0x390039: ???
Cmd #12 @ 0x2d0039: ??????????????????
Cmd #13 @ 0x390038: ???
Cmd #17 @ 0x2d0037: ??????????????????
Cmd #36 @ 0x1d00c4: ? ???
Cmd #37 @ 0x1fce0: ???
*****
CommandProcess: conhost.exe Pid: 3444
CommandHistory: 0x2b0360 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #36 @ 0x2800c4: *?+?(???
Cmd #37 @ 0x2acf08: +?(????
```

## Console

Tương tự như cmdscan, plugin tìm các lệnh mà kẻ tấn công nhập vào cmd.exe hoặc thực thi thông qua backdoor. Tuy nhiên, thay vì quét COMMAND\_HISTORY, plugin này sẽ quét

CONSOLE\_INFORMATION. Ưu điểm chính của plugin này là nó không chỉ in các lệnh mà kẻ tấn công đã nhập mà còn thu thập toàn bộ buffer màn hình (đầu vào và đầu ra). Ví dụ: thay vì chỉ nhìn thấy "dir", ta sẽ thấy chính xác những gì kẻ tấn công đã nhìn thấy, bao gồm tất cả các tệp và thư mục được liệt kê bởi lệnh "dir".

Console dump dữ liệu từ CONSOLE\_INFORMATION

Hiển thị các lệnh nhập trên shell

Giá trị hiển thị cho cả attacker thấy

```
(kali㉿kali)-[~/Downloads/nhombay_lab1] └─$ ./volatility_2.6_lin64_standalone -f find-me.bin --profile=Win7SP1x86 consoles
Volatility Foundation Volatility Framework 2.6
*****
ConsoleProcess: conhost.exe Pid: 2284
Console: 0x1281c0 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe
AttachedProcess: cmd.exe Pid: 1432 Handle: 0x5c
_____
CommandHistory: 0x200510 Application: sdelete.exe Flags: 
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
_____
CommandHistory: 0x200338 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 2 LastAdded: 1 LastDisplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 at 0x1fdb30: cd Desktop
Cmd #1 at 0x204570: sdelete.exe -p 3 -s This_is_Fl4g_f0r_100.pdf
_____
Screen 0x1e6198 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Black Eagle>cd Desktop

C:\Users\Black Eagle\Desktop>sdelete.exe -p 3 -s This_is_Fl4g_f0r_100.pdf

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

SDelete is set for 3 passes.
This_is_Fl4g_f0r_100.pdf ... deleted.

Files deleted: 1

C:\Users\Black Eagle\Desktop>sdelete.exe -p 3 -s This_is_Fl4g_f0r_100.pdf
SDelete v2.0 - Secure file delete
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

SDelete is set for 3 passes.
```

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

Đầu tiên thực hiện liệt kê các tiến trình

```
./volatility_2.6_lin64_standalone -f find-me.bin --profile=Win7SP1x86 pstree | grep "iexplore.exe\|gpg-agent.exe"
```

```
(kali㉿kali)-[~/Downloads/nhombay_lab1] └─$ ./volatility_2.6_lin64_standalone -f find-me.bin --profile=Win7SP1x86 pstree | grep "iexplore.exe\|gpg-agent.exe"
Volatility Foundation Volatility Framework 2.6
.. 0x849d030:iexplore.exe          2864   1336   17    638 2017-10-07 18:55:53 UTC+0000
.. 0x84cb7558:iexplore.exe          4064   2864   19    617 2017-10-07 18:56:02 UTC+0000
.. 0x8496e7b0:iexplore.exe          3704   2864   22    675 2017-10-07 18:55:53 UTC+0000
0x842d15d0:gpg-agent.exe           3576   3556   3     79 2017-10-07 18:45:41 UTC+0000
```

Thực hiện dump các tiến trình 2864 và 3576:

```
./volatility_2.6_lin64_standalone -f find-me.bin --profile=Win7SP1x86 memdump -p 3576 -D .
```

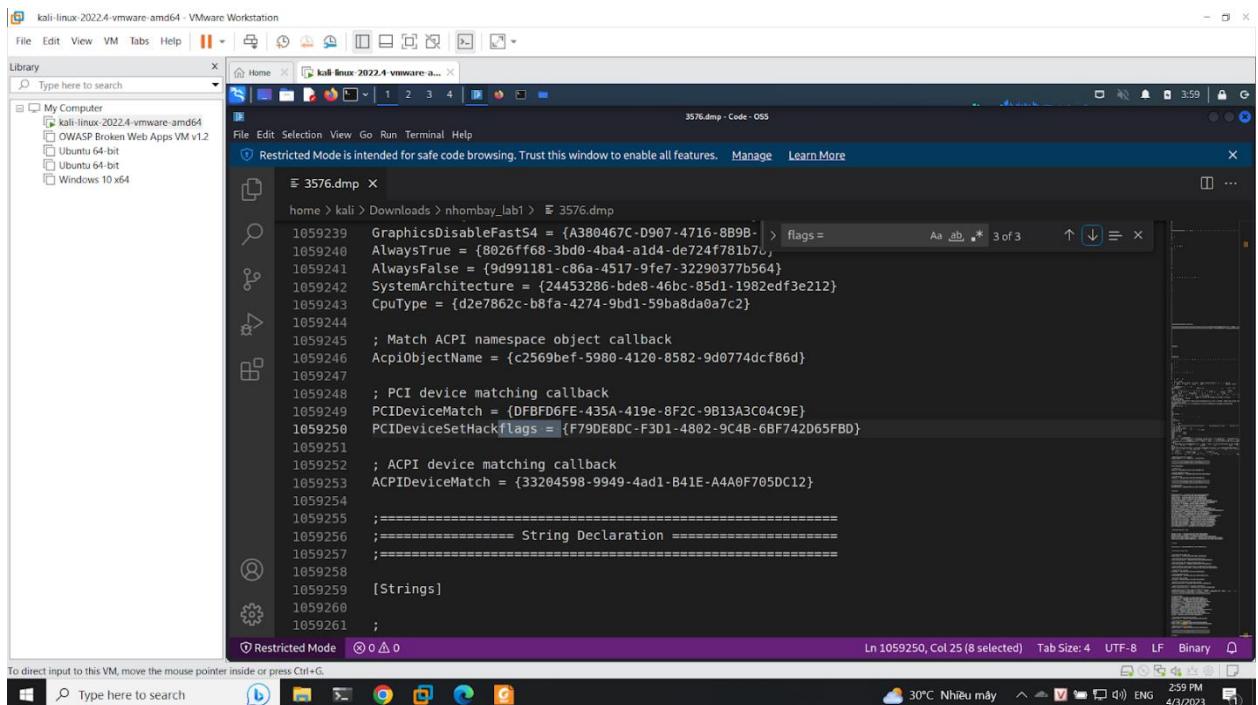
```
./volatility_2.6_lin64_standalone -f find-me.bin --profile=Win7SP1x86 memdump -p 2864 -D .
```

Ở đây ta quan sát các tiến trình thấy được các thông tin sau

flags = {F79DE8DC-F3D1-4802-9C4B-6BF742D65FBD}

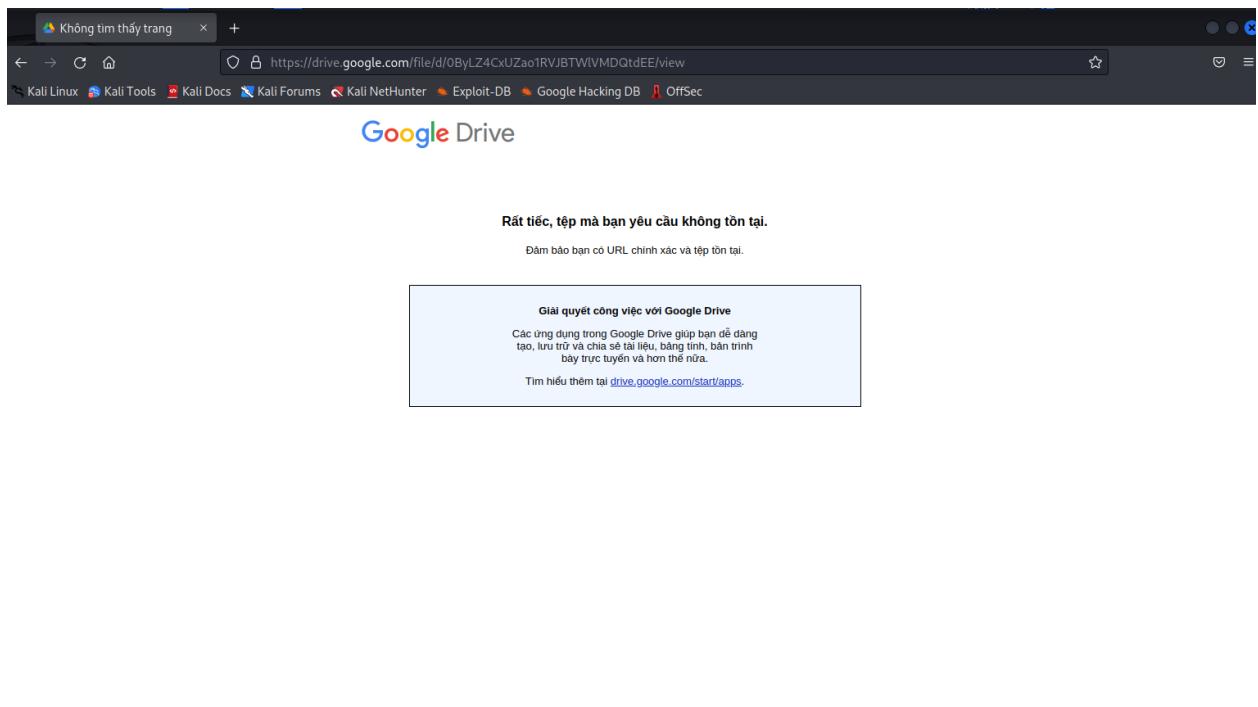
Th1s\_is\_Fl4g\_f0r\_100.pdf

```
home > kali > Downloads > nhombay_lab1 > 2864.dmp
169589 BiosDate = {182A2B31-D5B8-45ef-BB6D-646EBAEDD8F1}
169590 GraphicsDisableFastS4 = {A380467C-D967-4716-8B9B-
169591 AlwaysTrue = {8026ff68-3bd0-4ba4-alda-de724f781b78}
169592 AlwaysFalse = {9d991181-c86a-4517-9fe7-32290377b564}
169593 SystemArchitecture = {24453286-bde8-46bc-85d1-1982edf3e212}
169594 CpuType = {d2e7862c-b8fa-4274-9bd1-59ba8da0a7c2}
169595
169596 ; Match ACPI namespace object callback
169597 AcpiObjectName = {c2569bef-5980-4120-8582-9d0774dcf86d}
169598
169599 ; PCI device matching callback
169600 PCIDeviceMatch = {DFBF06FE-435A-419e-8F2C-9B13A3C04C9E}
169601 PCIDeviceSetHackFlags = {F79DE8DC-F3D1-4802-9C4B-6BF742D65FBD}
169602
169603 ; ACPI device matching callback
169604 ACPIDeviceMatch = {33204598-9949-4ad1-B41E-A4A0F705DC12}
169605
169606 =====
169607 ===== String Declaration =====
169608 =====
169609 [Strings]
169610
169611 ;
169612 ;
169613 ; Operators
```



Thực hiện string 3576.dmp | grep "Th1s\_is\_Fl4g\_f0r\_100.pdf" để xem flag

Nhưng do bài lab đã cũ nên việc vào drive để xem flag đã bị chặn



## 2. Kịch bản 02

Đã hoàn thành tại lớp.

- Kiểm tra thông tin file dump

volatility.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw imageinfo

```
C:\Windows\System32\cmd.exe
E:\NT334-PhapChungKTS\ThucHanh\Lab1>ls
Session-1-Memory-Forensics.pdf      volatility.exe
WIN-LEVQF1CLMR1-20181126-091622.raw

E:\NT334-PhapChungKTS\ThucHanh\Lab1>volatility.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw imageinfo
Volatility Foundation Volatility Framework 2.3.1
Determining profile based on KDBG search...

Suggested Profile(s) : Win7SP0x64, Win7SP1x64, Win2008R2SP0x64, Win2008R2SP1x64
AS Layer1 : AMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (E:\NT334-PhapChungKTS\ThucHanh\Lab1\WIN-LEVQF1CLMR1-20181126-091622.raw)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf80002bfe0a0L
Number of Processors : 2
Image Type (Service Pack) : 1
    KPCR For CPU 0 : 0xfffffff80002bffd00L
    KPCR For CPU 1 : 0xfffffff800009ef000L
    KUSER_SHARED_DATA : 0xfffffff8000000000L
Image date and time : 2018-11-26 09:16:31 UTC+0000
Image local date and time : 2018-11-26 16:16:31 +0700
```

- Kiểm tra biến môi trường có giá trị COMPUTERNAME

volatility.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64  
envars | grep COMPUTERNAME

```
C:\Windows\System32\cmd.exe
E:\NT334-PhapChungKTS\ThucHanh\Lab1>volatility.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 envars | grep COMPUTERNAME
Volatility Foundation Volatility Framework 2.3.1
 412 wininit.exe      0x0000000003ab2c0 COMPUTERNAME          WIN-LEVQF1CLMR1
 468 services.exe     0x0000000002c1320 COMPUTERNAME          WIN-LEVQF1CLMR1
 484 lsass.exe        0x00000000002f1320 COMPUTERNAME          WIN-LEVQF1CLMR1
 492 lsm.exe          0x0000000000d1320 COMPUTERNAME          WIN-LEVQF1CLMR1
 540 winlogon.exe    0x00000000001c0010 COMPUTERNAME          WIN-LEVQF1CLMR1
 636 svchost.exe     0x00000000002d1320 COMPUTERNAME          WIN-LEVQF1CLMR1
 700 vmauthlp.exe    0x0000000000281320 COMPUTERNAME          WIN-LEVQF1CLMR1
 744 svchost.exe     0x0000000000151320 COMPUTERNAME          WIN-LEVQF1CLMR1
 808 svchost.exe     0x0000000000241320 COMPUTERNAME          WIN-LEVQF1CLMR1
 872 svchost.exe     0x00000000001e1320 COMPUTERNAME          WIN-LEVQF1CLMR1
 900 svchost.exe     0x00000000000441320 COMPUTERNAME         WIN-LEVQF1CLMR1
 308 svchost.exe     0x0000000000301320 COMPUTERNAME          WIN-LEVQF1CLMR1
 760 svchost.exe     0x00000000000101320 COMPUTERNAME          WIN-LEVQF1CLMR1
1104 spoolsv.exe     0x0000000000271320 COMPUTERNAME          WIN-LEVQF1CLMR1
1148 svchost.exe     0x0000000000321320 COMPUTERNAME          WIN-LEVQF1CLMR1
1340 nessus-service 0x000000000002d1320 COMPUTERNAME          WIN-LEVQF1CLMR1
1372 nessusd.exe     0x00000000001e279f0 COMPUTERNAME          WIN-LEVQF1CLMR1
```

- Xem các tiến trình đang chạy

volatility.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64  
psscan

```
E:\NT334-PhapChungKTS\ThucHanh\Lab1>volatility.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 psscan
Volatility Foundation Volatility Framework 2.3.1
Offset(P)       Name           PID   PPID  PDB      Time created      Time exited
-----+-----+-----+-----+-----+-----+-----+
0x0000000002b4d8060 svchost.exe    308   468  0x00000000182d9000 2018-11-26 09:05:33 UTC+0000
0x0000000007d0ac610 wmpnetwk.exe  1720  468  0x000000000732f5000 2018-11-26 09:06:09 UTC+0000
0x0000000007d0c1060 chrome.exe    2440  2452 0x000000000271a9000 2018-11-26 09:14:08 UTC+0000
0x0000000007d22b690 WmiPrvSE.exe  2080  636  0x00000000006ed4000 2018-11-26 09:05:43 UTC+0000
0x0000000007d2c2210 WmiPrvSE.exe  2940  636  0x0000000000a7b0000 2018-11-26 09:06:02 UTC+0000
0x0000000007d2f4b30 SearchIndexer. 2428  468  0x000000000779ef000 2018-11-26 09:06:08 UTC+0000
0x0000000007d454b30 nessusd.exe   1372  1348 0x0000000009434000 2018-11-26 09:05:36 UTC+0000
0x0000000007d4716a0 VGAuthService. 1388  468  0x0000000006e198000 2018-11-26 09:05:36 UTC+0000
0x0000000007d447300 vmtoolsd.exe  1456  468  0x0000000000d39e000 2018-11-26 09:05:37 UTC+0000
0x0000000007d500060 taskhost.exe  1552  468  0x00000000010665000 2018-11-26 09:05:37 UTC+0000
0x0000000007d532060 sppsvc.exe   1976  468  0x0000000000c069000 2018-11-26 09:05:41 UTC+0000
0x0000000007d5a060 svchost.exe   1912  468  0x00000000009552000 2018-11-26 09:05:41 UTC+0000
0x0000000007d5c1b30 svchost.exe   1952  468  0x0000000000aadcc00 2018-11-26 09:05:41 UTC+0000
0x0000000007d5dd060 dwm.exe     2792  872  0x000000000739be000 2018-11-26 09:06:01 UTC+0000
0x0000000007d5eab30 dllhost.exe  1636  468  0x0000000004208000 2018-11-26 09:05:42 UTC+0000
0x0000000007d6e6b30 svchost.exe   872   468  0x000000000172c7000 2018-11-26 09:05:32 UTC+0000
```

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

volatility.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64  
hivelist

```
E:\NT334-PhapChungKTS\ThucHanh\Lab1>volatility.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
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\Syncache.hve
0xfffff8a005f30240 0x0000000001cd2240 \SystemRoot\System32\Config\DEFAULT
0xfffff8a005fc7010 0x00000000353c010 \SystemRoot\System32\Config\SECURITY
```

- Thực hiện truyền hashdump vào file hashes.txt

volatility.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64  
hashdump -y 0xfffff8a000024010 -s 0xfffff8a00172e010 > hashes.txt

```
E:\NT334-PhapChungKTS\ThucHanh\Lab1>volatility.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 hashdump -y 0xffffffff8a0024010 -s 0xfffffff8a00172e010 > hashes.txt
Volatility Foundation Volatility Framework 2.6

E:\NT334-PhapChungKTS\ThucHanh\Lab1>cat hashes.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
FL:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

- Lịch sử tiến trình cmd

volatility.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 consoles

```
E:\NT334-PhapChungKTS\ThucHanh\Lab1>volatility.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 consoles
Volatility Foundation Volatility Framework 2.3.1
*****
ConsoleProcess: conhost.exe Pid: 1648
Console: 0xffffd56200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: C:\Users\FL\Downloads\DumpIt\DumpIt.exe
Title: C:\Users\FL\Downloads\DumpIt\DumpIt.exe
AttachedProcess: DumpIt.exe Pid: 3388 Handle: 0x60
----
CommandHistory: 0x109430 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
----
Screen 0xee400 X:80 Y:300
Dump:
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiiche.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]
+ Processing...
```

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

Tìm process notepad.exe

không có tiến trình notepad

Memory Forensics								
Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start
0xfffffa80018bd990	System	4	0	95	530	—	0	2018-11-26 09:05:20 UTC+0000
0xfffffa8003288710	smss.exe	276	4	2	30	—	0	2018-11-26 09:05:20 UTC+0000
0xfffffa8002b1cb30	csrss.exe	356	340	9	575	0	0	2018-11-26 09:05:27 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
0xfffffa8003d2ba30	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	vmacthlp.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
0xfffffa800410f6e00	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	spoolsv.exe	1104	468	13	331	0	0	2018-11-26 09:05:33 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 09:05:35 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
0xfffffa800430060	taskhost.exe	1552	468	8	144	1	0	2018-11-26 09:05:37 UTC+0000
0xfffffa80043a060	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	dllhost.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 09:05:44 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
0xfffffa80044c2210	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

volatility.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64  
pslist | grep notepad

```
E:\NT334-PhapChungKTS\ThucHanh\Lab1>volatility.exe -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 pslist | grep notepad
Volatility Foundation Volatility Framework 2.6

E:\NT334-PhapChungKTS\ThucHanh\Lab1>
```

Không tìm thấy tiến trình nodepad

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

Thực hiện xem các tiến trình

(kali㉿kali)-[~/Downloads/nhombay_lab1]
\$ ./volatility_2.6_lin64_standalone -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit
0xfffffa80018bd990 System 4 0 95 530 0 0 2018-11-26 09:05:20 UTC+0000
0xfffffa8003288710 smss.exe 276 4 2 30 0 0 2018-11-26 09:05:20 UTC+0000
0xfffffa8002bicb30 csrss.exe 356 340 9 575 0 0 2018-11-26 09:05:27 UTC+0000
0xfffffa8003cb1030 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
0xfffffa8003d54030 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 vmacthl.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
0xfffffa8003d9050 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
0xfffffa800410f6e0 svchost.exe 900 468 39 1108 0 0 2018-11-26 09:05:32 UTC+0000
0xfffffa800755060 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 spoolsv.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
0xfffffa80042a730 vmtools.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
0xfffffa80043ea030 dllhost.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
0xfffffa80043dd060 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
0xfffffa800286403 vmtools.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
0xfffffa8004474b30 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
0xfffffa8001bd2b30 taskhost.exe 2904 990 5 89 0 0 2018-11-26 09:11:42 UTC+0000

Thực hiện dump tiến trình 3632

(kali㉿kali)-[~/Downloads/nhombay_lab1]
\$ ./volatility_2.6_lin64_standalone -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 memdump -D ./ -p 3632
Volatility Foundation Volatility Framework 2.6
*****
Writing explorer.exe [ 3632] to 3632.dmp

Chạy lệnh strings và 3632.dmp | grep "http://" để xem lịch sử mới nhất

(kali㉿kali)-[~/Downloads/nhombay_lab1]
\$ strings 3632.dmp   grep "http://"
<libraryDescription xmlns="http://schemas.microsoft.com/windows/2009/library">
<dpiAware xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
<http://ns.adobe.com/xap/1.0/

Kéo xuống phía dưới thì ta thấy được lịch sử mới nhất

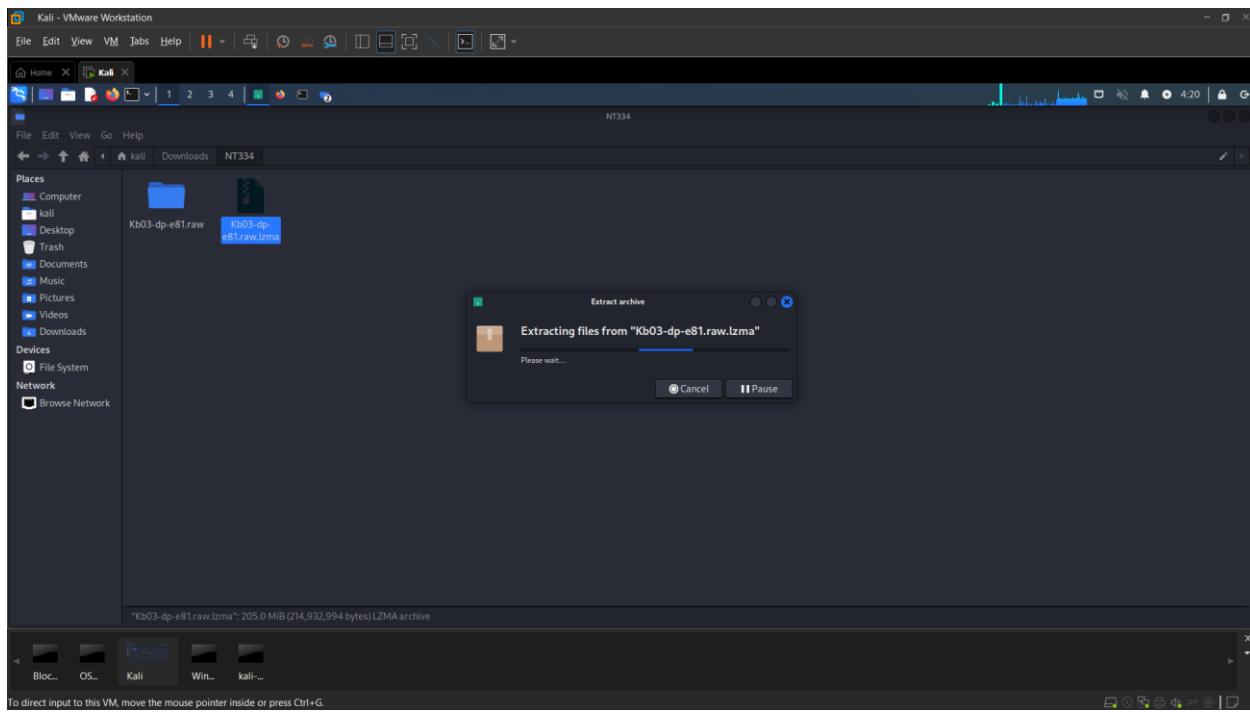
(kali㉿kali)-[~/Downloads/nhombay_lab1]
\$ http://ocsp.usertrust.com0
\$ http://www.usertrust.com1
<asmv3:windowsSettings xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">

### 3. Kịch bản 03

Đã hoàn thành tại lớp.

- Cung cấp bằng chứng xác định file được cho là file dump từ bộ nhớ máy ảo.
- Tìm flag cho file tài nguyên bên trên. Biết rằng flag có định dạng là CTF{flag}

Đầu tiên ta thực hiện Extract file



Thực hiện kiểm tra file dump bằng lệnh imageinfo

```
File Actions Edit View Help
└──(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ ./volatility_2.6_lin64_standalone -f Kb03-dp-e81.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug      : Determining profile based on KDBG search ...
Suggested Profile(s) : Win10x64
                    AS Layer1 : Win10AMD64PagedMemory (Kernel AS)
                    AS Layer2 : VirtualBoxCoreDumpElf64 (Unnamed AS)
                    AS Layer3 : FileAddressSpace (/home/kali/Downloads/nhombay_lab1/Kb03-dp-e8
1.raw)
                    PAE type : No PAE
                    DTB : 0x1aa000L
                    KUSER_SHARED_DATA : 0xfffffff78000000000L
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/nhombay_lab1]
$
```

Tiếp tục thực hiện pslist để kiểm tra các tiến trình

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64
0xfffffe00032553780	System	4	0	126	0	—	—
0 2016-04-04 16:12:33 UTC+0000							
0xfffffe0003389c040	smss.exe	268	4	2	0	—	—
0 2016-04-04 16:12:33 UTC+0000							
0xfffffe0003381b080	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							
0xfffffe00033efb440	services.exe	484	404	3	0	0	—
0 2016-04-04 16:12:34 UTC+0000							
0xfffffe00033f08080	lsass.exe	492	404	6	0	0	—
0 2016-04-04 16:12:34 UTC+0000							
0xfffffe00033ec5780	svchost.exe	580	484	16	0	0	—

Ta thấy được tiến trình 4092 đang chạy mspaint.exe

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							
0xCCCCCCCCCCCCCCCC	svchost.exe	628	624	1	0	1	—

Thực hiện dump tiến trình 4092

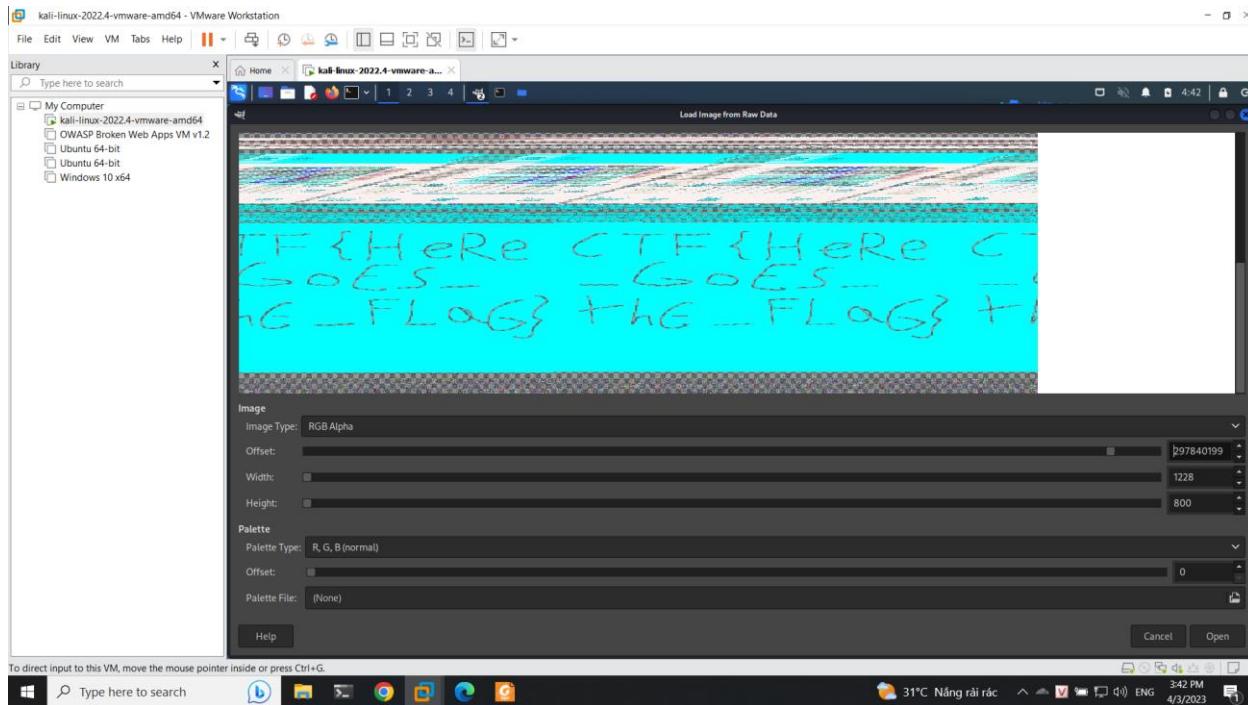
Volatility Foundation Volatility Framework 2.6							
*****							
Writing mspaint.exe [ 4092] to 4092.dmp							

Đổi đuôi .dmp thành .data để mở bằng gimp

File Actions Edit View Help							
(kali㉿kali)-[~/Downloads/nhombay_lab1]							
\$ gimp 4092.data							

```
gimp_device_info_set_device: trying to set GdkDevice
use' on GimpDeviceInfo which already has a device
gimp_device_info_set_device: trying to set GdkDevice
on GimpDeviceInfo which already has a device
```

Thực hiện điều chỉnh các thông số để có thể đọc được flag



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

#### 4. Kịch bản 04

## Challenge 1: Command & Control 2

Đầu tiên, ta sẽ dùng lệnh `imageinfo` để kiểm tra thông tin file dump. Ta có thể thấy được profile của file để sử dụng trong các lệnh tiếp theo.

Yêu cầu của bài này là sẽ tìm được COMPUTERNAME của file dump này. Theo như docs cmd thì plugin envars sẽ trả về giá trị các biến môi trường của quy trình, thường thì nó sẽ là số lượng CPU được cài đặt và kiến trúc phần cứng, thư mục hiện tại của quy trình, thư mục tạm thời, tên phiên, tên máy tính, tên người dùng và nhiều tạo phẩm thú vị khác. Hiện tại, ta đang cần tìm computernname, vì vậy ta sẽ dùng envar để tìm được như hình bên dưới:

```

kali㉿kali:~/Downloads/Vol2.6/volatility_2.6_x86_standalone$ ./vol.py -f /tmp/memdump.dmp --envvars
File Actions Edit View Help
468 csrss.exe      0x004307f0 OS           Windows_NT
468 csrss.exe      0x004307f0 Path          C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPo...
werShell\v1.0\     0x004307f0 PATHEXT       .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
468 csrss.exe      0x004307f0 PROCESSOR_ARCHITECTURE x86
468 csrss.exe      0x004307f0 PROCESSOR_IDENTIFIER x86 Family 6 Model 23 Stepping 6, GenuineIntel
468 csrss.exe      0x004307f0 PROCESSOR_LEVEL   6
468 csrss.exe      0x004307f0 PROCESSOR_REVISION 1706
468 csrss.exe      0x004307f0 PSModulePath    C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
468 csrss.exe      0x004307f0 SystemDrive      C:
468 csrss.exe      0x004307f0 SystemRoot      C:\Windows
468 csrss.exe      0x004307f0 TEMP          C:\Windows\TEMP
468 csrss.exe      0x004307f0 TMP           C:\Windows\TEMP
468 csrss.exe      0x004307f0 USERNAME      SYSTEM
468 csrss.exe      0x004307f0 windir        C:\Windows
560 services.exe   0x001207f0 ALLUSERSPROFILE C:\ProgramData
560 services.exe   0x001207f0 CommonProgramFiles C:\Program Files\Common Files
560 services.exe   0x001207f0 COMPUTERNAME   WIN-ETSA91RKCFP
560 services.exe   0x001207f0 ComSpec        C:\Windows\system32\cmd.exe
560 services.exe   0x001207f0 FP_NO_HOST_CHECK NO
560 services.exe   0x001207f0 NUMBER_OF_PROCESSORS 1
560 services.exe   0x001207f0 OS           Windows_NT
560 services.exe   0x001207f0 Path          C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPo...
werShell\v1.0\     0x001207f0 PATHEXT       .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
560 services.exe   0x001207f0 PROCESSOR_ARCHITECTURE x86
560 services.exe   0x001207f0 PROCESSOR_IDENTIFIER x86 Family 6 Model 23 Stepping 6, GenuineIntel
560 services.exe   0x001207f0 PROCESSOR_LEVEL   6

```

Sau đó, ta sẽ nhập flag: WIN-ETSA91RKCFP vào challenge và hoàn thành.

The validation flag is the workstation's hostname.

The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de

**Start the challenge**

**1 related ressource(s)**

- Volatility cheatsheet v2.4 (Forensic)

**Validation**

Well done, you won 15 Points

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

**Enter password**

**Send**

## Challenge 2: Command & Control 3

Trong câu này, đề bài yêu cầu tìm đường dẫn tuyệt đối của file thực thi nghi ngờ là malware. Trước tiên, chúng ta cần tìm file có các hành động bất thường trước. Em dùng plugin pstree để xem được các process đang chạy và quan hệ giữa chúng. Sau đó, chúng em tìm thấy có 1 process khá lạ ở explore.exe có process con là cmd.exe trong khi bên dưới cũng có 1 process explore.exe tương tự nhưng không hề chạy cmd.exe này.

```

Kali - VMware Workstation
File Edit View VM Tabs Help | X | 
Home X Kali 
File Actions Edit View Help
..:0x88cded40:sppsvc.exe      1872 560   4   143 2013-01-12 16:39:02 UTC+0000
..:0x8a102748:svchost.exe      1748 560   18  310 2013-01-12 16:38:58 UTC+0000
..:0x8a0f9c40:spoolsv.exe     1712 560   14  338 2013-01-12 16:38:58 UTC+0000
..:0x9541c7e0:wlmss.exe       336 560   4   45 2013-01-12 16:39:21 UTC+0000
..:0x8a1f5030:VMUpgradeHelppe 448 560   4   89 2013-01-12 16:39:21 UTC+0000
...:0x892ced40:winlogon.exe    500 448   3   111 2013-01-12 16:38:14 UTC+0000
...:0x88d03a00:cssrs.exe       468 448   10  471 2013-01-12 16:38:14 UTC+0000
...:0x87c595b0:conhost.exe     3228 468   2   54 2013-01-12 16:44:50 UTC+0000
...:0x87a9c288:conhost.exe     2600 468   1   35 2013-01-12 16:40:28 UTC+0000
...:0x954a826b0:conhost.exe    2168 468   2   49 2013-01-12 16:55:50 UTC+0000
...:0x87bd35b8:wmpnetwk.exe   3176 560   9   240 2013-01-12 16:40:48 UTC+0000
...:0x87ac0620:taskhost.exe    2352 560   8   149 2013-01-12 16:40:24 UTC+0000
...:0x897b5c20:svchost.exe     764 560   7   263 2013-01-12 16:38:23 UTC+0000
...:0x8962f7e8:lsm.exe        584 456   10  142 2013-01-12 16:38:16 UTC+0000
...:0x896427b8:lsass.exe      576 456   6   566 2013-01-12 16:38:16 UTC+0000
0x8929fd40:csrss.exe        404 396   9   469 2013-01-12 16:38:14 UTC+0000
0x87978d78:System           4   0   103  3257 2013-01-12 16:38:09 UTC+0000
...:0x88c3ed40:smss.exe       308 4   2   29 2013-01-12 16:38:09 UTC+0000
0x87ac6030:explorer.exe     2548 2484  24  766 2013-01-12 16:40:27 UTC+0000
...:0x87b6b030:explorer.exe   2772 2548  2   74 2013-01-12 16:40:34 UTC+0000
...:0x89898030:cmd.exe        1616 2772  2   101 2013-01-12 16:55:49 UTC+0000
...:0x95495c18:taskngr.exe    1232 2548  6   116 2013-01-12 16:42:29 UTC+0000
...:0x87bf7030:cmd.exe        3152 2548  1   23 2013-01-12 16:44:50 UTC+0000
...:0x87cbfd40:wmpmem-1.3.1. 3144 3152  1   23 2013-01-12 16:59:17 UTC+0000
...:0x898fe8c0:stikyNot.exe   2744 2548  8   135 2013-01-12 16:40:32 UTC+0000
...:0x87b784b0:AvastUI.exe    2720 2548  14  220 2013-01-12 16:40:31 UTC+0000
...:0x87b82438:VmwareTray.exe 2660 2548  5   80 2013-01-12 16:40:29 UTC+0000
...:0x87c6a2a0:swriter.exe    3452 2548  1   19 2013-01-12 16:41:01 UTC+0000

```

=> File thực thi này có vẻ khá bất thường nên chúng em dự đoán nó có thể là malware, tui em quyết định sẽ xem kỹ hơn khi thực thi file này nó đã chạy các lệnh nào bằng plugin cmdline. Bên dưới, chúng em đã kiểm tra cmdline của process explore.exe (1136) và thấy đường dẫn nó hoàn toàn khác so với đường dẫn của process đáng nghi trước đó (2772).

```

(kali㉿kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23418 cmdline -p 1136
Volatility Foundation Volatility Framework 2.6
*****
iexplore.exe pid: 1136
Command line : "C:\Program Files\Internet Explorer\iexplore.exe"

(kali㉿kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23418 cmdline -p 2772
Volatility Foundation Volatility Framework 2.6
*****
iexplore.exe pid: 2772
Command line : "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe"

(kali㉿kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]

```

=> Vậy rất có thể đường dẫn này chính là flag mà đề bài yêu cầu. Vì vậy, chúng em dùng tool hash online để hash nó đúng định dạng flag.

The screenshot shows a web-based MD5 Hash Generator tool. The input field contains the string 'C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\explore.exe'. Below the input field, there is a 'Generate' button. Underneath the button, the results are displayed in three rows: 'Your String' with the value 'C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\explore.exe', 'MD5 Hash' with the value '49979149632639432397b3a1df8cb43d' and a 'Copy' button, and 'SHA1 Hash' with the value '2b4d21a78d002ca6c0c5bd12b874e83fdd5a7804' and a 'Copy' button. A note at the bottom states: 'This MD5 hash generator is useful for encoding passwords, credit cards numbers and other sensitive date into MySQL, Postgress or other databases. PHP programmers, ASP programmers and anyone developing on MySQL, SQL, Postgress or similar should find this online tool an especially handy resource.'

Sau đó nộp bài thử với flag là: 49979149632639432397b3a1df8cb43d

=> Hoàn thành challenge.

The screenshot shows a challenge page from root-me.org. At the top, there is a password update dialog with fields for 'Username' (bington212@gmail.com) and 'Password' (redacted). Buttons for 'Update password' and 'No thanks' are present. Below the dialog, a message says 'is the md5 checksum'. The main content area includes a 'Start the challenge' button, a section for '2 related ressource(s)' with links to Microsoft's Sysinternals documentation and Volatility cheatsheet, a 'Validation' section with a success message ('Well done, you won 30 Points') and a voting link ('Don't forget to give your opinion on the challenge by voting :-)'), and a 'tweet it!' button. At the bottom, there is a 'Enter password' field and a 'Send' button.

**Challenge 4:**

Trong challenge này yêu cầu tìm ip:port của máy target kế tiếp đang bị malware nhắm tới. Ban đầu em thấy yêu cầu ip:port nên nghĩ sẽ liên quan tới mạng, nhưng khi dùng plugin netscan và chú ý vào process malware vừa rồi thì không thấy được kết quả gì.

kali@kali: ~/Downloads/Vol2.6/volatility_2.6_lin64_standalone						
0x1d6eedc0	TCPv6	:::49157	::::	LISTENING	928	svchost.exe
0x1d816a48	TCPv4	127.0.0.1:12025	0.0.0.0:0	LISTENING	1220	AvastSvc.exe
0x1d8270c0	TCPv4	127.0.0.1:12143	0.0.0.0:0	LISTENING	1220	AvastSvc.exe
0x1d8517b0	TCPv4	127.0.0.1:12119	0.0.0.0:0	LISTENING	1220	AvastSvc.exe
0x1d87b650	TCPv4	127.0.0.1:12995	0.0.0.0:0	LISTENING	1220	AvastSvc.exe
0x1d8a55d8	TCPv4	127.0.0.1:12465	0.0.0.0:0	LISTENING	1220	AvastSvc.exe
0x1d8cf310	TCPv4	127.0.0.1:12993	0.0.0.0:0	LISTENING	1220	AvastSvc.exe
0x1d8fad00	TCPv4	127.0.0.1:12563	0.0.0.0:0	LISTENING	1220	AvastSvc.exe
0x1d8ffdc0	TCPv4	127.0.0.1:27275	0.0.0.0:0	LISTENING	1220	AvastSvc.exe
0x1dbc89c8	TCPv4	127.0.0.1:2110	0.0.0.0:0	LISTENING	1220	AvastSvc.exe
0x1de5a288	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	832	svchost.exe
0x1de5c230	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	832	svchost.exe
0x1de5c230	TCPv6	:::49153	:::0	LISTENING	832	svchost.exe
0xdf689c8	TCPv4	127.0.0.1:12080	0.0.0.0:0	LISTENING	1220	AvastSvc.exe
0xd77fb78	TCPv4	192.168.1.66:58784	65.55.253.27:80	ESTABLISHED	1220	AvastSvc.exe
0x1d901bd0	TCPv4	192.168.1.66:49156	77.234.42.54:80	ESTABLISHED	1220	AvastSvc.exe
0x1d92e240	TCPv4	127.0.0.1:12080	127.0.0.1:49178	ESTABLISHED	1220	AvastSvc.exe
0x1d9ebdf8	TCPv4	192.168.1.66:58793	213.152.6.106:80	ESTABLISHED	1220	AvastSvc.exe
0x1dedb4f8	TCPv4	127.0.0.1:49178	127.0.0.1:12080	ESTABLISHED	2772	iexplore.exe
0xe034c80	UDPv4	192.168.1.66:137	*:*		4	System
0xe03e440	UDPv4	192.168.1.66:138	*:*		4	System
0x1e176d40	UDPv4	0.0.0.0:0	*:*		1172	svchost.exe
0x1e176d40	UDPV6	:::0	*:*		1172	svchost.exe
0x1e0348a0	TCPv4	192.168.1.66:139	0.0.0.0:0	LISTENING	4	System
0x1e1d7008	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	764	svchost.exe
0x1e1eeaa0	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	764	svchost.exe
0x1e1eeaa0	TCPv6	:::135	:::0	LISTENING	764	svchost.exe
0x1ef8688	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	456	wininit.exe

Vì vậy, em quyết định chuyển hướng làm, ban nãy chúng ta thấy file thực thi cmd.exe, vậy rất có thể là trong quá trình tấn công thì attacker này đã chạy ngầm một số lệnh gì đó, nên chúng em thử dùng plugin consoles để kiểm tra thử.

```
└$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23418 consoles
```

```

Kali - VMware Workstation
File Edit View VM Tabs Help || Home X Kali
File Actions Edit View Help
AttachedProcess: cmd.exe Pid: 3152 Handle: 0x64
CommandHistory: 0x3007a8 Application: winpmem-1.3.1.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
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

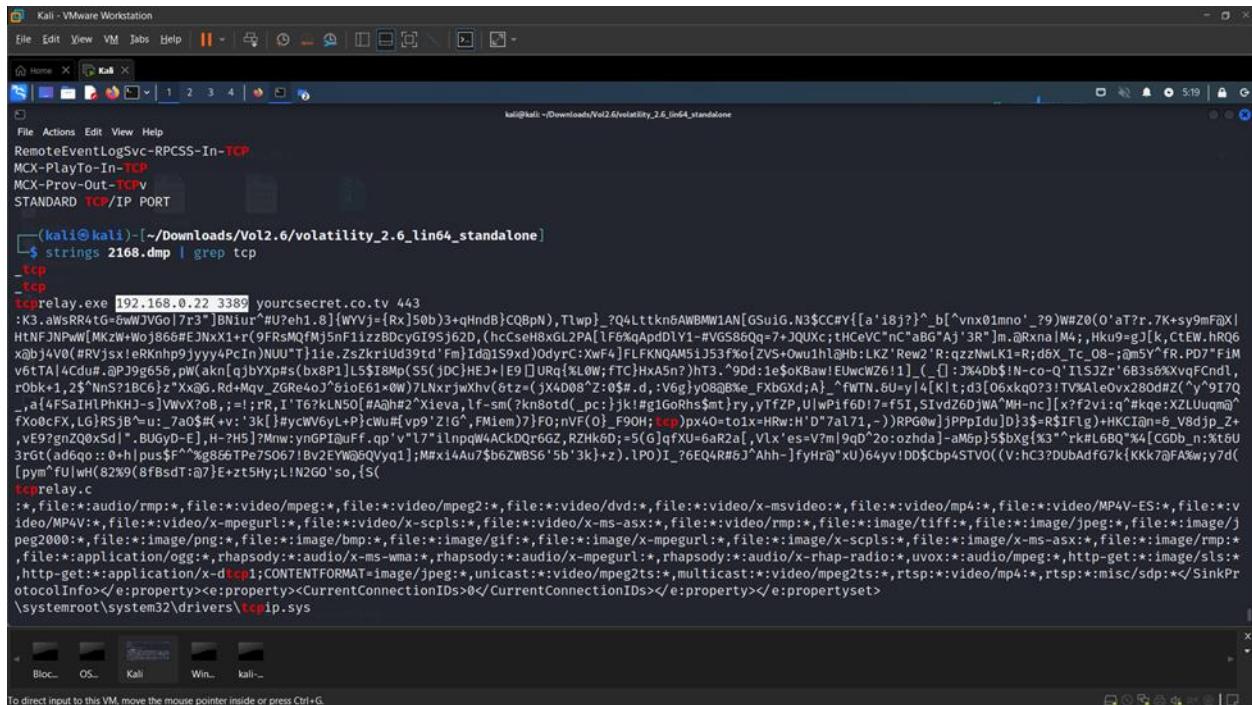
```

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

Trong khi kiểm tra, chúng em thấy các lệnh trong cmd có vẻ không có gì đặc biệt, nhưng ngoài ra thì cũng tìm thấy console process với PID 2168 trông có vẻ khá đáng nghi, có lẽ bên trong gọi lệnh gì đó. Vậy nên tụi em quyết định dump riêng process này để kiểm tra.

Dump xong, tụi em dùng strings để đọc được nội dung bên trong. Ban đầu em nghĩ ip:port thì chắc sẽ liên quan đến các protocol nên đã tìm thử với keyword TCP thì không thấy gì, nhưng tcp thì có một đoạn tcp replay.exe tới một ip:port như bên dưới. Đã vậy kể bên còn có chữ yoursecret => Em nghĩ đây là flag.

└─\$ strings 2168.dmp | grep tcp



Vậy nên em đã copy ip:port cho đúng định dạng: 192.168.0.22:3389 và nộp vào challenge => Hoàn thành.

Challenges/Forensic : Command > Command Reference - volatilityfound | gooogle dic - Tim trên Google

root-me.org/en/Challenges/Forensic/Command-Control-level-4?lang=en#validation\_challenge

Wikipedia - Vietnamese... Hé thống quản lý h... 16 games like Stard... Fe (sát) HO (xít clo... d Facebook Cửa hàng Chrome... vui Slack | chung | Lộp...

Root Me

402 visitors now

Newest members : l4louie, packdeber13, qualuwave, Goldfind, gabimaru, Boubig, bestien passet

Offers

APP Cybersecurity analyst  
CDI Cybersecurity consultant  
CDI Cybersecurity consultant  
CDI R&D engineer  
AUT R&D engineer

Chatbox

Atr3u5 30 March 2023 at 06:18  
hello guys. Do you have some suggestions of easy machines to root in CTF all day? I just solved the metasploitable 1 and 2.

fqa 20 March 2023 at 23:05  
привет, я новичок, не подскажите с чего начать?

Author: Thanatos, 16 February 2013

Level: Validated

Statement: Berthier, thanks to this new information about the processes running on the workstation, we can check that the 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

The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de

Start the challenge

1 related resource(s)

Volatility cheatsheet v2.4 (Forensic)

Validation

Well done, you won 35 Points!

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

tweet it!

## Challenge 5:

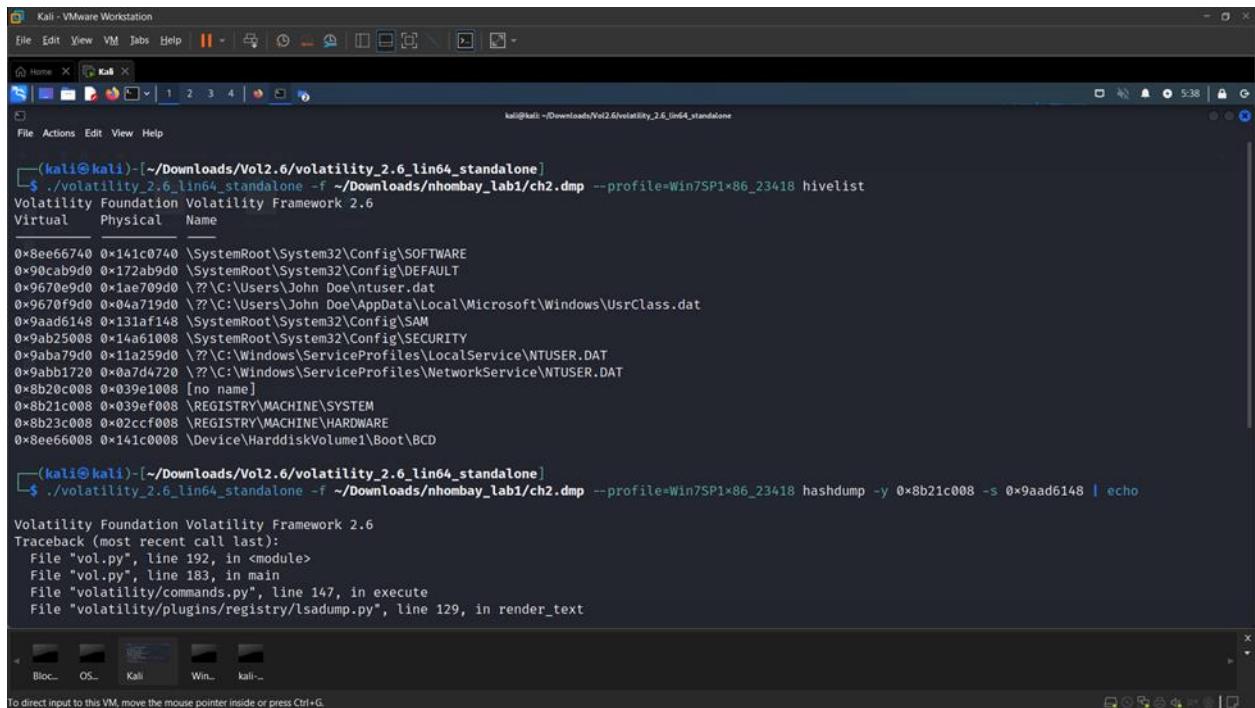
Tài liệu tham khảo.

<https://andreafortuna.org/2017/11/15/how-to-retrieve-users-passwords-from-a-windows-memory-dump-using-volatility/>

[http://systemmanager.ru/win2k\\_regestry.en/46661.htm](http://systemmanager.ru/win2k_regestry.en/46661.htm)

[http://systemmanager.ru/win2k\\_regestry.en/46658.htm](http://systemmanager.ru/win2k_regestry.en/46658.htm)

Đầu tiên, theo như hướng dẫn thì sẽ cần định vị địa chỉ ảo và đường dẫn đầy đủ trên ổ đĩa trước, chúng em sẽ dùng hivelist để thực hiện việc này.



```
(kali㉿kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23418 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual Physical Name
0x8ee66740 0x141c0740 \SystemRoot\System32\Config\SOFTWARE
0x90cab9d0 0x172ab9d0 \SystemRoot\System32\Config\DEFAULT
0x9670e9d0 0x1ae709d0 ??\C:\Users\John Doe\ntuser.dat
0x9670f9d0 0x04a719d0 ??\C:\Users\John Doe\AppData\Local\Microsoft\Windows\UsrClass.dat
0x9aa6d148 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

(kali㉿kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23418 hashdump -y 0x8b21c008 -s 0x9aad6148 | echo
Volatility Foundation Volatility Framework 2.6
Traceback (most recent call last):
  File "vol.py", line 192, in <module>
    File "vol.py", line 183, in main
    File "volatility/commands.py", line 147, in execute
      File "volatility/plugins/registry/lsadump.py", line 129, in render_text
```

Sau đó, có 2 đường dẫn và địa chỉ ảo cần chú ý là của SAM và SYSTEM trên hình. Theo như tài liệu thì đây là nơi lưu HKEY\_LOCAL\_MACHINE\SYSTEM key và HKEY\_LOCAL\_MACHINE\SAM key cần để trích xuất và giải mã thông tin xác thực miền đã lưu trong bộ nhớ cache được lưu trữ trong sổ đăng ký bằng hashdump.

```
Kali - VMware Workstation
File Edit View VM Tabs Help || Home Kali
File Actions Edi View Help
(kali㉿kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23418 hashdump -y 0x8b21c008 -s 0x9aad6148 | echo
Volatility Foundation Volatility Framework 2.6
Traceback (most recent call last):
  File "vol.py", line 192, in <module>
    File "vol.py", line 183, in main
    File "volatility/commands.py", line 147, in execute
      File "volatility/plugins/registry/lsadump.py", line 129, in render_text
IOError: [Errno 32] Broken pipe
Failed to execute script vol

(kali㉿kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23418 hashdump -y 0x8b21c008 -s 0x9aad6148 > ./test.txt
Volatility Foundation Volatility Framework 2.6

(kali㉿kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$ ls
2168.dmp AUTHORS.txt CREDITS.txt LEGAL.txt LICENSE.txt README.txt test.txt volatility_2.6_lin64_standalone

(kali㉿kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$ cat test.txt
Administrator:500:aad3b435b51404eeaa3d3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaa3d3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
John Doe:1000:aad3b435b51404eeaa3d3b435b51404ee:b9f917853e3dbf6e6831cce60725930:::

(kali㉿kali)-[~/Downloads/Vol2.6/volatility_2.6_lin64_standalone]
$
```

Sau đó, ta chạy hashdump với các địa chỉ ảo đã tìm được, thấy được file lưu password của các account trong hệ thống.

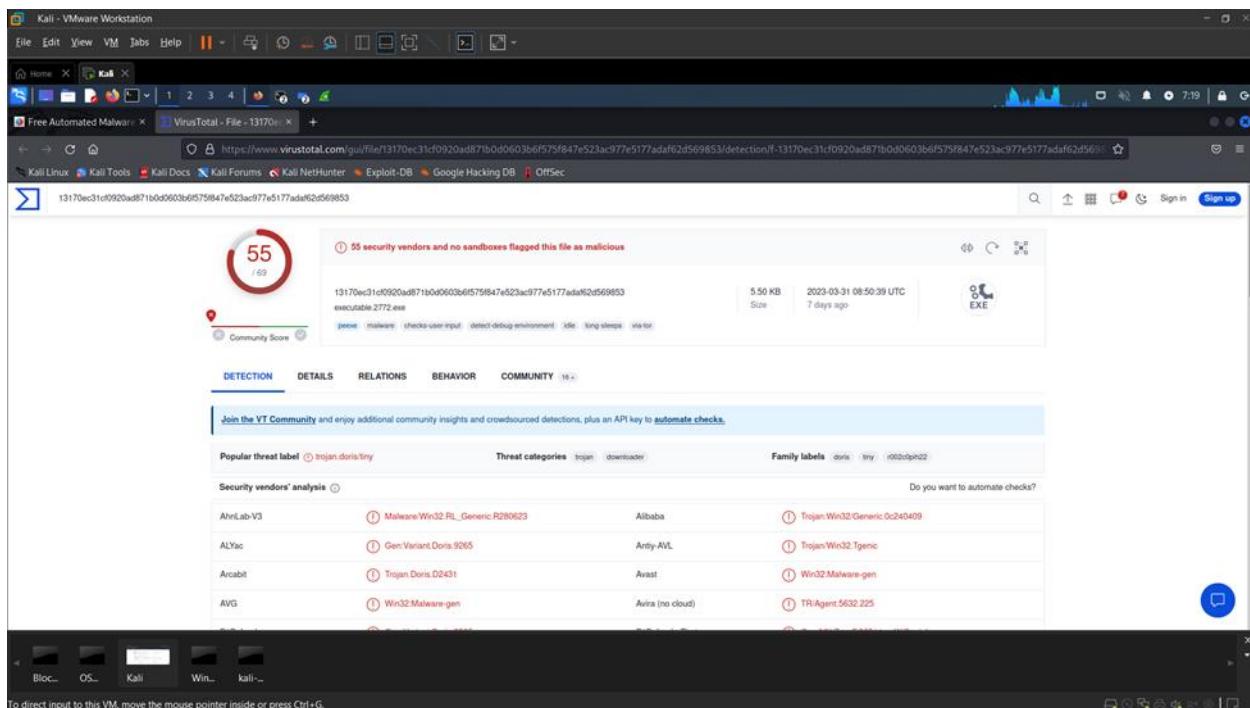
Cuối cùng, ta dùng tool crack hash để xem được password và nhập vào challenge flag: passw0rd.

## Challenge 6:

Trong challenge này, đề bài yêu cầu tìm được domain liên quan đến malware. Để làm được điều này, chúng em sẽ dump process 2772 ra trước và thử sử dụng tool malware analysis để phân tích.

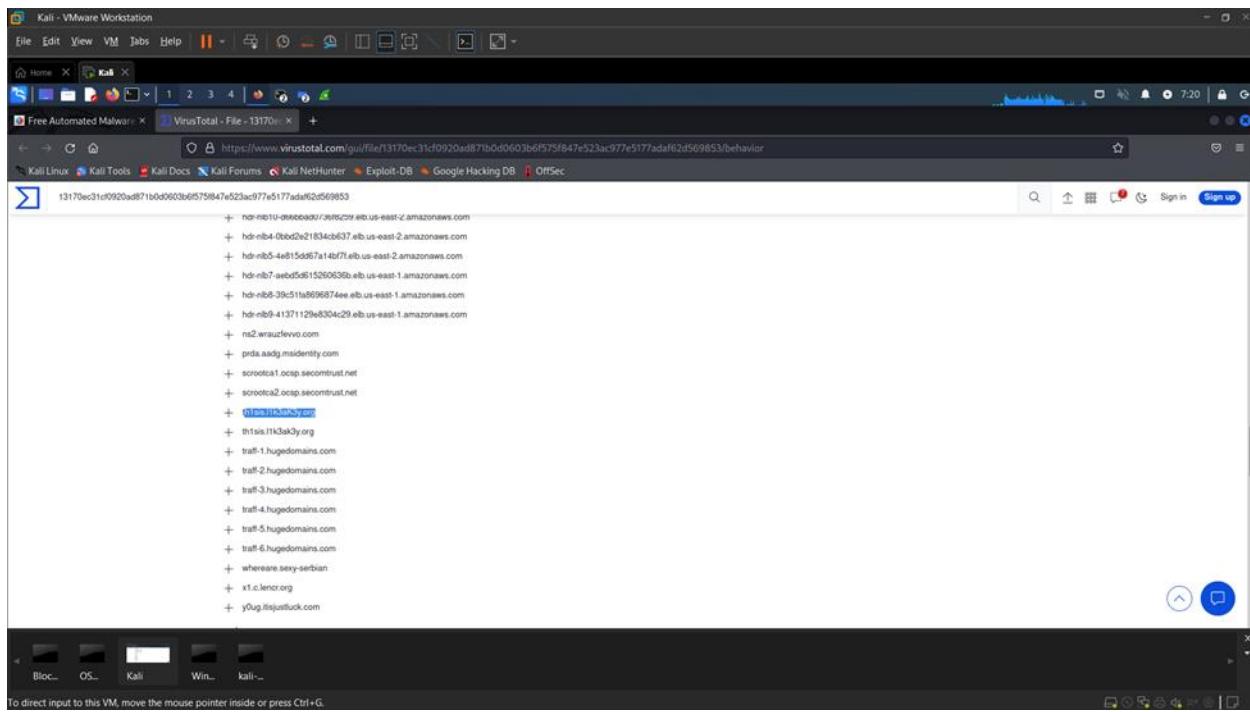
```
Kali - VMware Workstation
File Edit View VM Tabs Help || ×
Home Kali
File Actions Edit View Help
kali@kali:~/Downloads/Vol2.6/volatility_2.6_lin64_standalone
$ ./Volatility_2.6_lin64_standalone -f ~/Downloads/nhombay_lab1/ch2.dmp --profile=Win7SP1x86_23418 procdump -p 2772 -D ./dmp\ files
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase Name Result
0x87b6b030 0x00400000 iexplore.exe OK: executable.2772.exe
$
```

Dump xong, tụi em dùng Hybird Analysis và upload file đã dump ra để phân tích. Phần phân tích cho thấy file thực thi này đúng là mã độc.



Và khi kiểm tra thêm phần behavior ta có thể thấy được rất nhiều domain liên quan bị tấn công. Trong đó em thấy có 1 domain có vẻ đúng với format đề, vì vậy chúng em đoán đây là flag.

Paste flag vào trang rootme và hoàn thành bài challenge.



## 5. Kịch bản 05

Đầu tiên thực hiện xem thông tin file dump

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

```
kali@kali: ~/Downloads/nhombay_lab1
File Actions Edit View Help

└─(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ ./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, Win2008R
2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
           AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
           AS Layer2 : FileAddressSpace (/home/kali/Downloads/nhombay_la
b1/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 : 0xfffffff80002c44d00L
           KPCR for CPU 1 : 0xfffffff880009ef000L
           KUSER_SHARED_DATA : 0xfffffff780000000000L
           Image date and time : 2018-08-04 19:34:22 UTC+0000
           Image local date and time : 2018-08-04 22:34:22 +0300
```

Xem danh sách các hive

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

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ ./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
```

- Tìm tên và mật khẩu của tài khoản người dùng trong bộ nhớ
- Thực hiện việc ghi giá trị dump từ SAM và redirect output và file hashedPass5.txt
- ```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a0016d4010 > hashedPass5.txt
```

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a0016d4010 > hashedPass5.txt

Volatility Foundation Volatility Framework 2.6

(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ cat hashedPass5.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfed0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfed0d16ae931b73c59d7e0c089c0:::
Rick:1000:aad3b435b51404eeaad3b435b51404ee:518172d012f97d3a8fcc089615283940:::
```

- Tìm tên (ComputerName) và địa chỉ IP của máy tính mục tiêu.
- Thực hiện dịch ngược password bằng lsadump
- ```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win7SP1x64 lsadump
```

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win7SP1x64 lsadump
Volatility Foundation Volatility Framework 2.6
DefaultPassword
0x0000000000 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ( ..... 01010
0x000000010 4d 00 6f 00 72 00 74 00 79 00 49 00 73 00 52 00 M.o.r.t.y.I.s.R. 01101
0x000000020 65 00 61 00 6c 00 6c 00 79 00 41 00 6e 00 4f 00 e.a.l.l.y.A.n.O. 01110
0x000000030 74 00 74 00 65 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 vol-t.t.e.r..... 1852.dmp

DPAPI_SYSTEM
0x0000000000 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ,..... .
0x000000010 01 00 00 00 36 9b ba a9 55 e1 92 82 09 e0 63 4c ....6 ...U.....cL
0x000000020 20 74 63 14 9e d8 a0 4b 45 87 5a e4 bc f2 77 a5 .tc....KE.Z ...w.
0x000000030 25 3f 47 12 0b e5 4d a5 c8 35 cf dc 00 00 00 00 %%G ...M..5.....
```

Ta có được thông tin password là: **MortyIsReallyAnOtter**

Thực hiện băm bằng NTLM Password Hash thì ta thấy được đây là password của user Rick vì cùng giá trị băm đầu ra

The screenshot shows a web browser window with the title bar 'NTLM Password Hasher' and three dots at the top left. The main content area has a light blue background. At the top center is the title 'NTLM Password Hasher' in a large, dark blue serif font. Below it is the subtitle 'cross-browser testing tools' in a smaller, dark blue sans-serif font. In the center of the page is a block of text describing the tool's purpose: 'World's simplest online NTLM hash generator for web developers and programmers. Just paste your password in the form below, press the Calculate NTLM Hash button, and you'll get an NTLM hash. Press a button - get a hash. No ads, nonsense, or garbage.' Below this text is a blue rectangular button with a white 'Like' icon and the text 'Like 51K'. Further down is an announcement: 'Announcement: We just launched [Online Fractal Tools](#) - a collection of browser-based fractal generators. Check it out!' At the bottom of the page is a light blue box containing the generated NTLM hash: '518172D012F97D3A8FCC089615283940'. Below this box are two buttons: 'Calculate NTLM Hash' and 'Copy to clipboard (undo)'.

Tiếp theo ta sẽ thực hiện tìm tên computer bằng lệnh bên dưới bằng lệnh printkey với -o + địa chỉ ảo và -K là đường dẫn cụ thể, cố định của máy win7

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

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ ./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          ComputerName : (S) WIN-LO6FAF3DTFE
```

Thì ta thấy được tên computer là: WIN-LO6FAF3DTFE

Tiếp theo ta sẽ thực hiện scan network bằng netscan

./volatility\_2.6\_lin64\_standalone -f Kb05-dp-E81.vmem --profile=Win7SP1x64 netscan

Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner	Created
0x7d0f010	UDPv4	0.0.0.0:1900	*:*	2836	BitTorrent.exe	2018-08-04 19:27:17 UTC+0000	
0x7d2b3f0	UDPv4	192.168.202.131:6771	*:*	2836	BitTorrent.exe	2018-08-04 19:27:22 UTC+0000	
0x7d62f4c0	UDPv4	127.0.0.1:62307	*:*	2836	BitTorrent.exe	2018-08-04 19:27:17 UTC+0000	
0x7d62f920	UDPv4	192.168.202.131:62306	*:*	2836	BitTorrent.exe	2018-08-04 19:27:17 UTC+0000	
0x7d6424c0	UDPv4	0.0.0.0:50762	*:*	4076	chrome.exe	2018-08-04 19:33:37 UTC+0000	
0x7d6b4250	UDPv6	::1:1900	*:*	164	svchost.exe	2018-08-04 19:28:42 UTC+0000	
0x7d6e3230	UDPv4	127.0.0.1:6771	*:*	2836	BitTorrent.exe	2018-08-04 19:27:22 UTC+0000	
0x7d6ed650	UDPv4	0.0.0.0:5355	*:*	620	svchost.exe	2018-08-04 19:34:22 UTC+0000	
0x7d71c8a0	UDPv4	0.0.0.0:0	*:*	868	svchost.exe	2018-08-04 19:34:22 UTC+0000	
0x7d71c8a0	UDPv6	::0:0	*:*	868	svchost.exe	2018-08-04 19:34:22 UTC+0000	
0x7d74a390	UDPv4	127.0.0.1:52847	*:*	2624	bittorrent.e	2018-08-04 19:27:24 UTC+0000	
0x7d7602c0	UDPv4	127.0.0.1:52846	*:*	2308	bittorrent.e	2018-08-04 19:27:24 UTC+0000	
0x7d787010	UDPv4	0.0.0.0:165452	*:*	4076	chrome.exe	2018-08-04 19:33:42 UTC+0000	
0x7d789b50	UDPv4	0.0.0.0:50523	*:*	620	svchost.exe	2018-08-04 19:34:22 UTC+0000	
0x7d789b50	UDPv6	::50523	*:*	620	svchost.exe	2018-08-04 19:34:22 UTC+0000	
0x7d92a230	UDPv4	0.0.0.0:0	*:*	868	svchost.exe	2018-08-04 19:34:22 UTC+0000	
0x7d92a230	UDPv6	::0:0	*:*	868	svchost.exe	2018-08-04 19:34:22 UTC+0000	
0x7d9e8b50	UDPv4	0.0.0.0:20830	*:*	2836	BitTorrent.exe	2018-08-04 19:27:15 UTC+0000	
0x7df4f560	UDPv4	0.0.0.0:0	*:*	3856	WebCompanion.e	2018-08-04 19:34:22 UTC+0000	
0x7df8cb0	UDPv4	0.0.0.0:20830	*:*	2836	BitTorrent.exe	2018-08-04 19:27:15 UTC+0000	
0x7df8cb0	UDPv6	::20830	*:*	2836	BitTorrent.exe	2018-08-04 19:27:15 UTC+0000	
0x7dbbb390	TCPv4	0.0.0.0:9008	0.0.0.0:0	LISTENING	4	System	
0x7dbbb390	TCPv6	::9008	::0	LISTENING	4	System	
0x7d9a9240	TCPv4	0.0.0.0:8733	0.0.0.0:0	LISTENING	4	System	
0x7d9a9240	TCPv6	::8733	::0	LISTENING	4	System	
0x7d9e19e0	TCPv4	0.0.0.0:20830	0.0.0.0:0	LISTENING	2836	BitTorrent.exe	
0x7d9e19e0	TCPv6	::20830	::0	LISTENING	2836	BitTorrent.exe	
0x7d9e1c90	TCPv4	0.0.0.0:20830	0.0.0.0:0	LISTENING	2836	BitTorrent.exe	
0x7d42ba90	TCPv4	-:0	56.219.196.26:0	CLOSED	2836	BitTorrent.exe	
0x7d6124d0	TCPv4	192.168.202.131:49530	77.102.199.102:7575	CLOSED	708	LunarMS.exe	
0x7d62d690	TCPv4	192.168.202.131:49229	169.1.143.215:8999	CLOSED	2836	BitTorrent.exe	
0x7d634350	TCPv6	-:0	38db:c41a:80fa:ffff:138db:c41a:80fa::CLOSED	2836	BitTorrent.exe		
0x7d6f27f0	TCPv4	192.168.202.131:50381	71.198.155.180:34674	CLOSED	2836	BitTorrent.exe	
0x7d704010	TCPv4	192.168.202.131:50382	92.251.23.204:6881	CLOSED	2836	BitTorrent.exe	
0x7d708cf0	TCPv4	192.168.202.131:50364	91.140.89.116:31847	CLOSED	2836	BitTorrent.exe	
0x7d729620	TCPv4	-:50034	142.129.37.27:24578	CLOSED	2836	BitTorrent.exe	
0x7d72cbe0	TCPv4	192.168.202.131:50340	23.37.43.27:80	CLOSED	3496	Lawasoft.WCAss	
0x7d7365a0	TCPv4	192.168.202.131:50358	23.37.43.27:80	CLOSED	3856	WebCompanion.e	
0x7d81c890	TCPv4	192.168.202.131:50335	185.154.111.29:60405	CLOSED	2836	BitTorrent.exe	
0x7d8fd530	TCPv4	192.168.202.131:50327	23.37.43.27:80	CLOSED	3496	Lawasoft.WCAss	
0x7d9ccf0	TCPv4	192.168.202.131:50273	172.239.232.46:2997	CLOSED	2826	BitTorrent.exe	
0x7d99dcf0	TCPv4	192.168.202.131:50371	191.253.122.149:59163	CLOSED	2836	BitTorrent.exe	
0x7daefc0	UDPv4	0.0.0.0:0	*:*	3856	WebCompanion.e	2018-08-04 19:34:22 UTC+0000	
0x7daefc0	UDPv6	::0:0	*:*	3856	WebCompanion.e	2018-08-04 19:34:22 UTC+0000	

Ip address local: 192.168.202.131

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

Từ netscan, ta biết được các thông tin sau:

Trò chơi của user: LunarMS

Ip address của trò chơi: 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

Tên channel: Lunar-3

Thực hiện dump thông tin từ mem với pid 708

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



```
(kali㉿kali)-[~/Downloads/nhombay_lab1]  
$ ./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
```

Thực hiện lệnh string để xem thông tin

```
strings 708.dmp | grep "Lunar-3" -A 10 -B 10
```

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
└─$ strings 708.dmp | grep "Lunar-3" -A 10 -B 10
{qv1
b+Y,
,b+Y
b+YD Computer
Db+Y
c+Y\ kali
\b+Y Desktop
c+Yt
tb+Y4c+Y h
b+YLc+Y
Lunar-3
Lunar-4
L(dNVxdNV
L|eNV Pictures
{qf8
$m1Y Videos
4v+Y Downloads
TI,Y
lx+Yces
ty+Y
,y+Y\y+Y System
-- Network
magician
bowman
thief
pirate
Sound/
normal
pressed
disabled
mouseOver
keyFocused
Lunar-3
0tt3r8r33z3
Sound/UI.img/
BtMouseClick
Lunar-4
Lunar-1
Lunar-2
ScrollUp
Title
RollDown
WorldSelect
3 folders, 19 files; 10.1 GiB (10,894,076,722 bytes); Free space: 37.9 GiB
```

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.

Thực hiện xem lệnh clipboard để xem các thông tin bên trong

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

Handle	Object	Offset	Data
0x602e3	CF_UNICODETEXT	0xfffff900c1ad93f0	M@il_Provid0rs
0x10	CF_TEXT	0x10	
0x200000000000	0x150133L	0x200000000000	
0x1	CF_TEXT	0x150133	0xfffff900c1c1adc0

Ta có được mật khẩu là **M@il\_Provid0rs**

- 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
```

Name	Computer	Pid	PPid	Thds	Hnds	Time
0xfffffa801b27e060:explorer.exe		2728	2696	33	854	2018-08-04 19:27:04 UTC+0000
. 0xfffffa801b486b30:Rick And Morty		3820	2728	4	185	2018-08-04 19:32:55 UTC+0000
.. 0xfffffa801a4c5b30:vmware-tray.ex		3720	3820	8	147	2018-08-04 19:33:02 UTC+0000
.. 0xfffffa801b2f02e0:WebCompanion.e		2844	2728	0	—	2018-08-04 19:27:07 UTC+0000
.. 0xfffffa801a4e3870:chrome.exe		4076	2728	44	1160	2018-08-04 19:29:30 UTC+0000
.. 0xfffffa801a4eab30:chrome.exe		4084	4076	8	86	2018-08-04 19:29:30 UTC+0000
.. 0xfffffa801a5ef1f0:chrome.exe		1796	4076	15	170	2018-08-04 19:33:41 UTC+0000
.. 0xfffffa801aa0a090:chrome.exe		3924	4076	16	228	2018-08-04 19:29:51 UTC+0000
.. 0xfffffa801a635240:chrome.exe		3648	4076	16	207	2018-08-04 19:33:38 UTC+0000
.. 0xfffffa801a502b30:chrome.exe		576	4076	2	58	2018-08-04 19:29:31 UTC+0000
.. 0xfffffa801a4f7b30:chrome.exe		1808	4076	13	229	2018-08-04 19:29:32 UTC+0000
.. 0xfffffa801a7f98f0:chrome.exe		2748	4076	15	181	2018-08-04 19:31:15 UTC+0000
.. 0xfffffa801b5cb740:LunarMS.exe		708	2728	18	346	2018-08-04 19:27:39 UTC+0000
.. 0xfffffa801b1cdb30:vmtoolsd.exe		2804	2728	6	190	2018-08-04 19:27:06 UTC+0000
.. 0xfffffa801b290b30:BitTorrent.exe		2836	2728	24	471	2018-08-04 19:27:07 UTC+0000
.. 0xfffffa801b4c9b30:bittorrenttie.e		2624	2836	13	316	2018-08-04 19:27:21 UTC+0000
.. 0xfffffa801b4a7b30:bittorrenttie.e		2308	2836	15	337	2018-08-04 19:27:19 UTC+0000
0xfffffa8018d44740:System		4	0	95	411	2018-08-04 19:26:03 UTC+0000
. 0xfffffa801947e4d0:smss.exe		260	4	2	30	2018-08-04 19:26:03 UTC+0000
0xfffffa801a2ed060:wininit.exe		396	336	3	78	2018-08-04 19:26:11 UTC+0000
. 0xfffffa801ab377c0:services.exe		492	396	11	242	2018-08-04 19:26:12 UTC+0000
.. 0xfffffa801afe7800:svchost.exe		1948	492	6	96	2018-08-04 19:26:42 UTC+0000
.. 0xfffffa801ae92920:vmtoolsd.exe		1428	492	9	313	2018-08-04 19:26:27 UTC+0000
.. 0xfffffa801a572b30:cmd.exe		3916	1428	0	—	2018-08-04 19:34:22 UTC+0000
.. 0xfffffa801ae0f630:VGAuthService.		1356	492	3	85	2018-08-04 19:26:25 UTC+0000
.. 0xfffffa801abbdb30:vmacthlp.exe		668	492	3	56	2018-08-04 19:26:16 UTC+0000
.. 0xfffffa801aad1060:Lavasoft.WCAss		3496	492	14	473	2018-08-04 19:33:49 UTC+0000
.. 0xfffffa801a6af9f0:svchost.exe		164	492	12	147	2018-08-04 19:28:42 UTC+0000
.. 0xfffffa801ac2e9e0:svchost.exe		808	492	22	508	2018-08-04 19:26:18 UTC+0000
.. 0xfffffa801ac753a0:audiodg.exe		960	808	7	151	2018-08-04 19:26:19 UTC+0000
.. 0xfffffa801ae7f630:dllhost.exe		1324	492	15	207	2018-08-04 19:26:42 UTC+0000
.. 0xfffffa801a6c2700:mscorsvw.exe		3124	492	7	77	2018-08-04 19:28:43 UTC+0000
.. 0xfffffa801b232060:sppsvc.exe		2500	492	4	149	2018-08-04 19:26:58 UTC+0000
.. 0xfffffa801abeb30:svchost.exe		712	492	8	301	2018-08-04 19:26:17 UTC+0000
.. 0xfffffa801ad718a0:svchost.exe		1164	492	18	312	2018-08-04 19:26:23 UTC+0000
.. 0xfffffa801ac31b30:svchost.exe		844	492	17	396	2018-08-04 19:26:18 UTC+0000
.. 0xfffffa801b1fab30:dwm.exe		2704	844	4	97	2018-08-04 19:27:04 UTC+0000
.. 0xfffffa801988c2d0:PresentationFo		724	492	6	148	2018-08-04 19:27:52 UTC+0000
.. 0xfffffa801b603610:mscorsvw.exe		412	492	7	86	2018-08-04 19:28:42 UTC+0000
.. 0xfffffa8018e3c890:svchost.exe		604	492	11	376	2018-08-04 19:26:16 UTC+0000
.. 0xfffffa8019124b30:WmiPrvSE.exe		1800	604	9	222	2018-08-04 19:26:39 UTC+0000

Ta thấy tiến trình cha là Rick And Morty

Tiến trình con là vmware-tray.exe

Thực hiện cmdline để xem tiến trình chạy trên path ở pid 3820 và 3720

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

*****						
<pre>(kali㉿kali)-[~/Downloads/nhombay_lab1] \$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 cmdline -p 3820</pre>						
Volatility Foundation Volatility Framework 2.6 *****						

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

```
(kali㉿kali)-[~/Downloads/nhombay_lab1] $ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 cmdline -p 3720
Volatility Foundation Volatility Framework 2.6
*****
vmware-tray.exe pid: 3720
Command line : "C:\Users\Rick\AppData\Local\Temp\RarSFX0\vmware-tray.exe"
```

Ta có thể thấy được: **vmware-tray.exe** là tiến trình của mã độc

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

Nguyên nhân: người dùng sử dụng torrent, một giao thức peer to peer nên ta sẽ liệt kê các file liên quan đến đuôi torrent

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

```
(kali㉿kali)-[~/Downloads/nhombay_lab1] $ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 filescan | egrep "\*.torrent"
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
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
0x000000007dcfb6f0    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
```

Thực hiện dump 1 số file mẫu, ở đây là file có addr 0x000000007d8813c0

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

```
(kali㉿kali)-[~/Downloads/nhombay_lab1] $ ./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
```

Xem thông tin thì không có gì

```
(kali㉿kali)-[~/Downloads/nhombay_lab1] $ cat file.None.0xfffffa801af10010.dat
[ZoneTransfer]
ZoneId=3
```

Tiếp tục dump với addr 0x000000007dae9350

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

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ ./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 s
eason 1 download.exe.1.torrent
```

Xem thông tin như hình bên dưới

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ cat file.None.0xfffffa801b42c9e0.dat
d8:announce44:udp://tracker.openbittorrent.com:80/announce13:announce-list144:udp://tracker.openbittorrent.com:80/annouc
e142:udp://tracker.opentrackr.org:1337/announce10:created by17:BitTorrent/7.10.313:creation date1533150595
e8:encoding5:UTF-84:infod6:lengthi456670e4:name36:Rick And Morty season 1 download.exe12:piece lengthi16384e6:pieces
♦♦♦8♦♦♦!PC<^X•B.k_Rk♦!F♦J♦♦&LL♦Lw♦♦F♦'♦♦♦E,q♦c0<;0870♦♦♦3♦G♦~1♦♦♦P♦|♦!4^"♦♦IE♦♦q♦q♦n♦
duM♦$hs♦♦♦♦♦QZ♦♦oZ♦5>♦♦♦♦l♦H♦^♦N!♦h♦F♦♦♦♦3hq,]♦♦♦D♦d♦[y♦}Z♦♦)~♦-1♦♦♦3l♦0♦
♦;♦♦:♦MZ♦♦
♦.♦R♦9♦&iW1|♦H♦sg
♦ù♦c♦♦♦Ob
}♦♦♦w♦q♦j♦xt♦y^♦♦♦,h♦iO♦E♦♦♦Rz♦,♦b♦R♦"F♦`♦♦LQ♦kY♦By♦y♦\i#Ss♦♦X♦!b♦♦♦
♦K68:o♦♦♦qJx♦♦5s♦#♦}♦w~Q~YT♦5v♦x♦/XN♦♦♦♦♦♦♦",@EV♦♦♦♦2♦♦0g♦E♦/}♦B♦$♦V♦V♦$♦♦M2♦♦>L♦♦FR♦r♦F♦)$♦o9p♦♦♦.A♦E♦5♦
c♦\ER♦K♦P♦>0♦H♦f♦♦♦QI3♦BVM♦C♦.>r♦^♦u♦
♦♦Q]z♦bwF:u♦♦H♦@3e7:website19:M3an_T0rren7_4_R!cke
```

Ta thấy được thông tin như flag: **M3an\_T0rren7\_4\_R!cke**

Tiếp tục dump với addr 0x000000007dcfb6f0

```
./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64
dumpfiles -Q 0x000000007dcfb6f0 -D .
```

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 dumpfiles -Q 0x000000007dcfb6f0 -D .
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7dcfb6f0 None \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\BitTorrent\Rick And Morty s
eason 1 download.exe.1.torrent
```

Xem thông tin thì không có gì

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ cat file.None.0xfffffa801b51ccf0.dat
[ZoneTransfer]
ZoneId=3
```

- 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 đến từ **Google Chrome** thông qua tải file

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

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 pstree
Volatility Foundation Volatility Framework 2.6
Name          Pid  PPid  Thds  Hnds Time
0xfffffa801b27e060:explorer.exe      2728  2696   33   854 2018-08-04 19:27:04 UTC+0000
. 0xfffffa801b486b30:Rick And Morty  3820  2728    4   185 2018-08-04 19:32:55 UTC+0000
.. 0xfffffa801a4c5b30:vmware-tray.ex 3720  3820   8   147 2018-08-04 19:33:02 UTC+0000
. 0xfffffa801b2f02e0:WebCompanion.e  2844  2728    0   1160 2018-08-04 19:27:07 UTC+0000
. 0xfffffa801a4e3870:chrome.exe     4076  2728   44   1160 2018-08-04 19:29:30 UTC+0000
.. 0xfffffa801a4eab30:chrome.exe   4084  4076   8    86 2018-08-04 19:29:30 UTC+0000
.. 0xfffffa801a5ef1f0:chrome.exe   1796  4076   15   170 2018-08-04 19:33:41 UTC+0000
.. 0xfffffa801aa00a90:chrome.exe   3924  4076   16   228 2018-08-04 19:29:51 UTC+0000
.. 0xfffffa801a635240:chrome.exe   3648  4076   16   207 2018-08-04 19:33:38 UTC+0000
.. 0xfffffa801a502b30:chrome.exe   576   4076   2    58 2018-08-04 19:29:31 UTC+0000
.. 0xfffffa801a4f7b30:chrome.exe   1808  4076   13   229 2018-08-04 19:29:32 UTC+0000
.. 0xfffffa801a7f98f0:chrome.exe   2748  4076   15   181 2018-08-04 19:31:15 UTC+0000
. 0xfffffa801b5cb740:LunarMS.exe   708   2728   18   346 2018-08-04 19:27:39 UTC+0000
```

Tiếp theo ta sẽ scan các file lọc 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/nhombay_lab1]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 filescan | grep -i "history"
Volatility Foundation Volatility Framework 2.6
0x0000000007d45dcc0 18   1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Google\Chrome\User Data\Default\History
0x0000000007d62bdd0 17   1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist012018080420180805\index.dat
0x0000000007d6b580 18   1 R----- \Device\HarddiskVolume1\ProgramData\Microsoft\Windows Defender\Scans\History\CacheManager\MpsFc.bin
0x0000000007d6ea820 17   1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\Low\History.IE5\index.dat
0x0000000007d74eb30 1    1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\Low\History.IE5\index.dat
0x0000000007d7afdd0 1    1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\Low\History.IE5\index.dat
0x0000000007d79b5940 17   1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x0000000007dac7410 33   1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Google\Chrome\User Data\Default\History-journal
0x0000000007e1792c0 1    1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012018080420180805\index.dat
0x0000000007e43bd10 16   0 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012018080420180805\index.dat
0x0000000007e46f20 1    1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x0000000007e0e520 1    1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x0000000007e753810 1    0 R-rwd \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\desktop.ini
```

Ta sẽ thực hiện dump file ở addr 0x0000000007d45dcc0

`./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 dumpfiles -Q 0x0000000007d45dcc0 -D .`

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 dumpfiles -Q 0x0000000007d45dcc0 -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

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ file file.None.0xfffffa801a5193d0.dat
file.None.0xfffffa801a5193d0.dat: SQLite 3.x database, last written using SQLite version 3023001, file counter 24, database pages 47, cookie 0x17, schema 4, UTF-8, version-valid-for 24
```

Ta sẽ chuyển thông tin qua dạng sqlite để xem

`mv file.None.0xfffffa801a5193d0.dat chrome-history.sqlite`

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ mv file.None.0xfffffa801a5193d0.dat chrome-history.sqlite
```

Sử dụng sqlite3 để xem thông tin với .schema downloads

Xem trong current\_path và site\_url trong table downloads, ở đây ta thấy thông tin liên quan đến torrent, và nguồn tải đến từ **https://mail.com**

```
sqlite> select current_path , site_url from downloads;
C:\Users\Rick\Downloads\BitTorrent.exe|https://bittorrent.com/
C:\Users\Rick\Downloads\MSSetupv83.exe|https://mega.nz/
C:\Users\Rick\Downloads\Lunar Client & WZ.zip|https://mega.nz/
C:\Users\Rick\Downloads\Rick And Morty season 1 download.torrent|https://mail.com/
C:\Users\Rick\Downloads\Rick And Morty season 1 download.torrent|https://mail.com/
C:\Users\Rick\Downloads\Rick And Morty season 1 download.exe.torrent|https://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 lệnh strings để xem file có thêm thông tin  
strings Kb05-dp-E81.vmem | grep "@mail.com"

Ta thấy được thông tin địa chỉ email là: [rickopicko@mail.com](mailto:rickopicko@mail.com) và [RickoPicko@mail.com](mailto:RickoPicko@mail.com) kiểm tra lần lượt thì ta thấy [rickopicko@mail.com](mailto:rickopicko@mail.com) mới đem lại nhiều thông tin

Thực hiện string và lọc giá trị mail [rickopicko@mail.com](mailto:rickopicko@mail.com) để xem thông tin  
strings Kb05-dp-E81.vmem | grep -A 20 "<rickopicko@mail.com>"

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
└─$ strings Kb05-dp-E81.vmem | grep -A 20 "<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
```

Thì 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/nhombay_lab1]
└─$ ./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
```

Thấy có 2 địa chỉ báo về là READ\_IT.txt và Flag.txt ta sẽ thực hiện dump

./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 0x0000000007e410890 -D .
```

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
└─$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 dumpfiles -Q 0x0000000007d660500
-D .
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7d660500 None \Device\HarddiskVolume1\Users\Rick\Desktop\READ_IT.txt
file.None.0x7d660500.dat file.None.0x7d660500.dat file.None.0x7d660500.dat
(kali㉿kali)-[~/Downloads/nhombay_lab1]
└─$ ./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 dumpfiles -Q 0x0000000007e410890
-D .
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7e410890 None \Device\HarddiskVolume1\Users\Rick\Desktop\Flag.txt
```

Xem thông tin READ\_IT.txt

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
└─$ cat file.None.0xfffffa801b2def10.dat
Your files have been encrypted.
Read the Program for more information
read program for more information.
```

Xem thông tin Flag.txt

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
└─$ cat file.None.0xfffffa801b0532e0.dat
{♦$V♦\♦♦C(♦♦Ñ♦l1♦♦♦♦T♦r♦♦~♦{gШ♦♦♦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 .
```

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
└─$ ./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
```

Thực hiện dịch ngược file dump ta có được địa chỉ ví:

**1MmpEmebJkqXG8nQv4cjJSmxZQFVmFo63M**

```
ldfld   class [System.Windows.Forms]System.Windows.Forms.TextBox hidden_tear.Form3::textBox1
ldstr   a1mmpemebjkqxg8 // "1MmpEmebJkqXG8nQv4cjJSmxZQFVmFo63M"
callvirt instance void [System.Windows.Forms]System.Windows.Forms.Control::set_Text(string)
```

- 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/nhombay_lab1]
$ ./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/nhombay_lab1]
$ strings -e l 3720.dmp | grep -i "WIN-LO6FAF3DTFE" | sort | uniq
80000171WIN-LO6FAF3DTFE
-AdministratorWIN-LO6FAF3DTFE
\BaseNamedObjects\Global\WIN-LO6FAF3DTFE
computername=WIN-LO6FAF3DTFE
COMPUTERNAME=WIN-LO6FAF3DTFE
C:\Program Files\VMware\VMware Tools\vmtoolsd.exe (WIN-LO6FAF3DTFE)
\Device\NetbiosSmbWIN-LO6FAF3DTFEWORKGROUP
\Device\NetBT_Tcpip_{7F5B9219-B869-4AEA-84AF-CC6E4C2486FA}WIN-LO6FAF3DTFEWORKGROUP
-GuestWIN-LO6FAF3DTFE
Logoff PolicyWIN-LO6FAF3DTFE
logonserver=\WIN-LO6FAF3DTFE
LOGONSERVER=\WIN-LO6FAF3DTFE
NoneWIN-LO6FAF3DTFE
Password PolicyWIN-LO6FAF3DTFE
-RickWIN-LO6FAF3DTFE
RickWIN-LO6FAF3DTFE
User32 NegotiateWIN-LO6FAF3DTFE
userdomain=WIN-LO6FAF3DTFE
USERDOMAIN=WIN-LO6FAF3DTFE
USERNAME=WIN-LO6FAF3DTFE$
\\WIN-LO6FAF3DTFE
WIN-LO6FAF3DTFE
WIN-LO6FAF3DTFE$
WIN-LO6FAF3DTFE$WORKGROUP
WIN-LO6FAF3DTFE
WIN-LO6FAF3DTFE\Rick
WIN-LO6FAF3DTFE-Rick aDOBofVYUNVNmp7
WORKGROUP\WIN-LO6FAF3DTFE$
```

Ta có được mật khẩu trên ransomware là **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

```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ 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 .....
```

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

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

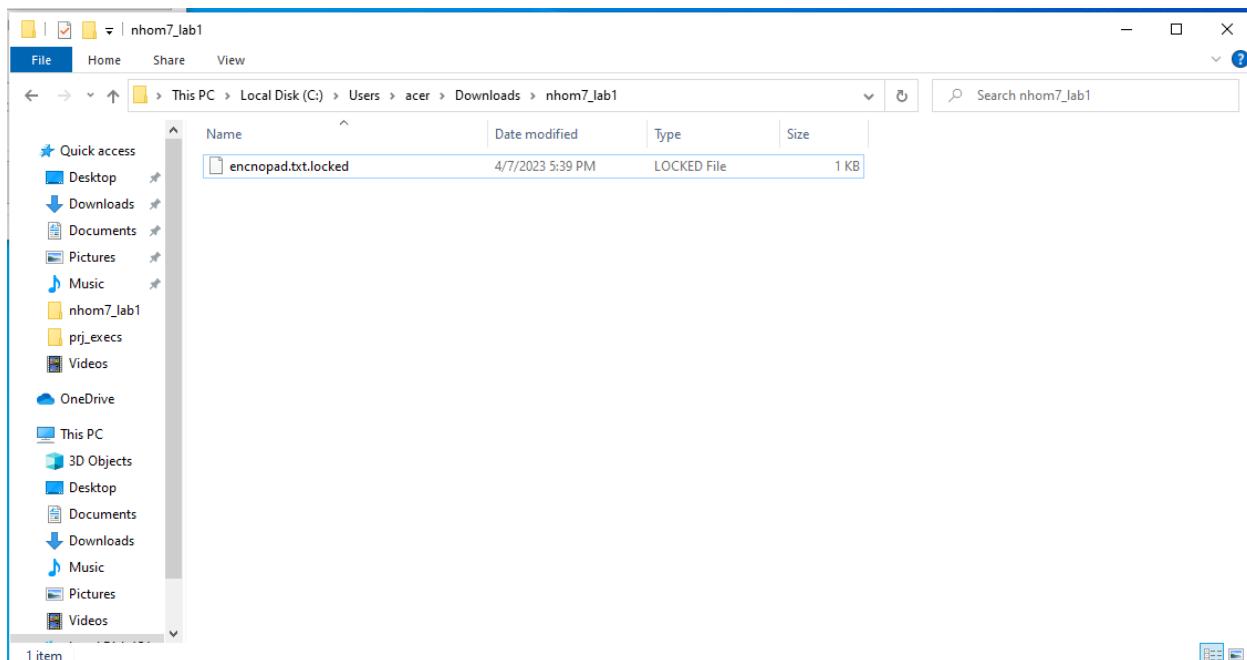
if=file.None.0xfffffa801b0532e0.dat là input file là file dump Flag.txt

of=encnopad.txt là output file encodepad.txt

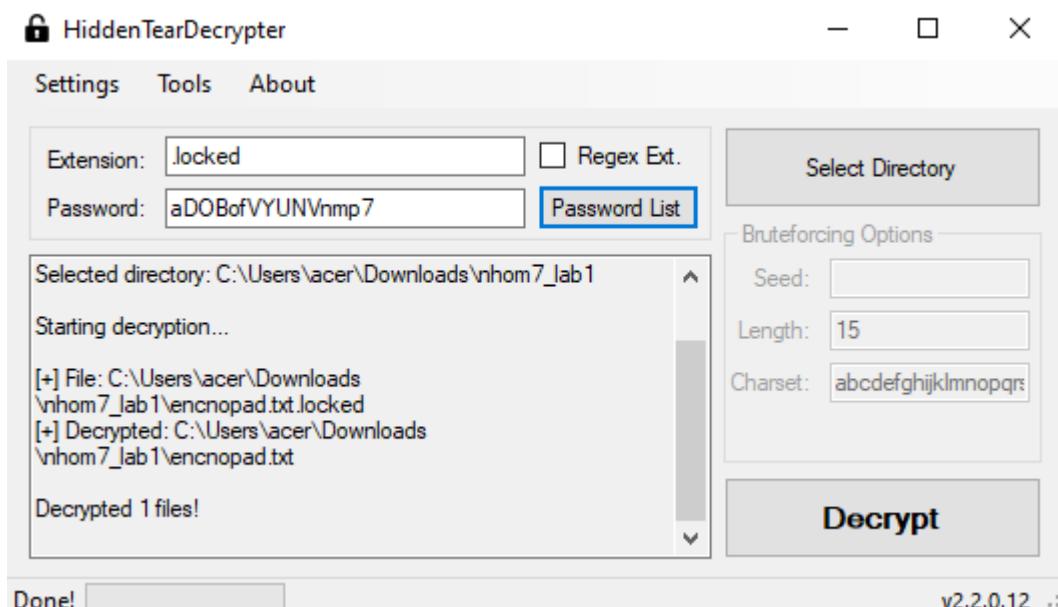
```
(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ dd bs=1 count=48 if=file.None.0xfffffa801b0532e0.dat of=encnopad.txt
48+0 records in
48+0 records out
48 bytes copied, 0.000311394 s, 154 kB/s

(kali㉿kali)-[~/Downloads/nhombay_lab1]
$ cat encnopad.txt
{♦$V♦\♦♦C(♦♦Ñ♦l1♦♦♦♦T♦r♦♦♦~♦{gW♦♦♦n>♦G♦
♦♦
```

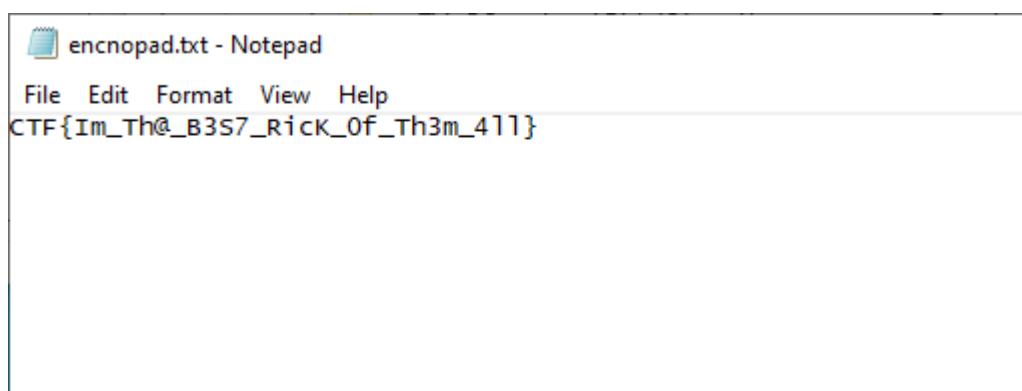
Sau đó ta sẽ copy file này sang máy window và add thêm .locked để thực hiện tool để dịch ngược lại



Ta sử dụng tool HiddenTearDecrypter để dịch ngược với password của ransomware và đường dẫn đến folder nhom7\_lab1



Sau khi decode xong ta thực hiện mở file lên để xem và ta có được flag



CTF{Im\_Th@\_B3S7\_RicK\_0f\_Th3m\_4ll}

---

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

## YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo 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]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

*Ví dụ: [NT101.H11.1]-Session1\_Group3.*

- 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 Lab.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại [courses.uit.edu.vn](http://courses.uit.edu.vn).

**Đánh giá:** Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

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

**HẾT**