



LAB 04

ĐIỀU TRA LỊCH SỬ TRUY CẬP WEB, BỘ NHỚ VÀ MẠNG

(Web browser, memory and network forensics)

Họ tên và MSSV: Trương Quang Long B2203727

Nhóm học phần: 01

- Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho tất cả bài thực hành của môn này.
- Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết. Hình minh họa chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.

1. Điều tra web history

- 1.1. Tải tập tin các tập tin [Lab02_04.7z.001](#), Lab02_04.7z.002, Lab02_04.7z.003 (đã có ở Lab 02), giải nén được tập tin cfreds_2015_data_leakage_pc.dd. Sử dụng công cụ FTK Imager, chọn chức năng File/Add Evidence Item; sau đó chọn nguồn dữ liệu là từ Image File. Thêm file dữ liệu cfreds_2015_data_leakage_pc.dd vào Evidence Tree.
- 1.2. Đi tới thư mục "Users\Informant\AppData\Local\Google\Chrome\User Data\Default". Ở giao diện File List, chọn các tập tin History. Click chuột phải chọn chức năng Export Files để trích xuất các tập tin trên.
- 1.3. Tải và cài đặt [DB Browser for SQLite](#)
- 1.4. Sử dụng SQLiteBrowser mở file History, tìm kiếm thông tin và trả lời các câu hỏi sau:

Chụp hình minh họa các kết quả thực hiện trên.

- 1.4.1. Thời gian người dùng truy cập URL
`http://forensicswiki.org/wiki/Anti-forensic_techniques`
- Người dùng truy cập trang web vào thứ 2, ngày 23/3/2015 vào lúc 2 giờ 17 phút chiều giờ GMT -4.

<code>https://www.google.com/url?...</code>		1	0	13071608239020034
<code>http://forensicswiki.org/wiki/Anti-...</code>	Anti-forensic techniques - ForensicsWiki	1	0	13071608239898079
<code>https://www.google.com/url?...</code>		1	0	13071608277947290

13071608239898079

Convert WebKit timestamp to human date

GMT : Monday, March 23, 2015 6:17:19 PM

Your time zone : Monday, March 23, 2015 2:17:19 PM GMT-04:00

Epoch/Unix time : 1427134639 (in seconds)

1.4.2. Thời gian icloudsetup.exe được download.

- Người dùng download tập tin icloud.setup vào ngày 23/3/2015 lúc 3 giờ 55 phút chiều GMT -4

Filter	Filter
C:\Users\informant\Downloads\icloudsetup.exe	13071614147290982
C:\Users\informant\Downloads\googledrivesync.exe	13071614190660454

13071614147290982

Convert WebKit timestamp to human date

GMT : Monday, March 23, 2015 7:55:47 PM

Your time zone : Monday, March 23, 2015 3:55:47 PM GMT-04:00

Epoch/Unix time : 1427140547 (in seconds)

1.4.3. Các từ khóa người dùng sử dụng để tìm kiếm thông tin trên Internet.

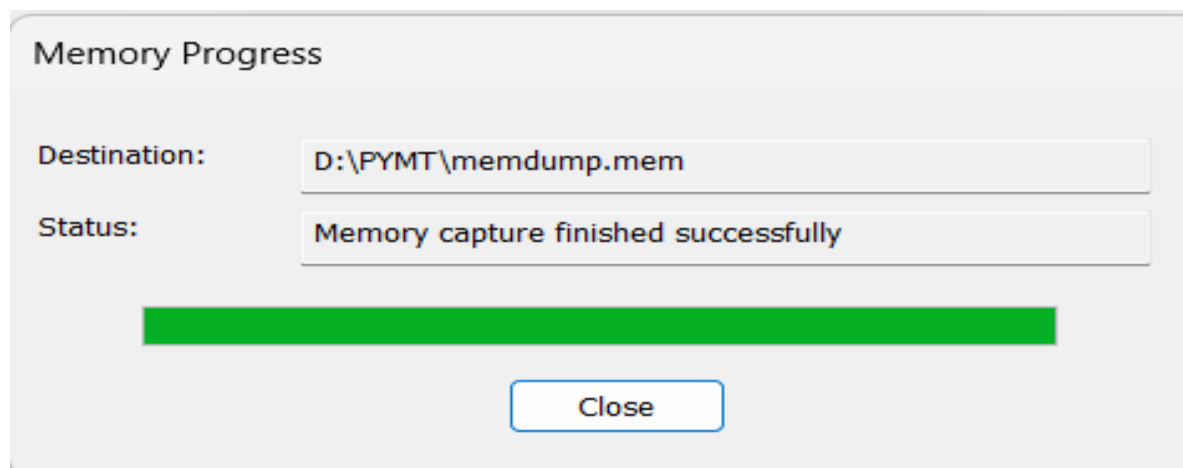
8	2	32	information leakage cases	information leakage cases
9	2	35	information leakage cases	information leakage cases
10	2	36	information leakage cases	information leakage cases
11	2	37	information leakage cases	information leakage cases
12	2	38	information leakage cases	information leakage cases
13	2	41	intellectual property theft	intellectual property theft
14	2	46	how to leak a secret	how to leak a secret

	Filter	Filter	Filter	Filter
1	2	21	outlook 2013 settings	outlook 2013 settings
2	2	23	emmy noether	Emmy Noether
3	2	24	data leakage methods	data leakage methods
4	2	28	leaking confidential information	leaking confidential information
5	2	29	leaking confidential information	leaking confidential information
6	2	30	leaking confidential information	leaking confidential information
7	2	31	information leakage cases	information leakage cases

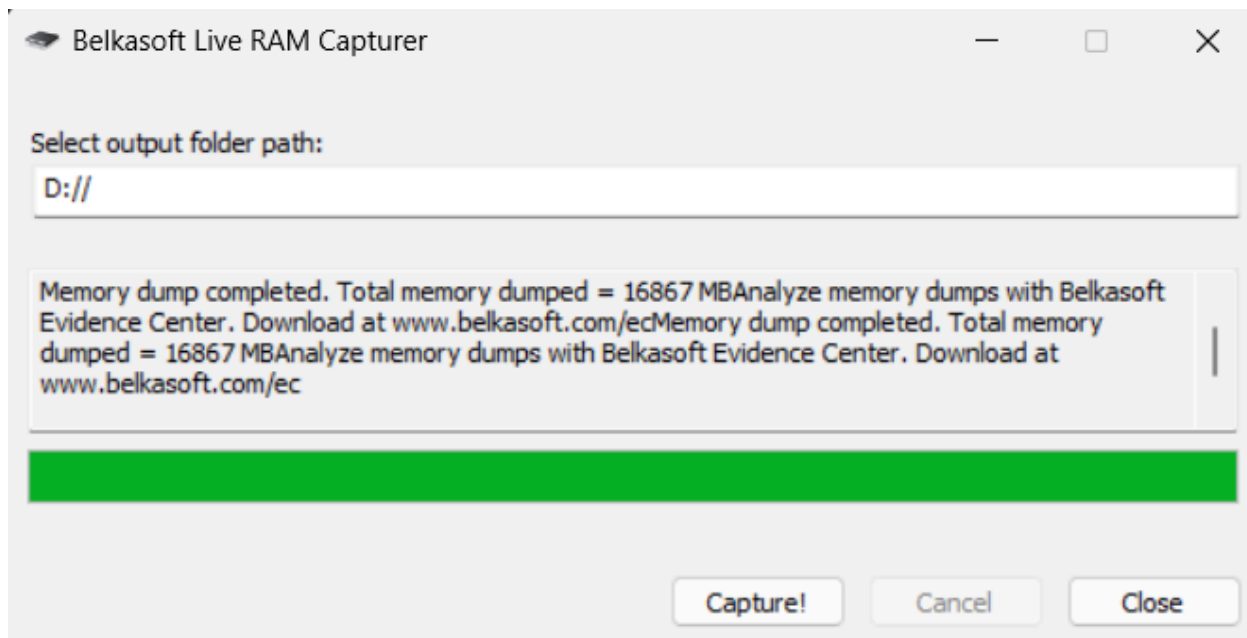
15	2	49	cloud storage	cloud storage
16	2	54	digital forensics	digital forensics
17	2	61	how to delete data	how to delete data
18	2	62	anti-forensics	anti-forensics
19	2	67	system cleaner	system cleaner
20	2	68	system cleaner	system cleaner
21	2	69	how to recover data	how to recover data
22	2	70	how to recover data	how to recover data
23	2	71	how to recover data	how to recover data
24	2	72	data recovery tools	data recovery tools
25	2	77	google	google
26	2	78	apple icloud	apple icloud
27	2	90	google drive	google drive
28	2	116	security checkpoint cd-r	security checkpoint cd-r

2. Điều tra bộ nhớ

2.1. Sử dụng công cụ FTK Imager để thu thập dữ liệu trên bộ nhớ RAM của máy tính cá nhân.



2.2. Tải và thực thi công cụ [Belkasoft RAM Capturer](#) để thu thập dữ liệu trên bộ nhớ RAM của máy tính cá nhân.



2.3. Cài đặt Volatility Framework trên máy ảo Kali

```
$git clone
https://github.com/volatilityfoundation/volatility3.git
$cd volatility3
$pip3 install -r requirements.txt
$python3 vol.py -h
```

```
(kali㉿kali)-[~/volatility3]
└─$ pip3 install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Collecting pefile>=2023.2.7
  Downloading pefile-2024.8.26-py3-none-any.whl (74 kB)
    ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 74.8/74.8 KB 1.1 MB/s eta 0:00:00
Requirement already satisfied: yara-python>=3.8.0 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 8)) (4.2.0)
Collecting capstone>=3.0.5
  Downloading capstone-5.0.3-py3-none-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (2.9 MB)
    ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 2.9/2.9 MB 9.5 MB/s eta 0:00:00
```

```
(kali㉿kali)-[~/volatility3]
└─$ ./vol.py -h
Volatility 3 Framework 2.10.0
usage: volatility [-h] [-c CONFIG]
                [--parallelism [{processes,threads,off}]] [-e EXTEND]
                [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG]
                [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE]
                [--write-config] [--save-config SAVE_CONFIG]
                [--clear-cache] [--cache-path CACHE_PATH] [--offline]
                [--filters FILTERS] [--single-location SINGLE_LOCATION]
                [--stackers [STACKERS ...]]
                [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
```

- 2.4. Tải và sao chép symbol table của các hệ điều hành cần hỗ trợ vào đường dẫn `volatility3/volatility/symbols` (không cần thực hiện)

```
(kali@kali)-[~/volatility3]
$ cp /media/sf_Downloads/memdump.mem ~
```

- 2.5. Tải tập tin [Lab04_01.7z](#), giải nén được tập tin `memdump.mem`. Kéo thả tập tin vào máy ảo Kali Linux (hoặc chia sẻ vào máy ảo).

- 2.6. Tìm kiếm thông tin và trả lời các câu hỏi sau:

- 2.6.1. Phiên bản của hệ điều hành

```
$/vol.py -f memdump.mem windows.info.Info
- Hệ điều hành Window 7.
```

```
Kernel Base      0x8183a000
DTB              0x122000
Symbols file:///home/kali/volatility3/volatility3/symbols/windows/ntkrpamp.pdb/37D328E3BAE5460F8E662756ED80951D-2.json.xz
Is64Bit False
IsPAE True
layer_name       0 WindowsIntelPAE
memory_layer     1 FileLayer
KdDebuggerDataBlock 0x81931c90
NTBuildLab       6001.18000.x86fre.longhorn_rtm.0
CSDVersion       1
KdVersionBlock   0x81931c68
Major/Minor      15.6001
MachineType      332
KeNumberProcessors 3405774849
SystemTime       2014-01-08 17:54:20+00:00
NtSystemRoot     C:\Windows
NtProductType    NtProductServer
NtMajorVersion   6
NtMinorVersion   0
PE MajorOperatingSystemVersion 6
PE MinorOperatingSystemVersion 0
PE Machine       332
PE TimeDateStamp Sat Jan 19 05:30:58 2008
```

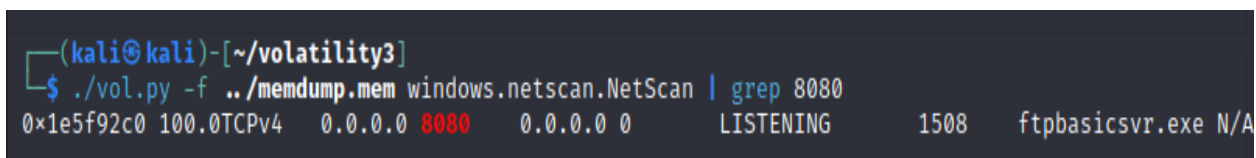
- 2.6.2. Giá trị băm của mật khẩu của tài khoản Waldo và Probe.

```
$/vol.py -f memdump.mem windows.hashdump.Hashdump
```

Administrator	500	aad3b435b51404eeaad3b435b51404ee	e19ccf75ee54e06b06a5907af13cef42
Guest	501	aad3b435b51404eeaad3b435b51404ee	31d6cfe0d16ae931b73c59d7e0c089c0
student	1000	aad3b435b51404eeaad3b435b51404ee	e19ccf75ee54e06b06a5907af13cef42
probe	1002	aad3b435b51404eeaad3b435b51404ee	e19ccf75ee54e06b06a5907af13cef42
waldo	1004	aad3b435b51404eeaad3b435b51404ee	cfeac129dc5e61b2eb9b2e7131fc7e2b
YOUR-NAME	1005	aad3b435b51404eeaad3b435b51404ee	958c8526e4252b277d8d70adbd2ea2ce

2.6.3. Chương trình đang hoạt động (lắng nghe) ở cổng 8080.

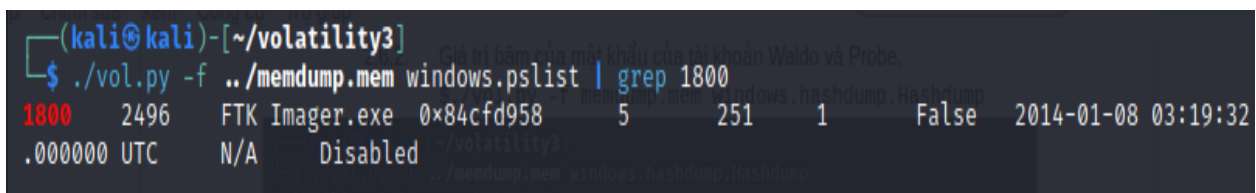
```
$/vol.py -f memdump.mem windows.netscan.NetScan |  
grep 8080
```



```
(kali@kali)-[~/volatility3]  
$ ./vol.py -f ../memdump.mem windows.netscan.NetScan | grep 8080  
0x1e5f92c0 100.0TCPv4 0.0.0.0 8080 0.0.0.0 0 LISTENING 1508 ftpbasicsvr.exe N/A
```

2.6.4. Tên tiến trình có mã số (PID) là 1800.

```
$/vol.py -f memdump.mem windows.pslist | grep 1800
```



```
(kali@kali)-[~/volatility3]  
$ ./vol.py -f ../memdump.mem windows.pslist | grep 1800  
1800 2496 FTK Imager.exe 0x84cfd958 5 251 1 False 2014-01-08 03:19:32  
.000000 UTC N/A Disabled
```

2.6.5. Tên chương trình ở thư mục “./Downloads” được thực thi lúc 23:12:30 ngày 2013-09-13.

```
$/vol.py -f memdump.memfile.dmp  
windows.registry.userassist.UserAssist | grep  
'Downloads\|2013-09-13'
```

Chụp hình minh họa các kết quả thực hiện trên.


```
(kali@kali)-[~/volatility3]
$ ./vol.py -f ../memdump.mem windows.registry.userassist.UserAssist | grep 'Downloads|2013-09-13'
* 0x9465f6a800000000 \Device\HarddiskVolume1\Users\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microso
ft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count 201
4-01-08 17:33:08.000000 UTC Value UEME_RUNPATH:C:\Users\Administrator\Downloads\DNSmon\setup.
exe 3 1 N/A N/A 2013-08-27 23:37:14.000000 UTC
* 0x9465f6a8 \Device\HarddiskVolume1\Users\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microso
ft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count 201
4-01-08 17:33:08.000000 UTC Value UEME_RUNPATH:C:\Users\Administrator\Downloads\PI2.3.2\Pois
on Ivy 2.3.2.exe 3 6 N/A N/A 2013-09-13 23:12:30.000000 UTC
* 0x9465f6a8 \Device\HarddiskVolume1\Users\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microso
ft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count 201
4-01-08 17:33:08.000000 UTC Value UEME_RUNPATH:C:\Users\Administrator\Downloads\PI2.3.2\evil2
.exe 3 2 N/A N/A 2013-09-13 22:29:21.000000 UTC
* 0x9465f6a8 \Device\HarddiskVolume1\Users\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microso
ft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count 201
4-01-08 17:33:08.000000 UTC Value UEME_RUNPATH:C:\Users\Administrator\Downloads\PI2.3.2\evil3
.exe 3 1 N/A N/A 2013-09-13 22:43:43.000000 UTC
* 0x9465f6a8 \Device\HarddiskVolume1\Users\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microso
ft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count 201
4-01-08 17:33:08.000000 UTC Value UEME_RUNPATH:C:\Users\Administrator\Downloads\PI2.3.2\evil4
.exe 3 2 N/A N/A 2013-09-13 22:45:30.000000 UTC
* 0x9465f6a8 \Device\HarddiskVolume1\Users\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microso
ft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count 201
4-01-08 17:33:08.000000 UTC Value UEME_RUNPIDL:%csidl2%\Accessories 3 1 N/A N/A
N/A 2013-09-13 23:11:02.000000 UTC
* 0x9465f6a8 \Device\HarddiskVolume1\Users\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microso
ft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count 201
4-01-08 17:33:08.000000 UTC Value UEME_RUNPIDL:%csidl2% 3 1 N/A N/A 201
3-09-13 23:11:02.000000 UTC
* 0x9465f6a8 \Device\HarddiskVolume1\Users\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microso
ft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count 201
4-01-08 17:33:08.000000 UTC Value UEME_RUNPATH:%csidl0%"services.msc" 3 1 N/A
N/A 2013-09-13 23:38:03.000000 UTC
* 0x9465f6a8 \Device\HarddiskVolume1\Users\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microso
ft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count 201
4-01-08 17:33:08.000000 UTC Value UEME_RUNPATH:C:\Users\Administrator\Downloads\AccessData FT
K Imager_3.1.4.exe 7 1 N/A N/A 2014-01-08 02:38:50.000000 UTC
* 0x9465f6a8 \Device\HarddiskVolume1\Users\Administrator\NTUSER.DAT NTUSER.DAT\Software\Microso
```

3. Phân tích mạng sử dụng Wireshark

- 3.1. Tải và cài đặt công cụ [Wireshark](#) trên máy tính cá nhân. Sử dụng công cụ Wireshark để bắt một số dữ liệu trên card mạng của máy tính cá nhân.
- 3.2. Tải và giải nén tập tin [Lab04_02.zip](#), giải nén được tập tin `rhino.log`.
- 3.3. Sử dụng công cụ Wireshark mở tập tin `rhino.log`. Lọc chọn những gói tin của dịch Telnet. Sử dụng chức năng "File" -> "Export Specified Packets" để xuất tất cả các gói tin lọc được, lưu vào tập tin có tên là `telnet.pcap`.
- 3.4. Tương tự Câu 3.3, lọc và xuất tất cả dữ liệu của mạng của dịch vụ FTP vào tập tin `ftp.pcap`
- 3.5. Dùng Wireshark mở tập tin `telnet.pcap`. Chọn tất cả các gói tin, sử dụng chức năng "Follow" -> "TCP Stream" để hiển thị dữ liệu gửi và nhận qua dịch vụ Telnet. Ở mục dưới bên phải của cửa sổ, thay đổi giá trị mục Stream để thấy các nội dung dữ liệu của các Stream.
 - Tìm tên tập tin chứa thông điệp gửi cho người dùng John.
Chụp hình minh họa kết quả thực hiện trên.
 - Tên tập tin là JOHNREADME.

```
total 1066
-rw-r--r--  1 gnome  cscistu    72 Apr 26  2004 JOHNREADME
-rwxr-xr-x  1 gnome  cscistu   2307 Feb 26 18:26 Xinitrc.XFce
-rw-r--r--  1 gnome  cscistu 230566 Apr 26  2004 contraband.zip
-rw-r--r--  1 gnome  cscistu   269 Feb 26 17:17 cshrc.user
-rw-r--r--  1 gnome  cscistu 117773 Apr 21 16:41 golden.jpg
-rw-r--r--  1 gnome  cscistu  65703 Apr 26 17:25 rhino1.jpg
-rw-r--r--  1 gnome  cscistu  96899 Apr 26  2004 rhino3.jpg
cook:[gnome]$
```

3.6. Tương tự Câu 3.5, mở tập tin `ftp.pcap`.

- Tìm tên tập tin thứ 3 được download thông qua dịch vụ FTP.
Chụp hình minh họa kết quả thực hiện trên.
- Tên tập tin thứ 3 được tải xuống là `contraband.zip`

```
STOR contraband.zip

150 Opening BINARY mode data connection for contraband.zip.
226 Transfer complete.

QUIT

221-You have transferred 230566 bytes in 1 files.
221-Total traffic for this session was 230914 bytes in 1 transfers.
221-Thank you for using the FTP service on cook.
221 Goodbye.
```

3.7. Sử dụng công cụ Wireshark mở lại tập tin `rhino.log`. Lọc tất cả dữ liệu data của mạng của dịch vụ FTP (`ftp-data`). Sử dụng chức năng "Follow" -> "TCP Stream" để hiển thị dữ liệu, chọn Stream: 0, chọn hiển thị dữ liệu dạng RAW. Sau đó save as dữ liệu thành tập tin có tên là `rhino1.jpg`. Chọn stream: 3, chọn hiển thị dữ liệu dạng RAW. Sau đó save as dữ liệu thành tập tin có tên là `secret.zip`

(chụp hình minh họa kết quả thực hiện)

- Hiển thị tập tin `rhino1.jpg`



- Dò mật khẩu giải nén `secret.zip`, hiển thị tập tin `rhino2.jpg`

✓ **Success!** Your password is recovered

Recovered password:

monkey



--- Hết ---