



LAB 02
ĐIỀU TRA CÁC HỆ THỐNG WINDOWS
(Windows 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. Phân tích hệ thống tập tin FAT và NTFS sử dụng FTK Imager và Active@ Disk Editor

- 1.1. Tải tập tin [Lab02_01.rar](#), giải nén được các file dữ liệu Lab02_01_1 và Lab02_01_2.
- 1.2. Sử dụng công cụ FTK Imager, chọn chức năng File/Add Evidence Item; sau đó chọn nguồn dữ liệu là từ Image File. Lần lượt thêm các file dữ liệu Lab02_01_1 và Lab02_01_2 vào Evidence Tree.
- 1.3. Sử dụng công cụ FTK Imager tìm kiếm thông tin và trả lời vào 2 bảng sau:

Image file	File system	Bytes per sector	Sector count	Bytes per cluster	Cluster count	Free cluster	Volume serial No.
Lab02_01_1	FAT32	512	249,341	1,024	120,574	120,229	929E-685 C
Lab02_01_2	NTFS	512	251,904	4,096	31,487	28,442	E6FE-1C5 F

	Lab02_01_1		Lab02_01_2	
File name	Start cluster	Start sector	Start cluster	Start sector
Bank Location.doc	398	8,984	14,867	118,936
interior safe.jpg	103	8,394	14,790	118,320
safe deposit bonds.xls	214	8,616	14,818	118,544

1.4. Sử dụng công cụ Active@ Disk Editor tìm kiếm thông tin và trả lời câu hỏi sau:

1.4.1. Sử dụng công cụ [Active@ Disk Editor](#), chọn chức năng File/Add Disk Image lần lượt thêm các file dữ liệu Lab02_01_1 và Lab02_01_2. Sử dụng chức năng “Open in Disk Editor” mở 2 tập tin trên. Mở tập tin Lab02_01_1 với “FAT boot sector” template và Lab02_01_2 với “NTFS boot sector” template. Trả lời vào 2 bảng sau:

	OEM ID		Bytes per sector		Sectors per cluster		Volume serial No.	
Image file	Offset	Value	Offset	Value	Offset	Value	Offset	Value
Lab02_01_1	003	MSDOS5.0	011	512	013	2	039	00 00 00 00
Lab02_01_2	003	NTFS	011	512	013	8	072	5F 1C FE E6 30 FE E6 8A

1.4.2. Cluster thứ 2176 (DEC) của Lab02_01_2 có đang được sử dụng hay không?

Hướng dẫn: sử dụng chức năng “Navigate/Go to sector” tới vị trí của cluster 2176 xem có chứa dữ liệu không?

Cluster 2176 không được sử dụng và không chứa dữ liệu.

Chụp hình minh họa kết quả thực hiện.

Offset	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	ASCII	Unicode
008912816	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
008912832	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
008912848	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
008912864	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
008912880	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
008912896	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
008912912	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
008912928	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
008912944	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
008912960	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
008912976	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
008912992	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
008913008	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
008913024	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

- 1.4.3. Giá trị Data runs (hệ HEX) của tập tin “Bank Location.doc” được lưu trong record của MFT là bao nhiêu? Giá trị đó có ý nghĩa gì?

Hướng dẫn: sử dụng chức năng Find tìm với từ khóa “Bank Location” để xác định vị trí record của tập tin “Bank Location.doc” trên MFT, tìm block Data attribute trên record (bắt đầu với giá trị “80 00 00 00”), tìm vị trí data runs trên Data attribute (bắt đầu từ byte có offset là x40).

Chụp hình minh họa kết quả thực hiện.

Giá trị Data runs của tập tin có giá trị là 21 0B 13 3A. Giá trị này có ý nghĩa là số 1 chỉ số byte tiếp theo đại diện cho kích thước của tập tin. 0B có nghĩa là kích thước của tập tin là 11 cluster. Số 2 chỉ 2 byte tiếp theo đại diện cho nơi bắt đầu của tập tin. 2 byte cuối đọc ngược lại là 3A13 có nghĩa là 14867 là cluster bắt đầu của tập tin.

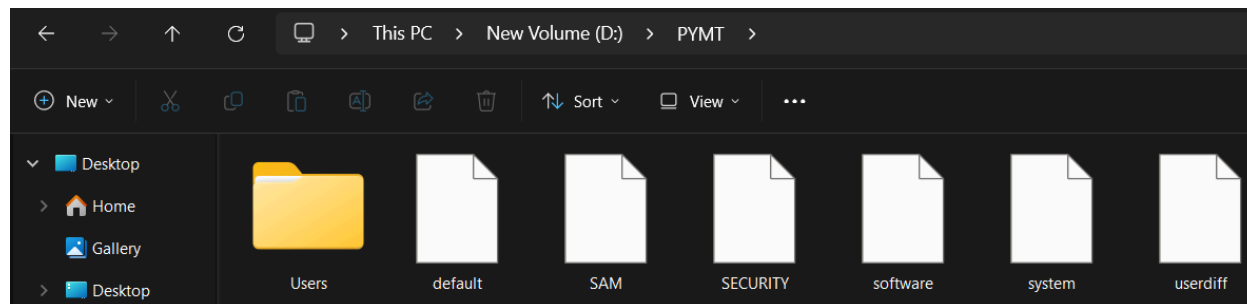
\$DATA	504		043043088	30 00 00 00 80 00 00 00	00 00 00 00 00 00 02 00
Data run	504		043043104	64 00 00 00 18 00 01 00	05 00 00 00 00 00 05 00
Size	504	0x21	043043120	DC 84 13 C6 5A F3 C9 01	DC 84 13 C6 5A F3 C9 01
Cluster count	505	11	043043136	DC 84 13 C6 5A F3 C9 01	DC 84 13 C6 5A F3 C9 01
First cluster	506	14867	043043152	00 B0 00 00 00 00 00 00	00 00 00 00 00 00 00 00
End marker	512	0xFFFFFFFF	043043168	20 00 00 00 00 00 00 00	11 01 42 00 61 00 6E 00
marks			043043184	6B 00 20 00 4C 00 6F 00	63 00 61 00 74 00 69 00
			043043200	6F 00 6E 00 2E 00 64 00	6F 00 63 00 00 00 00 00
mark	Offset		043043216	40 00 00 00 28 00 00 00	00 00 00 00 00 00 04 00
			043043232	10 00 00 00 18 00 00 00	E1 C1 E8 95 9B 5F DE 11
			043043248	98 A8 00 02 8A A5 21 D3	80 00 00 00 48 00 00 00
			043043264	01 00 00 00 00 00 01 00	00 00 00 00 00 00 00 00
			043043280	0A 00 00 00 00 00 00 00	40 00 00 00 00 00 00 00
			043043296	00 B0 00 00 00 00 00 00	00 B0 00 00 00 00 00 00
			043043312	00 B0 00 00 00 00 00 00	21 0B 13 3A 00 00 04 00

2. Trích xuất tập tin Windows registry sử dụng công cụ FTK Imager

- 2.1. Sử dụng công cụ FTK Imager, chọn chức năng File/Obtain, lựa chọn “Protected Files Password recovery and all registry files” để trích xuất các tập tin Windows registry và dữ liệu người dùng trên máy tính đang sử dụng. **Kết quả trích xuất bao gồm những tập tin và thư mục gì?**

Chụp hình minh họa kết quả thực hiện.

Kết quả bao gồm những tập tin default, SAM, SECURITY, software, system, userdiff và thư mục Users.

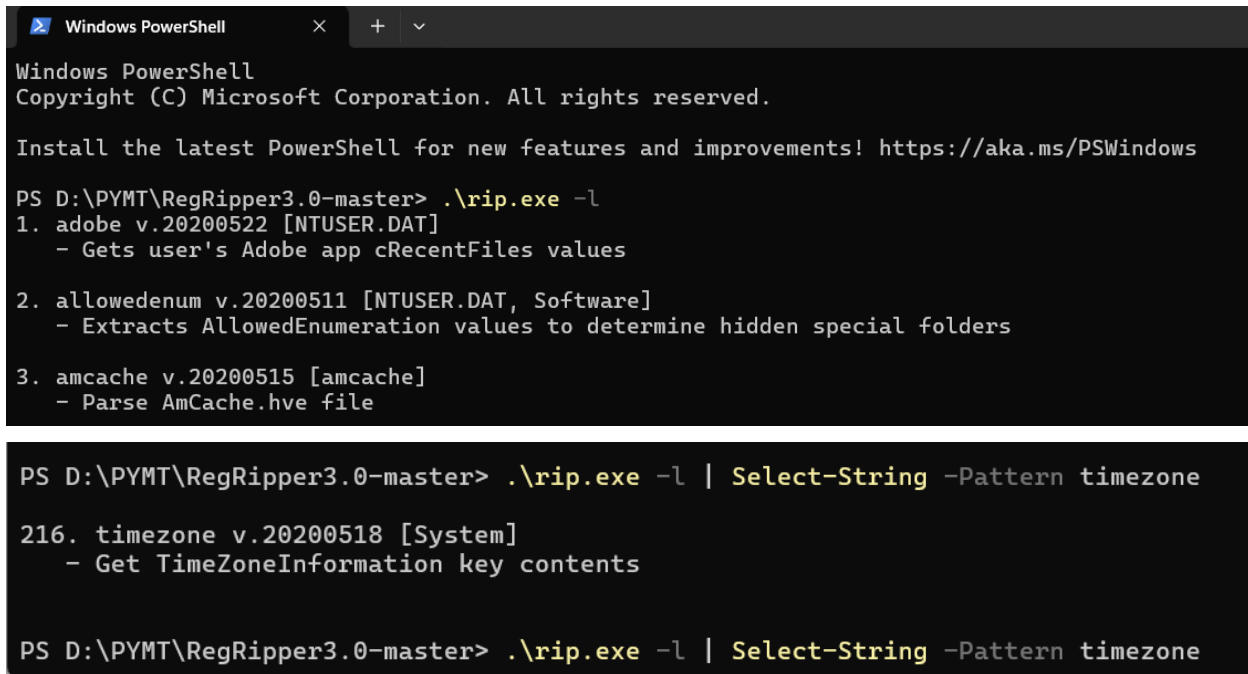


3. Phân tích Windows Registry sử dụng RegRipper

- 3.1. Tải tập tin các tập tin [Lab02_04.7z.001](#), Lab02_04.7z.002, Lab02_04.7z.003, 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.
- 3.2. Đi tới thư mục "Windows\System32\config". Ở giao diện File List, chọn các tập tin SYSTEM, SOFTWARE, SECURITY, SAM, và DEFAULT. Click chuột phải chọn chức năng Export Files để trích xuất các tập tin trên
- 3.3. Đi tới thư mục "Users". Lần lượt vào thư mục cá nhân của các người dùng admin11, default, informant, temporary, trích xuất các tập tin NTUSER.DAT của các người dùng, lần lượt đặt tên là NTUSER_Admin11.DAT, NTUSER_Default.DAT, NTUSER_Informant.DAT và NTUSER_Temporary.DAT.
- 3.4. Tải công cụ [RegRipper 3.0](#), ở môi trường Power Shell/CMD thực hiện các lệnh sau:

```
.\rip.exe
.\rip.exe -l
.\rip.exe -l | Select-String -Pattern timezone
```

Chụp hình minh họa kết quả thực hiện.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS D:\PYMT\RegRipper3.0-master> .\rip.exe -l
1. adobe v.20200522 [NTUSER.DAT]
   - Gets user's Adobe app cRecentFiles values

2. allowedenum v.20200511 [NTUSER.DAT, Software]
   - Extracts AllowedEnumeration values to determine hidden special folders

3. amcache v.20200515 [amcache]
   - Parse AmCache.hve file

PS D:\PYMT\RegRipper3.0-master> .\rip.exe -l | Select-String -Pattern timezone

216. timezone v.20200518 [System]
   - Get TimeZoneInformation key contents

PS D:\PYMT\RegRipper3.0-master> .\rip.exe -l | Select-String -Pattern timezone
```

```
PS D:\PYMT\RegRipper3.0-master> .\rip.exe
Rip v.3.0 - CLI RegRipper tool
Rip [-r Reg hive file] [-f profile] [-p plugin] [options]
Parse Windows Registry files, using either a single module, or a profile.

NOTE: This tool does NOT automatically process Registry transaction logs! The tool
does check to see if the hive is dirty, but does not automatically process the
transaction logs. If you need to incorporate transaction logs, please consider
using yarp + registryFlush.py, or rla.exe from Eric Zimmerman.

-r [hive] .....Registry hive file to parse
-d .....Check to see if the hive is dirty
-g .....Guess the hive file type
-a .....Automatically run hive-specific plugins
-aT .....Automatically run hive-specific TLN plugins
-f [profile].....use the profile
-p [plugin].....use the plugin
-l .....list all plugins
-c .....Output plugin list in CSV format (use with -l)
-s systemname.....system name (TLN support)
-u username.....User name (TLN support)
-uP .....Update default profiles
-h .....Help (print this information)

Ex: C:\>rip -r c:\case\system -f system
C:\>rip -r c:\case\ntuser.dat -p userassist
C:\>rip -r c:\case\ntuser.dat -a
C:\>rip -l -c

All output goes to STDOUT; use redirection (ie, > or >>) to output to a file.
```

3.5. Sử dụng công cụ RegRipper 3.0 tìm các thông tin sau:

- Phiên bản hệ điều hành và ngày cài đặt

.\rip.exe -r SOFTWARE -p winver

```
PS D:\PYMT\RegRipper3.0-master> .\rip.exe -r 'D:\PYMT\SOFTWARE' -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

ProductName           Windows 7 Ultimate
CSDVersion             Service Pack 1
BuildLab               7601.win7sp1_gdr.130828-1532
BuildLabEx             7601.18247.amd64fre.win7sp1_gdr.130828-1532
RegisteredOrganization
RegisteredOwner        informant
InstallDate            2015-03-22 14:34:26Z
PS D:\PYMT\RegRipper3.0-master>
```

- Múi giờ (Timezone) của máy.

.\rip.exe -r SYSTEM -p timezone

```
PS D:\PYMT\RegRipper3.0-master> .\rip.exe -r 'D:\PYMT\SYSTEM' -p timezone
Launching timezone v.20200518
timezone v.20200518
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time 2015-03-25 10:34:25Z
DaylightName -> @tzres.dll,-111
StandardName -> @tzres.dll,-112
Bias -> 300 (5 hours)
ActiveTimeBias -> 240 (4 hours)
TimeZoneKeyName-> Eastern Standard Time
Timeφûτ ¢ôHnτ ¢ôδΣτ ¢5pΓΆτ ¢¼nτ ¢nτ ¢δä
ùnτ ènτ ¢nτ ¢θ;âτ ¢ÿθ»»τ ¢ÿπτ ¢án¸Ä ¢ ¢Çπ» ¢ ¢ÿ ¢Çπτ ¢án¸Ä ¢ ¢ÿ ¢
```

- Tên máy tính.

`.\rip.exe -r SYSTEM -p compname`

```
PS D:\PYMT\RegRipper3.0-master> .\rip.exe -r 'D:\PYMT\SYSTEM' -p compname
Launching compname v.20090727
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName      = INFORMANT-PC
TCP/IP Hostname    = informant-PC
```

- Danh sách các người dùng trên máy.

`.\rip.exe -r SOFTWARE -p profilelist`

```
PS D:\PYMT\RegRipper3.0-master> .\rip.exe -r 'D:\PYMT\SOFTWARE' -p profilelist
Launching profilelist v.20200518
profilelist v.20200518
(Software) Get content of ProfileList key

Microsoft\Windows NT\CurrentVersion\ProfileList

Path       : %systemroot%\system32\config\systemprofile
SID        : S-1-5-18
LastWrite  : 2009-07-14 04:53:25Z

Path       : C:\Windows\ServiceProfiles\LocalService
SID        : S-1-5-19
LastWrite  : 2015-03-25 11:14:18Z

Path       : C:\Windows\ServiceProfiles\NetworkService
SID        : S-1-5-20
LastWrite  : 2015-03-25 11:14:18Z

Path       : C:\Users\informant
SID        : S-1-5-21-2425377081-3129163575-2985601102-1000
LastWrite  : 2015-03-25 15:30:57Z

Path       : C:\Users\admin11
SID        : S-1-5-21-2425377081-3129163575-2985601102-1001
LastWrite  : 2015-03-22 15:57:41Z

Path       : C:\Users\temporary
SID        : S-1-5-21-2425377081-3129163575-2985601102-1003
LastWrite  : 2015-03-22 15:56:58Z
```

- Thông tin lần đăng nhập cuối cùng vào máy.

`.\rip.exe -r SOFTWARE -p lastloggedon`

```
PS D:\PYMT\RegRipper3.0-master> .\rip.exe -r 'D:\PYMT\SOFTWARE' -p lastloggedon
Launching lastloggedon v.20200517
lastloggedon v.20200517
(Software) Gets LastLoggedOn* values from LogonUI key

LastLoggedOn
Microsoft\Windows\CurrentVersion\Authentication\LogonUI
LastWrite: 2015-03-25 13:05:47Z

LastLoggedOnUser      = .\informant
LastLoggedOnSAMUser   = informant-PC\informant
PS D:\PYMT\RegRipper3.0-master>
```

- Thông tin lần shutdown cuối cùng của máy.

.\rip.exe -r SYSTEM -P shutdown

```
PS D:\PYMT\RegRipper3.0-master> .\rip.exe -r 'D:\PYMT\SYSTEM' -p shutdown
Launching shutdown v.20200518
shutdown v.20200518
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
LastWrite time: 2015-03-25 15:31:05Z
ShutdownTime : 2015-03-25 15:31:05Z
PS D:\PYMT\RegRipper3.0-master> |
```

- Thông tin cấu hình mạng của máy.

.\rip.exe -r SYSTEM -P nic2

```
PS D:\PYMT\RegRipper3.0-master> .\rip.exe -r 'D:\PYMT\SYSTEM' -p nic2
Launching nic2 v.20200525
nic2 v.20200525
(System) Gets NIC info from System hive

Adapter: {846ee342-7039-11de-9d20-806e6f6e6963}
LastWrite Time: 2015-03-25 10:33:18Z

ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.
Adapter: {E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}
LastWrite Time: 2015-03-25 15:24:51Z
UseZeroBroadcast          0
EnableDeadGWDetect        1
EnableDHCP                 1
NameServer
Domain
RegistrationEnabled        1
RegisterAdapterName        0
DhcpIPAddress             10.11.11.129
DhcpSubnetMask             255.255.255.0
DhcpServer                 10.11.11.254
Lease                      1800
LeaseObtainedTime         2015-03-25 15:19:50Z
T1                         2015-03-25 15:34:50Z
T2                         2015-03-25 15:46:05Z
LeaseTerminatesTime       2015-03-25 15:49:50Z
AddressType                0
IsServerNapAware           0
DhcpConnForceBroadcastFlag 0
DhcpInterfaceOptions      , ỜƯ

ỜƯ

ỜƯ

ỜƯlocaldomainỜƯ ỜƯ ỜƯ ỜƯ ỜƯ

ỜƯ ỜƯ ỜƯ ỜƯ ỜƯ ỜƯ
DhcpGatewayHardware

PVỜƯỜƯ,
DhcpGatewayHardwareCount  1
DhcpNameServer            10.11.11.2
DhcpDefaultGateway        10.11.11.2
DhcpDomain                localdomain
DhcpSubnetMaskOpt         255.255.255.0
```


- Danh sách các phần mềm đã được cài vào máy.

.\rip.exe -r SOFTWARE -p installer

```
PS D:\PYMT\RegRipper3.0-master> .\rip.exe -r 'D:\PYMT\SOFTWARE' -p installer
Launching installer v.20200517
Launching installer v.20200517
(Software) Determines product install information

Installer
Microsoft\Windows\CurrentVersion\Installer\UserData

User SID: S-1-5-18
Key       : 00005109090090400100000000F01FEC
LastWrite: 2015-03-22 15:01:11Z
20150322 - Microsoft DCF MUI (English) 2013 15.0.4420.1017 (Microsoft Corporation)

Key       : 000051091A0090400100000000F01FEC
LastWrite: 2015-03-22 15:01:13Z
20150322 - Microsoft OneNote MUI (English) 2013 15.0.4420.1017 (Microsoft Corporation)

Key       : 000051091C0000000100000000F01FEC
LastWrite: 2015-03-22 15:01:46Z
20150322 - Microsoft Office 32-bit Components 2013 15.0.4420.1017 (Microsoft Corporation)

Key       : 000051091C0090400100000000F01FEC
LastWrite: 2015-03-22 15:01:04Z
20150322 - Microsoft Office Shared 32-bit MUI (English) 2013 15.0.4420.1017 (Microsoft Corporation)

Key       : 000051091E0090400100000000F01FEC
LastWrite: 2015-03-22 15:01:34Z
20150322 - Microsoft Office OSM MUI (English) 2013 15.0.4420.1017 (Microsoft Corporation)

Key       : 000051092E0090400100000000F01FEC
LastWrite: 2015-03-22 15:01:34Z
20150322 - Microsoft Office OSM UX MUI (English) 2013 15.0.4420.1017 (Microsoft Corporation)

Key       : 00005109440090400100000000F01FEC
LastWrite: 2015-03-22 15:01:03Z
20150322 - Microsoft InfoPath MUI (English) 2013 15.0.4420.1017 (Microsoft Corporation)

Key       : 00005109510090400100000000F01FEC
LastWrite: 2015-03-22 15:01:02Z
20150322 - Microsoft Access MUI (English) 2013 15.0.4420.1017 (Microsoft Corporation)

Key       : 00005109511090400100000000F01FEC
LastWrite: 2015-03-22 15:01:01Z
20150322 - Microsoft Office Shared Setup Metadata MUI (English) 2013 15.0.4420.1017 (Microsoft Corporation)
```

```
Key       : 46B5A9879DD95AB419A50FCFA0B1B7EF
LastWrite: 2015-03-23 20:01:01Z
20150323 - Apple Software Update 2.1.3.127 (Apple Inc.)

Key       : 55120087520F0704583BC74035657110
LastWrite: 2015-03-23 20:00:45Z
20150323 - Apple Application Support 3.0.6 (Apple Inc.)

Key       : A089CE062ADB6BC44A720BA745894BAC
LastWrite: 2015-03-22 15:16:03Z
20150322 - Google Update Helper 1.3.26.9 (Google Inc.)

Key       : B18863C615E01324D920FB129466D443
LastWrite: 2015-03-23 20:02:46Z
20150323 - Google Drive 1.20.8672.3137 (Google, Inc.)

Key       : C28643E881181F13CBC489DC69571E2C
LastWrite: 2015-03-25 14:54:35Z
20150325 - Microsoft .NET Framework 4 Extended 4.0.30319 (Microsoft Corporation)

Key       : DFC90B5F2B0FFA63D84FD16F6BF37C4B
LastWrite: 2015-03-25 14:52:08Z
20150325 - Microsoft .NET Framework 4 Client Profile 4.0.30319 (Microsoft Corporation)
```


- Danh sách các chương trình đã được thực thi bởi người dùng informant

.\rip.exe -r NTUSER_Informant.DAT -p userassist

```
PS D:\PYMT\RegRipper3.0-master> .\rip.exe -r 'D:\PYMT\New folder\NTUSER_Informant.DAT' -p userassist
Launching userassist v.20170204
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time 2015-03-22 14:35:01Z

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
2015-03-25 15:28:47Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\xpsrchvw.exe (1)
2015-03-25 15:24:48Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office\Office15\WINWORD.EXE (4)
2015-03-25 15:21:30Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Google\Drive\googledrivesync.exe (1)
2015-03-25 15:15:50Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\CCleaner\CCleaner64.exe (1)
2015-03-25 15:12:28Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Eraser\Eraser.exe (1)
2015-03-25 14:57:56Z
  C:\Users\informant\Desktop\Download\ccsetup504.exe (1)
2015-03-25 14:50:14Z
  C:\Users\informant\Desktop\Download\Eraser 6.2.0.2962.exe (1)
2015-03-25 14:46:05Z
  Microsoft.InternetExplorer.Default (5)
2015-03-25 14:42:47Z
  Microsoft.Windows.MediaPlayer32 (1)
2015-03-25 14:41:03Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office\Office15\OUTLOOK.EXE (5)
2015-03-24 21:05:38Z
  Chrome (7)
2015-03-24 18:31:55Z
  Microsoft.Windows.StickyNotes (13)
2015-03-24 14:16:37Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\rundll32.exe (1)
2015-03-23 20:27:33Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office\Office15\POWERPNT.EXE (2)
2015-03-23 20:26:50Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office\Office15\EXCEL.EXE (1)
2015-03-23 20:10:19Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe (4)
2015-03-22 15:24:47Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\slui.exe (3)
2015-03-22 15:12:32Z
  C:\Users\informant\Desktop\Download\IE11-Windows6.1-x64-en-us.exe (1)
2015-03-22 14:33:13Z
  Microsoft.Windows.GettingStarted (14)
  Microsoft.Windows.MediaCenter (13)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\calc.exe (12)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (10)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (9)
  Microsoft.Windows.RemoteDesktop (8)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\magnify.exe (7)
  {6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Games\Solitaire\solitaire.exe (6)
```

4. Phân tích NTFS \$MFT

4.1. Quay lại Câu 4.2, đi tới thư mục gốc trích xuất tập tin "\$MFT".

4.2. Tải và sử dụng chương trình "[MFTECmd](#)" để chuyển dữ liệu của file "\$MFT" sang định dạng XML/JSON/CSV.

```
.\MFTECmd.exe -f .\ $MFT --csv F:\ --csvf MFT.csv
```

```
PS D:\PYMT\Get-ZimmermanTools\net6> .\MFTECmd.exe -f 'D:\PYMT\LAB\ $MFT' --csv 'D:\PYMT\LAB\'
MFTECmd version 1.2.2.1

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f D:\PYMT\LAB\ $MFT --csv D:\PYMT\LAB\

Warning: Administrator privileges not found!

File type: Mft

Processed D:\PYMT\LAB\ $MFT in 0.9139 seconds

D:\PYMT\LAB\ $MFT: FILE records found: 76,714 (Free records: 1,366) File size: 76.2MB
CSV output will be saved to D:\PYMT\LAB\20240908142729_MFTECmd_ $MFT_Output.csv
```

4.3. Tải và sử dụng công cụ [Timeline Explorer](#) để mở tập tin MFT.csv. Tìm thông tin về các mốc thời gian của tập tin icloudsetup.exe

Chụp hình minh họa kết quả thực hiện.

Created0x10	Created0x30	Last Modified0x10	Last Modified0x30	Last Record Change0
=	=	=	=	=
2015-03-23 19:55:47		2015-03-23 19:56:53	2015-03-23 19:56:52	2015-03-23 19:56:53
2015-03-23 19:55:47		2015-03-23 19:56:53	2015-03-23 19:56:52	2015-03-23 19:56:53
2015-03-23 20:00:18		2015-03-23 20:02:02	2015-03-23 20:00:18	2015-03-23 20:02:02

5. Phân tích NTFS USN Journal \$J

5.1. Quay lại Câu 4.2, đi tới thư mục "NTFS\root\\$Extend\ \$UsnJrnl" trích xuất tập tin "\$J".

5.2. Tải và sử dụng chương trình "[MFTECmd](#)" để chuyển dữ liệu của file "\$J" sang định dạng XML/JSON/CSV.

```
.\MFTECmd.exe -f .\ $J --csv --csv F:\ --csvf J.csv
```

```
PS D:\PYMT\Get-ZimmermanTools\net6> .\MFTECmd.exe -f 'D:\PYMT\LAB\$J' --csv 'D:\PYMT\LAB\'
MFTECmd version 1.2.2.1

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f D:\PYMT\LAB\$J --csv D:\PYMT\LAB\

Warning: Administrator privileges not found!

File type: UsnJournal

Processed D:\PYMT\LAB\$J in 0.3401 seconds

Usn entries found in D:\PYMT\LAB\$J: 317,137
CSV output will be saved to D:\PYMT\LAB\20240908143327_MFTECmd_$J_Output.csv
```

- 5.3. Sử dụng công cụ Timeline Explorer để mở tập tin J.csv. Tìm thông tin về thời gian của tập tin Google Drive.lnk bị xóa.

Chụp hình minh họa kết quả thực hiện.

199706	<input type="checkbox"/>	2015-03-23 20:02:45	Google Drive.lnk
199707	<input type="checkbox"/>	2015-03-23 20:02:45	Google Drive.lnk
199708	<input type="checkbox"/>	2015-03-23 20:02:45	Google Drive.lnk
201257	<input type="checkbox"/>	2015-03-23 20:05:32	Google Drive.lnk
201258	<input type="checkbox"/>	2015-03-23 20:05:32	Google Drive.lnk
201259	<input type="checkbox"/>	2015-03-23 20:05:32	Google Drive.lnk
201260	<input type="checkbox"/>	2015-03-23 20:05:32	Google Drive.lnk
201261	<input type="checkbox"/>	2015-03-23 20:05:32	Google Drive.lnk
201262	<input type="checkbox"/>	2015-03-23 20:05:32	Google Drive.lnk
231087	<input type="checkbox"/>	2015-03-24 15:16:27	Google Drive.lnk
231088	<input type="checkbox"/>	2015-03-24 15:16:27	Google Drive.lnk
316690	<input type="checkbox"/>	2015-03-25 15:23:31	Google Drive.lnk

6. Phân tích Windows Prefetch

- 6.1. Quay lại Câu 4.2, đi tới thư mục “Windows\Prefetch” trích xuất tập tin “IEXPLORE.EXE-4B6C9213.pf”.

- 6.2. Tải và sử dụng chương trình “[PECmd](#)” để hiển thị thông tin thực thi của trình duyệt IExplorer.

```
.\PECmd.exe -f .\IEXPLORE.EXE-4B6C9213.pf
```

Chụp hình minh họa kết quả thực hiện.

```
PS D:\PYMT\Get-ZimmermanTools\net6> .\PECmd.exe -f 'D:\PYMT\LAB\IEXPLORE.EXE-4B6C9213.pf'
PECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -f D:\PYMT\LAB\IEXPLORE.EXE-4B6C9213.pf

Warning: Administrator privileges not found!

Keywords: temp, tmp

Processing D:\PYMT\LAB\IEXPLORE.EXE-4B6C9213.pf

Created on: 2024-09-08 14:36:24
Modified on: 2024-09-08 14:36:24
Last accessed on: 2024-09-08 14:37:58

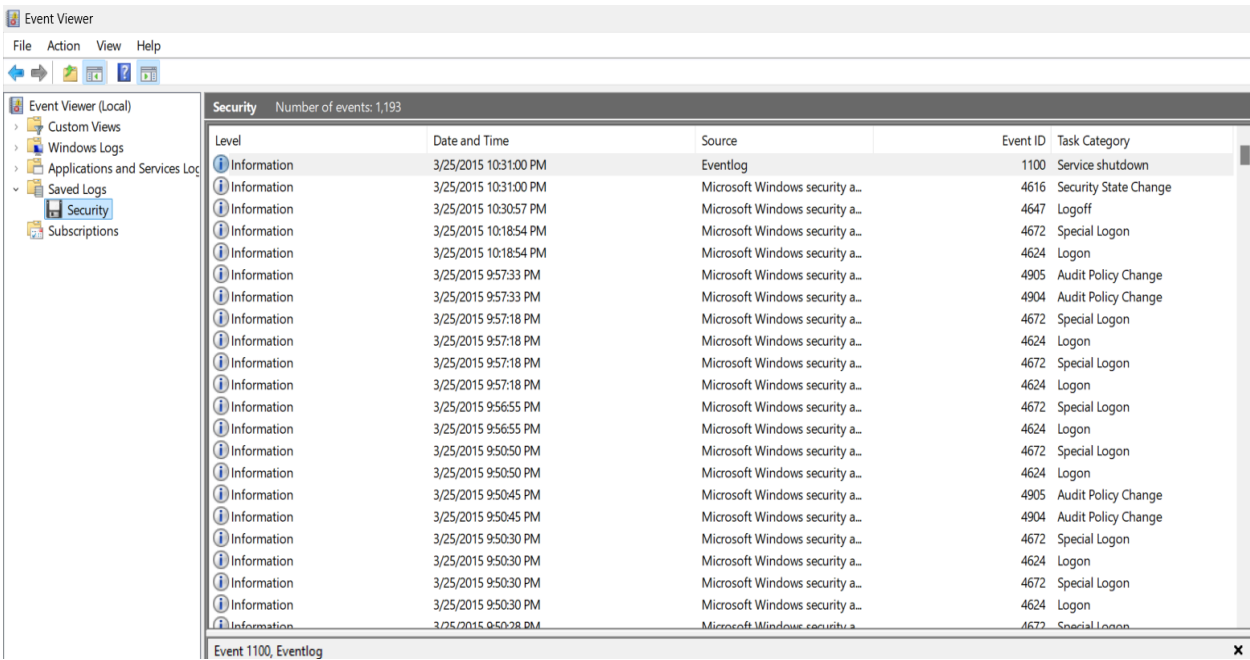
Executable name: IEXPLORE.EXE
Hash: 4B6C9213
File size (bytes): 464,154
Version: Windows Vista or Windows 7

Run count: 14
Last run: 2015-03-25 15:22:07
```

7. Phân tích Windows Event Log

- 7.1. Quay lại Câu 4.2, đi tới thư mục “Windows\System32\winevt\Logs”, trích xuất tập tin “Security.evtx”
- 7.2. Sử dụng chương trình Event Viewer trên Windows để mở tập tin “Security.evtx”.

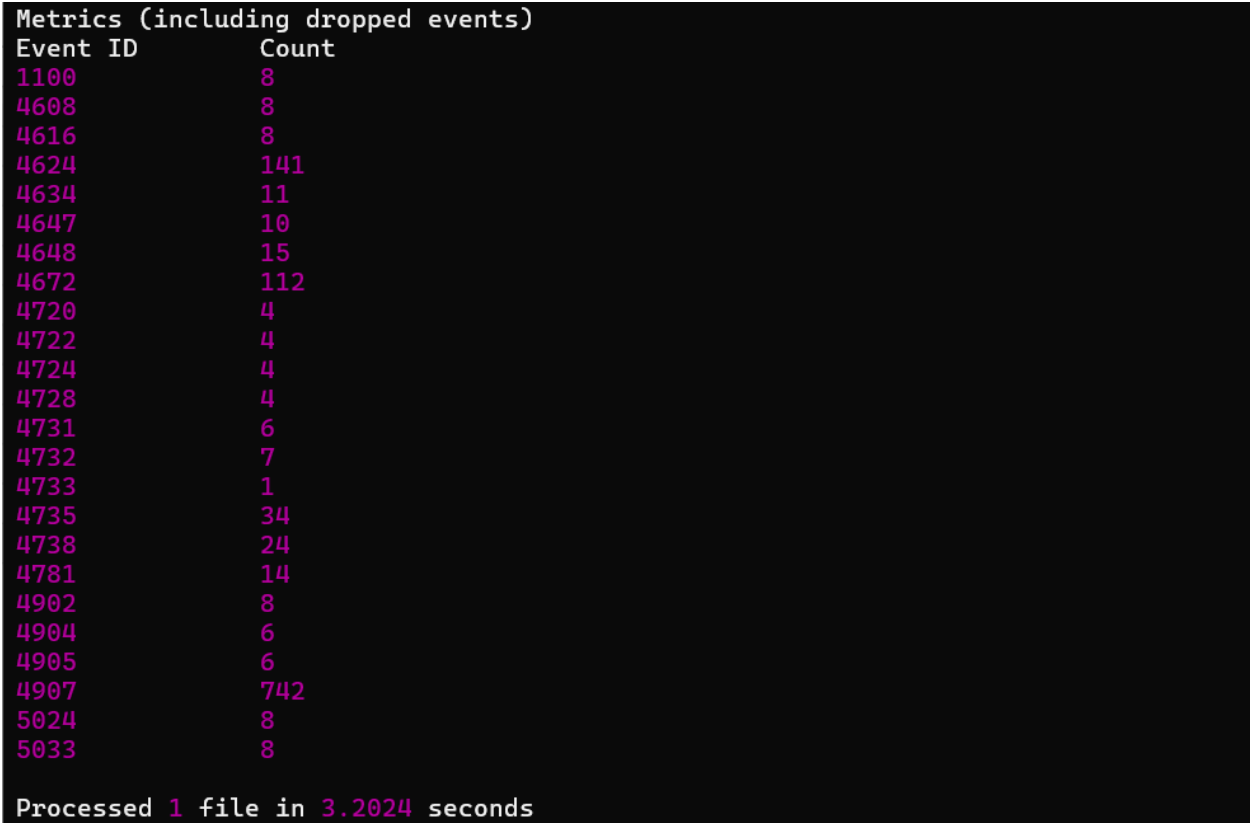
Chụp hình minh họa kết quả thực hiện.



7.3. Tải và sử dụng công cụ [EvtxECmd](#) để chuyển dữ liệu của file “Security.evtx” sang định dạng XML/JSON/CSV

```
.\EvtxECmd.exe -f .\Security.evtx --csv D:\ --csvf security.csv
```

Chụp hình minh họa kết quả thực hiện.



Sử dụng công cụ Timeline Explorer để mở tập tin security.csv. Tìm thông tin về các sự kiện A user account was created (EventID: 4720) .

Chụp hình minh họa kết quả thực hiện.

Record Number	Event Record Id	Time Created	Event Id	Level	Provider
=	=	=	=	🚫	🚫
111	111	2015-03-22 14:33:54	4720	LogAlways	Microsoft-Windows-Security-Auditing
984	984	2015-03-22 15:51:54	4720	LogAlways	Microsoft-Windows-Security-Auditing
995	995	2015-03-22 15:52:30	4720	LogAlways	Microsoft-Windows-Security-Auditing
1006	1006	2015-03-22 15:53:01	4720	LogAlways	Microsoft-Windows-Security-Auditing

--- Hết ---