THE DEPARTMENT OF
COMPUTER SCIENCE & ENGINEERING
計算機科學及工程學系

香港科技大學
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

COMP 4632
Practicing Cybersecurity: Attacks and Counter-measures

Week 12 Lab Exercise

Topic: Digital Forensics Investigation

Lab Objective

This lab is composed of two parts, "Windows Artefact Examination" and "Log Analysis". A simple case background is provided for both parts and this lab aims at achieving the following objectives:

- Experience how to examine the windows artefact on an image
- Experience how to perform log analysis across various log files

Unlike previous lab, there is no step by step instruction on the investigation. Instead, hints will be given in each question in order to facilitate your tasks.

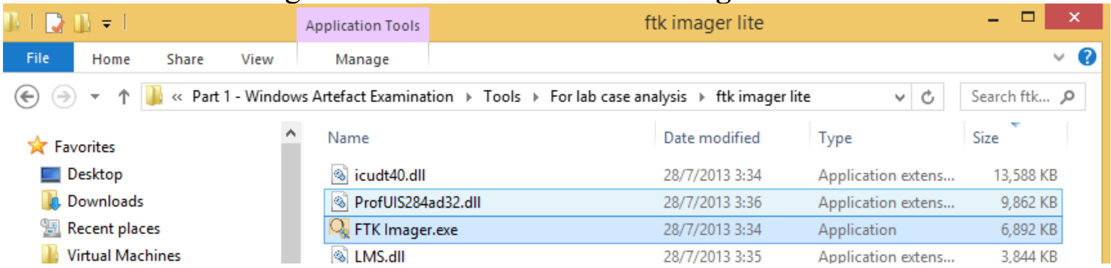
**The case content is purely fictional and for education purpose only*

Task 1 – Familiarize Your Tools

During an investigation, you may need to use tools to facilitate your information digging in the evidence (i.e. image of a harddisk) or log analysis. The following tasks are going to have brief introduction on some tools which can help you to do the basic searching in task 2 and 3.

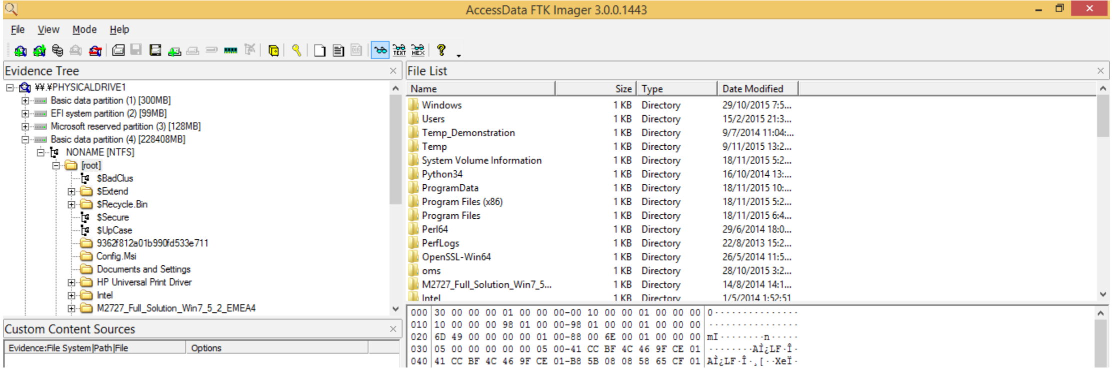
Task 1.1 FTK Imager Lite – Harddisk / Image Examination

- Go to "ftk imager lite" folder and run **FTK Imager.exe**



Name	Date modified	Type	Size
icudt40.dll	28/7/2013 3:34	Application extens...	13,588 KB
ProfUIS284ad32.dll	28/7/2013 3:36	Application extens...	9,862 KB
FTK Imager.exe	28/7/2013 3:34	Application	6,892 KB
LMS.dll	28/7/2013 3:35	Application extens...	3,844 KB

- File tab -> Add Evidence Item… -> Physical Drive* -> Browse… -> Select the your physical harddisk **choose image file for task 2*

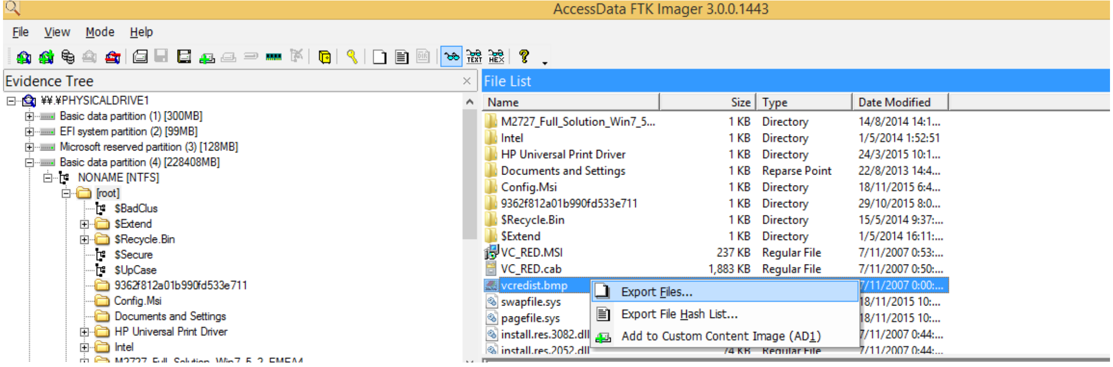


```
¥¥.¥PHYSICALDRIVE1
  Basic data partition (1) [300MB]
  EFI system partition (2) [99MB]
  Microsoft reserved partition (3) [128MB]
  Basic data partition (4) [228408MB]
    NONAME [NTFS]
      [root]
        $BadClus
        $Extend
        $Recycle.Bin
        $Secure
        $UpCase
        9362f812a01b990fd533e711
        Config.Msi
        Documents and Settings
        HP Universal Print Driver
        Intel
        M2727_Full_Solution_Win7_5_2_EMEA4
```

Name	Size	Type	Date Modified
Windows	1 KB	Directory	29/10/2015 7:5...
Users	1 KB	Directory	15/2/2015 21:3...
Temp_Demonstration	1 KB	Directory	9/7/2014 11:04:...
Temp	1 KB	Directory	9/11/2015 13:2...
System Volume Information	1 KB	Directory	18/11/2015 5:2...
Python34	1 KB	Directory	16/10/2014 13:...
ProgramData	1 KB	Directory	18/11/2015 10:...
Program Files (x86)	1 KB	Directory	18/11/2015 5:2...
Program Files	1 KB	Directory	18/11/2015 6:4...
Perl64	1 KB	Directory	29/6/2014 18:0...
PerfLogs	1 KB	Directory	22/8/2013 15:2...
OpenSSL-Win64	1 KB	Directory	26/5/2014 11:5...
oms	1 KB	Directory	28/10/2015 3:2...
M2727_Full_Solution_Win7_5...	1 KB	Directory	14/8/2014 14:1...
Intel	1 KB	Directory	1/5/2014 1:52:51

```
000 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00 0···············
010 10 00 00 00 98 01 00 00-98 01 00 00 01 00 00 00 ················
020 6D 49 00 00 00 00 01 00-88 00 6E 00 01 00 00 00 mI········n·····
030 05 00 00 00 00 00 05 00-41 CC BF 4C 46 9F CE 01 ········AÌ¿LF·Î·
040 41 CC BF 4C 46 9F CE 01-B8 5B 08 08 58 65 CF 01 AÌ¿LF·Î·¸[··XeÏ·
```

- For any files you want to recover, right click the "File List" view -> Export Files… -> Choose saving location for the recovered file



AccessData FTK Imager 3.0.0.1443

Evidence Tree

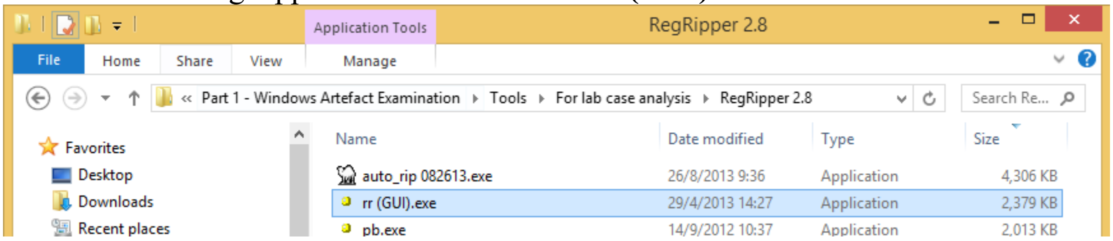
- ¥¥.¥PHYSICALDRIVE1
  - Basic data partition (1) [300MB]
  - EFI system partition (2) [99MB]
  - Microsoft reserved partition (3) [128MB]
  - Basic data partition (4) [228408MB]
    - NONAME [NTFS]
      - [root]
        - $BadClus
        - $Extend
        - $Recycle.Bin
        - $Secure
        - $UpCase
        - 9362f812a01b990fd533e711
        - Config.Msi
        - Documents and Settings
        - HP Universal Print Driver
        - Intel
        - M2727_Full_Solution_Win7_5_2_EMEA4

File List

Name	Size	Type	Date Modified
M2727_Full_Solution_Win7_5...	1 KB	Directory	14/8/2014 14:1...
Intel	1 KB	Directory	1/5/2014 1:52:51
HP Universal Print Driver	1 KB	Directory	24/3/2015 10:1...
Documents and Settings	1 KB	Reparse Point	22/8/2013 14:4...
Config.Msi	1 KB	Directory	18/11/2015 6:4...
9362f812a01b990fd533e711	1 KB	Directory	29/10/2015 8:0...
$Recycle.Bin	1 KB	Directory	15/5/2014 9:37:...
$Extend	1 KB	Directory	1/5/2014 16:11:...
VC_RED.MSI	237 KB	Regular File	7/11/2007 0:53:...
VC_RED.cab	1,883 KB	Regular File	7/11/2007 0:50:...
vcredist.bmp			7/11/2007 0:00:...
swapfile.sys			18/11/2015 10:...
pagefile.sys			18/11/2015 10:...
install.res.3082.dll			7/11/2007 0:44:...
install.res.2052.dll	74 KB	Regular File	7/11/2007 0:44:...

Task 1.2 Reg Ripper – Windows Registry Analysis

- Prior to analyze Windows registry with the Reg Ripper, registry hives are required to be exported via the FTK Imager. They are located in the following directories in Win7 environment.
  - *C:\Windows\System32\Config\*
  - *C:\Users\<user profile>*
- Go to "RegRipper 2.8" folder and run **rr (GUI).exe**

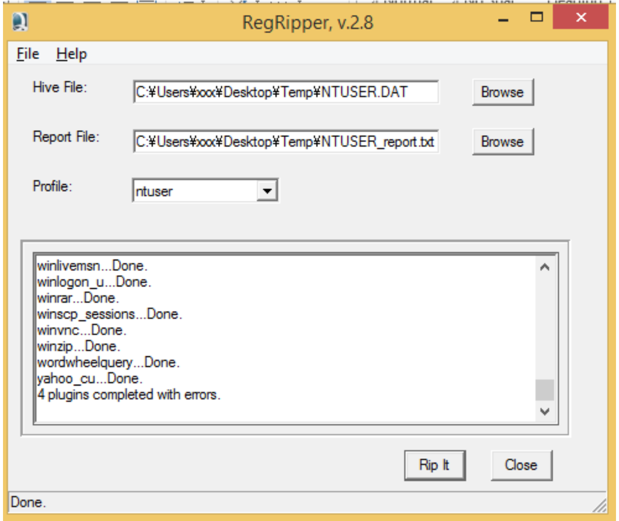


RegRipper 2.8

« Part 1 - Windows Artefact Examination › Tools › For lab case analysis › RegRipper 2.8

Name	Date modified	Type	Size
auto_rip 082613.exe	26/8/2013 9:36	Application	4,306 KB
rr (GUI).exe	29/4/2013 14:27	Application	2,379 KB
pb.exe	14/9/2012 10:37	Application	2,013 KB

- Choose the Hive File location, Report File location
- Choose Profile -> Click "Rip It" **Be noted that wrong profile will cause error*
  - E.g. **ntuser** profile should be selected when analyzing **NTUSER.DAT**



RegRipper, v.2.8

Hive File: C:¥Users¥xxx¥Desktop¥Temp¥NTUSER.DAT

Report File: C:¥Users¥xxx¥Desktop¥Temp¥NTUSER_report.txt

Profile: ntuser

```
winlivemsn...Done.
winlogon_u...Done.
winrar...Done.
winscp_sessions...Done.
winvnc...Done.
winzip...Done.
wordwheelquery...Done.
yahoo_cu...Done.
4 plugins completed with errors.
```

Done.

- Start digging information from the report file

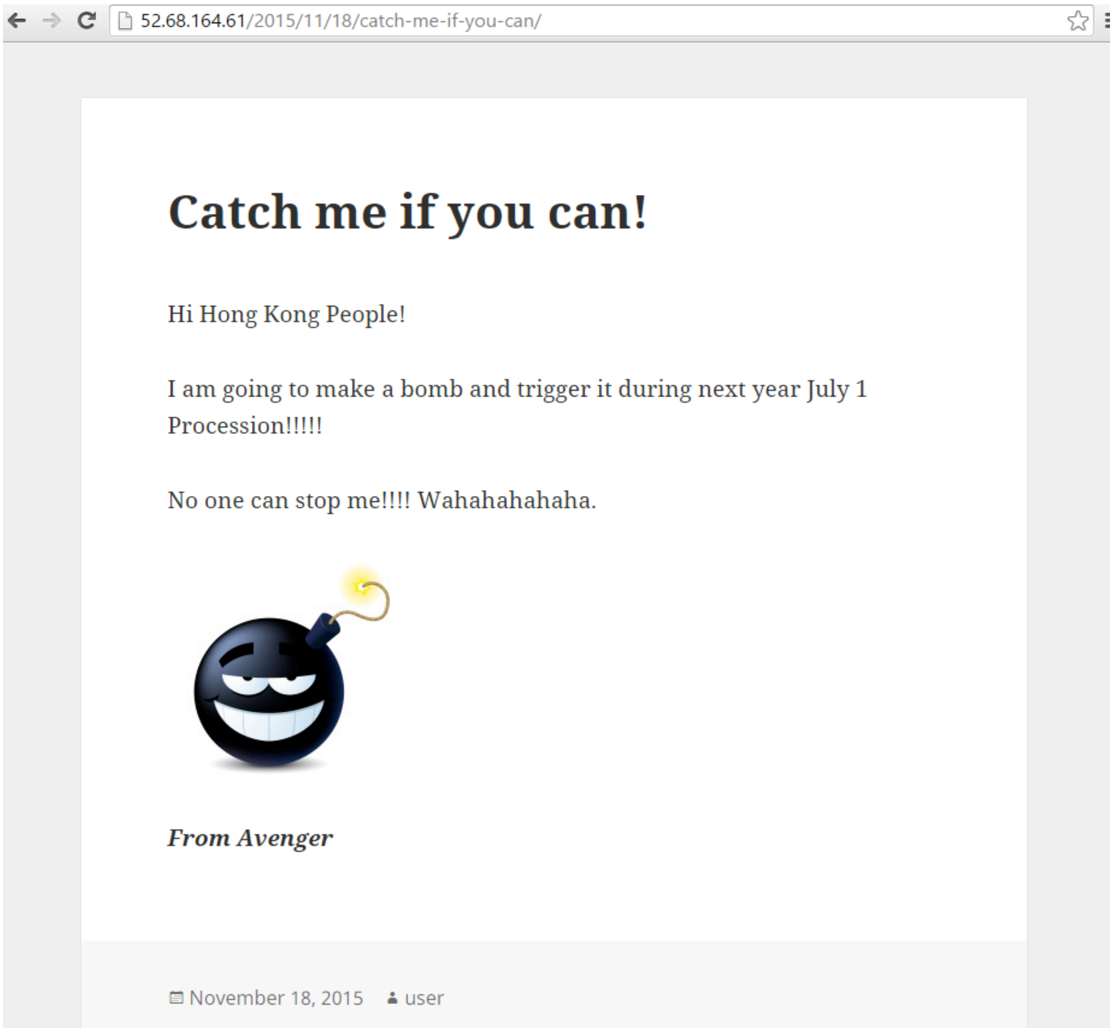
Task 1.3 Other Tools – For your self-learning

Other tools, such as WFA, autoruns.exe, event log explorer, were also provided. They are also used in real case analysis. Try to explore more if you are interested in them.

Task 2 – Windows Artefact Examination

Case Background

On 18 Nov 2015, Police Force received an anonymous report saying that there was a post on a blog mentioned that the blog owner was going to make a bomb and decide to make it explode during July 1 procession in 2016.



52.68.164.61/2015/11/18/catch-me-if-you-can/

Catch me if you can!

Hi Hong Kong People!

I am going to make a bomb and trigger it during next year July 1 Procession!!!!!

No one can stop me!!!! Wahahahahaha.

From Avenger

November 18, 2015 user

Police Force performed information gathering from internet and obtained the IP address of the blog owner. Finally, on 19 Nov 2015, Policy Force successfully located the home address of the blog owner by tracing the IP address, and then obtained warrant for collecting evidence (collected a notebook in this case) from the suspect. However, the suspect denied that **he did not know about the blog** and **never posted such message** on internet.

You are the digital forensic investigator. On 20 Nov 2015, Policy Force passed a cloned suspect's harddisk for you to examine. You are required to prove the word of the suspect.

You can use the following tools to complete the following questions

- *FTK Imager Lite*
- *Reg Ripper*
- *SQLiteDatabaseBrowserPortable*

**Other tools are welcome*

Guiding Questions

1. **What is the computer name and IP address(es) of the host? (Hint: registry hive)**
2. **What is the size of file system? (Hint: Find in FTK Imager)**
3. **How many user accounts in the host?**
4. **Any deleted files you can recover or find from recycle bin?**
5. **Any recent opened files you can find from registry?**
6. **Any visited website you observed?**

## Questions 1

From the information you observed in the image, what is your view toward the word of suspect? Please provide two fact findings and describe how they are found to support your view. (1.5 marks)

The following hints can help you answer this question.

- *Browser History*

- *File Recovery*

## Bonus Questions

1. **Is there any other potential incident you observed from the image? Please provide screenshot or any analysis result. (1 mark)**

2. **Where was the blog hosted? Briefly explain how you observe this. (0.5 mark)**

Task 3 – Log Analysis

Case Background

On 17 Nov night, the lecturer discovered that the exam website main page (i.e. index.php) was being defaced. Since the lecturer was busy with preparing the exam questions, you, an IT administrator, were asked to help investigate this incident. You collected a **pcap file** from the network and **access log** of the web server for analysis. You are required to figure out the following information.

Guiding Questions

1. **What is the entry point of the log analysis?**
2. **List out all IP addresses which accessed the web server.**
3. **What is the IP address of the attacker?**
4. **What vulnerabilities did the attacker discover in the application?**

##Questions 2

Describe the overall attack pattern leading to the web defacement in point form (1.5 mark)

The following hints can help you answer this question.

- *How attacker performed information gathering*

- *How attacker exploited the vulnerability*

##Bonus Questions

1. **Other than the web defacement, what kinds of sensitive information was leaked? (0.5 mark)**

The following hint can help you answer this question.

- *You need to find clues in access log and retrieve the related information from pcap file*

2. **List out all the ports (6 ports in total) opened on the web server. (0.5 mark)**

The following hint can help you answer this question.

- *Think how to filter them out from the pcap file*

3. **What attack / action did the attacker attempt to the active services apart from the web service? (0.5 mark)**

End of Lab