Digital Forensics Lab

Cyber Security Department

CYL-2002

Fall 2024

Lab #01

Instructor:

Ubaid Ullah

Fahad Waheed

Understanding the principles and methodologies of Digital Forensics

Read the following carefully, most of the information is brief and precise, you can find out more using the reference material provided.

Reference Material: https://www.eccouncil.org/cybersecurity/what-is-digital-forensics/

Digital Forensics lifecycle:

Digital forensics is a specialized field that involves the systematic examination and analysis of digital devices, networks, and electronic data to uncover evidence for legal investigations. The process of digital forensics typically involves several key steps, which are as follows:

Identification: This initial step involves identifying and documenting the digital devices or systems that may contain relevant evidence. This includes computers, mobile phones, servers, or any other storage media that could potentially hold valuable information.

Preservation: Once identified, the next step is to ensure the preservation of the digital evidence. This involves creating a forensic image or making an exact copy of the storage media without modifying or altering the original data. This ensures the integrity and authenticity of the evidence.

Collection: After preserving the evidence, the forensic investigator collects the relevant data from the digital devices or systems. This may include files, emails, chat logs, browsing history, or other forms of electronic data that could be crucial to the investigation.

Examination and Analysis: In this phase, the forensic expert carefully examines and analyzes the collected data. Various techniques and tools are employed to uncover hidden or deleted information, recover encrypted files, and reconstruct timelines of events. This step aims to identify and extract potential evidence that may support or refute the investigative hypothesis.

Reconstruction: Once the evidence has been identified, the forensic expert reconstructs the sequence of events or actions that took place. This involves piecing together fragments of data, examining system logs, and reconstructing digital activities to establish a clear understanding of what occurred.

Documentation and Reporting: All findings, observations, and analysis conducted during the digital forensics process are thoroughly documented and reported. The report provides a comprehensive overview of the investigation, including the methodology used, the evidence collected, the analysis performed, and the conclusions drawn.

Presentation: If required, the forensic expert may present the findings in a court of law or to relevant stakeholders. This involves explaining the technical aspects of the investigation in a clear and concise manner, ensuring that the presented evidence is easily understood and compelling.

These steps are crucial for the successful execution of a digital forensics' investigation, allowing investigators to gather, analyze, and present evidence that can play a significant role in legal proceedings and decision-making processes.

Linux command line fundamentals

This section serves as an introduction to the Linux command line tools which are essential for digital forensics.

There are many Linux commands that can be useful in forensics, but some of the most essential ones include:

ls — used to list the files and directories in a directory

The ls command lets you see a list of all the files and folders in a specific folder

```
$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Videos
```

cd — used to change the current working directory

The cd command lets you change the folder that you are currently working in.

```
$ cd Desktop/
```

cat — used to display the contents of a file

The cat command (short for "concatenate") lets you print the contents of a file.

```
$ cat file.txt
Hello World!
```

strings — used to display the printable strings in a file

The strings command allows you to see human-readable strings of characters inside a file which is helpful in identifying any suspicious strings.

```
$ strings file.txt
Hello World!
$ strings /bin/bash
/lib64/ld-linux-x86-64.so.2
 $DJ
CDDB
E`%
`0
"BB1
B8:
0D@kB
) 9E4
NR l
 "?$aD
!A8H
h% H0A
Hap5
($B
d> 7
<SNIP>
```

grep — used to search for a specific string or a pattern in a file or multiple files

The grep command is extremely useful for searching a string in large files, such as log files. It can speed up investigations dramatically by letting you search for patterns like URLs, E-mail addresses, MD5 hashes, and more.

```
$ grep "Hello" file.txt
Hello World!
```

find — used to search for files and directories

The find command can be used to locate different types of files, directories, files with specific permissions, recently modified files.

```
$ find . -type d
.
./Music
./Public
./Downloads
./Desktop
./.config
./.config/autostart
./.config/xfce4
./.config/xfce4/panel
./.config/cherrytree
./.config/powershell
./Pictures
./Documents
./.java
./.java/.userPrefs
./.java/.userPrefs/burp
./Videos
```

Notice how the output above returns a few more directories than the ls command.

md5sum, sha1sum — used to compute the MD5 and SHA1 hashes of a file

Both of these commands take an input and generate a fixed-length string, also known as a hash or a checksum. If the contents of the file change, even slightly, its hash will be different. This can be useful for detecting if a file has been modified or tampered with.

```
$ md5sum file.txt
8ddd8be4b179a529afa5f2ffae4b9858  file.txt
$ sha1sum file.txt
a0b65939670bc2c010f4d5d6a0b3e4e4590fb92b  file.txt
```

netstat — used to display information about the network connections on a system

This tool provides useful information about active connections on a system. The information displayed by this tool includes local and remote addresses and ports of active connections.

```
$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.0.106:44300     239.237.117.34.bc:https ESTABLISHED
tcp        0      0 192.168.0.106:39884     93.184.220.29:http      ESTABLISHED
tcp        0      0 192.168.0.106:58308     ec2-52-39-122-167:https ESTABLISHED
tcp        0      0 192.168.0.106:56910     static-48-7-129-15:http ESTABLISHED
udp        0      0 192.168.0.106:bootpc    192.168.0.1:bootps      ESTABLISHED
```

file — used to determine the type of a file based on its contents

The file command can be used to identify files such as text, image, audio, video, and executable files. It can also be used to identify unknown files that may potentially be malicious.

```
$ file /etc/passwd
/etc/passwd: ASCII text
$ file image.png
image.png: PNG image data, 562 x 424, 8-bit/color RGB, non-interlaced
```

xxd — used to print hex dump of a given file

The xxd command is useful to print hex dump of a given file or standard input. It can also convert a hex dump back to its original binary form.

```
$ xxd image.jpg
00000000: ffd8 ffe0 0010 4a46 4946 0001 0101 0048  ......JFIF.....H
00000010: 0048 0000 ffdb 0043 0005 0304 0404 0305  .H.....C........
00000020: 0404 0405 0505 0607 0c08 0707 0707 0f0b  ................
00000030: 0b09 0c11 0f12 1211 0f11 1113 161c 1713  ................
00000040: 141a 1511 1118 2118 1a1d 1d1f 1f1f 1317  ......!.........
00000050: 2224 221e 241c 1e1f 1eff db00 4301 0505  "$".$.......C...
```

hexedit — used to edit files in hexadecimal format

The hexedit tool lets you edit raw bytes of a file in an interactive way. It is often used for repairing corrupted files.

ps — used to list the process running on the system

The ps command lets you see a list of all the processes that are currently running on your computer. The information it provides includes the process ID, user, state, and command that started the process.

```
$ ps
    PID TTY          TIME CMD
   1824 pts/0    00:00:09 zsh
   2879 pts/0    00:00:05 sublime_text
   2924 pts/0    00:00:00 plugin_host-3.3
   2927 pts/0    00:00:00 plugin_host-3.8
  22666 pts/0    00:00:00 ps
```

Magic Bytes

Magic bytes, also known as magic numbers or file signatures, are a sequence of bytes found at the beginning of a file that uniquely identifies the file type or format. These bytes serve as a clue for software applications or utilities to determine the nature and characteristics of a file, even when the file extension is missing or incorrect.

Magic bytes are typically a fixed sequence of binary values and are specific to each file type. They are defined by file format specifications or conventions agreed upon by developers and organizations. When a program encounters a file, it reads the initial bytes and compares them against known magic byte patterns to identify the file's format.

For example, a JPEG image file typically starts with the magic bytes "FF D8 FF" in hexadecimal representation. If a utility encounters these bytes at the beginning of a file, it can confidently determine that the file is a JPEG image. Run the following command:

```
xxd -l 16 image.jpg
```

The -l option is used to specify the number of bytes to display. In this example, we are displaying 16 bytes, but you can adjust the number as needed.

The xxd command will display the hexadecimal representation of the first 16 bytes of the file, along with the corresponding ASCII characters on the right-hand side (if printable).

How can we find Magic Bytes of all different file types? I've a solution for that. Navigate to the following site here you'll find Magic bytes of all different file formats.
https://www.garykessler.net/library/file_sigs.html

For editing hex bytes, you can use any hex editor. I use hexed.it

Important Instruction: Please do not submit your answers within this lab manual. Instead, create a separate document for your solutions and submit it using the following naming convention: i22xxxx_Lab01.

Task 01: What is wrong with dog.png. Hint Cyberchef

Ans:

Task 02: Can you check Image.jpg and recover the file. Flag format FLAG{text_in_image}. Hint: Check for magic bytes in hexed and match them with jpg magic bytes on Gary Kessler's site.

Ans:

Task 03: Does changing the extension change magic bytes of the file. Try and add screenshots with explanation.

Ans:

Task 04: Can you recover the challenge.png file. Flag format flag{}.

Ans:

Task 05: What if magic bytes are totally out of place, how can we check for file type? Hint:

"I have wheels, yet I'm not a car.

I am big, but I'm not a star.

Pull me along, I'll carry your load.

Inside me, stories are often showed."

Ans:

Task 06 [Bonus]: Can you recover Boss.png?

Ans: