บจก.สยามถนัดแฮก

NCSA CTF Boot Camp #2

Digital Forensics

Responsible: Mr. Peeratach Butto
Version (Date): 1.0 (2024-09-14)
Confidentiality class: Public

whoami

Pichaya (LongCat) Morimoto
Lead Penetration Tester
Siam Thanat Hack Co., Ltd.

Peeratach (Peter) Butto
Penetration Tester
Siam Thanat Hack Co., Ltd.

Yasinthon (Not) Khemprakhon
Penetration Tester
Siam Thanat Hack Co., Ltd.

Disclaimer

- จุดประสงค์ของการบรรยาย นี้เพื่อแบ่งปันความรู้ ทางด้านความปลอดภัยระบบสารสนเทศ
- ไม่สนับสนุนการนำความรู้ทางด้านความปลอดภัยฯ ไปใช้ในทางที่ผิดกฎหมายทั้งหมด
- ตัวอย่างโค้ด และรูปใน การบรรยาย นี้ เป็นระบบจำลองของทางผู้บรรยาย ไม่ใช่ระบบลูกค้า

Agenda (Day 1)

เวลา	รายละเอียด
09.15 - 09.45	ความรู้เบื้องต้นเกี่ยวกับ CTF
09.45 - 10.30	Network Security
10.30 - 10.45	พักเบรก
10.45 - 12.00	Web Application Security
12.00 - 13.00	พักรับประทาน อาหารกลางวัน
13.00 - 14.30	Digital Forensics
14.30 - 14.45	พักเบรก
14.45 - 16.00	Pwnable & Reverse Engineering
16.00 - 18.00	เข้าห้องพัก
18.00 - 19.00	รับประทานอาหารเย็น
19.00 - 21.00	เสวนาแนะแนวเส้นทางอาชีพ

Content Overview

- Digital Forensics คืออะไร
- ประเภทของการ Digital Forensics
  - ไฟล์ Log
  - ไฟล์ Disk Image
  - ไฟล์อื่น ๆ เช่น มัลแวร์ หรือ เอกสาร Word
- การวิเคราะห์ข้อมูล Log
- ตัวอย่างโปรแกรมที่เกี่ยวข้อง
- การวิเคราะห์ข้อมูล Metadata
  - Hex Editor
- ลองทำแลป !
  - Lab 1: วิเคราะห์ Access.log
  - Lab 2: วิเคราะห์ Metadata file image
  - Lab 3: Verify zip

Digital Forensics คืออะไร

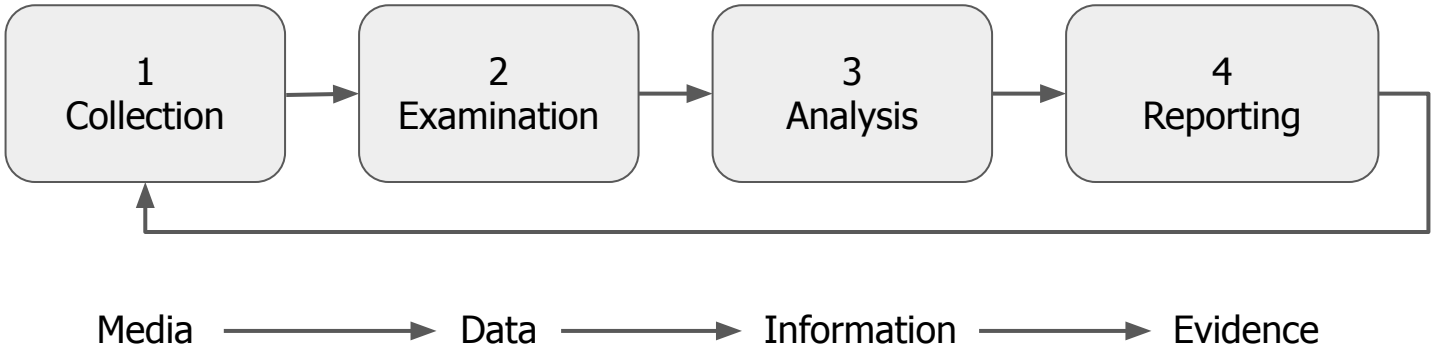
ที่มา: https://www.americanscientist.org

เป็นกระบวนการเก็บรวบรวม วิเคราะห์ และรักษาหลักฐานที่ได้จากระบบดิจิทัล เพื่อนำมาใช้ในการสืบสวนหรือดำเนินคดีทางกฎหมาย

หลักฐานเหล่านี้อาจมาจาก

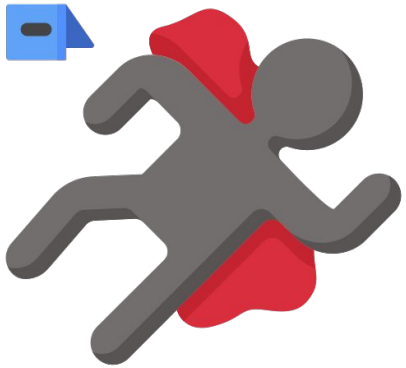
- อุปกรณ์คอมพิวเตอร์
- โทรศัพท์มือถือ
- เครือข่าย
- หรืออุปกรณ์จัดเก็บข้อมูลอื่น ๆ

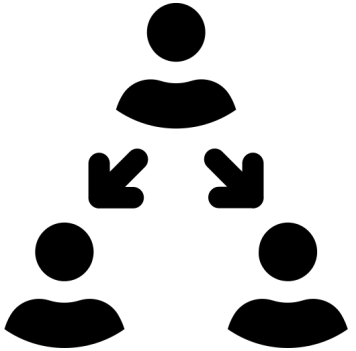
The Process of Digital Forensics



NIST SP 800-86 - Digital Forensics
Flow Standard

Digital Forensics





Digital Forensics (Real World) VS (CTF)

VS

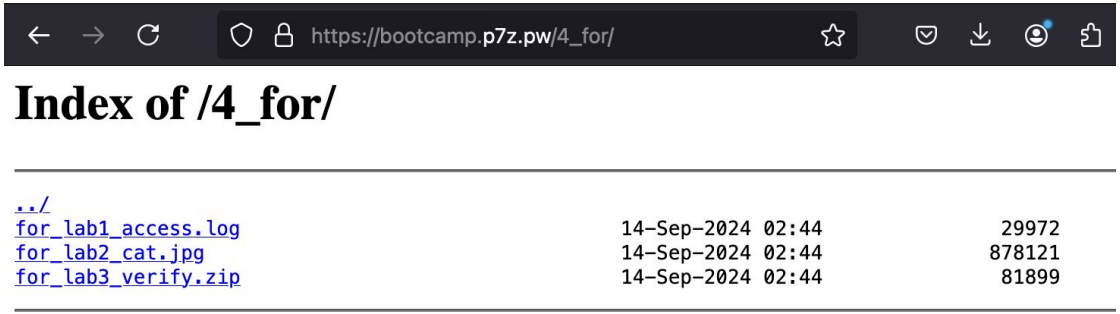
Detective Conan" The Dark Footprint: Part 2"

ประเภทของการ Digital Forensics

- Log Analysis
- File Analysis
- Memory Forensics
- Disk Forensics
- Malware Analysis
- etc.

ดาวน์โหลดไฟล์แลป

https://bootcamp.p7z.pw/4_for/



ทำความรู้จัก Log

Log File

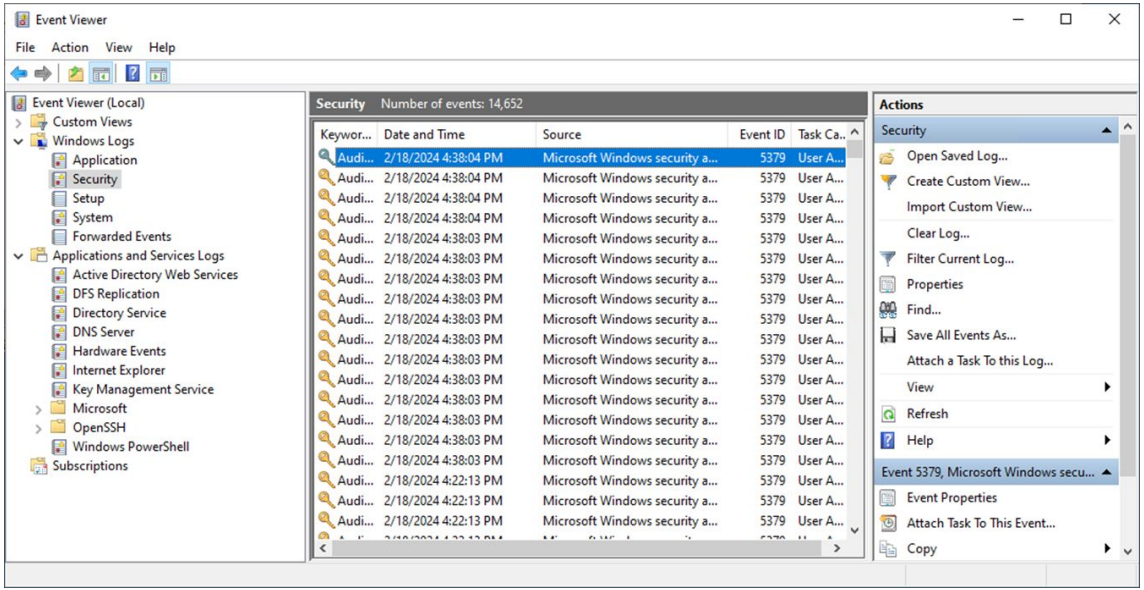
- Application Log
- Security Log
- Server Log
- System Log
- Network Log
- Database Log

```
192.168.1.1 - - [01/Sep/2024:12:00:00 +0000] "GET /index.html HTTP/1.1" 200 1024 "https://example.com/home" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36"
192.168.1.2 - - [01/Sep/2024:12:05:30 +0000] "POST /login HTTP/1.1" 302 512 "https://example.com/login" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Firefox/89.0"
192.168.1.3 - - [01/Sep/2024:12:10:15 +0000] "GET /about.html HTTP/1.1" 200 2048 "https://example.com/home" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0"
192.168.1.4 - - [01/Sep/2024:12:15:45 +0000] "GET /images/logo.png HTTP/1.1" 200 4096 "https://example.com/index.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Safari/537.36"
192.168.1.5 - - [01/Sep/2024:12:20:30 +0000] "GET /contact.html HTTP/1.1" 404 256 "https://example.com/home" "Mozilla/5.0 (Linux; Android 10; Pixel 4 XL) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.77 Mobile Safari/537.36"
```

The Path of Log File on Windows

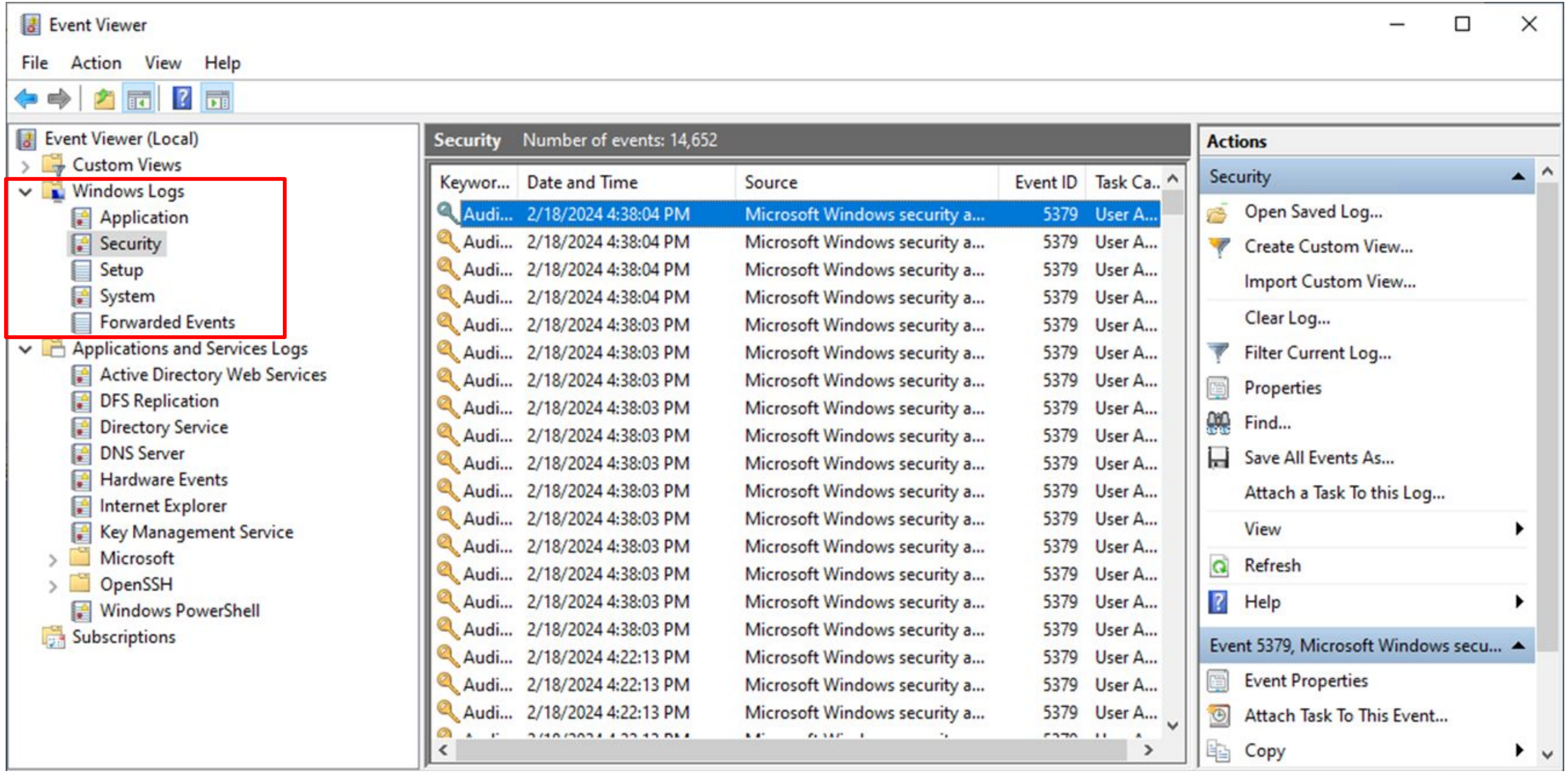
บน Windows ไฟล์ Log มักถูกจัดการผ่าน Event Viewer และจะถูกเก็บในรูปแบบของ Event Logs และเก็บไว้ที่ %SystemRoot%\System32\Winevt\Logs\ เช่น C:\Windows\System32\Winevt\Logs\

1. Application Log
2. System Log
3. Security Log
4. Setup Log
5. Forwarded Events Log

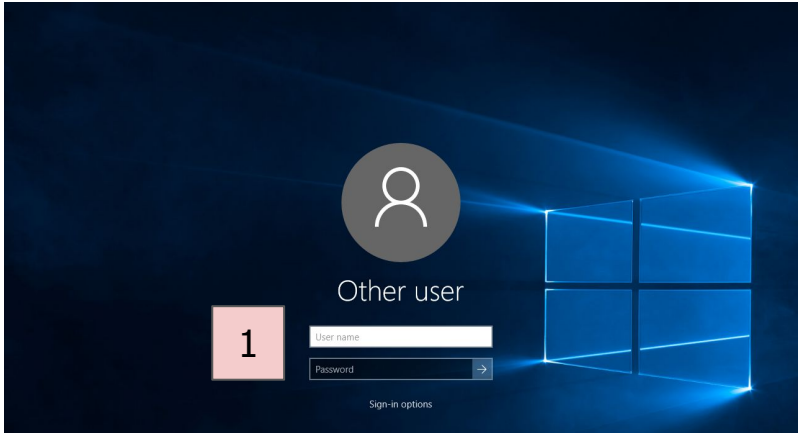


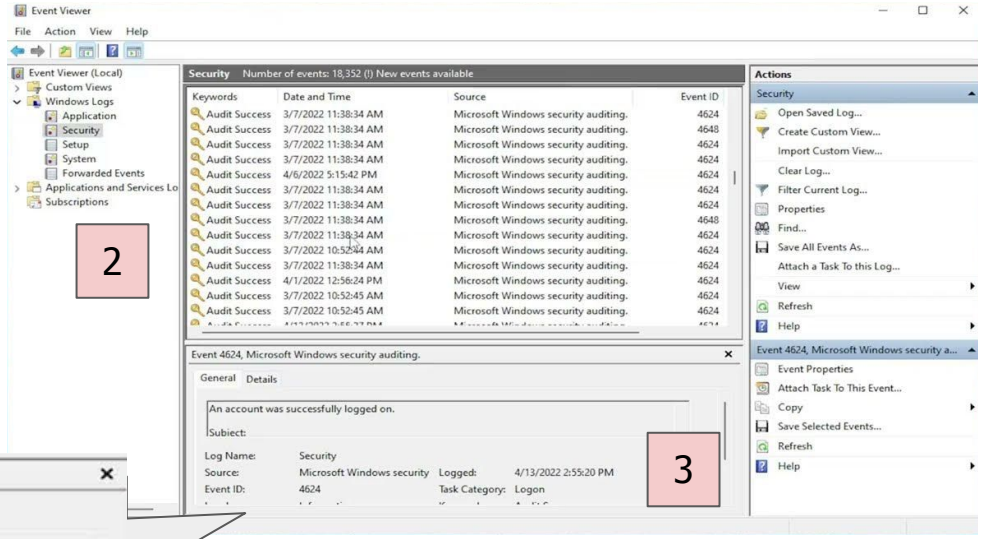
ที่มา: https://techcommunity.microsoft.com

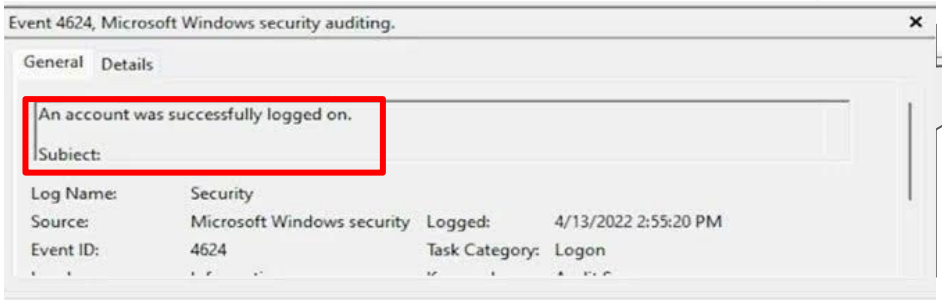
C:\Windows\System32\Winevt\Logs\



Windows Security Log



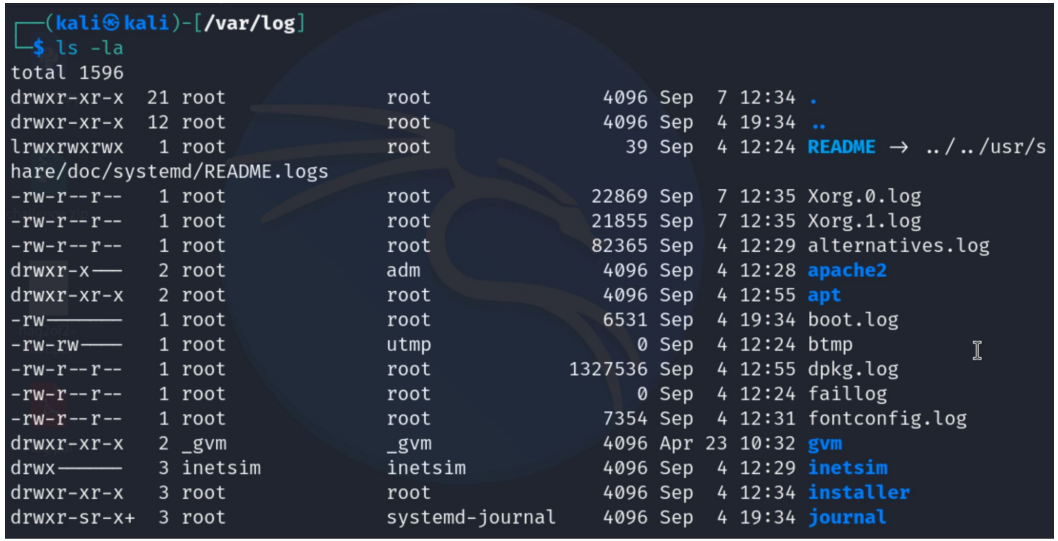




The Path of Log Files on Linux

บน Linux ไฟล์ Log มักถูกเก็บไว้ที่ /var/log/

1. syslog
2. auth.log
3. boot.log
4. cron.log
5. apache2/ หรือ httpd/
6. mysql/ หรือ mariadb/
7. kern.log



/var/log

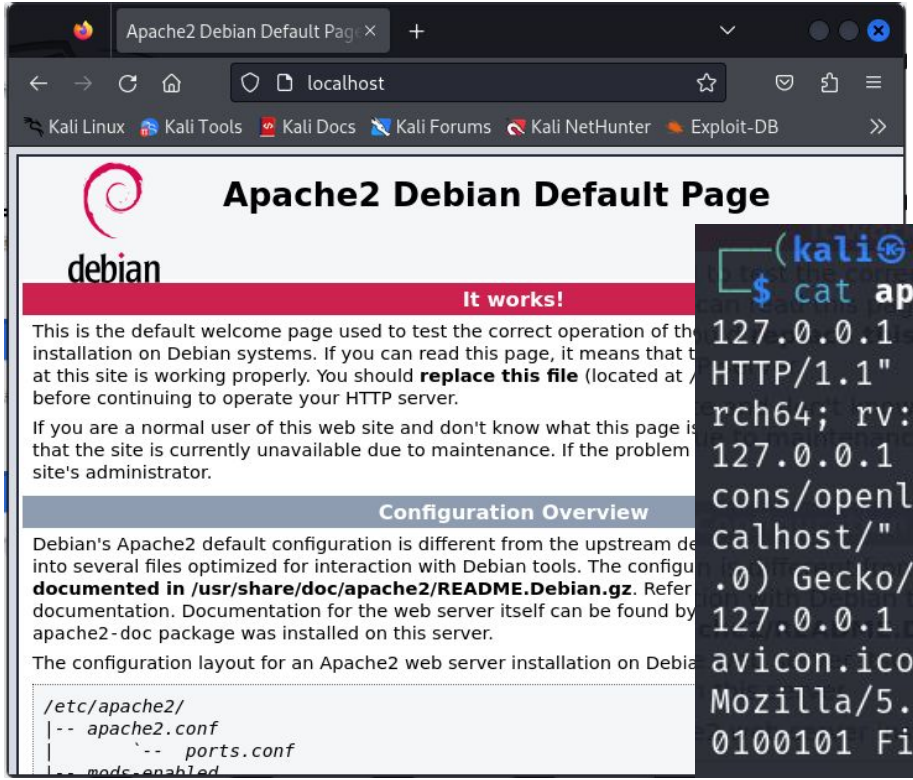
```
┌──(kali㉿kali)-[/var/log]
└─$ ls -la
total 1596
drwxr-xr-x  21 root             root             4096 Sep  7 12:34 .
drwxr-xr-x  12 root             root             4096 Sep  4 19:34 ..
lrwxrwxrwx   1 root             root               39 Sep  4 12:24 README → ../../usr/s
hare/doc/systemd/README.logs
-rw-r--r--   1 root             root            22869 Sep  7 12:35 Xorg.0.log
-rw-r--r--   1 root             root            21855 Sep  7 12:35 Xorg.1.log
-rw-r--r--   1 root             root            82365 Sep  4 12:29 alternatives.log
drwxr-x---   2 root             adm              4096 Sep  4 12:28 apache2
drwxr-xr-x   2 root             root             4096 Sep  4 12:55 apt
-rw-------   1 root             root             6531 Sep  4 19:34 boot.log
-rw-rw----   1 root             utmp                0 Sep  4 12:24 btmp
-rw-r--r--   1 root             root          1327536 Sep  4 12:55 dpkg.log
-rw-r--r--   1 root             root                0 Sep  4 12:24 faillog
-rw-r--r--   1 root             root             7354 Sep  4 12:31 fontconfig.log
drwxr-xr-x   2 _gvm             _gvm             4096 Apr 23 10:32 gvm
```

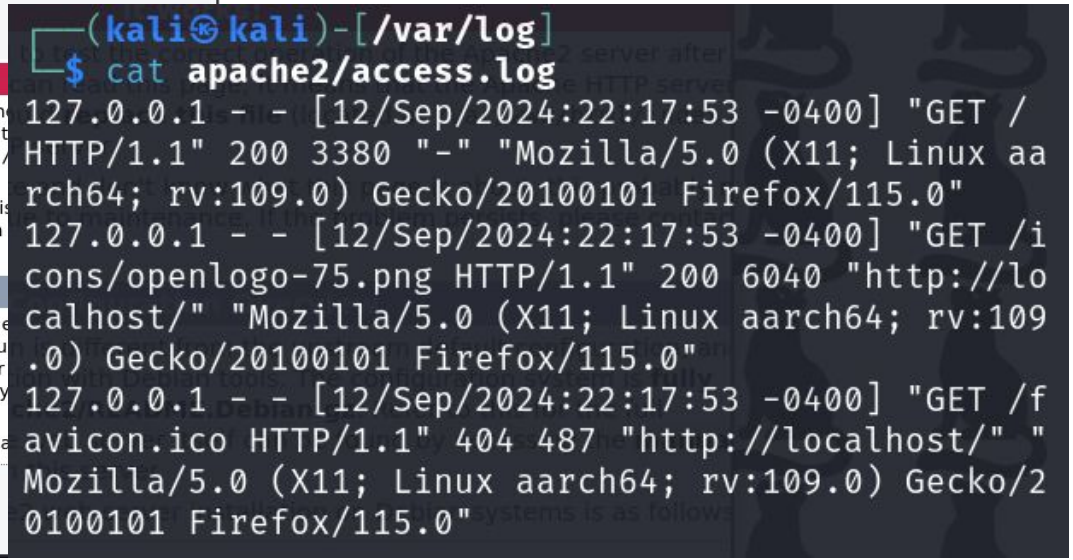
/var/log

```
┌──(kali㉿kali)-[/var/log/apache2]
└─$ ls
access.log  error.log  other_vhosts_access.log
```

```
┌──(kali㉿kali)-[/var/log]
└─$ ls -la
total 1596
drwxr-xr-x  21 root             root             4096 Sep  7 12:34 .
drwxr-xr-x  12 root             root             4096 Sep  4 19:34 ..
lrwxrwxrwx   1 root             root               39 Sep  4 12:24 README → ../../usr/s
hare/doc/systemd/README.logs
-rw-r--r--   1 root             root            22869 Sep  7 12:35 Xorg.0.log
-rw-r--r--   1 root             root            21855 Sep  7 12:35 Xorg.1.log
-rw-r--r--   1 root             root            82365 Sep  4 12:29 alternatives.log
drwxr-x---   2 root             adm              4096 Sep  4 12:28 apache2
drwxr-xr-x   2 root             root             4096 Sep  4 12:55 apt
-rw-------   1 root             root             6531 Sep  4 19:34 boot.log
-rw-rw----   1 root             utmp                0 Sep  4 12:24 btmp
-rw-r--r--   1 root             root          1327536 Sep  4 12:55 dpkg.log
-rw-r--r--   1 root             root                0 Sep  4 12:24 faillog
-rw-r--r--   1 root             root             7354 Sep  4 12:31 fontconfig.log
drwxr-xr-x   2 _gvm             _gvm             4096 Apr 23 10:32 gvm
```

ตัวอย่าง access.log





Explain Web Server Log

192.168.1.2 - - [01/Sep/2024:12:05:30 +0000] "POST /login HTTP/1.1" 302 512 "https://example.com/login" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Firefox/89.0"

Explain Web Server Log

192.168.1.2 - - → ที่อยู่ IP ของผู้ใช้ที่เข้าถึงเว็บไซต์

[01/Sep/2024:12:05:30 +0000] → วันที่และเวลาเมื่อคำขอถูกส่งไปที่เซิร์ฟเวอร์

"POST /login HTTP/1.1" → ข้อมูลเกี่ยวคำขอ HTTP ที่ถูกส่งมา (Request)

302 → สถานะการร้องขอที่ตอบกลับจากเซิร์ฟเวอร์ (Response Code)

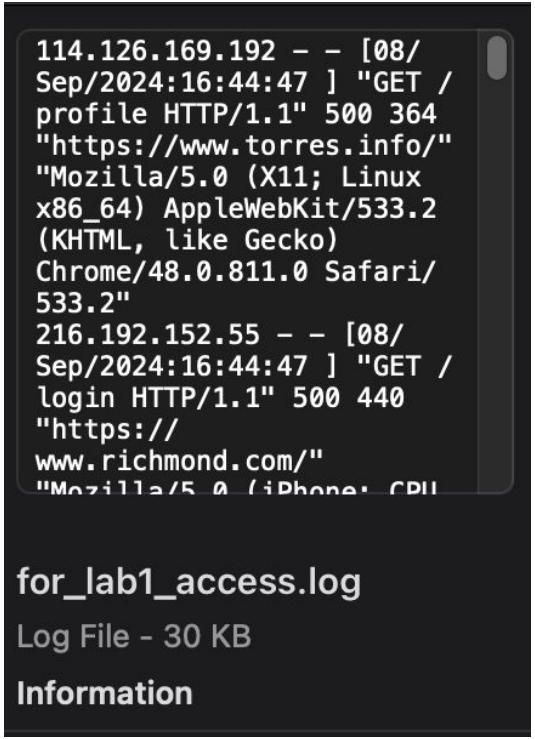
512 → ขนาดของข้อมูลที่ส่งกลับจากเซิร์ฟเวอร์ในหน่วยไบต์ (Respone Data)

"https://example.com/login" → เว็บไซต์ที่ผู้ใช้ต้องการเข้าถึง

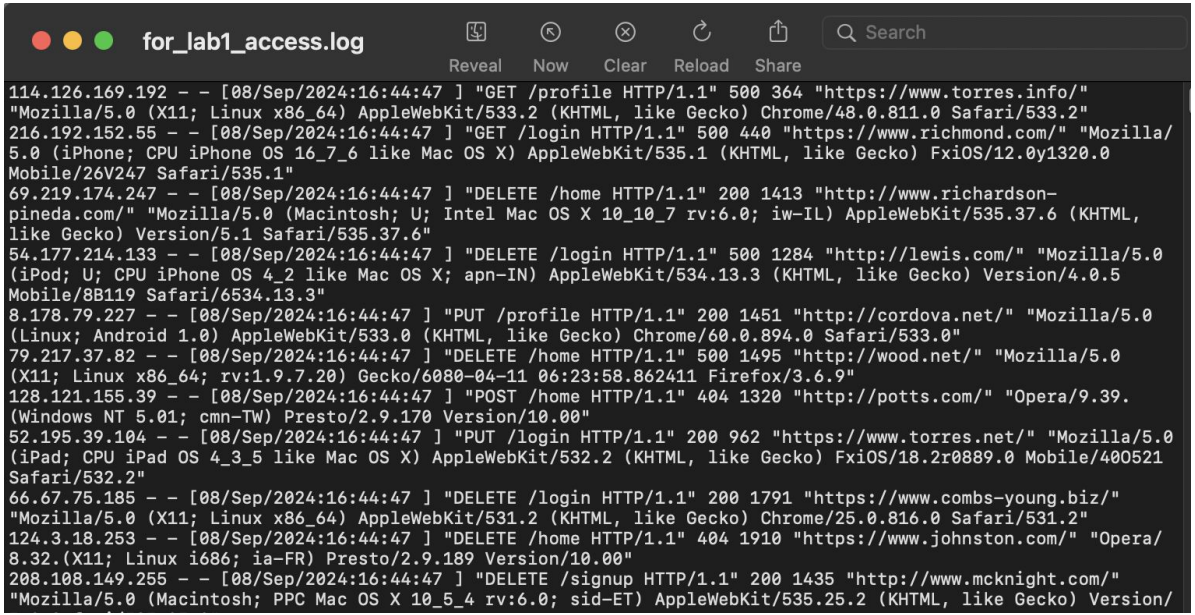
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Firefox/89.0" → User Agent: ข้อมูลเกี่ยวกับเบราว์เซอร์ที่ผู้ใช้งาน

ทำ Lab เกี่ยวกับ Log ไฟล์

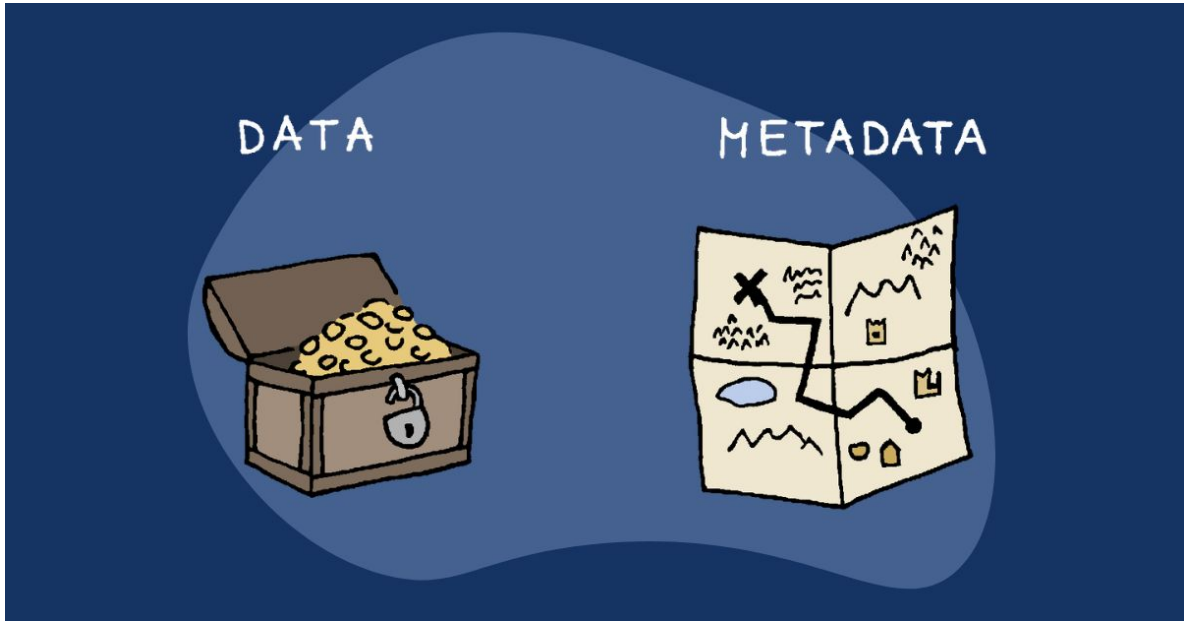
Practice Time: Log Analysis



Find the Flag in for_lab1_access.log



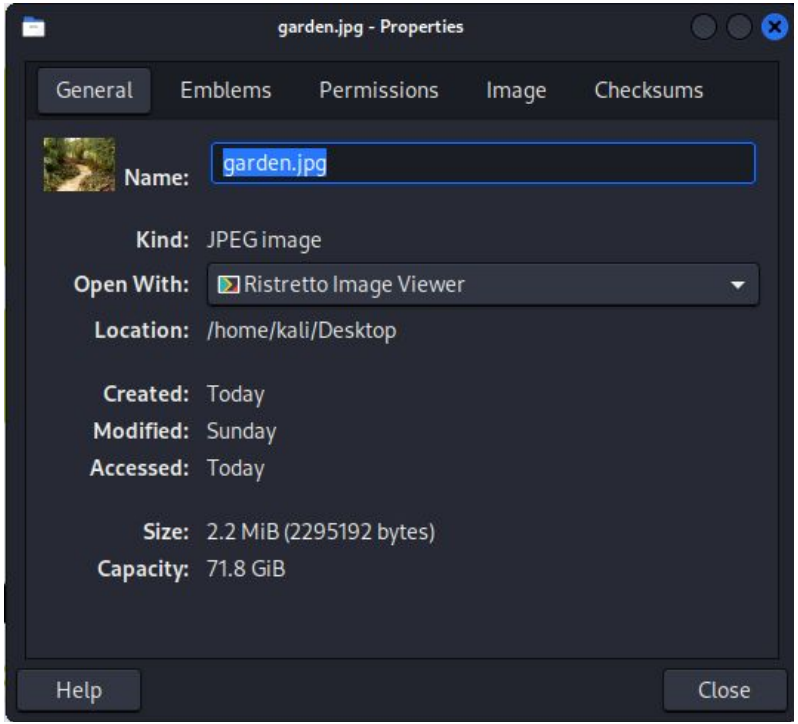
Metadata



https://dataedo.com/blog/data-vs-metadata

EXIF Data is metadata attached to photos which can include location, time, and device information.

Metadata



ที่มา: https://picoctf.org

เครื่องมือในการวิเคราะห์ Metadata

Offline Tool

- ExifTool
- Binwalk
- pdfinfo

Online Tool

- https://gchq.github.io/CyberChef/
- https://exif.tools/
- etc.

ExifTool

```
root@kali:~# exiftool -h
Syntax:  exiftool [OPTIONS] FILE

Consult the exiftool documentation for a full list of options.
```

ตัวอย่างการใช้งาน ExifTool

```
┌──(kali㉿kali)-[~/Desktop]
└─$ exiftool garden.jpg
ExifTool Version Number         : 12.76
File Name                       : garden.jpg
Directory                       : .
File Size                       : 2.3 MB
File Modification Date/Time     : 2024:09:04 13:06:45-0
4:00
File Access Date/Time           : 2024:09:09 13:31:31-0
4:00
File Inode Change Date/Time     : 2024:09:04 13:07:40-0
4:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Profile CMM Type                : Linotronic
Profile CMM Type                : Linotronic
Profile Version                 : 2.1.0
Profile Class                   : Display Device Profil
e
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 1998:02:09 06:49:00
Profile File Signature          : acsp
Primary Platform                : Microsoft Corporation
CMM Flags                       : Not Embedded, Indepen
dent
Device Manufacturer             : Hewlett-Packard
Device Model                    : sRGB
Device Attributes               : Reflective, Glossy, P
ositive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Hewlett-Packard
Profile ID                      : 0
Profile Copyright               : Copyright (c) 1998 He
wlett-Packard Company
```

ตัวอย่างคำสั่ง ExifTool

0) **แยกข้อมูลออกจากไฟล์**

```
$ exiftool a.jpg
```

1) **เขียน Metadata ลงในไฟล์**

```
$ exiftool -artist=me a.jpg
```

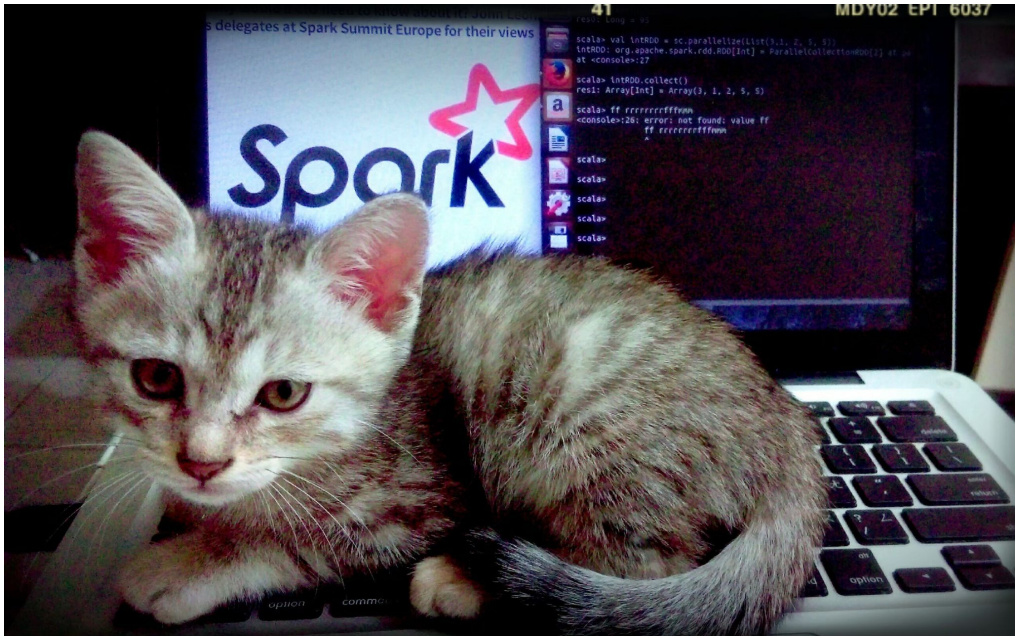
2) **เขียน Metadatas Properties ลงในไฟล์**

```
$ exiftool -artist="Phil Harvey" -copyright="2011 Phil Harvey" a.jpg
```

ดูเพิ่มเติมได้ที่: https://exiftool.org/examples.html

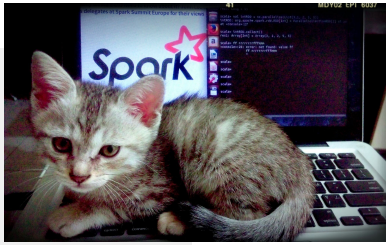
Practice Time: Information

Find the Flag in for_lab2_cat.jpg



ตัวอย่างโจทย์จาก https://picoctf.org

Practice Time: Information




```
$ exiftool for_lab2_cat.jpg
ExifTool Version Number         : 12.76
File Name                       : cat.jpg
Directory                       : .
File Size                       : 878 kB
File Modification Date/Time     : 2024:09:04 15:38:20+00:00
File Access Date/Time           : 2024:09:04 15:41:40+00:00
File Inode Change Date/Time     : 2024:09:04 15:39:40+00:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.02
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Current IPTC Digest             : 7a78f3d9cfb1ce42ab5a3aa30573d617
Copyright Notice                : PicoCTF
Application Record Version      : 4
XMP Toolkit                     : Image::ExifTool 10.80
License                         : picoCTF{ME74D47A_HIDD3N_3b9209a2}
Rights                          : PicoCTF
```

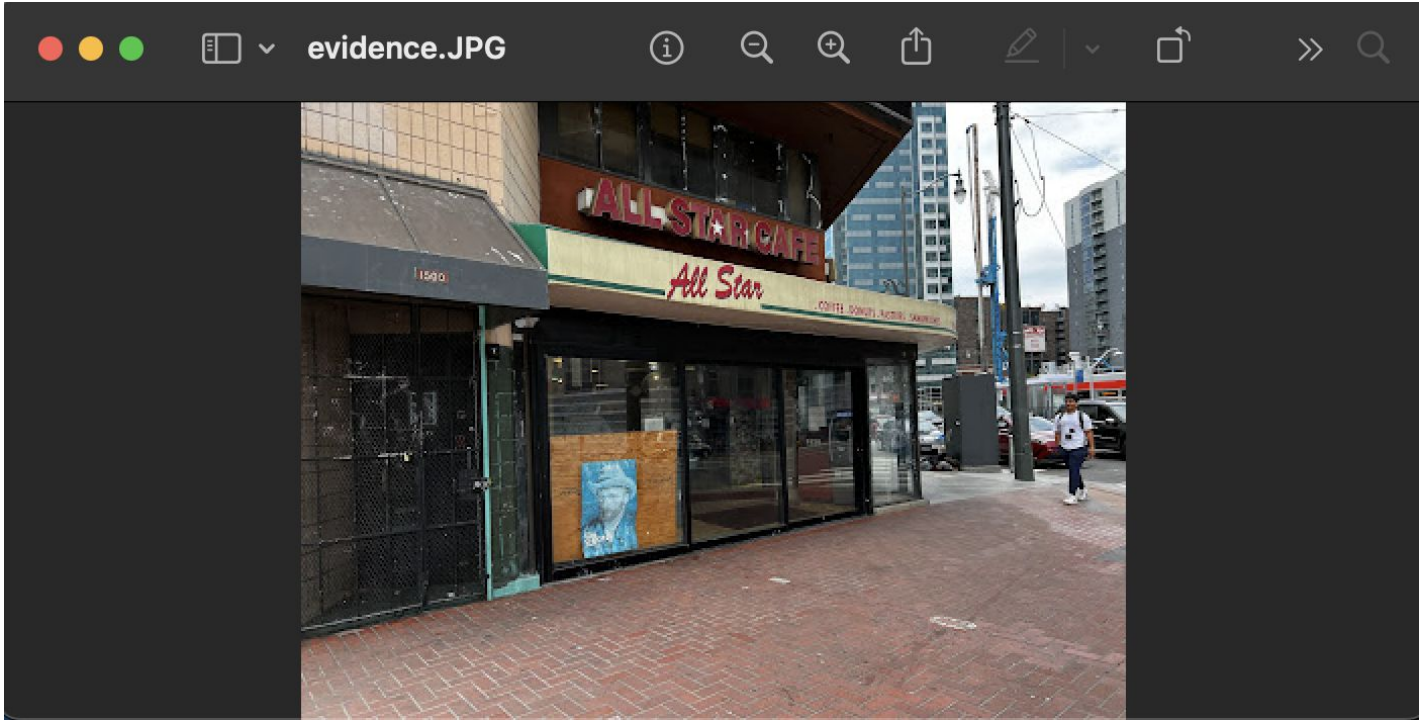
Forensics - โจทย์สมมติ

สถานการณ์:

หน่วยสืบสวนกำลังตามหาผู้ต้องสงสัยในการโจรกรรมเงินจำนวนมหาศาล ผู้ต้องสงสัยหนีไปพร้อมกับเงินและได้หลบซ่อนตัว โดยใช้รถยนต์เป็นพาหนะ ข้อมูลเพียงอย่างเดียวที่ตำรวจมีคือรูปถ่ายหนึ่งรูปที่ถ่ายจากกล้องมือถือในวันเกิดเหตุ อย่างไรก็ตาม พิกัด GPS จากรูปนั้นอาจเป็นเบาะแสสำคัญที่จะนำไปสู่สถานที่ที่ผู้ต้องสงสัยกำลังใช้รถยี่ห้อ Toyota ในการหลบหนีแต่ไม่ทราบรุ่นของรถ

Forensics - โจทย์สมมติ

หลักฐานจากโจทย์ evidence.jpg



Forensics - โจทย์สมมติ

ใช้ exiftool เพื่อดู Metadata ของหลักฐาน

```
$ exiftool evidence.JPG
ExifTool Version Number         : 12.76
File Name                       : evidence.JPG
Directory                       : .
File Size                       : 59 kB
File Modification Date/Time     : 2024:09:13 15:15:30-04:00
File Access Date/Time           : 2024:09:13 15:15:30-04:00
File Inode Change Date/Time     : 2024:09:13 15:15:30-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
```

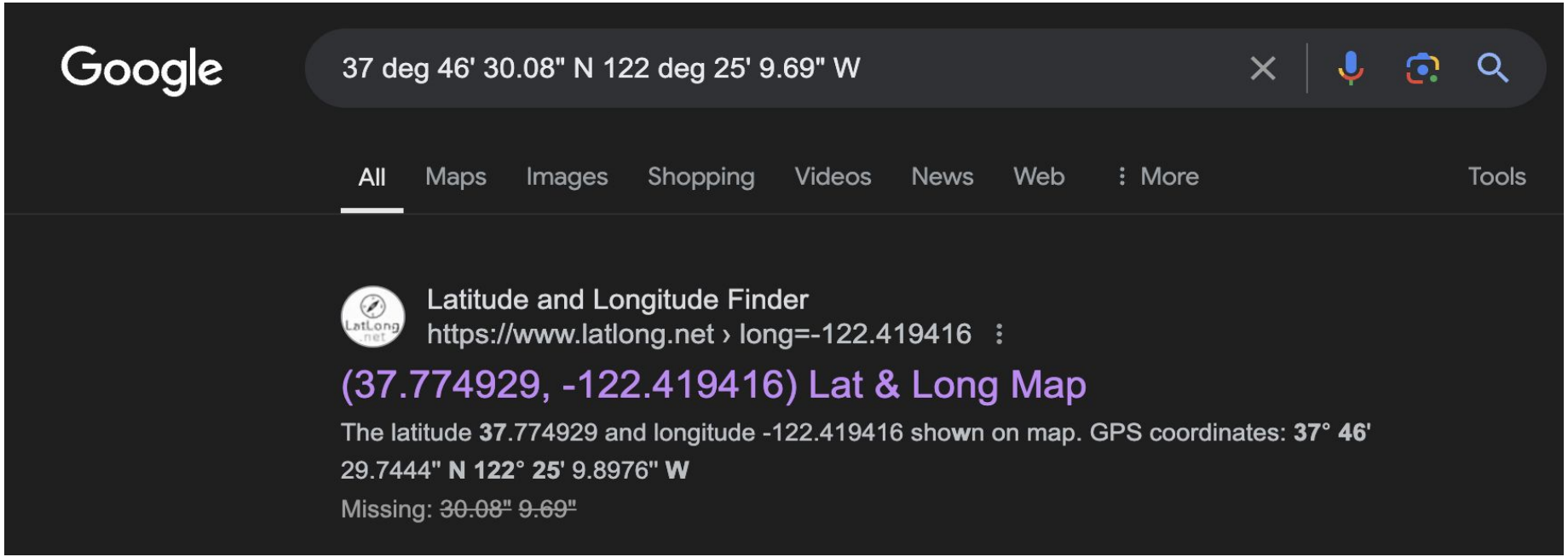
Forensics - โจทย์สมมติ

ใช้ exiftool เพื่อดู Metadata ของหลักฐาน

```
GPS Version ID                  : 2.3.0.0
GPS Latitude Ref                : North
GPS Longitude Ref               : West
Image Width                     : 408
Image Height                    : 306
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 408x306
Megapixels                      : 0.125
GPS Latitude                    : 37 deg 46' 30.08" N
GPS Longitude                   : 122 deg 25' 9.69" W
GPS Position                    : 37 deg 46' 30.08" N, 122 deg 25' 9.69" W
```

Forensics - โจทย์สมมติ

ค้นหา พิกัด GPS บน Google Search

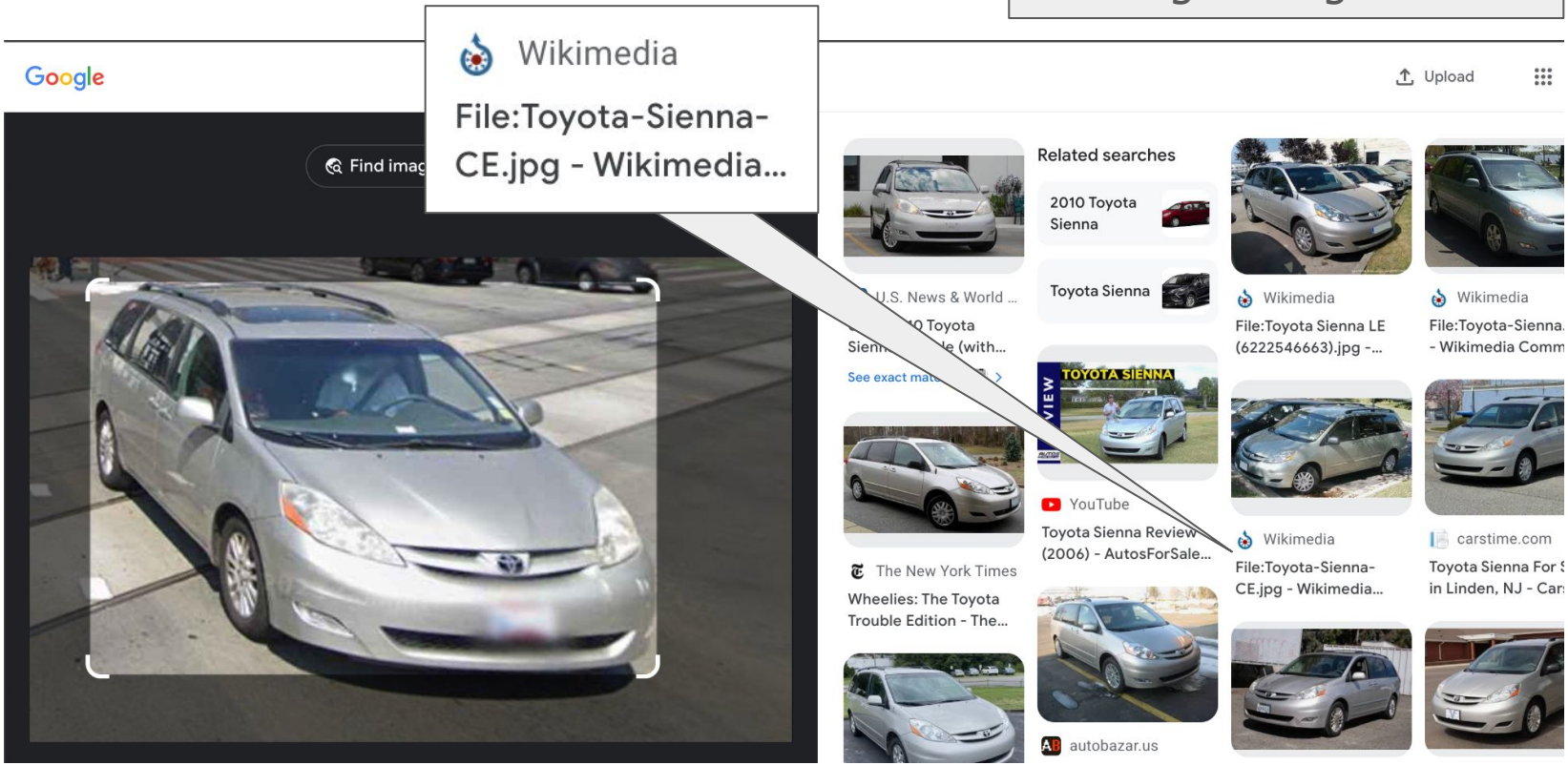


Forensics - โจทย์สมมติ

ค้นหา พิกัด GPS บน Google Map

Forensics - โจทย์สมมติ

ใช้ Google Image Search



File Format

File Format

ที่มา: https://www.thebrandcollective.co.za

File Format

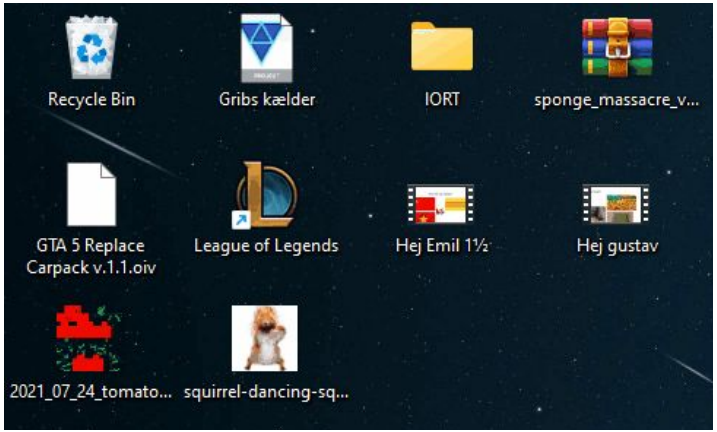
note.txt

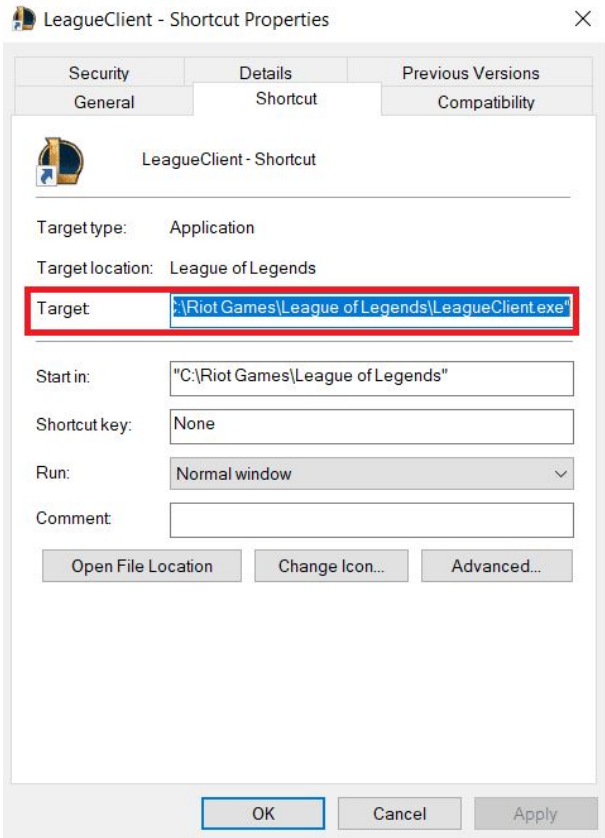
```
1  Hello, world
2
3  This is my first text.
4
5
```

File Format


.EXE


PARTY
HOME
TFT
CLASH
SR - NORMAL DRAFT
doublelift
Riot kuniso
Tewtsmagewts
Barackprobama
Julie Beanz
FIND MATCH

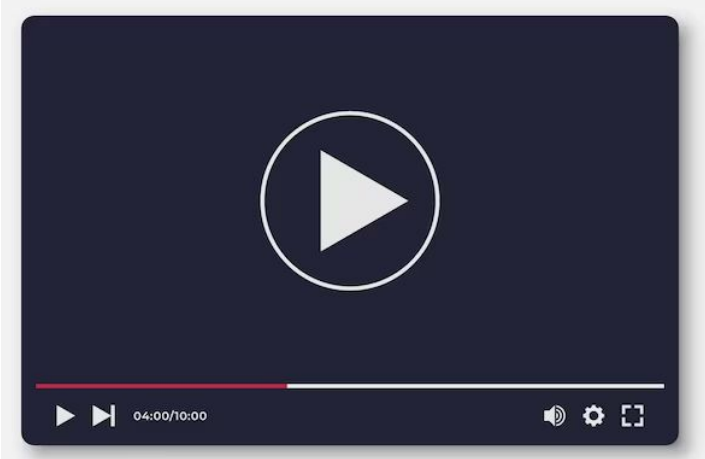

Recycle Bin
Gribs kælder
IORT
sponge_massacre_v...
GTA 5 Replace Carpack v.1.1.oiv
League of Legends
Hej Emil 1½
Hej gustav
2021_07_24_tomato...
squirrel-dancing-sq...


LeagueClient - Shortcut Properties
Security
Details
Previous Versions
General
Shortcut
Compatibility
LeagueClient - Shortcut
Target type: Application
Target location: League of Legends
Target: :\Riot Games\League of Legends\LeagueClient.exe"
Start in: "C:\Riot Games\League of Legends"
Shortcut key: None
Run: Normal window
Comment:
Open File Location
Change Icon...
Advanced...
OK
Cancel
Apply

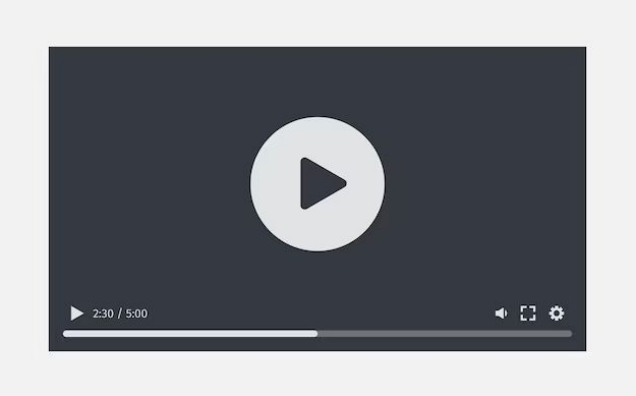
File Format

garden.jpg

File Format

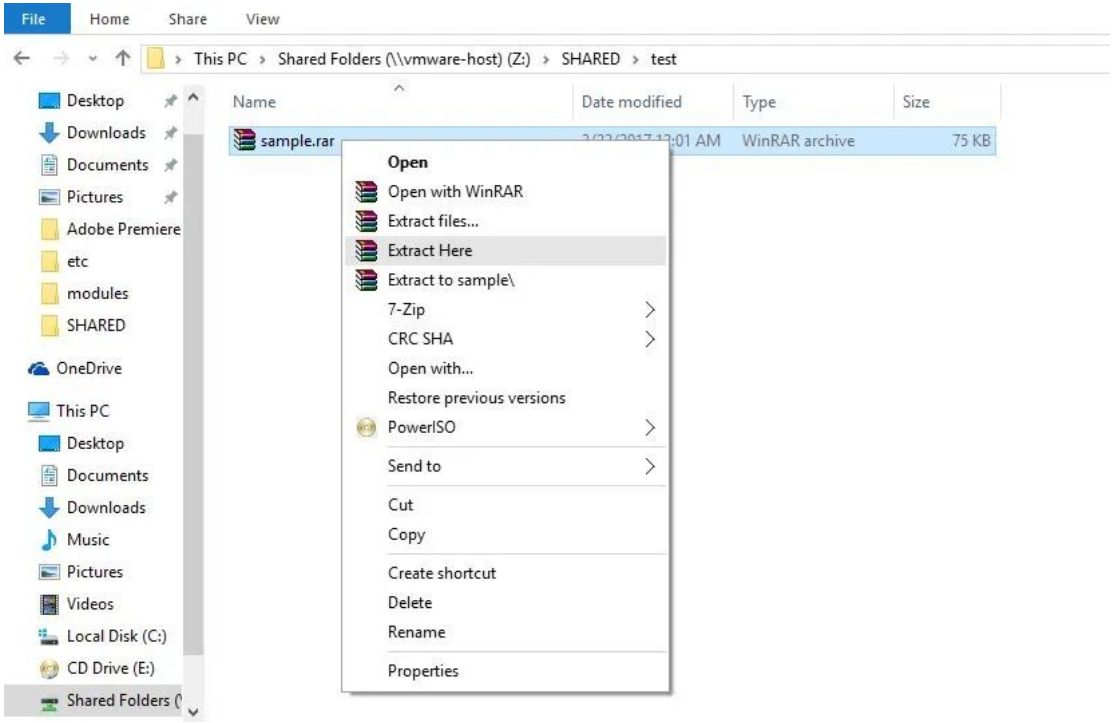


ที่มา: https://www.freepik.com

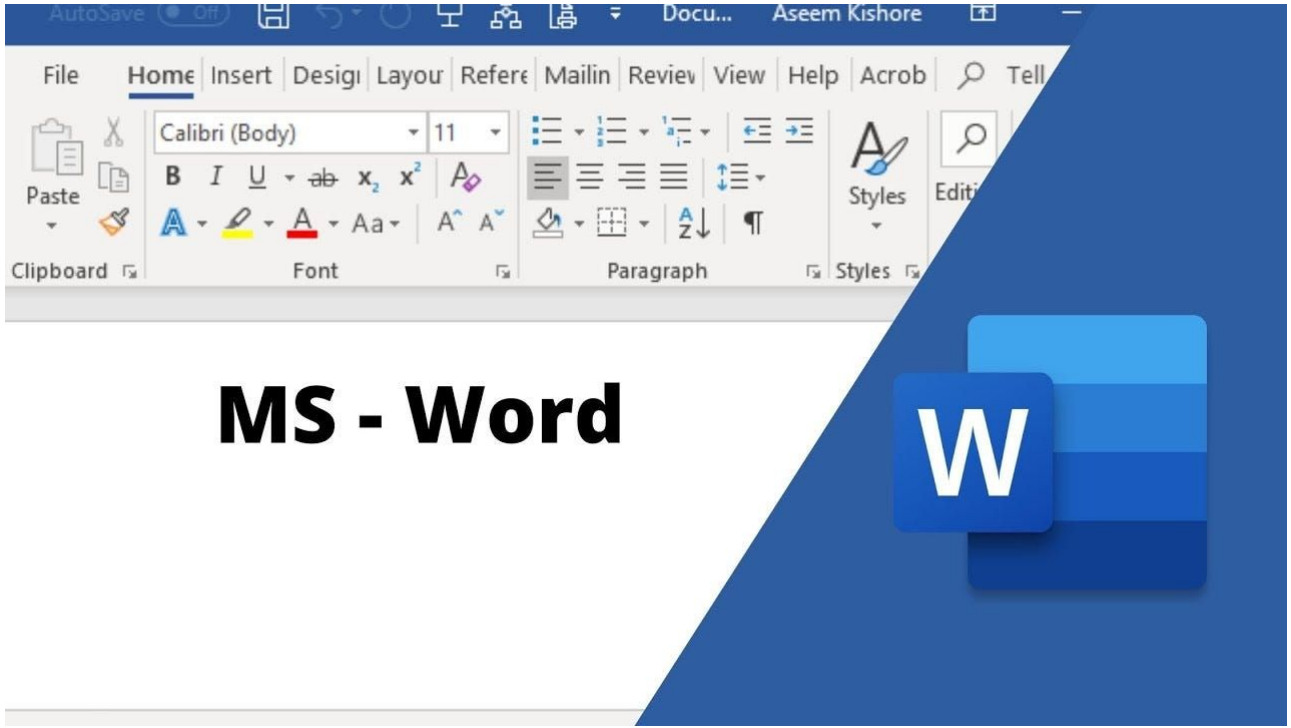


File Format


.RAR
.ZIP


File
Home
Share
View
This PC › Shared Folders (\\vmware-host) (Z:) › SHARED › test
Desktop
Downloads
Documents
Pictures
Adobe Premiere
etc
modules
SHARED
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CD Drive (E:)
Shared Folders (
Name
Date modified
Type
Size
sample.rar
WinRAR archive
75 KB
Open
Open with WinRAR
Extract files...
Extract Here
Extract to sample\
7-Zip
CRC SHA
Open with...
Restore previous versions
PowerISO
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties

File Format



ที่มา: https://medium.com/@naira-nicol

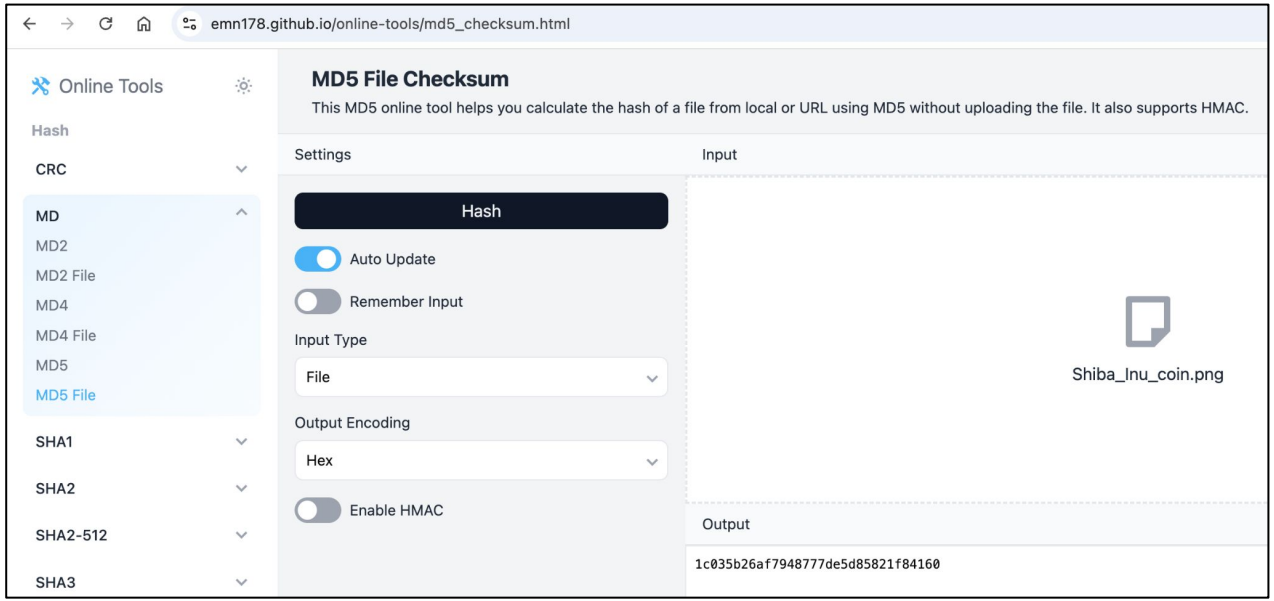
เครื่องมือที่ใช้ในการวิเคราะห์ File Format

Offline Tool

- Hex Editor
- ExifTool
- File
- Checksum
  - md5sum
  - sha1sum
  - sha256sum
  - etc.

Online Tool

- https://gchq.github.io/CyberChef/
- https://emn178.github.io/online-tools/md5_checksum.html



File command

```
┌──(kali㉿kali)-[~/Desktop]
└─$ file cat.jpg
cat.jpg: JPEG image data, JFIF standard 1.02, aspect ratio, density
1×1, segment length 16, Exif Standard: [TIFF image data, big-endian,
 direntries=5, xresolution=74, yresolution=82, resolutionunit=1, cop
yright=Hello, World], baseline, precision 8, 2560×1598, components 3
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ file admin.php
admin.php: PHP script, ASCII text
```

File command

```
┌──(kali㉿kali)-[~/Desktop]
└─$ file info.pdf
info.pdf: PDF document, version 1.3, 1 page(s)
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ file archive.zip
archive.zip: Zip archive data, at least v2.0 to extract, compression
 method=deflate
```

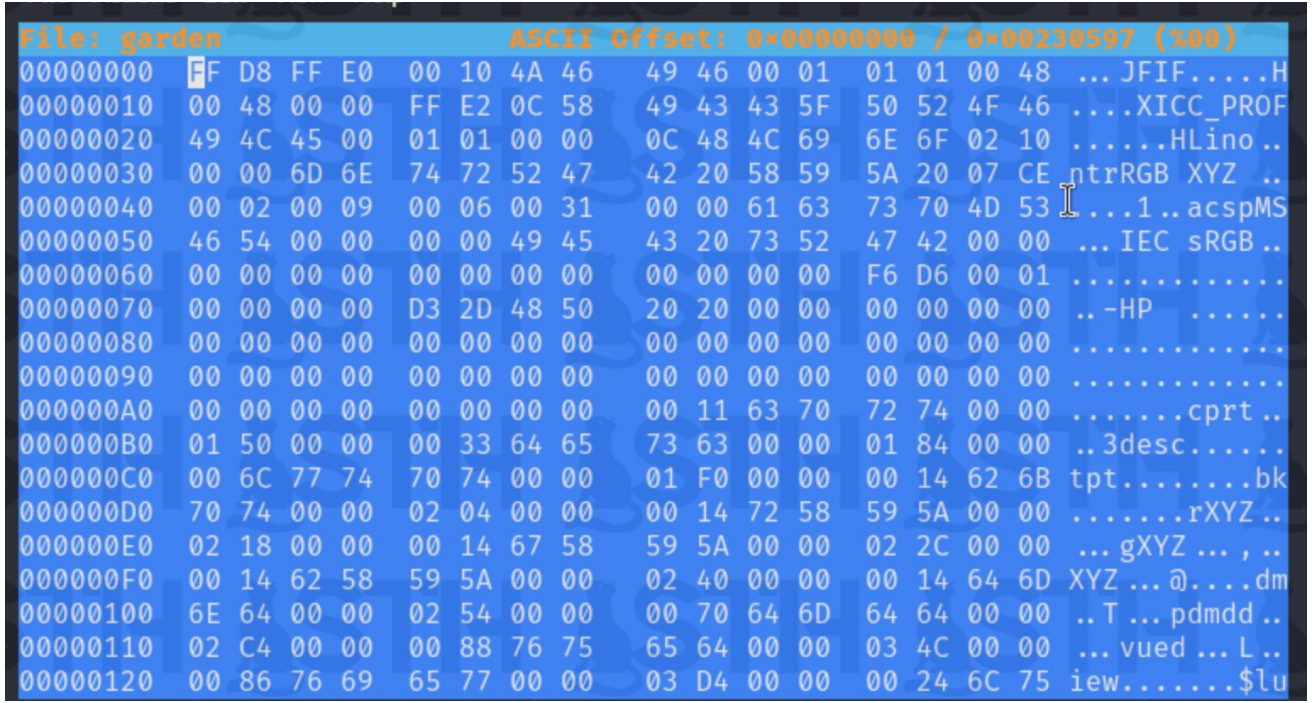
File Signature

Hex signature	ISO 8859-1	Offset	Extension	Description
23 21	#!	0		Script or data to be passed to the program following the shebang (#!)[1]
02 00 5a 57 52 54 00 00 00 00 00 00 00 00 00 00	STX NUL ZWRT NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL NUL	0	cwk	Claris Works word processing doc
00 00 02 00 06 04 06 00 08 00 00 00 00 00	NUL NUL STX NUL ACK EOT ACK NUL BS NUL NUL NUL NUL NUL	0	wk1	Lotus 1-2-3 spreadsheet (v1) file
25 50 44 46 2D	%PDF–	0	pdf	PDF document[34]
30 26 B2 75 8E 66 CF 11 A6 D9 00 AA 00 62 CE 6C	0&²uŽfÏ DC1 ¦Ù NUL ª NUL bÎl	0	asf wma wmv	Advanced Systems Format[35]

https://en.wikipedia.org/wiki/List_of_file_signatures

Hex Editor

$ hexeditor garden



File Signature

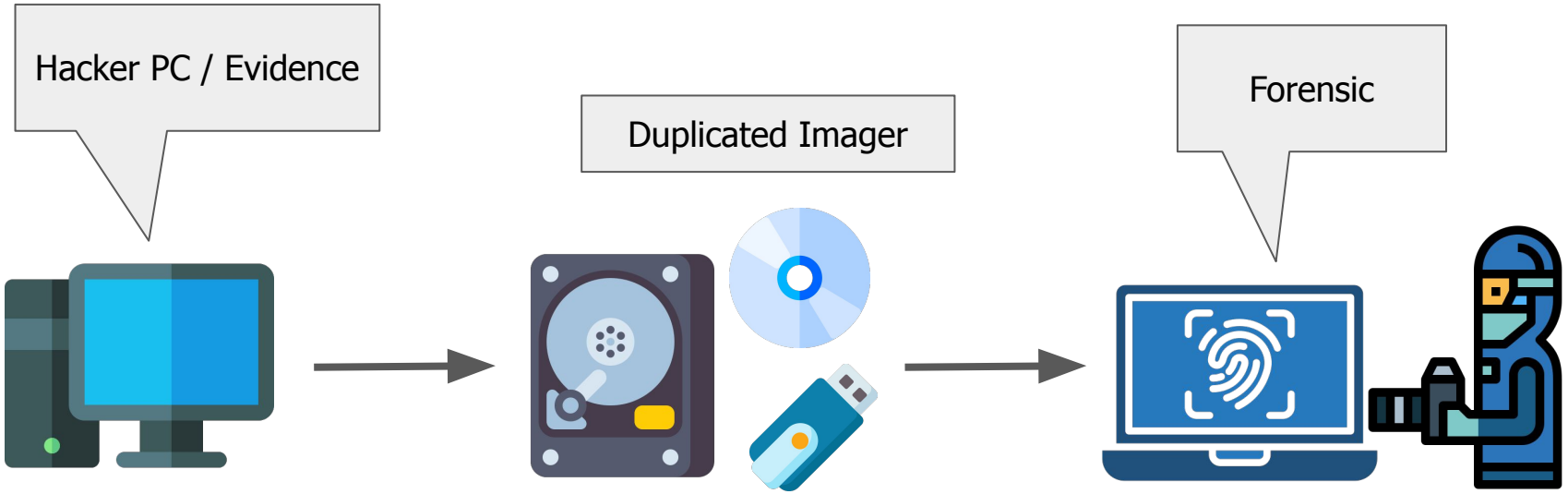
FF D8 FF DB	ÿØÿÛ	0	jpg jpeg	JPEG raw or in the JFIF or Exif file format[16]
FF D8 FF E0 00 10 4A 46 49 46 00 01	ÿØÿà NUL DLE JFIF NUL SOH			
FF D8 FF EE	ÿØÿî			
FF D8 FF E1 ?? ?? 45 78 69 66 00 00	ÿØÿá??Exif NUL NUL			
FF D8 FF E0	ÿØÿà	0	jpg	JPEG raw or in the JFIF or Exif file format[16]

ทำไม File Format และ File Signature ถึงสำคัญ?

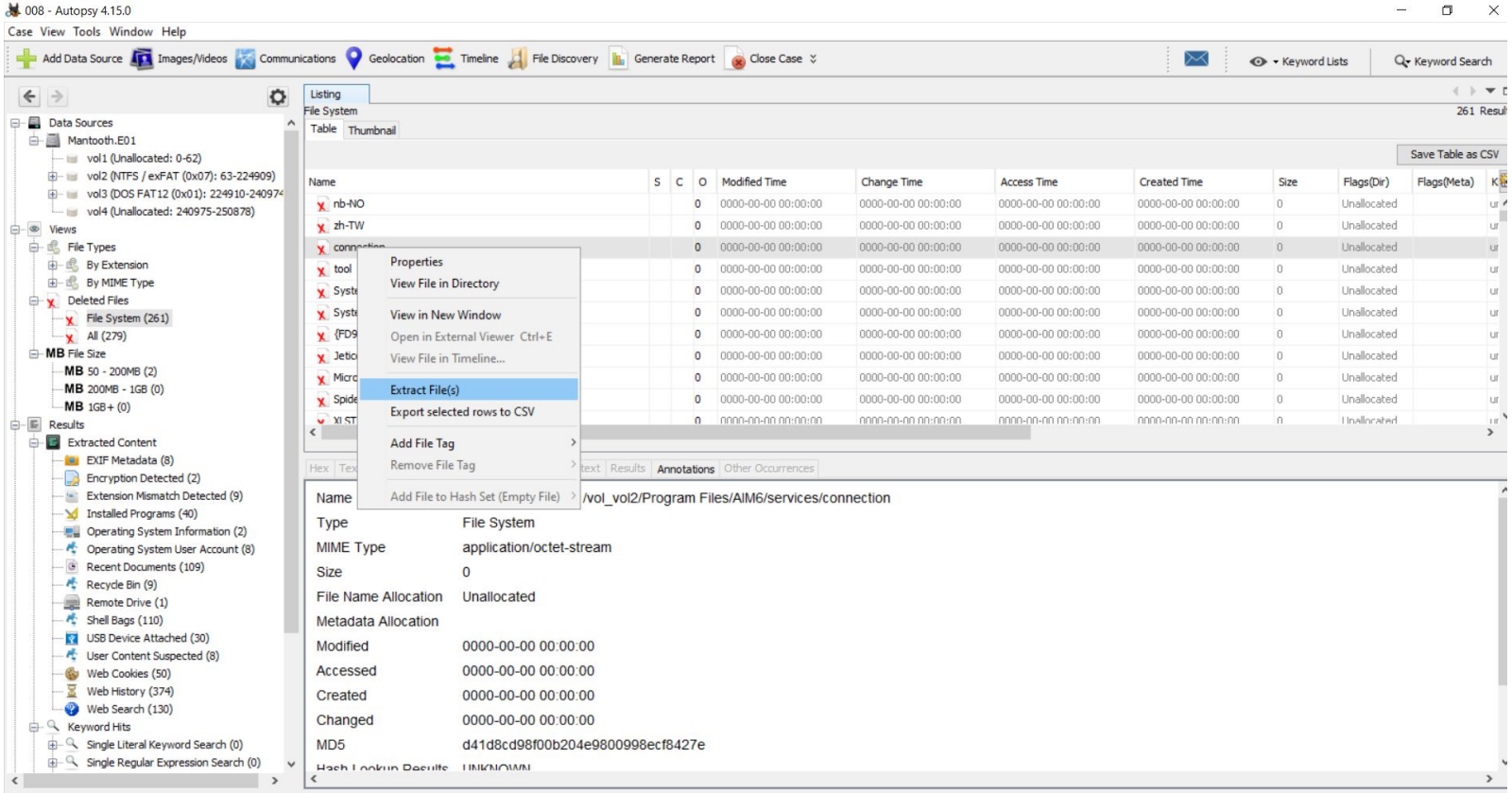
- ระบุประเภทของไฟล์
- ตรวจสอบความถูกต้องของไฟล์
- กู้คืนข้อมูล
- ตรวจสอบความปลอดภัย

Disk Imaging

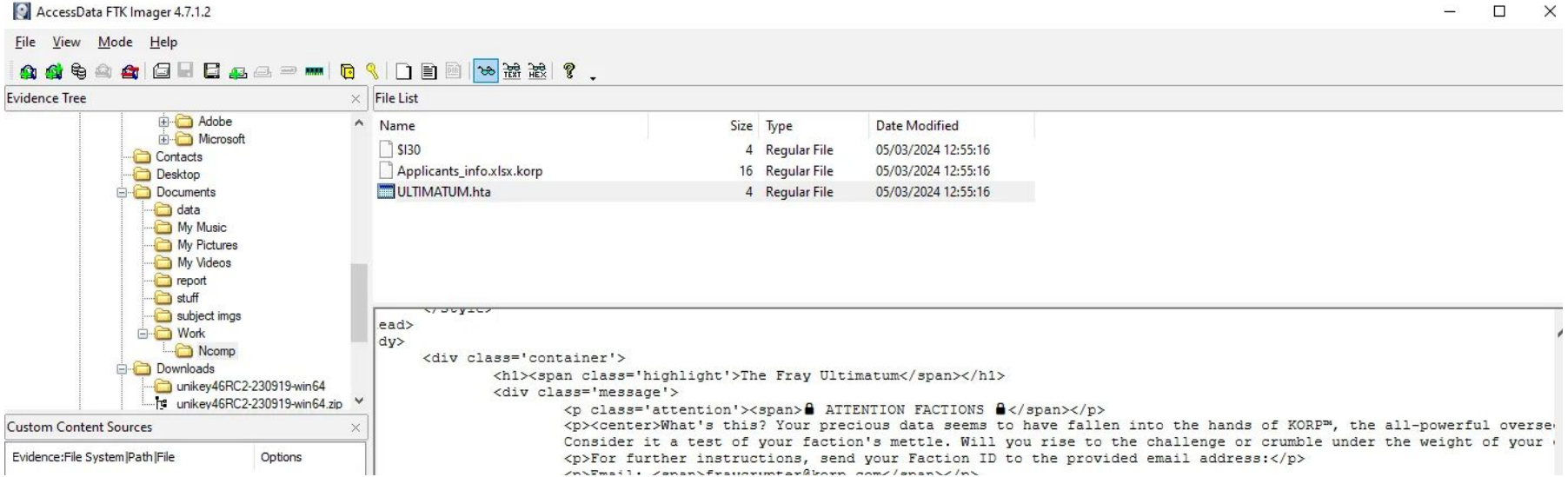
Disk Imaging



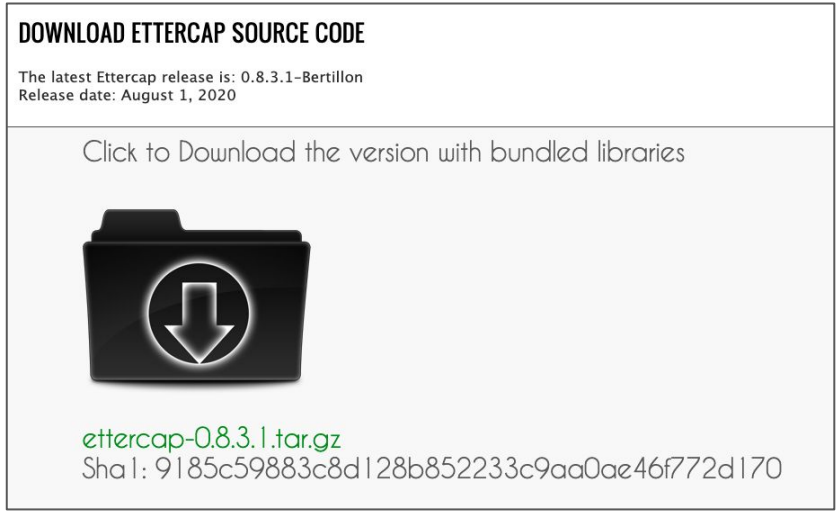
ตัวอย่าง Autopsy



ตัวอย่าง FTK Imager



File hash (Checksum)



1. ตรวจสอบความสมบูรณ์ของไฟล์
2. ช่วยในการยืนยันว่าไฟล์ที่ดาวน์โหลดมาจากแหล่งที่มาที่เชื่อถือได้

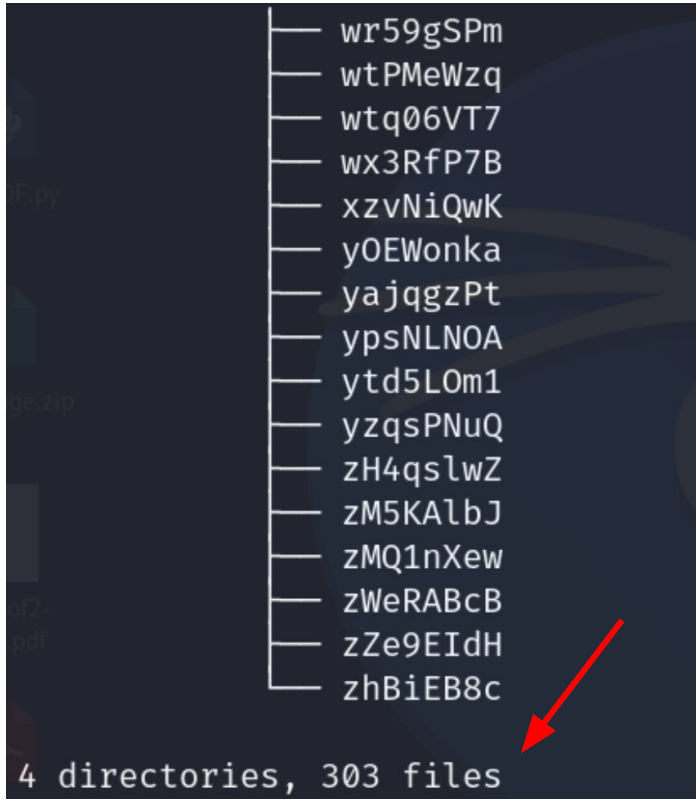
PREVIOUS VERSIONS

Release Date	FileName	Version	Sha-1 Hash
Jul 1, 2019	ettercap-0.8.3.tar.gz	0.8.3-Bertillon	1db39315b2b2b574dc1eb3f7ae72871ad2391e2f
Jul 1, 2019	ettercap-0.8.3.tar.gz (source only)	0.8.3-Bertillon	90f2a397966d721868a1fb49c5ecaba0f0af72d0
Mar 14, 2015	ettercap-0.8.2.tar.gz	0.8.2-Ferri	7e528632ca01c5977da1a0af56a5e05fbc383832
Mar 14, 2015	ettercap-0.8.2.tar.gz (source only)	0.8.2-Ferri	04f50925a5f3b2555371075a048ab7bfe3892976
Oct 16, 2014	ettercap-0.8.1.tar.gz	0.8.1-Lombroso	66362ce69cd9b82b9eb8ea6a52048700704a7d9b
Oct 16, 2014	ettercap-0.8.1.tar.gz (source only)	0.8.1-Lombroso	1179923d94954cd6e00117c3492c4ca3991bc401
Sep 21, 2013	ettercap-0.8.0.tar.gz	0.8.0-Lacassagne	008fca94bbd67b578699300eb321766cd41fbfff
Mar 26, 2013	ettercap-0.7.6.tar.gz	0.7.6-Locard	55818952a8c28beb1b650f3ccc9600a2d784a18f

3. การป้องกันการปลอมแปลง
4. ใช้ในการตรวจจับข้อผิดพลาดที่อาจเกิดขึ้นระหว่างการถ่ายโอนข้อมูล

Forensic Lab 3 : Verify

ตัวอย่างโจทย์จาก
https://picoctf.org



Identification

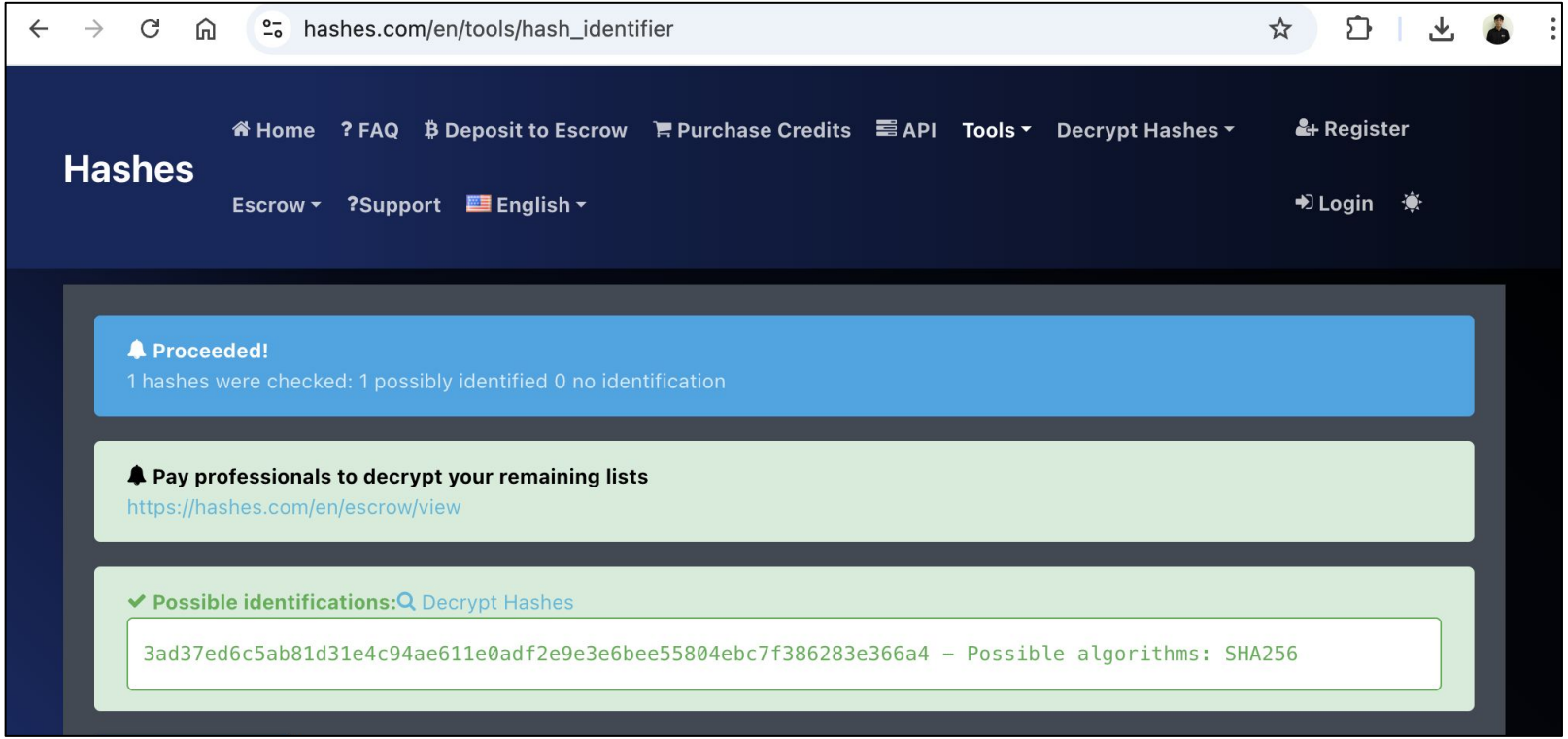
?

DATA

```
┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ cat checksum.txt
3ad37ed6c5ab81d31e4c94ae611e0adf2e9e3e6bee55804ebc7f386283e366a4

┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ cat files/0agQiFLS
RliF1vdIPAyu97ed5JRBhtZkNAuMHAEo1lthk9ky87Z6qdpqNhHUQEul2zxx9zY

┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ cat files/0pEkV2ds
KRhaBTB9ByUUwhhLbbHvOybGIwoO7QXHLRKgDAcYYpGiisJ5mKUz623IMNxN6HJ

┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ cat files/0wWA41ot
6f28qnMeSfYMP6Sq0XVshA99u4obPxptpqkBXXamzmOfhRLHdGKoeqKJIM6otSl
```

Hash Identifier

https://hashes.com/en/tools/hash_identifier



hashid

```
┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ hashid "3ad37ed6c5ab81d31e4c94ae611e0adf2e9e3e6bee55804ebc7f386283e366a4"
Analyzing '3ad37ed6c5ab81d31e4c94ae611e0adf2e9e3e6bee55804ebc7f386283e366a4'
[+] Snefru-256
[+] SHA-256
[+] RIPEMD-256
[+] Haval-256
[+] GOST R 34.11-94
[+] GOST CryptoPro S-Box
[+] SHA3-256
[+] Skein-256
[+] Skein-512(256)
```

sha256sum

```
┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ sha256sum files/0agQiFLS
885ac35e179e1b2746dcd163d980938090168c594dd7567bf1d60bdd11557df1  files/0agQiFLS
```

```
┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ ls files/
0agQiFLS  8cSetvuU  FmmWrIZ7  MwfNVxMB  SXltVhZT  XrAdESZl  covwBpER  kLFFhUci  t3YK8diU
0pEkV2ds  8sqe8FVs  GhWI4eJh  MzdMfZHa  SbFIvoSj  XrvFYdDg  cxKJcozU  l4lFl66y  tLG9HM3a
0wWA41ot  92q4JPFx  GkM1UPTw  NFea6BFS  SkQZlbB2  Xw38pYK0  dINee6RV  lUsUQJ4B  uJzNSw96
0yVzp2am  9EMX68VB  GoGhbQto  NgY5gymg  TBQytfqs  Xxuckerf  dS2gaUE4  m2KQa1Hp  uQyUDnOZ
12GUEFi0  9nlUSB5k  GodaoG3e  NopiZGwa  TSJCXwIT  Y4u4wEGY  dVJ9IeAT  m5cOAhxS  v6LGqmwI
12R70dbh  A0aXQwRy  H3rLRpMi  O2eRM15N  TTjLO7LQ  YCf9VpOR  dZVnOthw  mVEKZ3oW  v8sVJPvD
1EQhRC4i  AKEjqj8u  HG1OKGnm  OVCZKr6X  ThekmVcy  YG1pCKDt  dkV6p1DF  mcjegRRr  vCUbox39
1FjaHS3F  AeCM4Vvt  HPGHI002  OX3IlkB9  TqHFzH54  YPNiaCgG  dtc6oz6G  n05ZtlwX  vTgToTLG
1cYEYb6L  AhVRy5sU  HRSTilo9  OYpH5Rfs  Tui6wJfr  YdulsHwq  e018b574  n7C2bpPk  vfN94Ek3
1iXLQGXR  Aqg5GrWn  HchfFzCW  Opx3E3FO  TwspwefZ  YdxjMT1r  e7irOvB1  nDjOINiw  vnr7vUto
```

sha256sum

```
┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ sha256sum files/*
885ac35e179e1b2746dcd163d980938090168c594dd7567bf1d60bdd11557df1  files/0agQiFLS
d3cdff8222104727892c6c5f306efccec1ebe53e1510b575dabf838e5c17619b  files/0pEkV2ds
a67c3339a9661ea181bf073e543b47580011bd210b3306497a4ae8c9a2124bd7  files/0wWA41ot
2940827966c3d8b31f87ab008d471dffb0f80c918a669eb34d00909adaf4d406  files/0yVzp2am
645e24226aa77f498951e38713e103659fb7bb41ceccf7cc6268c226ad03d4b9  files/1EQhRC4i
441db2a78012080ec0c3b80d2b5b6d66720297b65db195ead59ea646a0674c6e  files/1FjaHS3F
5170556dbf37f1aab8cb439c7fd8f3e56f8e4aa41ee2e86379ef4190f7623b6f  files/1cYEYb6L
bf5e0d888b16e034331f90067b41834ae50673d9dcffa4c76ee4416836cbe919  files/1iXLQGXR
8313a303c94d4fd615073aedded65df0cdee87d5fd074c25c847b064291ff4b3  files/2hOQXHZC
d63d4ee0d986694f4df69960d5c54c8ea8c3822dd5b5be1065406bb9c03b8a6c  files/2nsMaCTj
16bda5067a52a32595ac140466be993b585c75b0557e012ec874ac813fdd73fd  files/2zpsEiQJ
99c46603b95fcb29d95bc71106fadb95df93182e119097522d8d9efc823b4ef0  files/3BrlDAbo
807309a496177fd97eae436d0158e21cc5f15ee43adc6a0275015e8785c7e4e1  files/3PmKbHhH
```

Step to Verify

```
┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ sha256sum files/* > checksum-all-file.txt

┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ ls
checksum-all-file.txt  checksum.txt  decrypt.sh  files

┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ cat checksum.txt
3ad37ed6c5ab81d31e4c94ae611e0adf2e9e3e6bee55804ebc7f386283e366a4

┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ cat checksum-all-file.txt | grep "3ad37ed6c5ab81d31e4c94ae611e0adf2e9e3e6bee55804ebc7
86283e366a4"
3ad37ed6c5ab81d31e4c94ae611e0adf2e9e3e6bee55804ebc7f386283e366a4  files/e018b574
```

Step to Verify

```
┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ ls
checksum-all-file.txt  checksum.txt  decrypt.sh  files

┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ cp files/e018b574 .

┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ ls
checksum-all-file.txt  checksum.txt  decrypt.sh  e018b574  files

┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ ./decrypt.sh e018b574
Error: 'e018b574' is not a valid file. Look inside the 'files' folder with 'ls -R'!

┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ cat e018b574
Salted__◆m◆uI◆◆◆◆8◆◆;◆Z◆q◆E◆+L◆◆◆◆◆G(%Al6q?k◆◆◆◆◆◆◆◆$◆qE◆
```

Step to Verify

```
        # Check if the provided argument is a file and not a folder
        if [ ! -f "/home/ctf-player/drop-in/$file_name" ]; then
            echo "Error: '$file_name' is not a valid file. Look inside the 'files' folder with 'ls -R'!"
            exit 1
        fi

        # If there's an error reading the file, print an error message
        if ! openssl enc -d -aes-256-cbc -pbkdf2 -iter 100000 -salt -in "/home/ctf-player/drop-in/$file_na
" -k picoCTF; then
            echo "Error: Failed to decrypt '$file_name'. This flag is fake! Keep looking!"
        fi


┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$

┌──(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
└─$ openssl enc -d -aes-256-cbc -pbkdf2 -iter 100000 -salt -in e018b574 -k picoCTF
picoCTF{trust_but_verify_e018b574}
```

Thank you !!

แถม !!!!

Binwalk

```
┌──(kali㉿kali)-[~/Desktop]
└─$ binwalk dolls.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0×0             PNG image, 594 x 1104, 8-bit/color RGBA, non-interlaced
3226          0×C9A           TIFF image data, big-endian, offset of first image director
y: 8
272492        0×4286C         Zip archive data, at least v2.0 to extract, compressed size
: 378954, uncompressed size: 383938, name: base_images/2_c.jpg
651612        0×9F15C         End of Zip archive, footer length: 22
```

```
Exif Image Height               : 1104
Pixels Per Unit X               : 5669
Pixels Per Unit Y               : 5669
Pixel Units                     : meters
XMP Toolkit                     : XMP Core 5.4.0
Apple Data Offsets              : (Binary data 28 bytes, use -b option to extract)
Warning                         : [minor] Trailer data after PNG IEND chunk
Image Size                      : 594×1104
Megapixels                      : 0.656
```

Binwalk

```
┌──(kali㉿kali)-[~/Desktop]
└─$ unzip dolls.jpg
Archive:  dolls.jpg
warning [dolls.jpg]:  272492 extra bytes at beginning or within zipfile
  (attempting to process anyway)
  inflating: base_images/2_c.jpg
```

```
┌──(kali㉿kali)-[~/Desktop/base_images]
└─$ binwalk 2_c.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0×0             PNG image, 526 x 1106, 8-bit/color RGBA, non-interlaced
3226          0×C9A           TIFF image data, big-endian, offset of first image director
y: 8
187707        0×2DD3B         Zip archive data, at least v2.0 to extract, compressed size
: 196043, uncompressed size: 201445, name: base_images/3_c.jpg
383805        0×5DB3D         End of Zip archive, footer length: 22
383916        0×5DBAC         End of Zip archive, footer length: 22
```

Binwalk

```
┌──(kali㉿kali)-[~/Desktop/base_images/base_images]
└─$ ls
3_c.jpg

┌──(kali㉿kali)-[~/Desktop/base_images/base_images]
└─$ binwalk 3_c.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0×0             PNG image, 428 x 1104, 8-bit/color RGBA, non-interlaced
3226          0×C9A           TIFF image data, big-endian, offset of first image directory:
123606        0×1E2D6         Zip archive data, at least v2.0 to extract, compressed size:
essed size: 79807, name: base_images/4_c.jpg
201423        0×312CF         End of Zip archive, footer length: 22
```

Binwalk

```
┌──(kali㉿kali)-[~/Desktop/base_images/base_images/base_images]
└─$ unzip 4_c.jpg
Archive:  4_c.jpg
warning [4_c.jpg]:  79578 extra bytes at beginning or within zipfile
  (attempting to process anyway)
  inflating: flag.txt

┌──(kali㉿kali)-[~/Desktop/base_images/base_images/base_images]
└─$ ls
4_c.jpg  flag.txt

┌──(kali㉿kali)-[~/Desktop/base_images/base_images/base_images]
└─$ cat flag.txt
picoCTF{bf6acf878dcbd752f4721e41b1b1b66b}
```

อยากให้น้อง ๆ ไปฝึกอะไรเพิ่ม