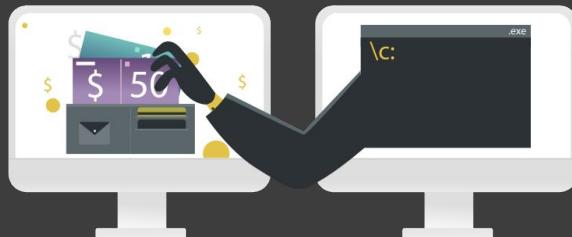


NCSA CTF Boot Camp #2

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.



Yasinthorn (Not) Khemprakhon

Penetration Tester
Siam Thanat Hack Co., Ltd.



Disclaimer

- จุดประสงค์ของการบรรยาย นี้เพื่อแบ่งปันความรู้ ทางด้านความปลอดภัยระบบสารสนเทศ
- ไม่สนับสนุนการนำความรู้ทางด้านความปลอดภัยฯ ไปใช้ในทางที่ผิดกฎหมายทั้งหมด
- ตัวอย่างโค้ด และรูปในการบรรยาย 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	ส่วนตัวแนะนำเส้นทางอาชีพ

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
- ลองทำแลบ!
 - Lab 1: วิเคราะห์ Access.log
 - Lab 2: วิเคราะห์ Metadata file image
 - Lab 3: Verify zip



Digital Forensics คืออะไร

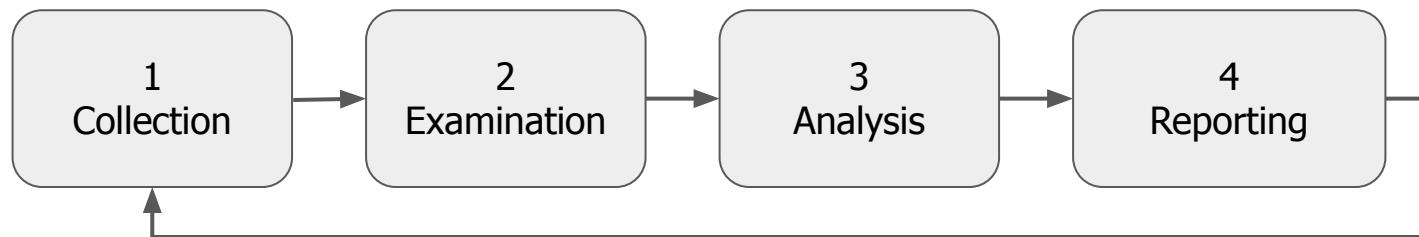


เป็นกระบวนการเก็บรวบรวม วิเคราะห์ และรักษาหลักฐานที่ได้จากระบบดิจิทัล เพื่อนำมาใช้ในการสืบสวนหรือดำเนินคดีทางกฎหมาย

หลักฐานเหล่านี้อาจมาจากการ

- อุปกรณ์คอมพิวเตอร์
- โทรศัพท์มือถือ
- เครื่อข่าย
- หรืออุปกรณ์เจัดเก็บข้อมูลอื่น ๆ

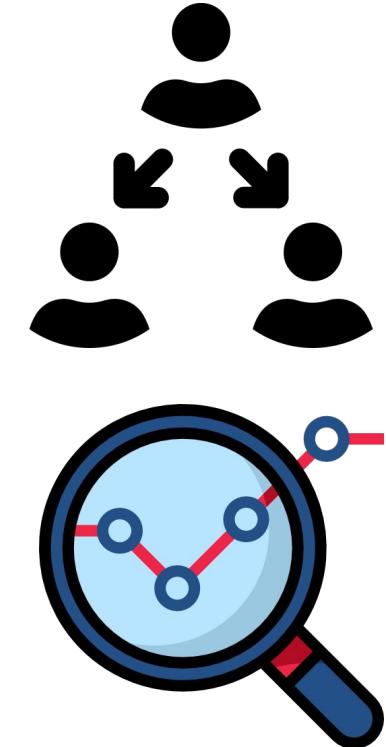
The Process of Digital Forensics



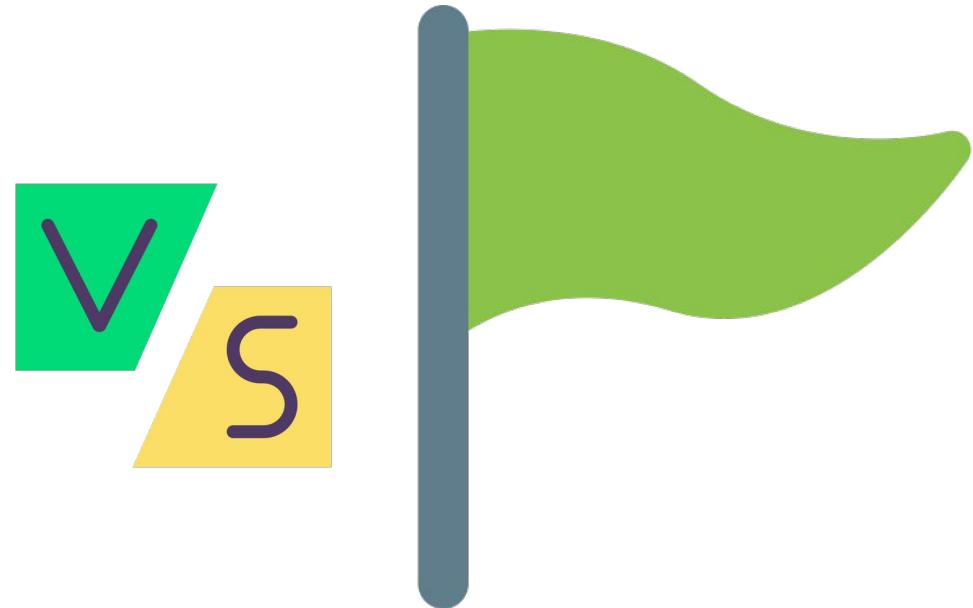
Media → Data → Information → Evidence

NIST SP 800-86 - Digital Forensics
Flow Standard

Digital Forensics



Digital Forensics (Real World) VS (CTF)



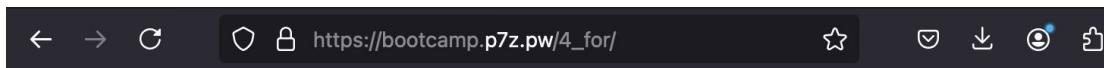
"Detective Conan" The Dark Footprint: Part 2"

ประเภทของการ Digital Forensics

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

ดาวน์โหลดไฟล์แลป

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



Index of /4_for/

..		
for_lab1_access.log	14-Sep-2024 02:44	29972
for_lab2_cat.jpg	14-Sep-2024 02:44	878121
for_lab3_verify.zip	14-Sep-2024 02:44	81899



ทำความรู้จัก Log

Log File

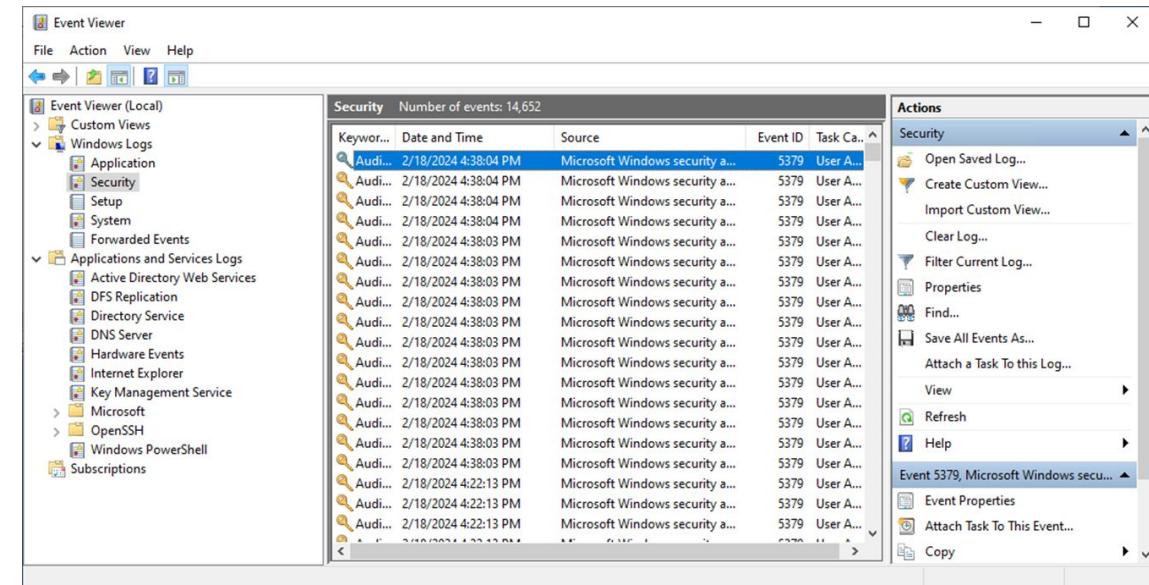
- Application Log
- Security Log
- Server Log
- System Log
- Network Log
- Database Log

```
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"
```

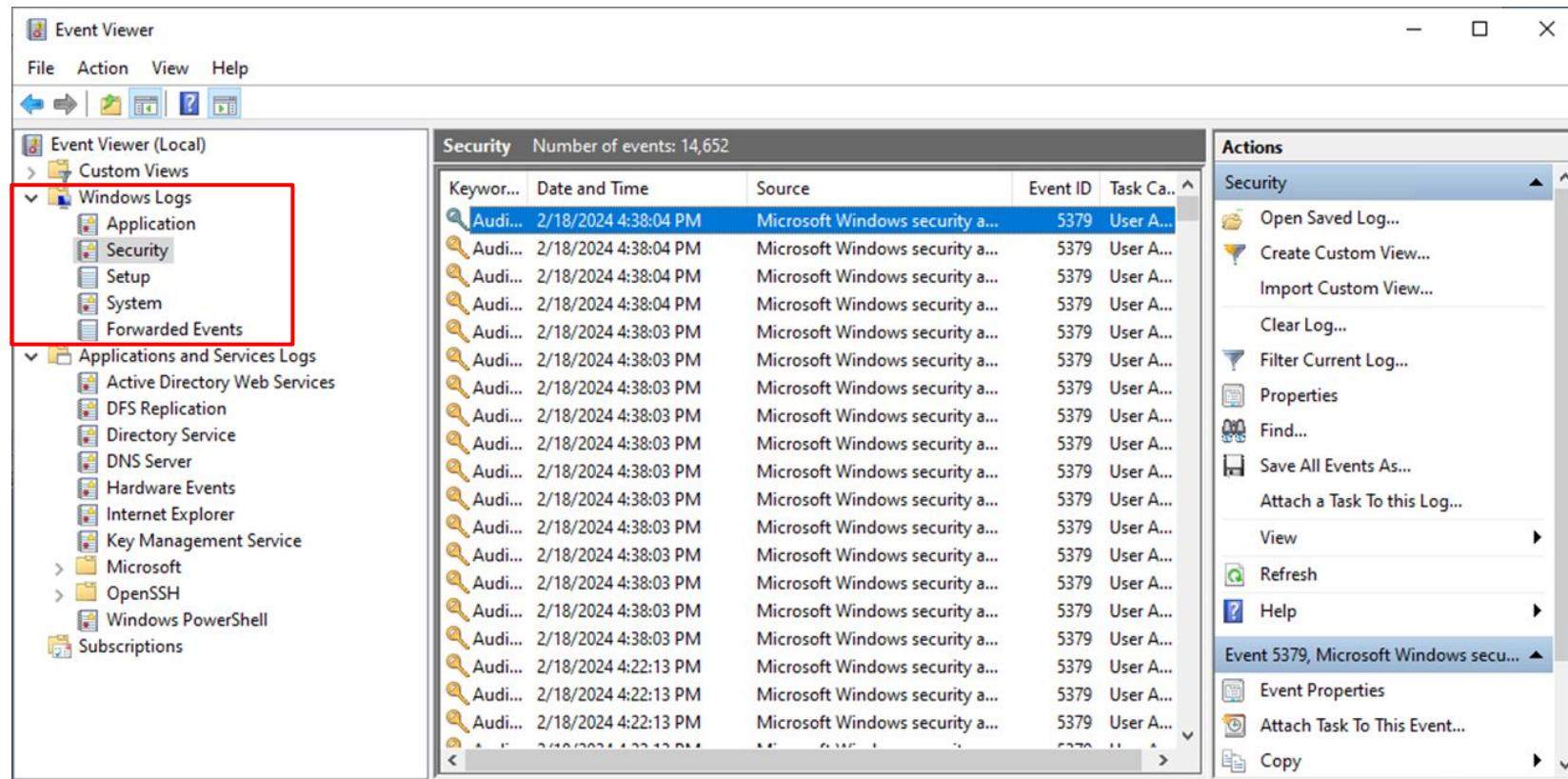
The Path of Log File on Windows

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



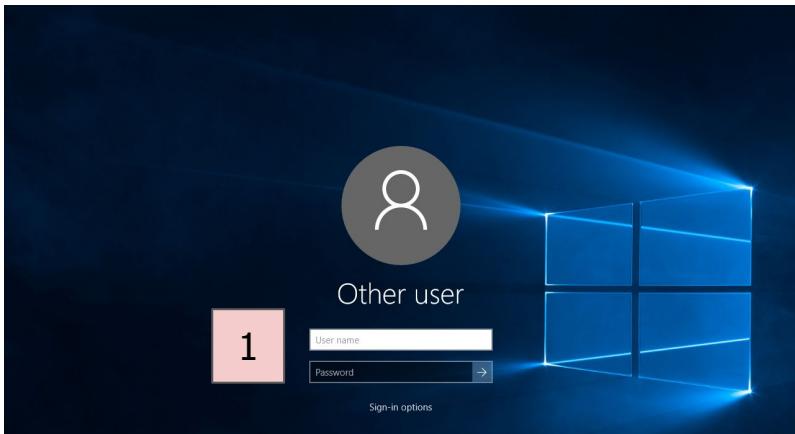
C:\Windows\System32\Winevt\Logs\



The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs, with the 'Windows Logs' section expanded, specifically focusing on the 'Security' log. This section is highlighted with a red box. The main pane shows a list of security events with columns for Keyword, Date and Time, Source, Event ID, and Task Category. Most events are for Microsoft Windows security and have an Event ID of 5379. The right pane contains an 'Actions' menu with various options like Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Properties, Find..., Save All Events As..., Attach a Task To this Log..., View, Refresh, Help, Event Properties, Attach Task To This Event..., and Copy. The 'Event Properties' option is currently selected.

Keyword	Date and Time	Source	Event ID	Task Category
Audi...	2/18/2024 4:38:04 PM	Microsoft Windows security a...	5379	User A...
Audi...	2/18/2024 4:38:04 PM	Microsoft Windows security a...	5379	User A...
Audi...	2/18/2024 4:38:04 PM	Microsoft Windows security a...	5379	User A...
Audi...	2/18/2024 4:38:04 PM	Microsoft Windows security a...	5379	User A...
Audi...	2/18/2024 4:38:03 PM	Microsoft Windows security a...	5379	User A...
Audi...	2/18/2024 4:38:03 PM	Microsoft Windows security a...	5379	User A...
Audi...	2/18/2024 4:38:03 PM	Microsoft Windows security a...	5379	User A...
Audi...	2/18/2024 4:38:03 PM	Microsoft Windows security a...	5379	User A...
Audi...	2/18/2024 4:38:03 PM	Microsoft Windows security a...	5379	User A...
Audi...	2/18/2024 4:38:03 PM	Microsoft Windows security a...	5379	User A...
Audi...	2/18/2024 4:38:03 PM	Microsoft Windows security a...	5379	User A...
Audi...	2/18/2024 4:38:03 PM	Microsoft Windows security a...	5379	User A...
Audi...	2/18/2024 4:38:03 PM	Microsoft Windows security a...	5379	User A...
Audi...	2/18/2024 4:38:03 PM	Microsoft Windows security a...	5379	User A...
Audi...	2/18/2024 4:22:13 PM	Microsoft Windows security a...	5379	User A...
Audi...	2/18/2024 4:22:13 PM	Microsoft Windows security a...	5379	User A...
Audi...	2/18/2024 4:22:13 PM	Microsoft Windows security a...	5379	User A...

Windows Security Log



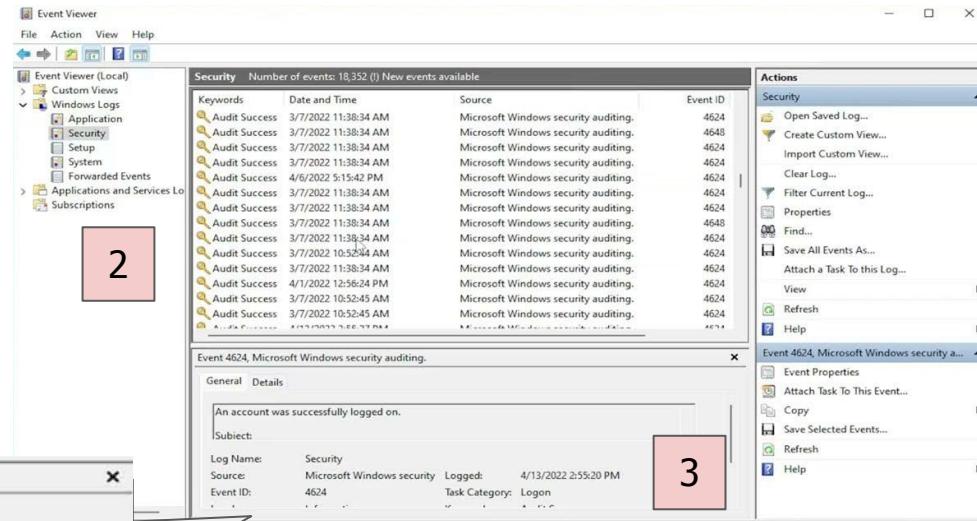
Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Log Name: Security
Source: Microsoft Windows security Logged: 4/13/2022 2:55:20 PM
Event ID: 4624 Task Category: Logon



The image shows the Windows Event Viewer application. The left pane displays a tree view of logs, with the 'Security' log selected. The right pane shows a list of audit success events. A red box labeled '2' is overlaid on the event list. The bottom pane shows a detailed view of the first event (Event ID 4624). A red box labeled '3' is overlaid on the event details.

Keywords	Date and Time	Source	Event ID
Audit Success	3/7/2022 11:38:34 AM	Microsoft Windows security auditing.	4624
Audit Success	3/7/2022 11:38:34 AM	Microsoft Windows security auditing.	4624
Audit Success	3/7/2022 11:38:34 AM	Microsoft Windows security auditing.	4624
Audit Success	3/7/2022 11:38:34 AM	Microsoft Windows security auditing.	4624
Audit Success	4/6/2022 5:15:42 PM	Microsoft Windows security auditing.	4624
Audit Success	3/7/2022 11:38:34 AM	Microsoft Windows security auditing.	4624
Audit Success	3/7/2022 11:38:34 AM	Microsoft Windows security auditing.	4624
Audit Success	3/7/2022 11:38:34 AM	Microsoft Windows security auditing.	4624
Audit Success	3/7/2022 10:52:04 AM	Microsoft Windows security auditing.	4624
Audit Success	3/7/2022 11:38:34 AM	Microsoft Windows security auditing.	4624
Audit Success	4/1/2022 12:56:24 PM	Microsoft Windows security auditing.	4624
Audit Success	3/7/2022 10:52:45 AM	Microsoft Windows security auditing.	4624
Audit Success	3/7/2022 10:52:45 AM	Microsoft Windows security auditing.	4624

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Log Name: Security
Source: Microsoft Windows security Logged: 4/13/2022 2:55:20 PM
Event ID: 4624 Task Category: Logon

The Path of Log Files on Linux

บน Linux ไฟล์ Log มักถูกเก็บไว้ที่ `/var/log/`

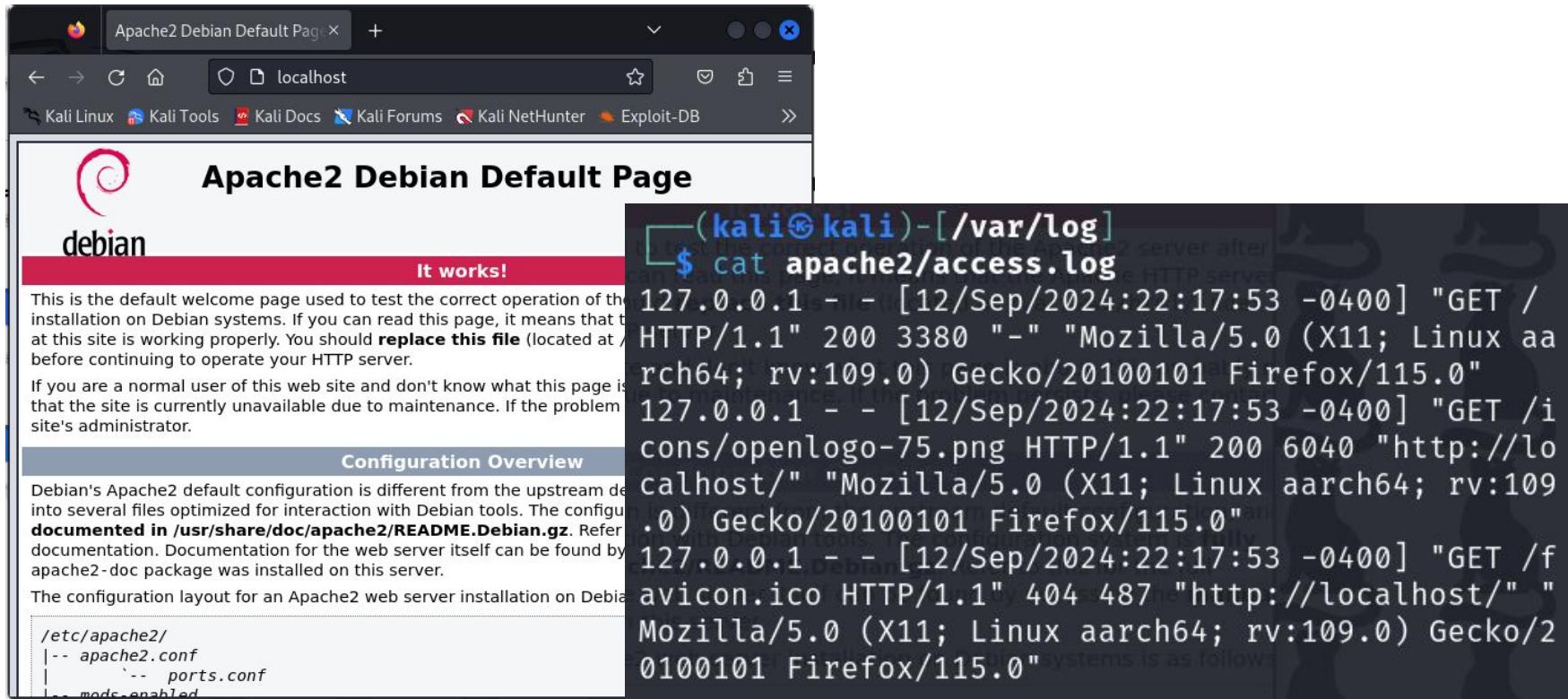
1. syslog
2. auth.log
3. boot.log
4. cron.log
5. apache2/ หรือ httpd/
6. mysql/ หรือ mariadb/
7. kern.log

```
(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
drwx-----  3 inetsim       inetsim   4096 Sep  4 12:29 inetsim
drwxr-xr-x  3 root          root      4096 Sep  4 12:34 installer
drwxr-sr-x+ 3 root          systemd-journal 4096 Sep  4 19:34 journal
```

/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
```


ตัวอย่าง access.log



Apache2 Debian Default Page

debian

It works!

This is the default welcome page used to test the correct operation of the installation on Debian systems. If you can read this page, it means that this site is working properly. You should **replace this file** (located at /var/www/html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is, then the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream distribution. It is split into several files optimized for interaction with Debian tools. The configuration is documented in /usr/share/doc/apache2/README.Debian.gz. Refer to the documentation. Documentation for the web server itself can be found by reading the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian is as follows:

```
/etc/apache2/
|-- apache2.conf
|   '-- ports.conf
|       '-- mod-available
```

```
(kali㉿kali)-[~/Documents]
$ cat apache2/access.log
127.0.0.1 - - [12/Sep/2024:22:17:53 -0400] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [12/Sep/2024:22:17:53 -0400] "GET /icons/openlogo-75.png HTTP/1.1" 200 6040 "http://localhost/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [12/Sep/2024:22:17:53 -0400] "GET /favicon.ico HTTP/1.1" 404 487 "http://localhost/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
```

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 (Response 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

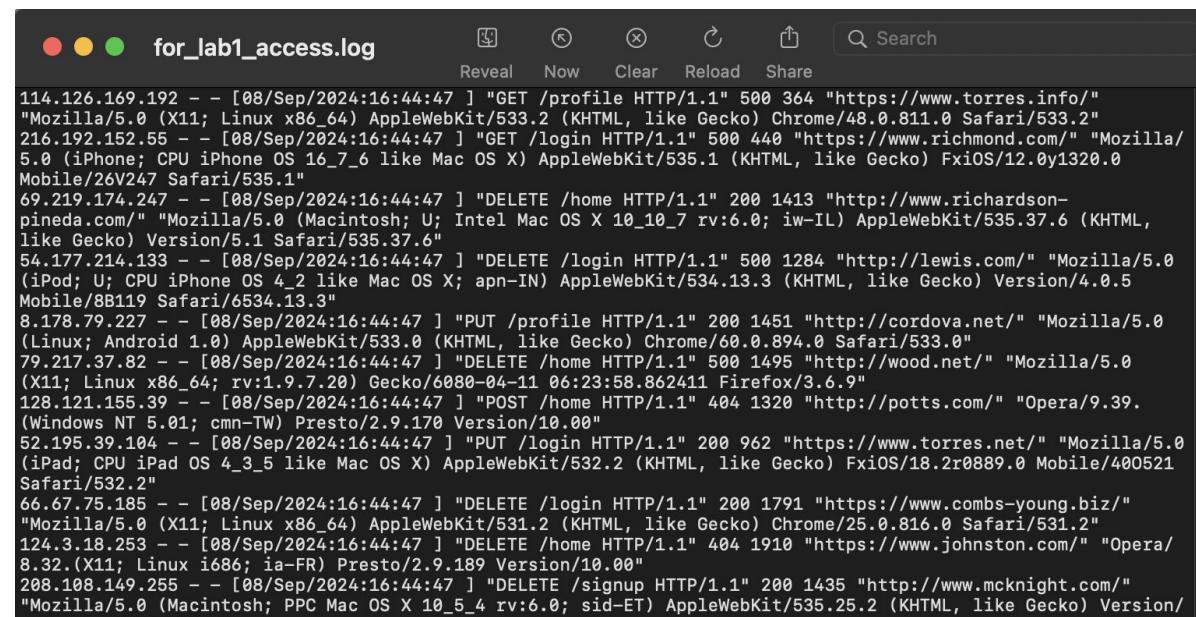
```
114.126.169.192 -- [08/Sep/2024:16:44:47] "GET /profile HTTP/1.1" 500 364 "https://www.torres.info/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/533.2 (KHTML, like Gecko) Chrome/48.0.811.0 Safari/533.2"
216.192.152.55 -- [08/Sep/2024:16:44:47] "GET /login HTTP/1.1" 500 440 "https://www.richmond.com/" "Mozilla/5.0 (iPhone; CPU iPhone OS 16_7_6 like Mac OS X) AppleWebKit/535.1 (KHTML, like Gecko) FxiOS/12.0y1320.0 Mobile/26V247 Safari/535.1"
69.219.174.247 -- [08/Sep/2024:16:44:47] "DELETE /home HTTP/1.1" 200 1413 "http://www.richardson-pineda.com/" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_10_7 rv:6.0; iw-IL) AppleWebKit/535.37.6 (KHTML, like Gecko) Version/5.1 Safari/535.37.6"
54.177.214.133 -- [08/Sep/2024:16:44:47] "DELETE /login HTTP/1.1" 500 1284 "http://lewis.com/" "Mozilla/5.0 (iPod; U; CPU iPhone OS 4_2 like Mac OS X; apn-IN) AppleWebKit/534.13.3 (KHTML, like Gecko) Version/4.0.5 Mobile/8B119 Safari/6534.13.3"
8.178.79.227 -- [08/Sep/2024:16:44:47] "PUT /profile HTTP/1.1" 200 1451 "http://cordova.net/" "Mozilla/5.0 (Linux; Android 1.0) AppleWebKit/533.0 (KHTML, like Gecko) Chrome/60.0.894.0 Safari/533.0"
79.217.37.82 -- [08/Sep/2024:16:44:47] "DELETE /home HTTP/1.1" 500 1495 "http://wood.net/" "Mozilla/5.0 (X11; Linux x86_64; rv:1.9.7.20) Gecko/6880-04-11 06:23:58.862411 Firefox/3.6.9"
128.121.155.39 -- [08/Sep/2024:16:44:47] "POST /home HTTP/1.1" 404 1320 "http://potts.com/" "Opera/9.39. (Windows NT 5.01; cmn-TW) Presto/2.9.170 Version/10.00"
52.195.39.104 -- [08/Sep/2024:16:44:47] "PUT /login HTTP/1.1" 200 962 "https://www.torres.net/" "Mozilla/5.0 (iPad; CPU iPad OS 4_3_5 like Mac OS X) AppleWebKit/532.2 (KHTML, like Gecko) FxiOS/18.2r0889.0 Mobile/400521 Safari/532.2"
66.67.75.185 -- [08/Sep/2024:16:44:47] "DELETE /login HTTP/1.1" 200 1791 "https://www.combs-young.biz/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/531.2 (KHTML, like Gecko) Chrome/25.0.816.0 Safari/531.2"
124.3.18.253 -- [08/Sep/2024:16:44:47] "DELETE /home HTTP/1.1" 404 1910 "https://www.johnston.com/" "Opera/8.32.(X11; Linux i686; ia-FR) Presto/2.9.189 Version/10.00"
208.108.149.255 -- [08/Sep/2024:16:44:47] "DELETE /signup HTTP/1.1" 200 1435 "http://www.mcknight.com/" "Mozilla/5.0 (Macintosh; PPC Mac OS X 10_5_4 rv:6.0; sid-ET) AppleWebKit/535.25.2 (KHTML, like Gecko) Version/
```

for_lab1_access.log

Log File - 30 KB

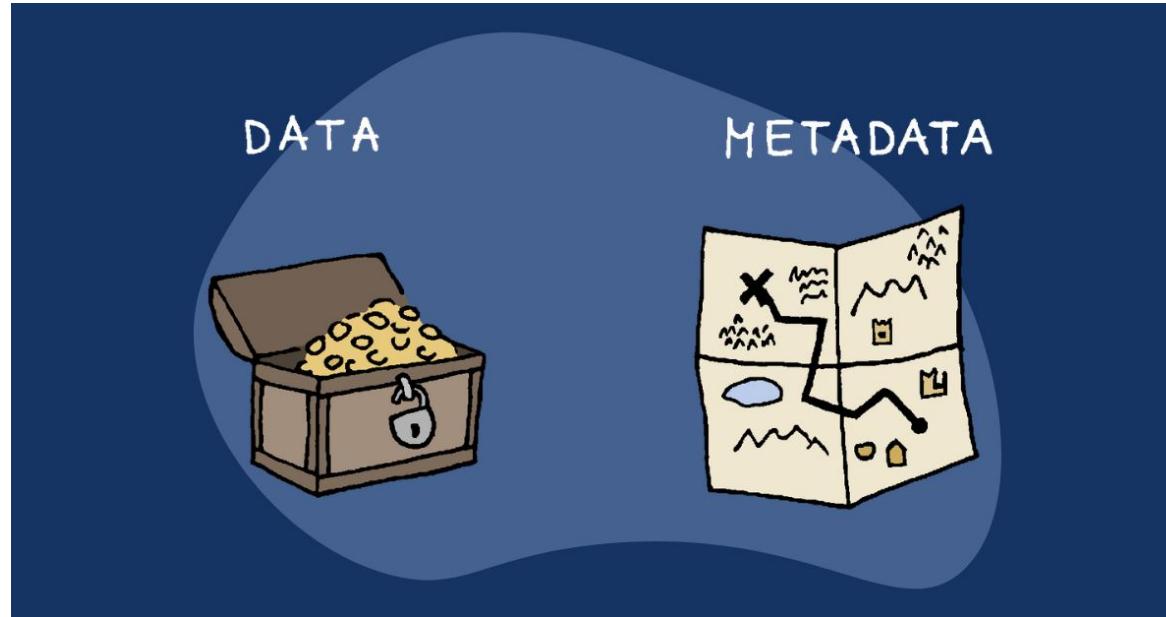
Information

Find the Flag in for_lab1_access.log



```
for_lab1_access.log
Reveal Now Clear Reload Share
Search
114.126.169.192 -- [08/Sep/2024:16:44:47] "GET /profile HTTP/1.1" 500 364 "https://www.torres.info/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/533.2 (KHTML, like Gecko) Chrome/48.0.811.0 Safari/533.2"
216.192.152.55 -- [08/Sep/2024:16:44:47] "GET /login HTTP/1.1" 500 440 "https://www.richmond.com/" "Mozilla/5.0 (iPhone; CPU iPhone OS 16_7_6 like Mac OS X) AppleWebKit/535.1 (KHTML, like Gecko) FxiOS/12.0y1320.0 Mobile/26V247 Safari/535.1"
69.219.174.247 -- [08/Sep/2024:16:44:47] "DELETE /home HTTP/1.1" 200 1413 "http://www.richardson-pineda.com/" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_10_7 rv:6.0; iw-IL) AppleWebKit/535.37.6 (KHTML, like Gecko) Version/5.1 Safari/535.37.6"
54.177.214.133 -- [08/Sep/2024:16:44:47] "DELETE /login HTTP/1.1" 500 1284 "http://lewis.com/" "Mozilla/5.0 (iPod; U; CPU iPhone OS 4_2 like Mac OS X; apn-IN) AppleWebKit/534.13.3 (KHTML, like Gecko) Version/4.0.5 Mobile/8B119 Safari/6534.13.3"
8.178.79.227 -- [08/Sep/2024:16:44:47] "PUT /profile HTTP/1.1" 200 1451 "http://cordova.net/" "Mozilla/5.0 (Linux; Android 1.0) AppleWebKit/533.0 (KHTML, like Gecko) Chrome/60.0.894.0 Safari/533.0"
79.217.37.82 -- [08/Sep/2024:16:44:47] "DELETE /home HTTP/1.1" 500 1495 "http://wood.net/" "Mozilla/5.0 (X11; Linux x86_64; rv:1.9.7.20) Gecko/6880-04-11 06:23:58.862411 Firefox/3.6.9"
128.121.155.39 -- [08/Sep/2024:16:44:47] "POST /home HTTP/1.1" 404 1320 "http://potts.com/" "Opera/9.39. (Windows NT 5.01; cmn-TW) Presto/2.9.170 Version/10.00"
52.195.39.104 -- [08/Sep/2024:16:44:47] "PUT /login HTTP/1.1" 200 962 "https://www.torres.net/" "Mozilla/5.0 (iPad; CPU iPad OS 4_3_5 like Mac OS X) AppleWebKit/532.2 (KHTML, like Gecko) FxiOS/18.2r0889.0 Mobile/400521 Safari/532.2"
66.67.75.185 -- [08/Sep/2024:16:44:47] "DELETE /login HTTP/1.1" 200 1791 "https://www.combs-young.biz/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/531.2 (KHTML, like Gecko) Chrome/25.0.816.0 Safari/531.2"
124.3.18.253 -- [08/Sep/2024:16:44:47] "DELETE /home HTTP/1.1" 404 1910 "https://www.johnston.com/" "Opera/8.32.(X11; Linux i686; ia-FR) Presto/2.9.189 Version/10.00"
208.108.149.255 -- [08/Sep/2024:16:44:47] "DELETE /signup HTTP/1.1" 200 1435 "http://www.mcknight.com/" "Mozilla/5.0 (Macintosh; PPC Mac OS X 10_5_4 rv:6.0; sid-ET) AppleWebKit/535.25.2 (KHTML, like Gecko) Version/
```

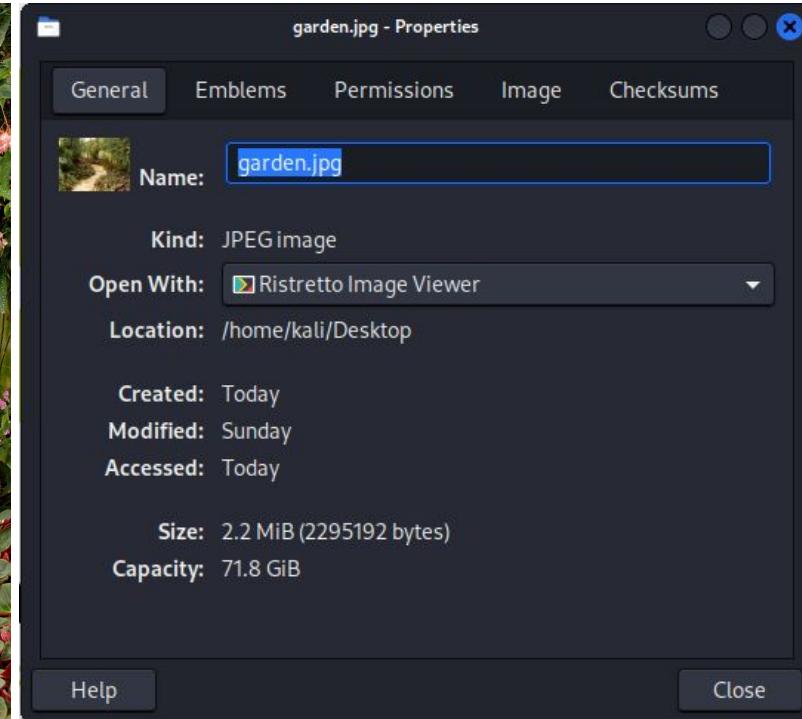
Metadata



<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.

Forensics

Detect File Type

Scan for Embedded Files

Extract Files

YARA Rules

Remove EXIF

Extract EXIF

Extract RGBA

View Bit Plane

Randomize Colour Palette

Extract LSB

ELF Info

ExifTool

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

Consult the exiftool documentation for a full list of options.

← → ⌂ ⌄ exiftool.org

ExifTool by Phil Harvey

Read, Write and Edit Meta Information!

Also available --> [Utility to fix Nikon NEF images corrupted by Nikon software](#)

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
File Access Date/Time       : 2024:09:09 13:31:31-0
File Inode Change Date/Time : 2024:09:04 13:07:40-0
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
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
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
```



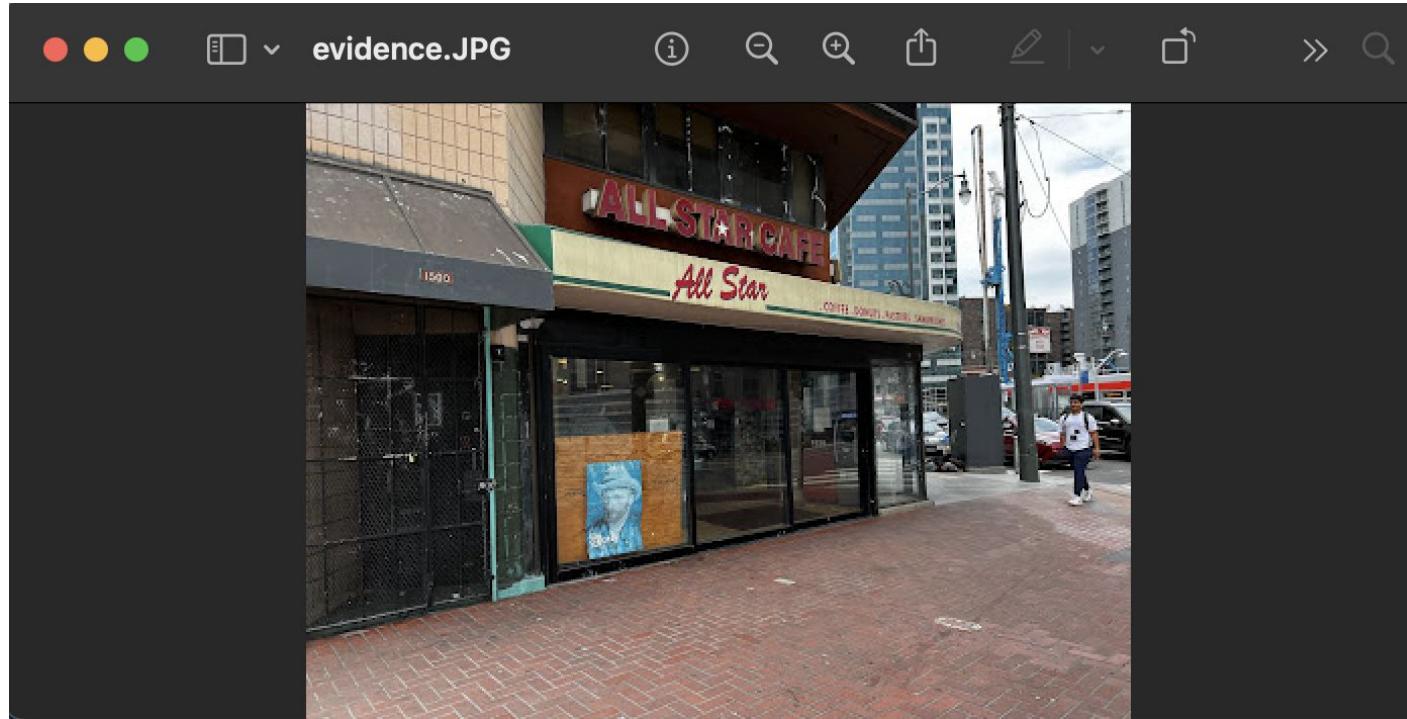
Forensics - โจทย์สมมติ

สถานการณ์:

หน่วยสืบสวนกำลังตามหาผู้ต้องสงสัยในการจกรรมเงินจำนวน
มหาศาล ผู้ต้องสงสัยหนีไปพร้อมกับเงินและได้หลบซ่อนตัว โดยใช้
รถยนต์เป็นพาหนะ ข้อมูลเพียงอย่างเดียวที่ตำรวจมีคือรูปถ่ายหนึ่งรูป
ที่ถ่ายจากกล้องมือถือในวันเกิดเหตุ อย่างไรก็ตาม พิกัด GPS จากรูป
นั้นอาจเป็นเบาะแสสำคัญที่จะนำไปสู่สถานที่ที่ผู้ต้องสงสัยกำลังใช้รถ
ยี่ห้อ Toyota ใน การหลบหนีแต่ไม่ทราบรุ่นของรถ

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
```

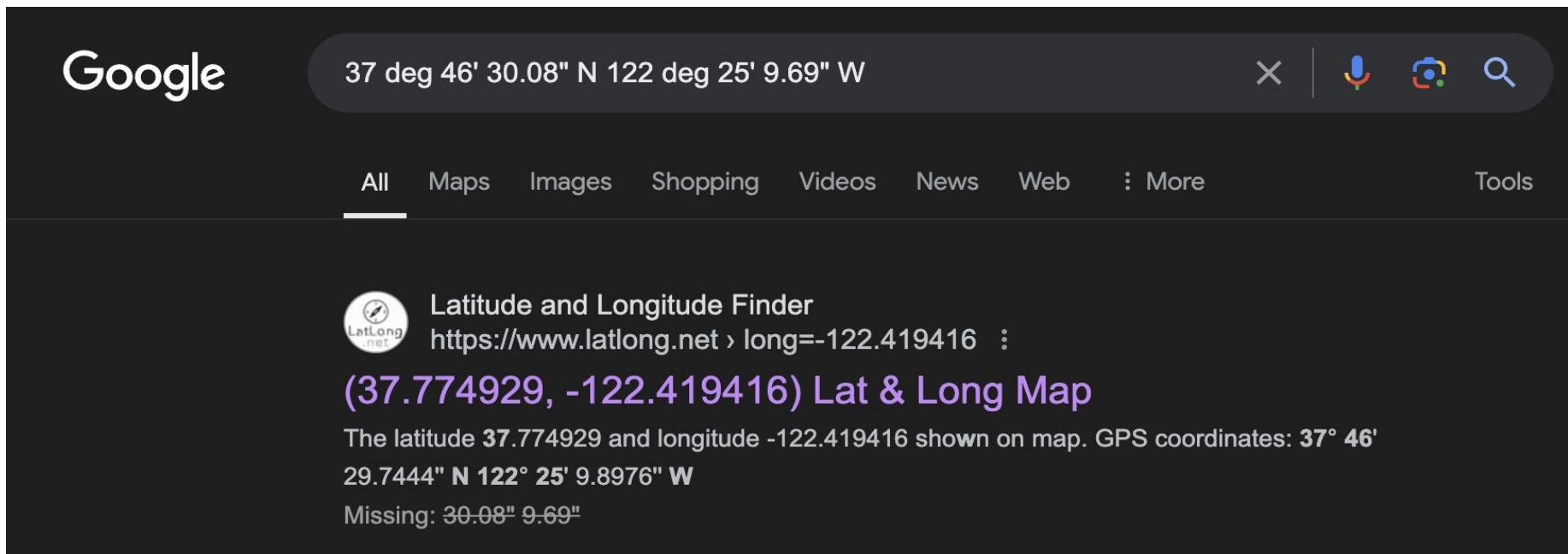
Forensics - โจทย์สมมติ

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



Google

37 deg 46' 30.08" N 122 deg 25' 9.69" W

X |   

All Maps Images Shopping Videos News Web More Tools

 Latitude and Longitude Finder
<https://wwwlatlong.net> › long=-122.419416 :

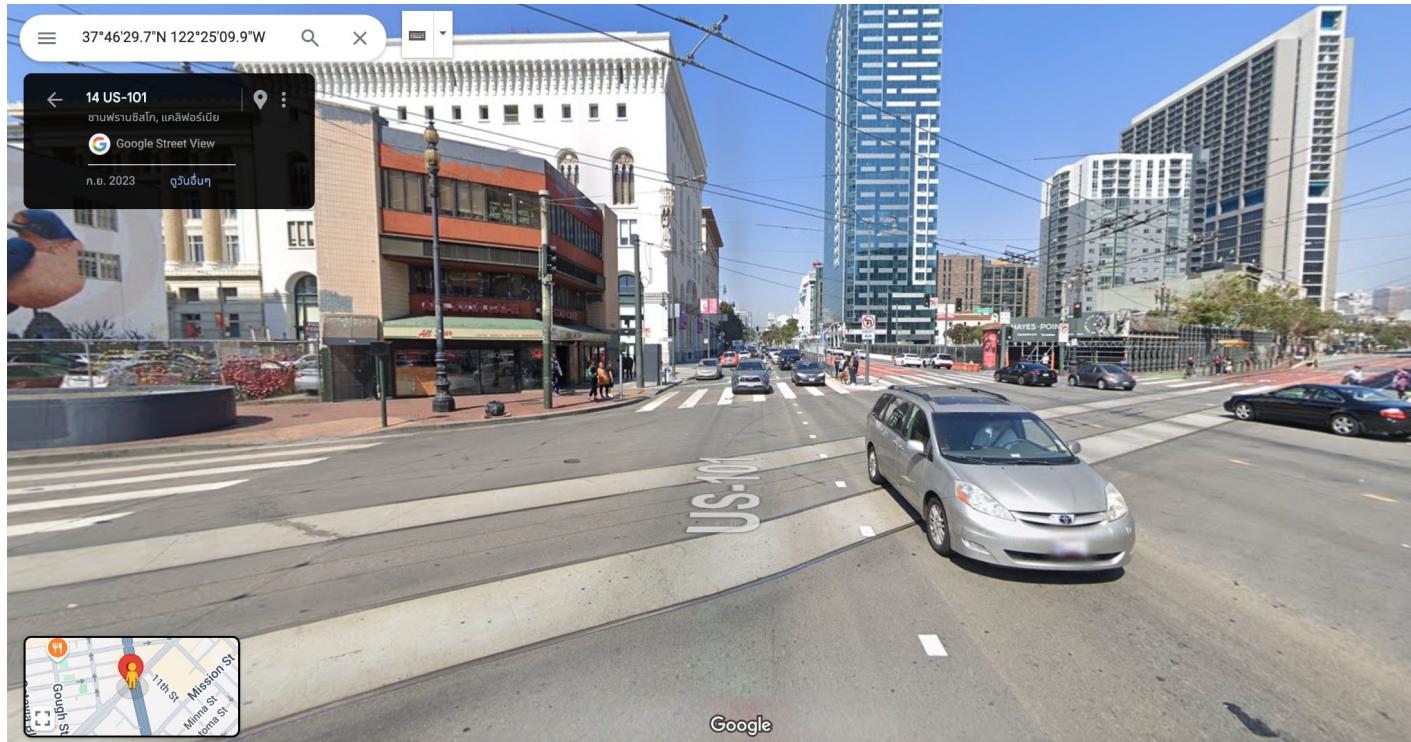
(37.774929, -122.419416) Lat & Long Map

The latitude 37.774929 and longitude -122.419416 shown on map. GPS coordinates: 37° 46'
29.7444" N 122° 25' 9.8976" W

Missing: 30.08" 9.69"

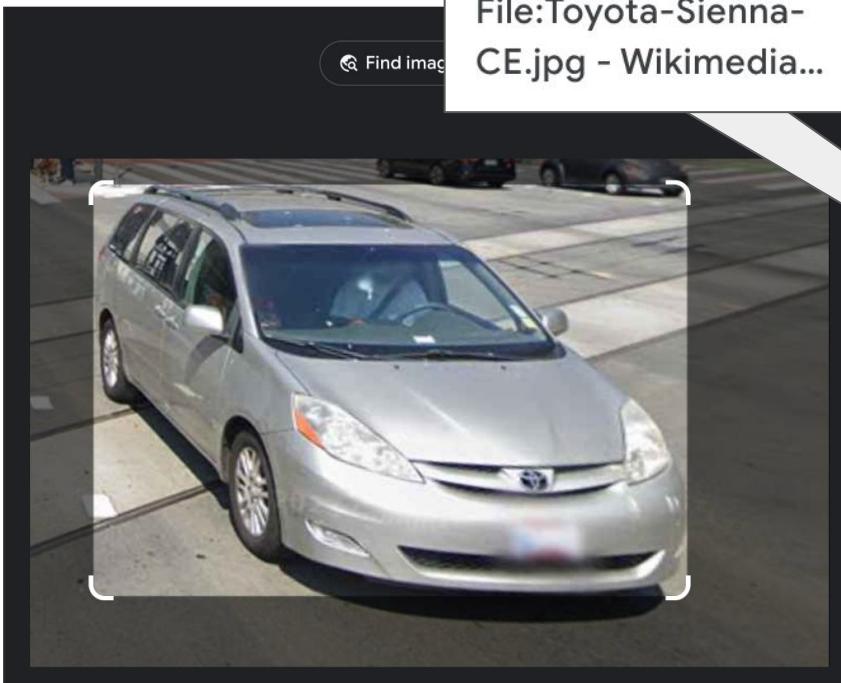
Forensics - โจทย์สมมติ

ค้นหา พิกัด GPS บน Google Map



Forensics - โจทย์สมมติ

Google



Wikimedia

File:Toyota-Sienna-CE.jpg - Wikimedia...

Find image

ใช้ Google Image Search

Upload



U.S. News & World ...
2010 Toyota Sienna ...
See exact match



The New York Times
Wheelies: The Toyota ...
Trouble Edition - The...



Related searches

2010 Toyota Sienna



Toyota Sienna



Wikimedia
File:Toyota Sienna LE ...



Wikimedia
File:Toyota-Sienna- ...



YouTube
Toyota Sienna Review ...



autobazar.us

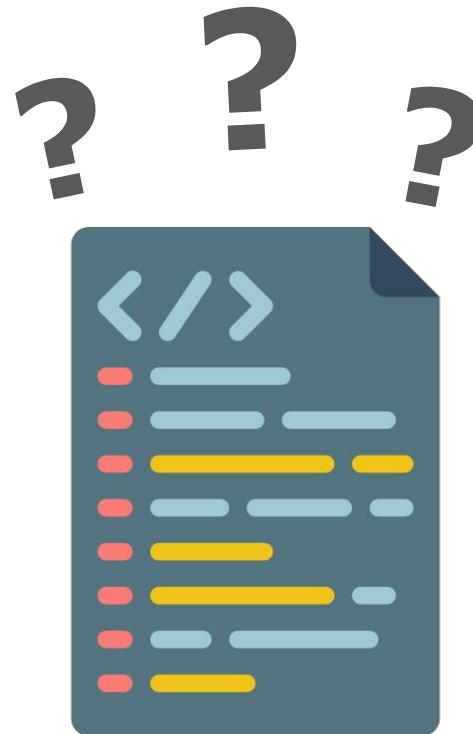


Wikimedia
File:Toyota-Sienna-CE.jpg - Wikimedia...



carstime.com
Toyota Sienna For \$...

File Format



File Format

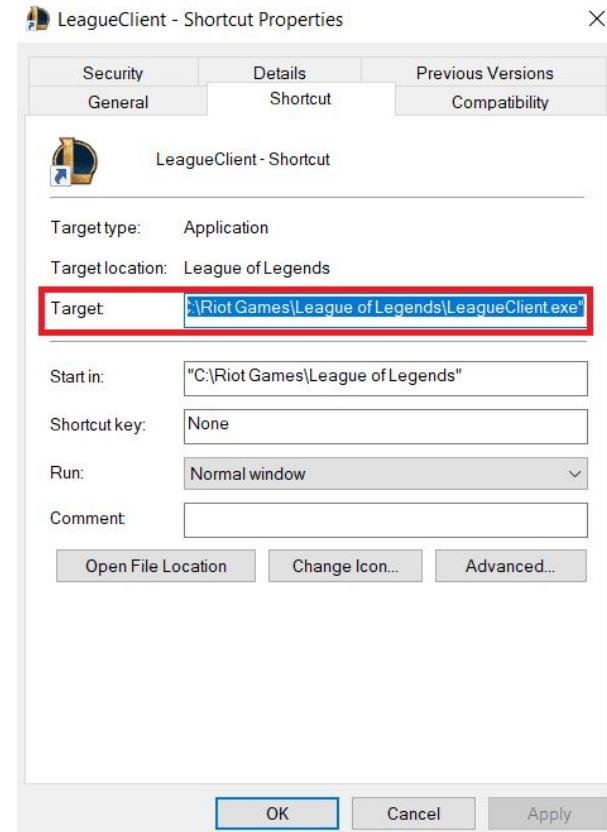
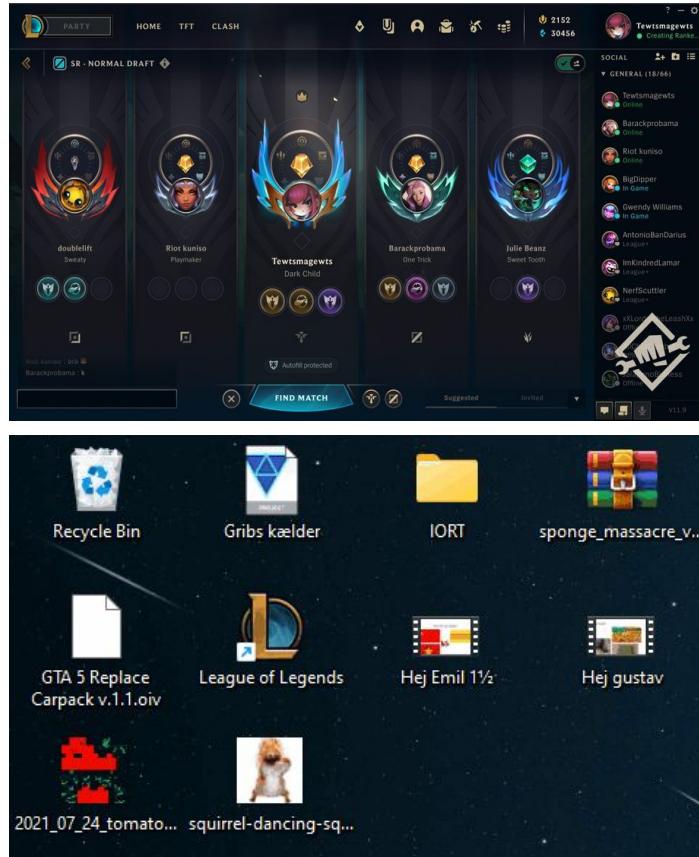


File Format

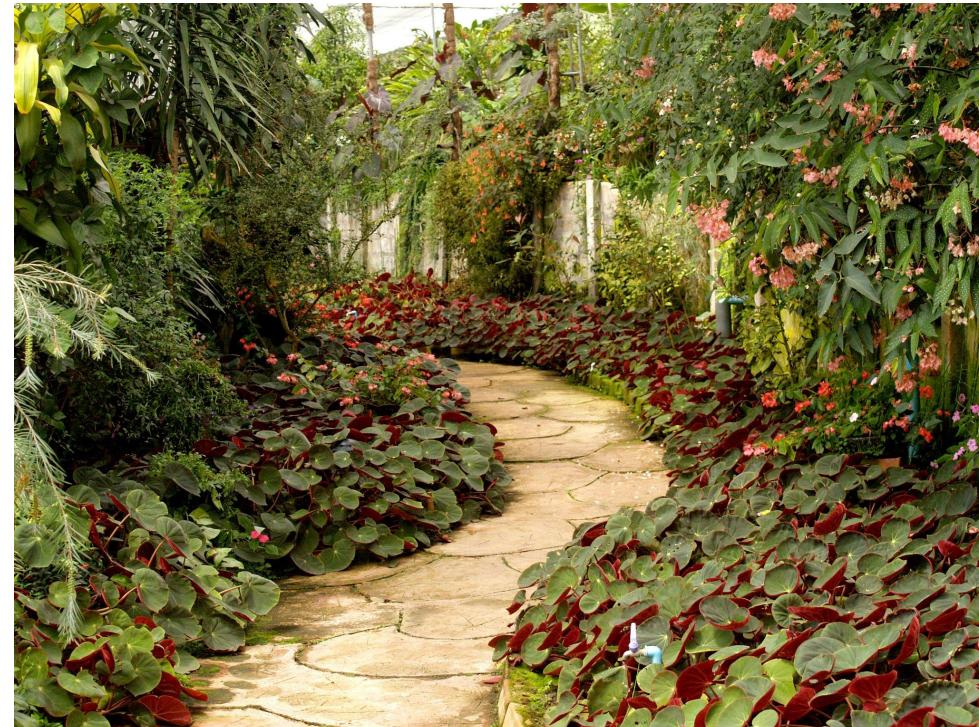


```
▶ note.txt •  
1 Hello, world  
2  
3 This is my first text.  
4  
5
```

File Format

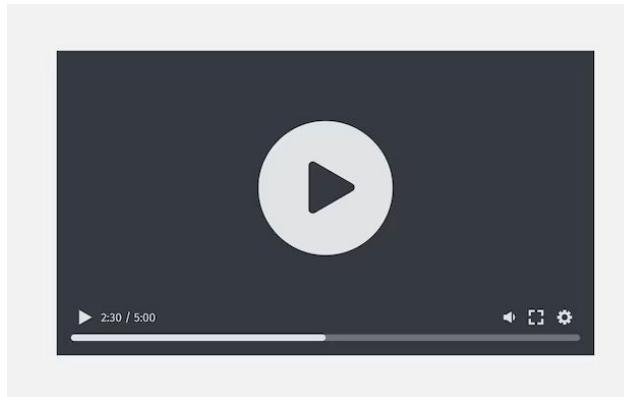
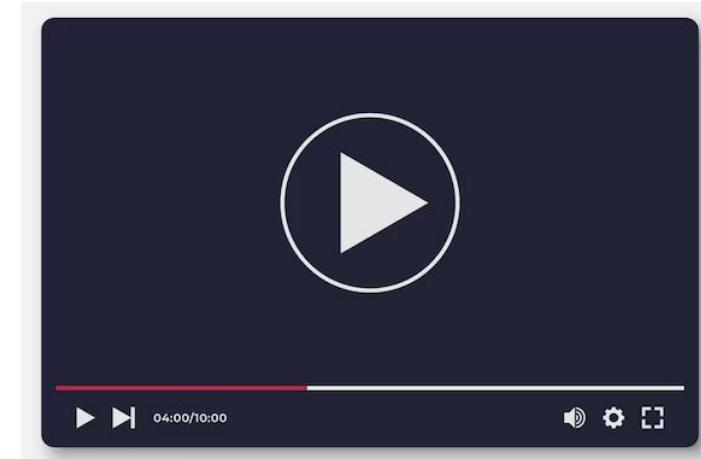


File Format



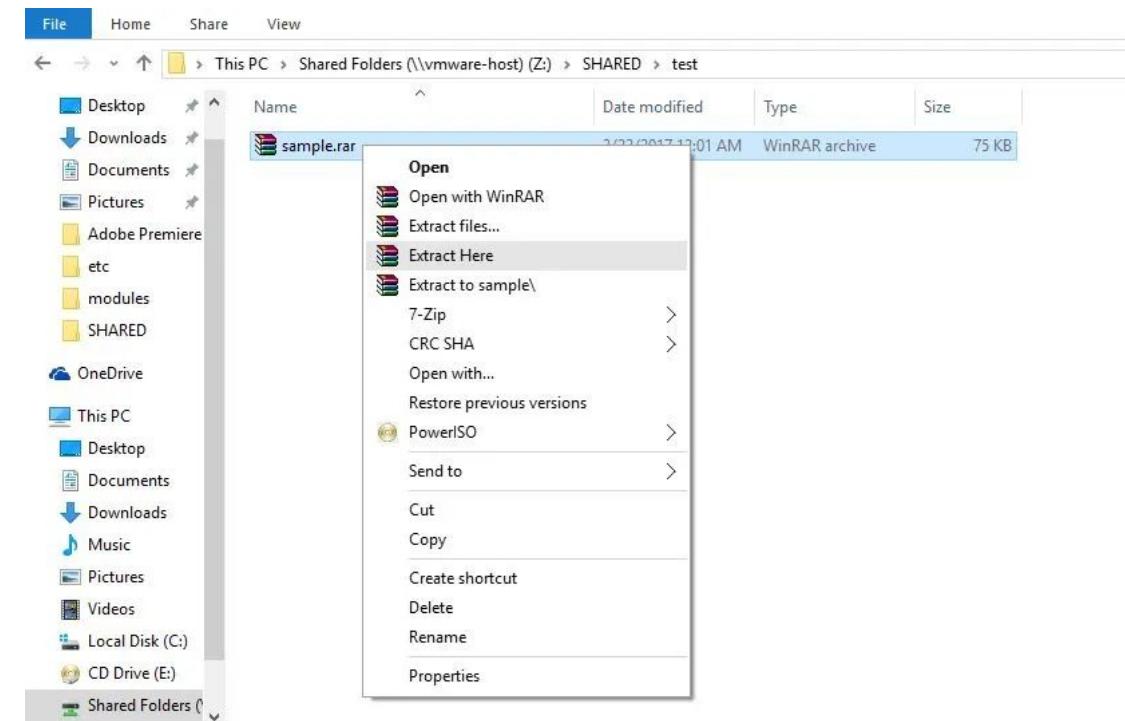
garden.jpg

File Format



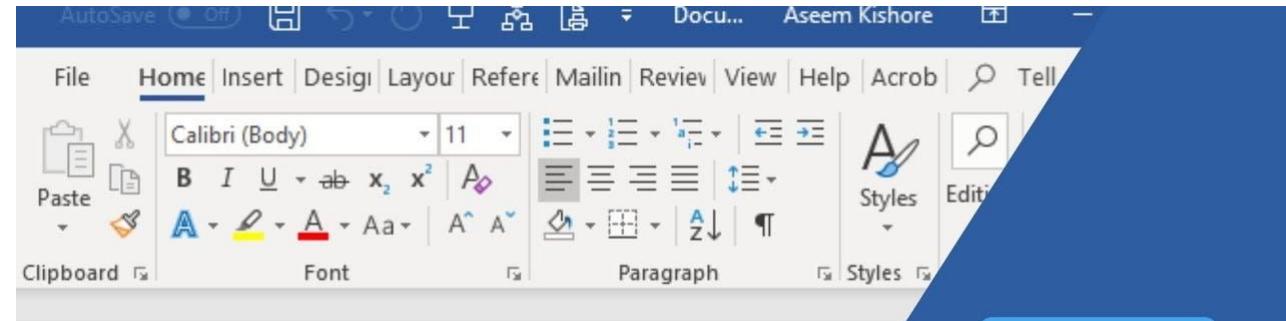
ที่มา: <https://www.freepik.com>

File Format



A screenshot of a Windows File Explorer window. The path is 'This PC > Shared Folders (\vmware-host) (Z:) > SHARED > test'. A file named 'sample.rar' is selected. A context menu is open, showing options: Open, Open with WinRAR, Extract files..., Extract Here (which is highlighted), Extract to sample\, 7-Zip, CRC SHA, Open with..., Restore previous versions, PowerISO, Send to, Cut, Copy, Create shortcut, Delete, Rename, and Properties.

File Format



MS - Word



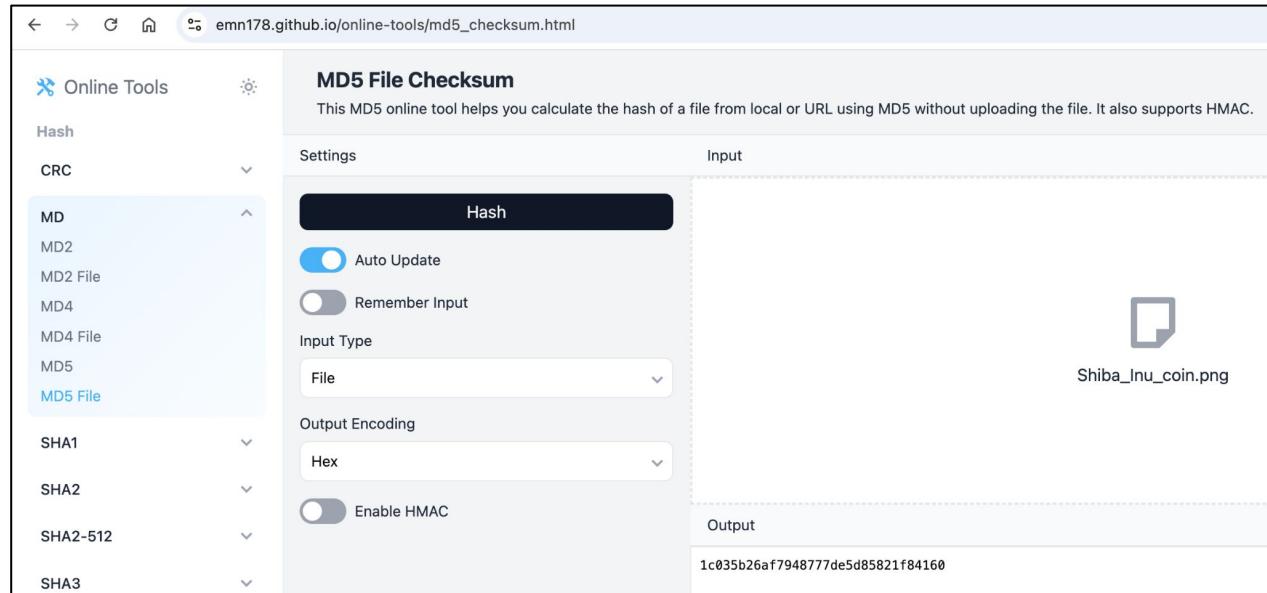
เครื่องมือที่ใช้ในการวิเคราะห์ File Format

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, copyright>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	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 DLT 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&²uŽfÍ ÐÍ ;Ù NUL à NUL bÍl	0	asf wma wmv	Advanced Systems Format ^[35]

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

Hex Editor

\$ hexeditor garden

File: garden	ASCII	Offset: 0x00000000 / 0x00230597 (%00)
00000000	FF D8 FF E0	00 10 4A 46 49 46 00 01 01 01 00 48 ... JFIF.....H
00000010	00 48 00 00	FF E2 0C 58 49 43 43 5F 50 52 4F 46XICC_PROF
00000020	49 4C 45 00	01 01 00 00 0C 48 4C 69 6E 6F 02 10HLino..
00000030	00 00 6D 6E	74 72 52 47 42 20 58 59 5A 20 07 CE ntrRGB XYZ ..
00000040	00 02 00 09	00 06 00 31 00 00 61 63 73 70 4D 53 I...1..acspMS
00000050	46 54 00 00	00 00 49 45 43 20 73 52 47 42 00 00 ... IEC sRGB ..
00000060	00 00 00 00	00 00 00 00 00 00 00 00 F6 D6 00 01
00000070	00 00 00 00	D3 2D 48 50 20 20 00 00 00 00 00 00 ..-HP
00000080	00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00
00000090	00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00
000000A0	00 00 00 00	00 00 00 00 00 11 63 70 72 74 00 00cprt ..
000000B0	01 50 00 00	00 33 64 65 73 63 00 00 01 84 00 00 ..3desc.....
000000C0	00 6C 77 74	70 74 00 00 01 F0 00 00 00 14 62 6B tpt.....blk
000000D0	70 74 00 00	02 04 00 00 00 14 72 58 59 5A 00 00rXYZ ..
000000E0	02 18 00 00	00 14 67 58 59 5A 00 00 02 2C 00 00 ... gXYZ ... , ..
000000F0	00 14 62 58	59 5A 00 00 02 40 00 00 00 14 64 6D XYZ ... @....dm
00000100	6E 64 00 00	02 54 00 00 00 70 64 6D 64 64 00 00 ..T ... pdmdd ..
00000110	02 C4 00 00	00 88 76 75 65 64 00 00 03 4C 00 00 ... vued ... L ..
00000120	00 86 76 69	65 77 00 00 03 D4 00 00 00 24 6C 75 iew.....\$lu

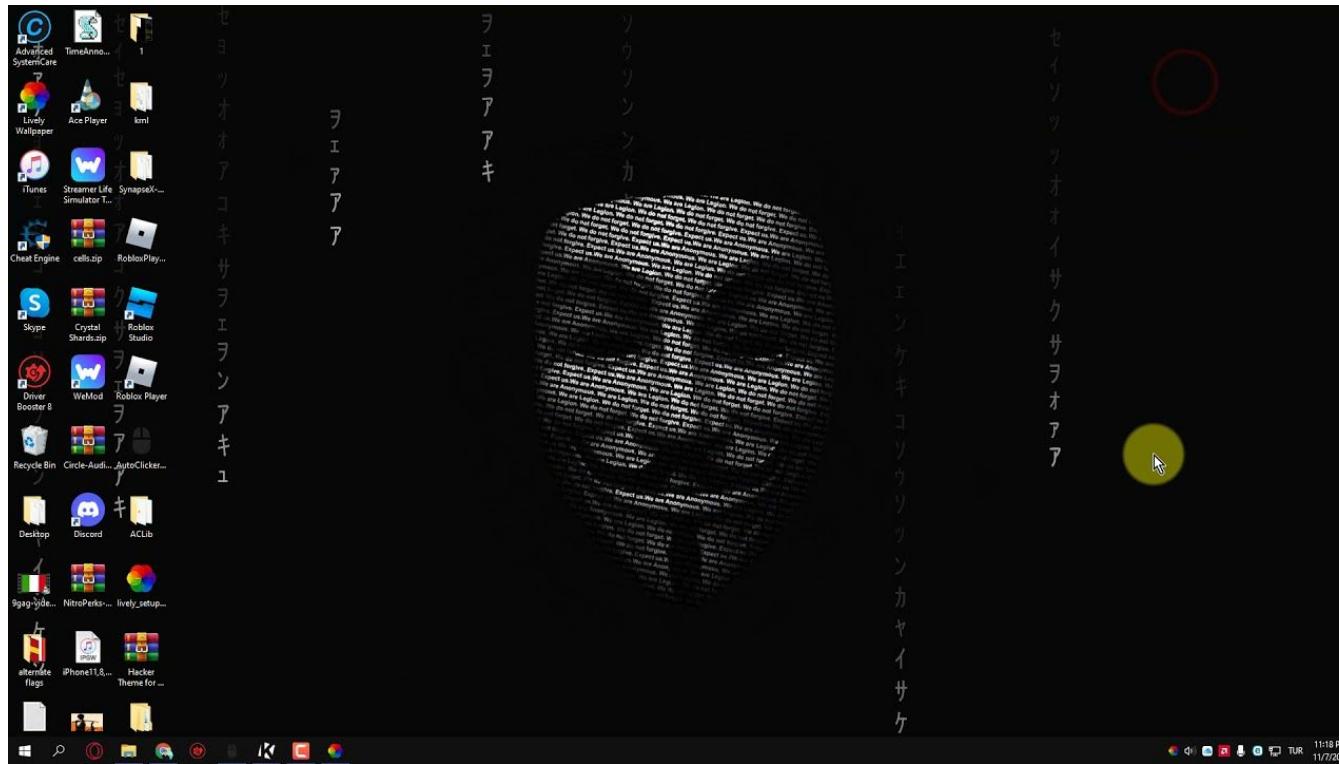
File Signature

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

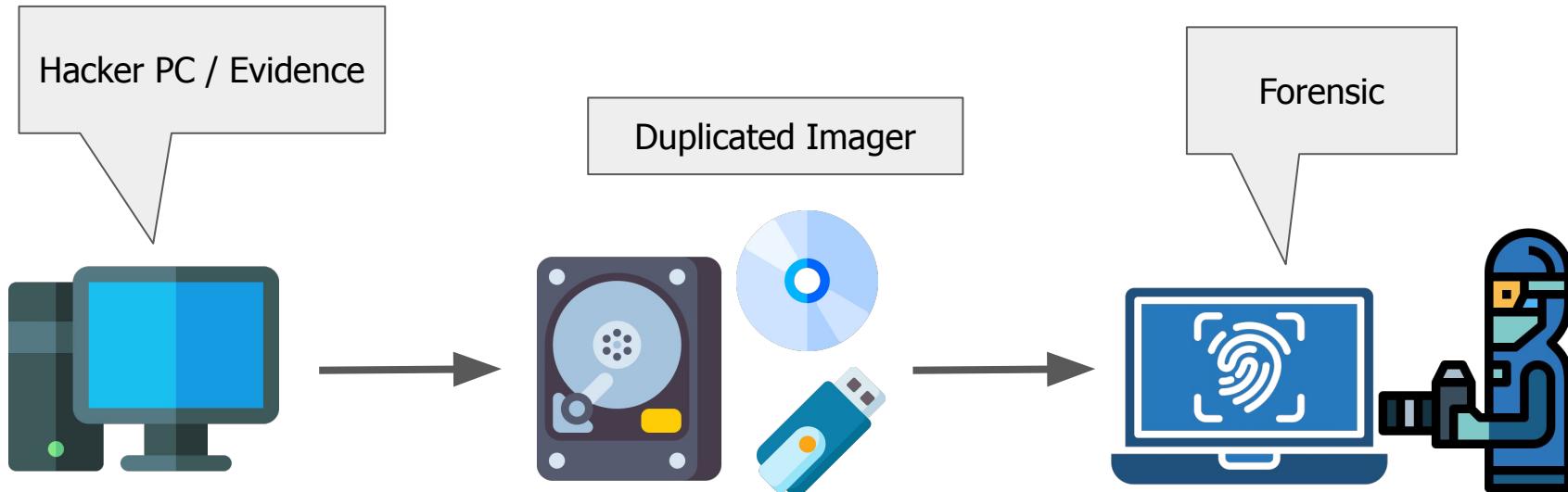
ทำไม File Format และ File Signature ถึงสำคัญ?

- ระบุประเภทของไฟล์
- ตรวจสอบความถูกต้องของไฟล์
- ภัยคุกคามข้อมูล
- ตรวจสอบความปลอดภัย

Disk Imaging



Disk Imaging



ตัวอย่าง Autopsy

008 - Autopsy 4.15.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline File Discovery Generate Report Close Case

261 Results

Listing File System

Table Thumbnail

Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta) K

nb-NO 0 0000-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Unallocated ur

zh-TW 0 0000-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Unallocated ur

connection 0 0000-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Unallocated ur

tool 0 0000-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Unallocated ur

Syst 0 0000-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Unallocated ur

Syst 0 0000-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Unallocated ur

{FD9 0 0000-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Unallocated ur

Jetio 0 0000-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Unallocated ur

Micro 0 0000-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Unallocated ur

Spide 0 0000-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Unallocated ur

XIST 0 0000-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0 Unallocated ur

Save Table as CSV

Extract File(s)

Export selected rows to CSV

Add File Tag Remove File Tag

text Results Annotations Other Occurrences

Add File to Hash Set (Empty File) /vol_vol2/Program Files/ALM6/services/connection

Name

Type File System

MIME Type application/octet-stream

Size 0

File Name Allocation Unallocated

Metadata Allocation

Modified 0000-00-00 00:00:00

Accessed 0000-00-00 00:00:00

Created 0000-00-00 00:00:00

Changed 0000-00-00 00:00:00

MD5 d41d8cd98f00b204e9800998ecf8427e

Hash Lookup Details UNKNOWN

Single Literal Keyword Search (0)

Single Regular Expression Search (0)

File Sources

Data Sources

Mantooth.E01

vol1 (Unallocated: 0-62)

vol2 (NTFS / exFAT (0x07): 63-224909)

vol3 (DOS FAT12 (0x01): 224910-240974)

vol4 (Unallocated: 240975-250878)

Views

File Types

By Extension

By MIME Type

Deleted Files

File System (261)

All (279)

MB File Size

MB 50 - 200MB (2)

MB 200MB - 1GB (0)

MB 1GB+ (0)

Results

Extracted Content

EXIF Metadata (8)

Encryption Detected (2)

Extension Mismatch Detected (9)

Installed Programs (40)

Operating System Information (2)

Operating System User Account (8)

Recent Documents (109)

Recycle Bin (9)

Remote Drive (1)

Shell Bags (110)

USB Device Attached (30)

User Content Suspected (8)

Web Cookies (50)

Web History (374)

Web Search (130)

Keyword Hits

Single Literal Keyword Search (0)

Single Regular Expression Search (0)

ตัวอย่าง FTK Imager

AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree File List

Name	Size	Type	Date Modified
\$130	4	Regular File	05/03/2024 12:55:16
Applicants_info.xlsx.korp	16	Regular File	05/03/2024 12:55:16
ULTIMATUM.hta	4	Regular File	05/03/2024 12:55:16

Custom Content Sources Evidence:File System|Path|File Options

File List

```
</><!-->
<ead>
  <dy>
    <div class='container'>
      <h1><span class='highlight'>The Fray Ultimatum</span></h1>
      <div class='message'>
        <p><span>⚠ ATTENTION FACTIONS ⚠</span></p>
        <p>What's this? Your precious data seems to have fallen into the hands of KORP™, the all-powerful overseer. Consider it a test of your faction's mettle. Will you rise to the challenge or crumble under the weight of your faction's power?</p>
        <p>For further instructions, send your Faction ID to the provided email address:</p>
        <a href="mailto:fray.ultimatum@korp.com">fray.ultimatum@korp.com</a>
      </div>
    </div>
  </dy>
</ead>
```

File hash (Checksum)

DOWNLOAD ETTERCAP SOURCE CODE

The latest Etercap release is: 0.8.3.1-Bertillon
Release date: August 1, 2020

Click to Download the version with bundled libraries



[ettercap-0.8.3.1.tar.gz](#)

Sha1: 9185c59883c8d128b852233c9aa0ae46f772d170

3. การป้องกันการปลอมแปลง

4. ใช้ในการตรวจจับข้อผิดพลาดที่อาจเกิดขึ้นระหว่างการถ่ายโอนข้อมูล

- ตรวจสอบความสมบูรณ์ของไฟล์
- ช่วยในการยืนยันว่าไฟล์ที่ดาวน์โหลดมาจากการแพร่ที่มาที่เชื่อถือได้

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	7e528632ca01c5977da1a0af56a5e05fb383832
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	008fc9a4bbbd67b578699300eb321766cd41fbfff
Mar 26, 2013	ettercap-0.7.6.tar.gz	0.7.6-Locard	55818952a8c28beb1b650f3ccc9600a2d784a18f

Forensic Lab 3 : Verify



ตัวอย่างโจทย์จาก
<https://picoctf.org>

```
(kali㉿kali)-[~/Desktop]
$ tree home
home
└── ctf-player
    └── drop-in
        ├── checksum.txt
        ├── decrypt.sh
        └── files
            ├── 0agQiFLS
            ├── 0pEkV2ds
            ├── 0wWA41ot
            ├── 0yVzp2am
            ├── 12GUEFi0
            ├── 12R70dbh
            ├── 1EQhRC4i
            ├── 1FjaHS3F
            ├── 1cYEYb6L
            ├── 1iXLQGXR
            ├── 2h0QXHZC
            └── 2nsMaCTj
```

```
wr59gSPm
wtPMeWzq
wtq06VT7
wx3RfP7B
xzvNiQwK
yOEWonka
yajqgzPt
ypsNLNOA
ytd5LOm1
yzqsPNuQ
zH4qslwZ
zM5KAlbJ
zMQ1nXew
zWeRABcB
zZe9EIIdH
zhBiEB8c
```

4 directories, 303 files

Identification

?

D
A
T
A

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

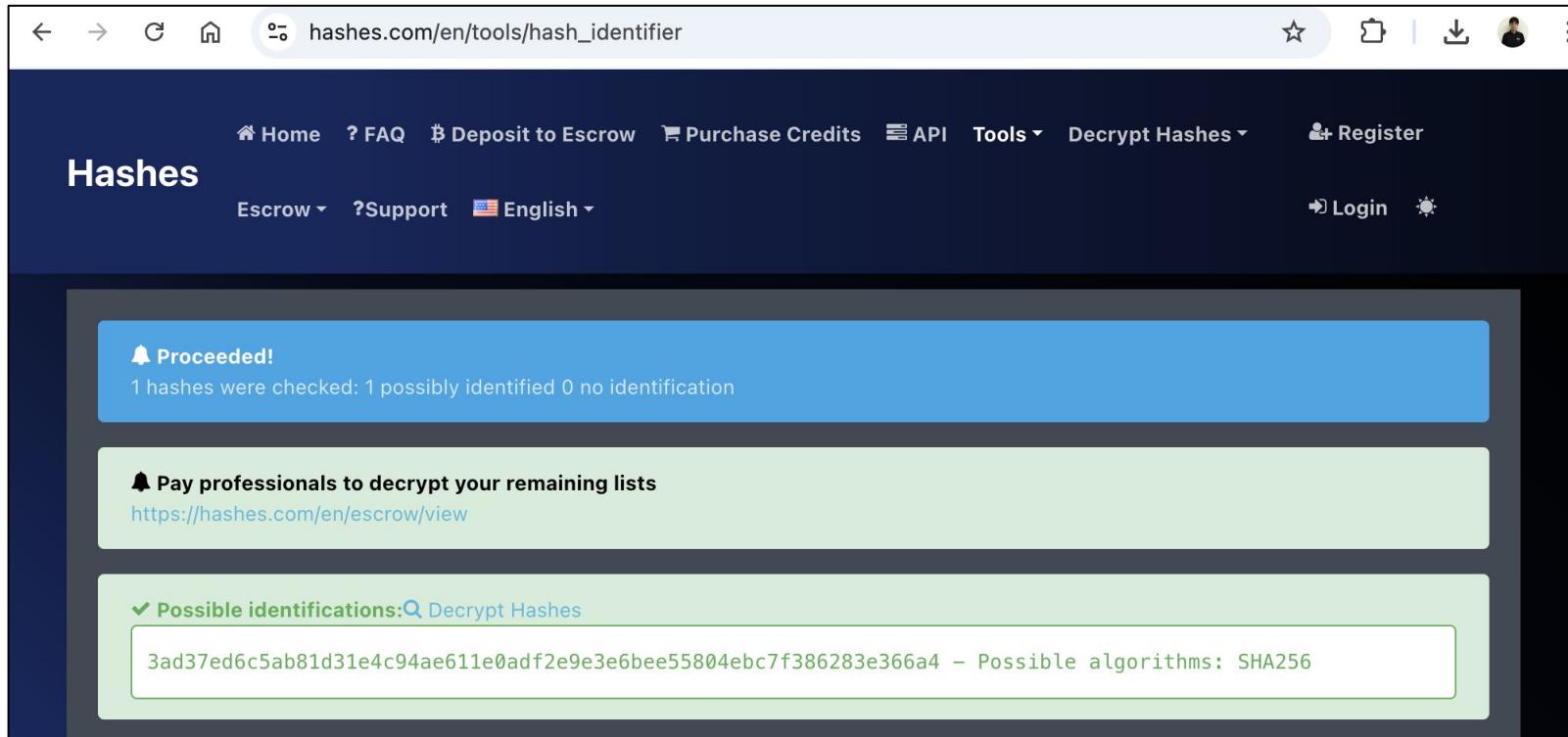
(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
$ cat files/0agQiFLS
RlIF1vdIPAYu97ed5JRBhtZkNAuMHAEo1lthk9ky87Z6qdpqNhHUQEul2zxx9zY

(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
$ cat files/0pEkV2ds
KRhaBTB9ByUUwhhLbbHvOybGIwo07QXHLRKgDACYYpGiisJ5mKUz623IMNxN6HJ

(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
$ cat files/0wWA41ot
6f28qnMeSFYMP6Sq0XVshA99u4obPxptpqkBXXamzmOfhRLHdGKoeqKJIM6otSl
```

Hash Identifier

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



The screenshot shows the Hashes.com website interface for identifying hashes. The URL in the address bar is https://hashes.com/en/tools/hash_identifier. The main navigation menu includes Home, FAQ, Deposit to Escrow, Purchase Credits, API, Tools (dropdown), Decrypt Hashes (dropdown), Register, Login, and language selection (English). A prominent blue banner at the top displays a success message: "Proceeded! 1 hashes were checked: 1 possibly identified 0 no identification". Below this, a green banner encourages users to "Pay professionals to decrypt your remaining lists" with a link to <https://hashes.com/en/escrow/view>. The bottom section shows a green box containing a possible identification for the hash `3ad37ed6c5ab81d31e4c94ae611e0adf2e9e3e6bee55804ebc7f386283e366a4`, which is identified as SHA256.

hashes.com/en/tools/hash_identifier

Home FAQ Deposit to Escrow Purchase Credits API Tools Decrypt Hashes Register

Hashes

Escrow Support English

Login

Proceeded!
1 hashes were checked: 1 possibly identified 0 no identification

Pay professionals to decrypt your remaining lists
<https://hashes.com/en/escrow/view>

Possible identifications: [Decrypt Hashes](#)

3ad37ed6c5ab81d31e4c94ae611e0adf2e9e3e6bee55804ebc7f386283e366a4 – Possible algorithms: SHA256

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	l m2KQa1Hp	uQyUDnOZ
12GUEFi0	9nlUSB5k	GodaoG3e	NoPiZGwa	TSJCXwIT	Y4u4wEGY	dVJ9IeAT	m5c0AhxS	v6LGqmwI
12R70dbh	A0aXQwRy	H3rLRpMi	O2eRM15N	TTjL07LQ	YCf9VpOR	dZVn0thw	mVEKZ3oW	v8sVJPvD
1EQhRC4i	AKEjqj8u	HG10KGnm	OVCZKr6X	ThekmVcy	YG1pCKDt	dkV6p1DF	mcjegRRr	vCUbox39
1FjaHS3F	AeCM4Vvt	HPGHI002	OX3IlkB9	TqHFzH54	YPNiaCgG	dtc6oz6G	n05ZtlwX	vTgToTLG
1cYEYb6L	AhVRy5sU	HRSTilo9	OYpH5Rfs	Tui6wJfr	YdulsHwq	e018b574	n7C2bpPk	vfN94Ek3
1iXLQGXRX	Aqg5GrWn	HchffFzCW	Opx3E3FO	TwspwefZ	YdxjMT1r	e7ir0vB1	nDj0INiw	vnr7vUto

sha256sum

```
(kali㉿kali)-[~/Desktop/home/ctf-player/drop-in]
$ sha256sum files/*
```

885ac35e179e1b2746dcd163d980938090168c594dd7567bf1d60bdd11557df1	files/0agQiFLS
d3cdff8222104727892c6c5f306efccce1ebe53e1510b575dabf838e5c17619b	files/0pEkV2ds
a67c3339a9661ea181bf073e543b47580011bd210b3306497a4ae8c9a2124bd7	files/0wWA41ot
2940827966c3d8b31f87ab008d471dffb0f80c918a669eb34d00909adaf4d406	files/0yVzp2am
645e24226aa77f498951e38713e103659fb7bb41ceccf7cc6268c226ad03d4b9	files/1EqhRC4i
441db2a78012080ec0c3b80d2b5b6d66720297b65db195ead59ea646a0674c6e	files/1FjaHS3F
5170556dbf37f1aab8cb439c7fd8f3e56f8e4aa41ee2e86379ef4190f7623b6f	files/1cYEYb6L
bf5e0d888b16e034331f90067b41834ae50673d9dcffa4c76ee4416836cbe919	files/1iXLQGXr
8313a303c94d4fd615073aedded65df0cdee87d5fd074c25c847b064291ff4b3	files/2h0QXHZC
d63d4ee0d986694f4df69960d5c54c8ea8c3822dd5b5be1065406bb9c03b8a6c	files/2nsMaCTj
16bda5067a52a32595ac140466be993b585c75b0557e012ec874ac813fdd73fd	files/2zpsEiQJ
99c46603b95fc29d95bc71106fadbf95df93182e119097522d8d9efc823b4ef0	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'!
genQR.py      flag2of2-
final.pdf

[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 !!

ແກ່ນ !!!

Binwalk



DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 594 x 1104, 8-bit/color RGBA, non-interlaced
3226	0xC9A	TIFF image data, big-endian, offset of first image director
y: 8		
272492	0x4286C	Zip archive data, at least v2.0 to extract, compressed size
: 378954, uncompressed size: 383938, name: base_images/2_c.jpg		
651612	0x9F15C	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	0x0	PNG image, 526 x 1106, 8-bit/color RGBA, non-interlaced
3226	0xC9A	TIFF image data, big-endian, offset of first image director
y: 8		
187707	0x2DD3B	Zip archive data, at least v2.0 to extract, compressed size
: 196043, uncompressed size: 201445, name: base_images/3_c.jpg		
383805	0x5DB3D	End of Zip archive, footer length: 22
383916	0x5DBAC	End of Zip archive, footer length: 22



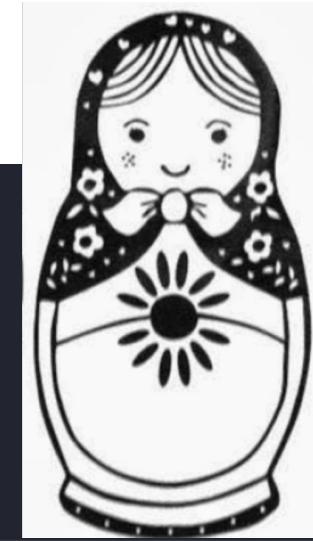
Binwalk

```
(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	0x0	PNG image, 428 x 1104, 8-bit/color RGBA, non-interlaced
3226	0xC9A	TIFF image data, big-endian, offset of first image directory:
123606	0x1E2D6	Zip archive data, at least v2.0 to extract, compressed size:
esssed size: 79807, name: base_images/4_c.jpg		
201423	0x312CF	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  test.JPG image

└──(kali㉿kali)-[~/Desktop/base_images/base_images/base_images]
    $ cat flag.txt
picoCTF{bf6acf878dcfd752f4721e41b1b1b66b}
```



อยากรู้ว่า ฯ ไปฝึกอะไรเพิ่ม