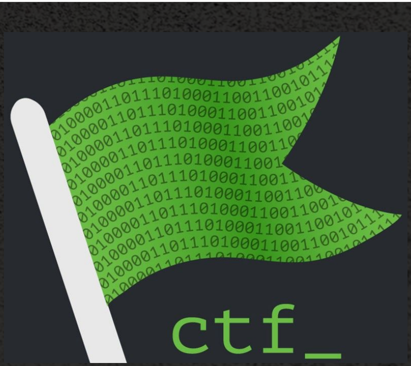
CTFd Platform: http://10.11.3.22:8000/

Register using **fake email and password**

IEEE
Universiti Utara Malaysia
Student Branch

CTF Workshop



Agenda:

1 Intro to Linux

2 Forensic

3 OSINT

4 Web Exploitation

5 Cryptography

./what_is_ctf

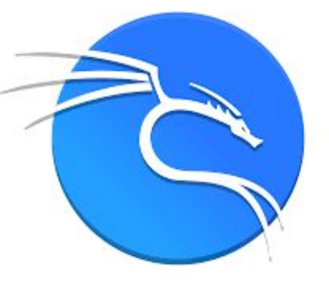
- Cyber-competition solve challenges to find flag
- CTF -> Capture The Flag 🚩🚩🚩
- Types of CTF:
  1. Jeopardy Style (Category-based)
  2. Attack-Defend (Red vs Blue)
  3. Battle of Malware Bypass and EDR (DEFCON 32)

- The goal of each CTF challenge is to find a hidden file or piece of information (the “flag”) somewhere in the target environment.
- secretly hidden in purposefully-vulnerable programs or websites

./why_ctf

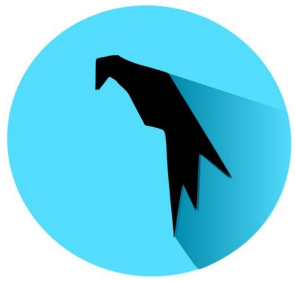
- Hands-On Experience
  - Real-world vulnerabilities, programming, teamwork
- Low Commitment
  - Happen in 24 hours mostly
- Career Kickstart
  - Companies hiring intern with CTF experience
- Community Building
  - Malaysia Top CTF Team

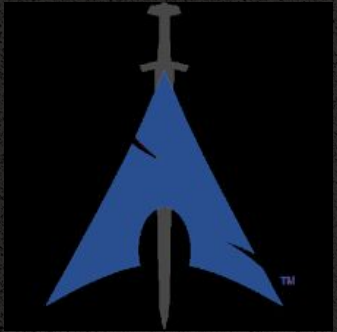
./intro_linux



- 600 penetration testing and forensic tools
- Most wide used and well-support community
- Debian based

- 600 penetration testing and forensic tools
- Attractive environment
- Faster Performance
- Office and basic media tools

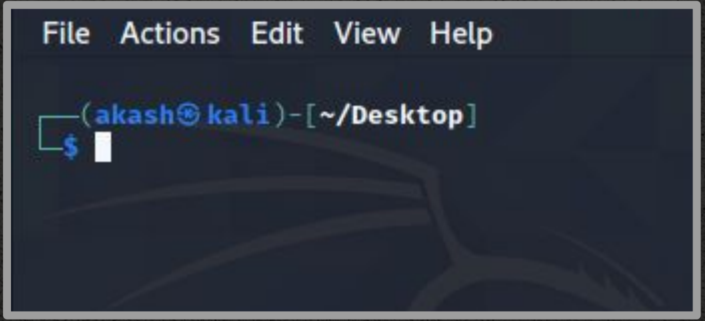




- Arch based (pacman)
- 2700 tools
- For advanced pentester
- Highly customizable and lightweight
- Complex learning curve

List of Common Tools:
https://www.kali.org/tools/
https://parrotsec.org/docs/category/tools/
https://blackarch.org/tools.html

./intro_linux



```
┌──(akash㉿kali)-[~/Desktop]
└─$ 
```

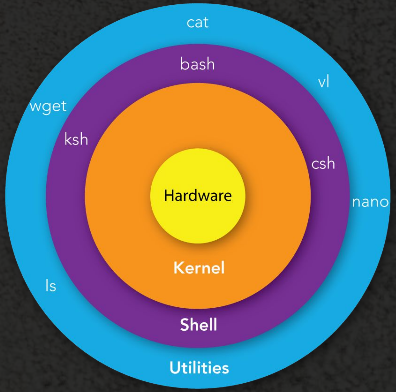
<- This is your Linux Terminal

Is the same as Windows Command Prompt and Powershell, but different

Ctrl+Alt+T to open terminal

Why use Terminal, why not GUI:

1. Speed, Efficiency and Flexibility
2.Remote Access and SSH
3. Lightweight (GUI consume more RAM space)
4. Control & Precision
5. Automation using bash scripting

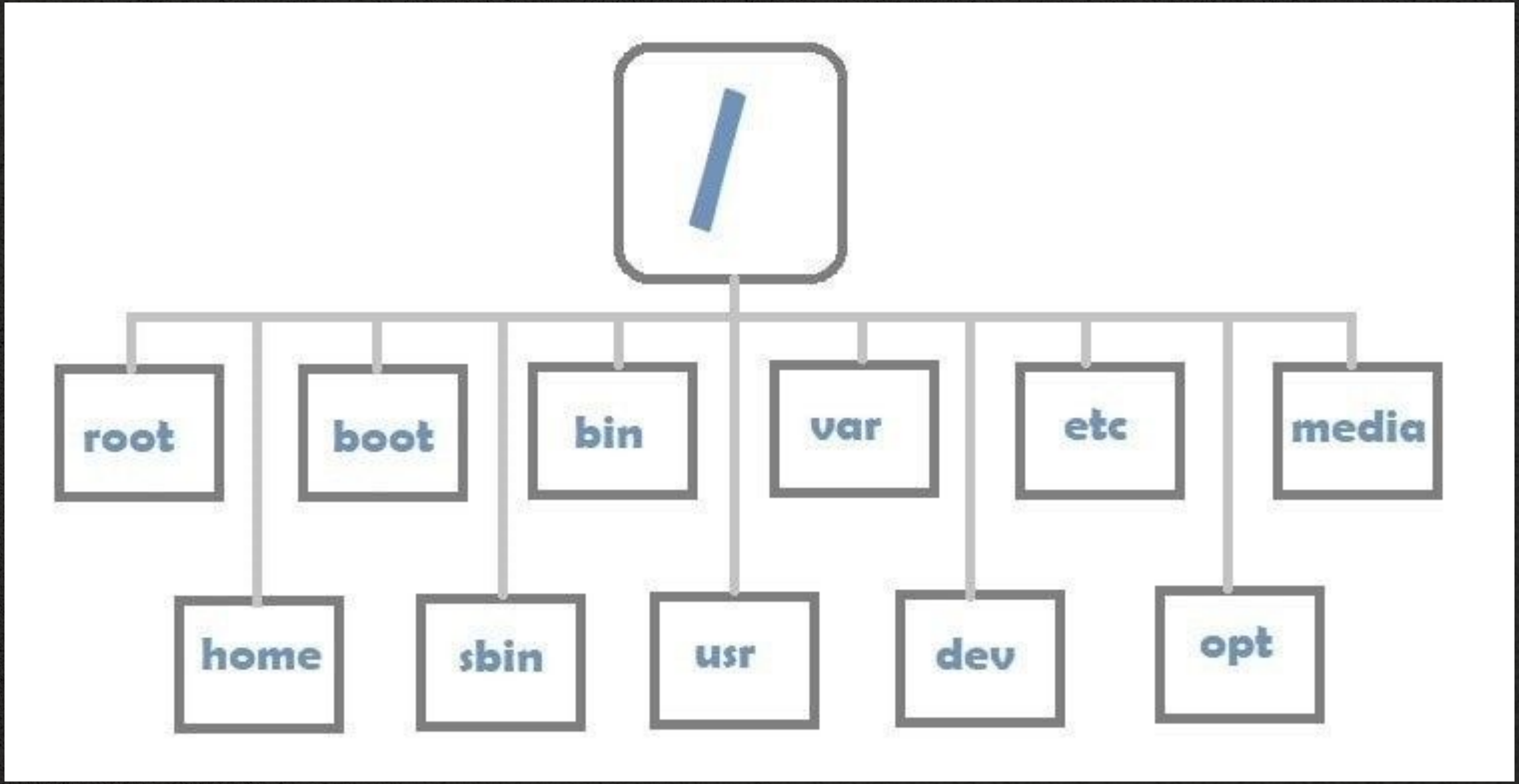


./intro_linux

Lets try some commands:

`$ echo “Hello World”`	Print string, this case “Hello World”
`$ pwd`	Print Working Directory
`$ cd /`	Change to Root directory
`$ cd root`	Change “root” directory with root privileges
`$ sudo su`	Super-User Do (switch to Root Privileges)
`$ cd root`	Change Directory to Root Directory
`$ exit`	Exit from Root Privileges, “exit” again will close terminal
`$ cd ~`	Change to home directory

./intro_linux



./intro_linux

Let's try a lil bit harder commands:

`$ cd ~/Desktop`	Change directory to Desktop
`$ mkdir test1 && cd test1`	Make new directory “test1” and go into “test1”
`$ gedit test-1.txt`	Make new txt file “test-1.txt”
`$ cd .. && mkdir test2`	Go out of “test1” directory and make new directory “test 2
`$ cp test1/test-1.txt test2/`	Copy “test-1.txt” from “test1” to “test2” directory
`$ rm test1/test-1.txt`	Remove/delete “test-1.txt” from test1 directory
`$ cd test2 && cat test-1.txt`	Change directory to “test2” and concat “test-1.txt”
`$ mv test-1.txt test-2.txt`	Rename “test-1.txt” to “test-2.txt”

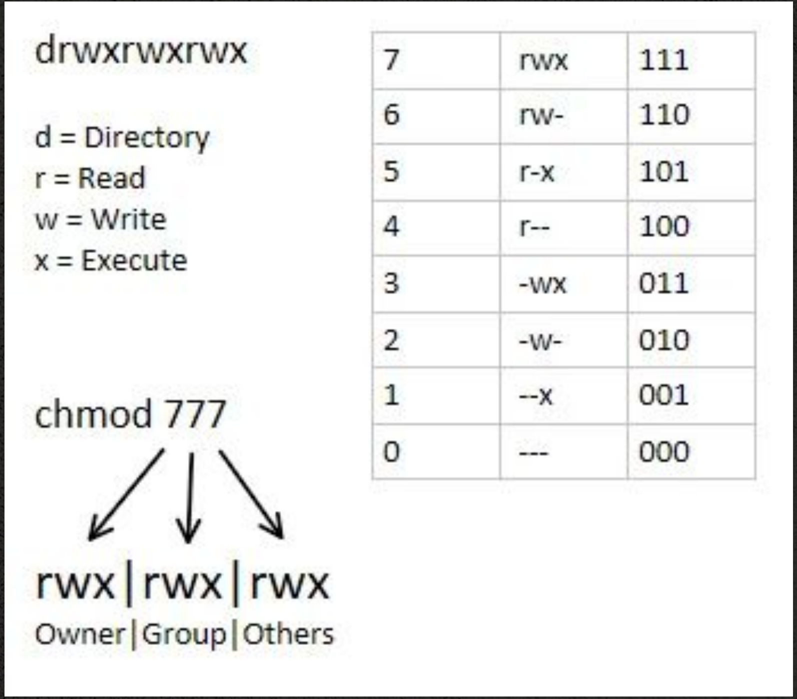
./intro_linux

Summary of simple commands:

`$ ls`	List all the files in a directory
`$ pwd`	Show current working directory path
`$ cd`	Change directory
`$ mkdir`	Create a new directory
`$ rm`	Deletes a file
`$ cp`	Copies files and directory, for directory use <`$ cp -r`>
`$ mv`	Moves or rename files and directories
`$ file`	Check a file type

Let's find some flagzz

./intro_linux



drwxrwxrwx

d = Directory
r = Read
w = Write
x = Execute

chmod 777

rwx|rwx|rwx
Owner|Group|Others

7	rwx	111
6	rw-	110
5	r-x	101
4	r--	100
3	-wx	011
2	-w-	010
1	--x	001
0	---	000

To view the permissions for all files in directory:

```
$ ls -lah
```

Read by owner -> 400
Write by owner -> 200
Execute by owner -> 100
Read by group -> 040
Write by group -> 020
Execute by group -> 010
Read by others -> 004
Write by others-> 002
Execute by others ->001

./run_memes

Let’s take 5 and enjoy some memes

```
$ alias cd='rm -rf'
```

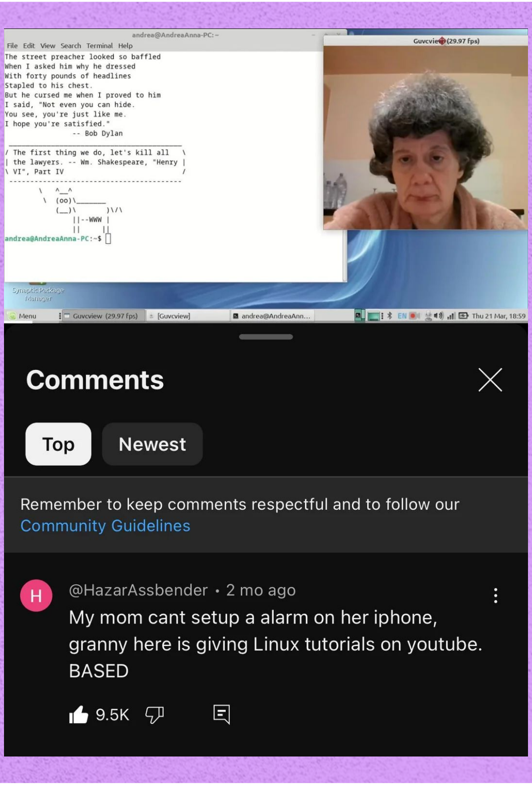
This command means when user type in $ cd, instead of changing directory, it deletes files and directories

./run_memes

When a malicious site downloads an .exe file into your Linux machine
YOU HAVE NO POWER HERE

CAT COMMAND
HAS NOTHING TO DO WITH CATS
quickmeme.com

./run_memes



```
The street preacher looked so baffled
When I asked him why he dressed
With forty pounds of headlines
Stapled to his chest.
But he cursed me when I proved to him
I said, "Not even you can hide.
You see, you're just like me.
I hope you're satisfied."
                -- Bob Dylan
 ________________________________________
/ The first thing we do, let's kill all  \
| the lawyers. -- Wm. Shakespeare, "Henry |
\ VI", Part IV                           /
 ----------------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||--WWW |
                ||     ||
andrea@AndreaAnna-PC:~$ 
```

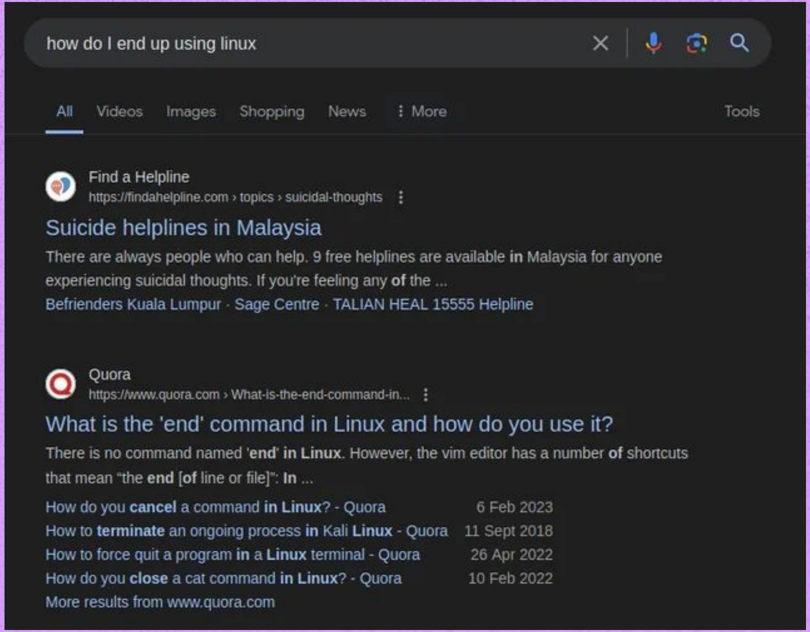
Comments

Remember to keep comments respectful and to follow our Community Guidelines

@HazarAssbender • 2 mo ago

My mom cant setup a alarm on her iphone, granny here is giving Linux tutorials on youtube. BASED

9.5K



how do I end up using linux

Find a Helpline
https://findahelpline.com › topics › suicidal-thoughts

Suicide helplines in Malaysia

There are always people who can help. 9 free helplines are available **in** Malaysia for anyone experiencing suicidal thoughts. If you're feeling any **of** the ...

Befrienders Kuala Lumpur · Sage Centre · TALIAN HEAL 15555 Helpline

Quora
https://www.quora.com › What-is-the-end-command-in...

What is the 'end' command in Linux and how do you use it?

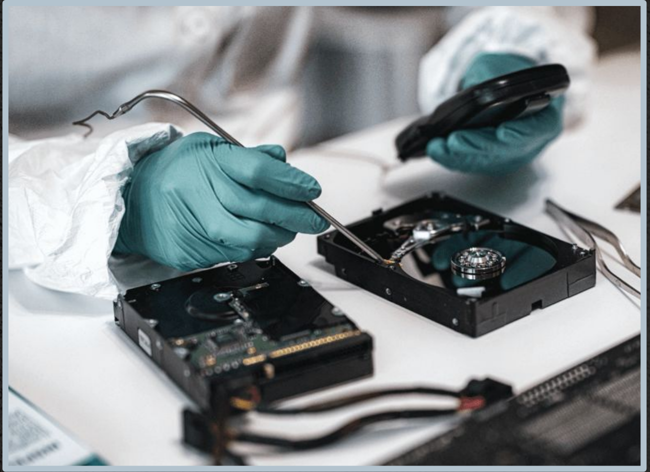
There is no command named '**end**' **in Linux**. However, the vim editor has a number **of** shortcuts that mean "the **end** [**of** line or file]": **In** ...

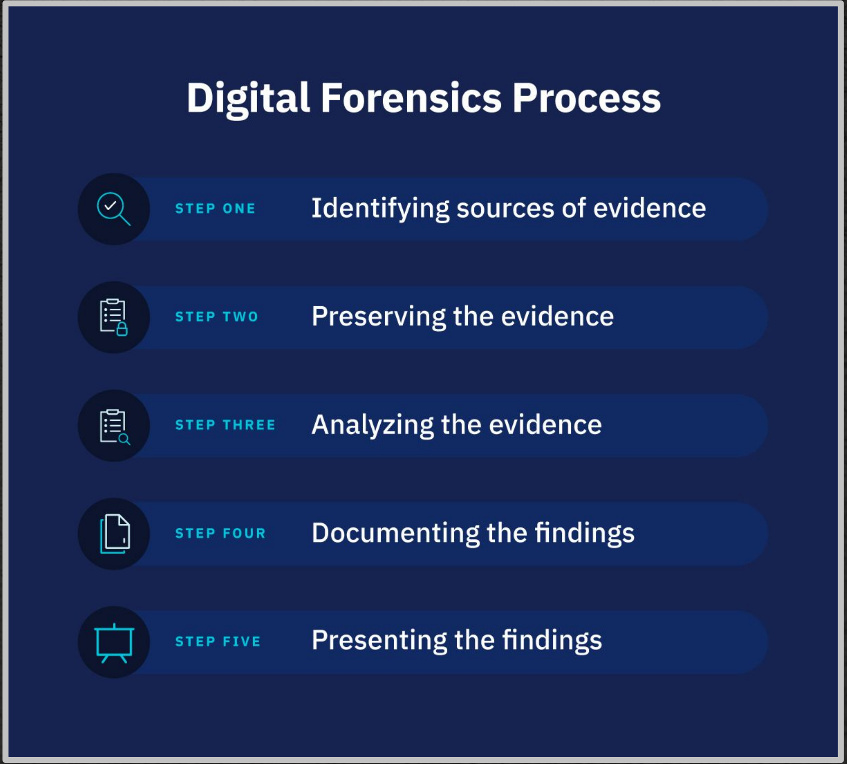
How do you **cancel** a command **in Linux**? - Quora 6 Feb 2023
How to **terminate** an ongoing process **in** Kali **Linux** - Quora 11 Sept 2018
How to force quit a program **in** a **Linux** terminal - Quora 26 Apr 2022
How do you **close** a cat command **in Linux**? - Quora 10 Feb 2022
More results from www.quora.com

./forensic_intro

Forensic is the activity of recovering digital trail left on device or network.

Many methods to find data which was deleted, not stored, or worse covertly recorded.





Digital Forensics Process

STEP ONE Identifying sources of evidence

STEP TWO Preserving the evidence

STEP THREE Analyzing the evidence

STEP FOUR Documenting the findings

STEP FIVE Presenting the findings

./forensic_intro

Usually some similar themes:

- Look for little weird tricks
  - Can a zip file appended to JPEG ?
  - Can a file both a PDF and an exe ?

- Application of off-the-shelf software
  - Oh it's a dump of virtual memory
  - There's a Python script somewhere to parses dump of virtual memory to rebuild all process memory from PTEs

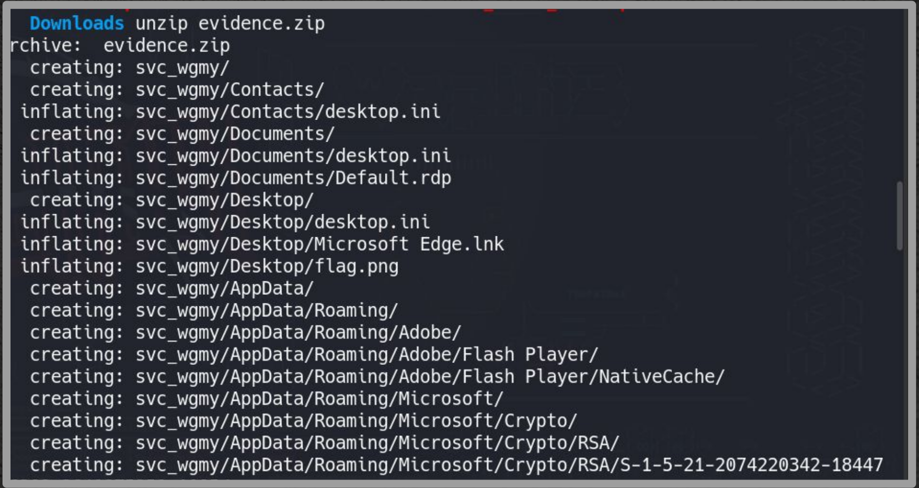
- File Format Identification
  - Magic bytes, header data and trailer data (89 50 4E 47)
  - Corrupted file hex signature

- Filesystem (DIsk Image), PCAP, Memory Dump, Syslog and etc

./forensic_archive_files

- CTF Challenges usually contained in a zip, 7z, rar, tar or tgz file
- Goal: To extract a file from the archive and file the flag from a file that is embedded or hidden

1. Zip file
   - $ unzip
   - $ zipdetails -v
   - $ zipinfo
2. RAR file
   - $ unrar x
3. 7z file
   - $ 7z x
4. tar.gz file
   - $ tar xzvf



```
 Downloads unzip evidence.zip
rchive:  evidence.zip
   creating: svc_wgmy/
   creating: svc_wgmy/Contacts/
  inflating: svc_wgmy/Contacts/desktop.ini
   creating: svc_wgmy/Documents/
  inflating: svc_wgmy/Documents/desktop.ini
  inflating: svc_wgmy/Documents/Default.rdp
   creating: svc_wgmy/Desktop/
  inflating: svc_wgmy/Desktop/desktop.ini
  inflating: svc_wgmy/Desktop/Microsoft Edge.lnk
  inflating: svc_wgmy/Desktop/flag.png
   creating: svc_wgmy/AppData/
   creating: svc_wgmy/AppData/Roaming/
   creating: svc_wgmy/AppData/Roaming/Adobe/
   creating: svc_wgmy/AppData/Roaming/Adobe/Flash Player/
   creating: svc_wgmy/AppData/Roaming/Adobe/Flash Player/NativeCache/
   creating: svc_wgmy/AppData/Roaming/Microsoft/
   creating: svc_wgmy/AppData/Roaming/Microsoft/Crypto/
   creating: svc_wgmy/AppData/Roaming/Microsoft/Crypto/RSA/
   creating: svc_wgmy/AppData/Roaming/Microsoft/Crypto/RSA/S-1-5-21-2074220342-18447
```

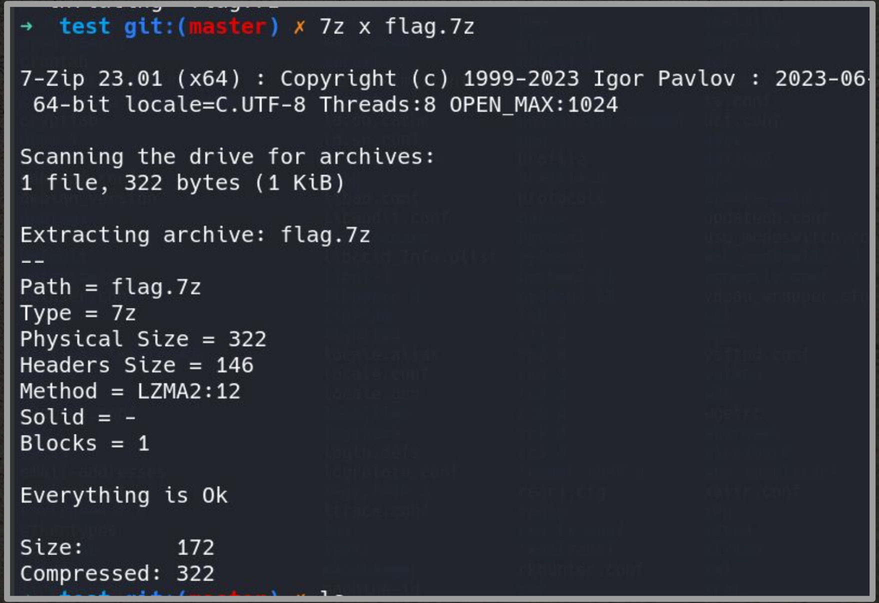
./forensic_archive_files

- CTF Challenges usually contained in a zip, 7z, rar, tar or tgz file
- Goal: To extract a file from the archive and file the flag from a file that is embedded or hidden

5. XZ file
- $ xz -d

6. bz2 file
- $ bzip2 -d

7. gzip file
- $ gzip -d



```
➜  test git:(master) ✗ 7z x flag.7z

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06
 64-bit locale=C.UTF-8 Threads:8 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 322 bytes (1 KiB)

Extracting archive: flag.7z
--
Path = flag.7z
Type = 7z
Physical Size = 322
Headers Size = 146
Method = LZMA2:12
Solid = -
Blocks = 1

Everything is Ok

Size:       172
Compressed: 322
```

./run_forensic_meme

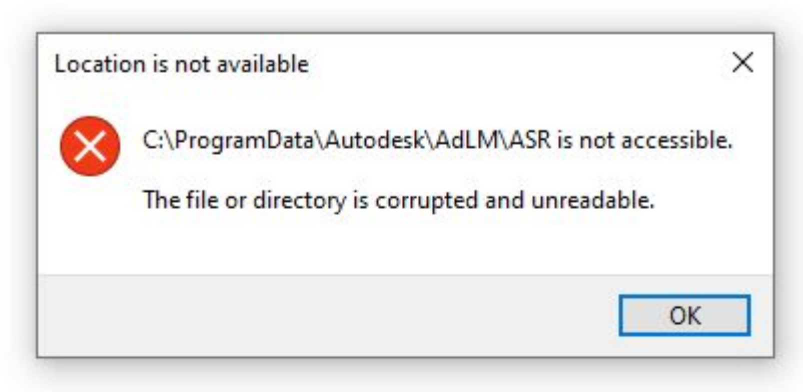
WHEN THEY TELL YOU DIGITAL FORENSICS IS A LOT OF GOOGLING THINGS
You just insulted my entire FIELD OF KNOWLEDGE
But yes.
imgflip.com

IS TRUE, FORENSIC DOES GOOGLE A LOT

./forensic_file_analysis

What is File Forensic:

- The practise of analyzing digital files to recover evidence or understand file properties and contents



Location is not available

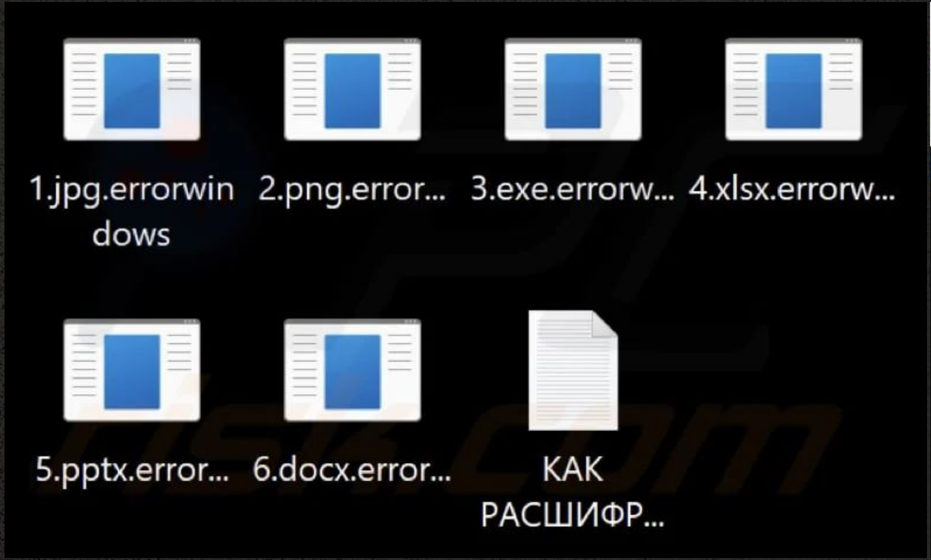
C:\ProgramData\Autodesk\AdLM\ASR is not accessible.

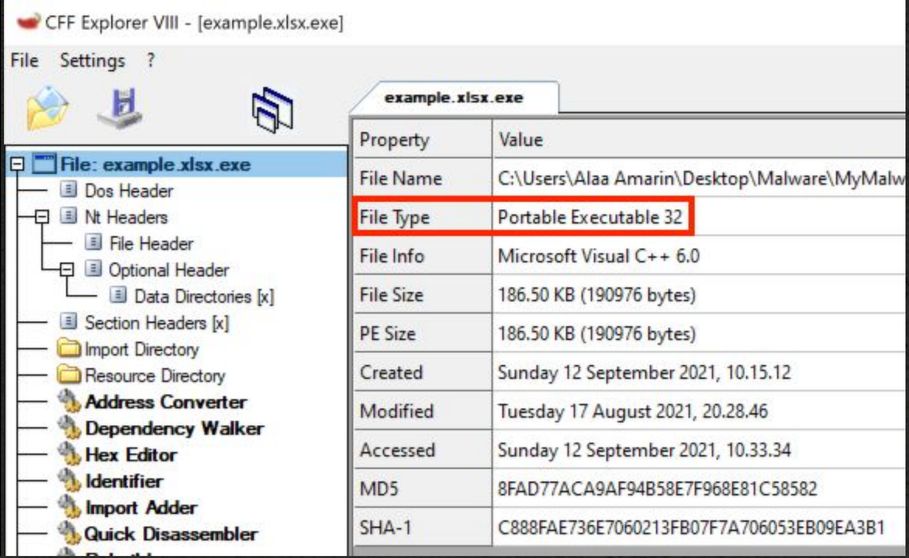
The file or directory is corrupted and unreadable.

Purpose:

- Recover deleted or hidden information
- Understand file creation and modification details
- Identify malicious software or unauthorized changes

./forensic_file_analysis





Property	Value
File Name	C:\Users\Alaa Amarin\Desktop\Malware\MyMalw
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	186.50 KB (190976 bytes)
PE Size	186.50 KB (190976 bytes)
Created	Sunday 12 September 2021, 10.15.12
Modified	Tuesday 17 August 2021, 20.28.46
Accessed	Sunday 12 September 2021, 10.33.34
MD5	8FAD77ACA9AF94B58E7F968E81C58582
SHA-1	C888FAE736E7060213FB07F7A706053EB09EA3B1

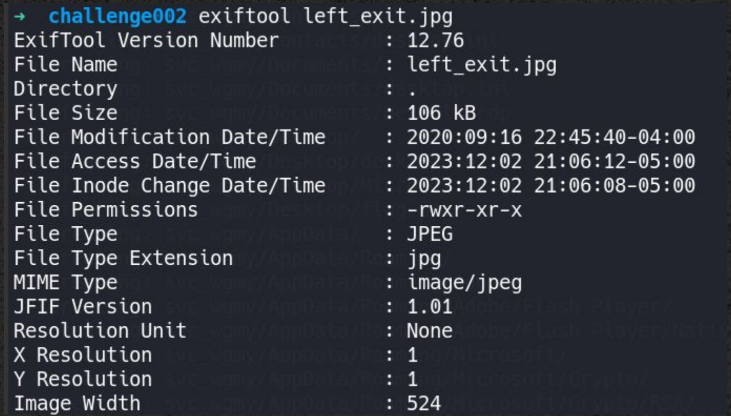
./forensic_file_analysis

Tools for file analysis:

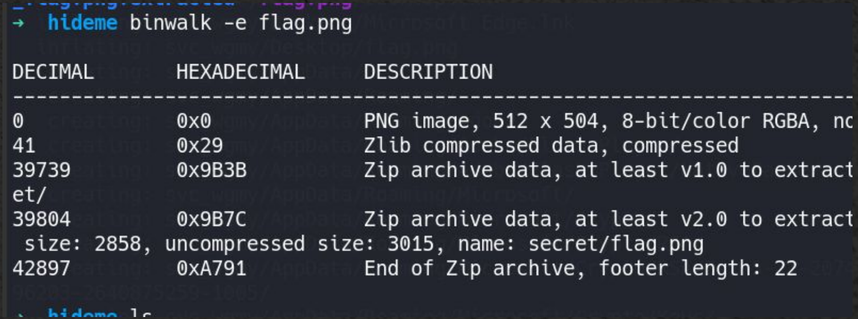
1. $ exiftool
- Extract all metadata of a digital file

2. $ ghex (for advanced use $ xxd)
- View, edit data from any file
- Also used by kids who cheat at computer games, by adding score or lives to saved games.

3. $ binwalk
- File extraction (embedded file within the main file)
- Signature Scanning (Magic Hex)



```
→  challenge002 exiftool left_exit.jpg
ExifTool Version Number         : 12.76
File Name                       : left_exit.jpg
Directory                       : .
File Size                       : 106 kB
File Modification Date/Time     : 2020:09:16 22:45:40-04:00
File Access Date/Time           : 2023:12:02 21:06:12-05:00
File Inode Change Date/Time     : 2023:12:02 21:06:08-05:00
File Permissions                : -rwxr-xr-x
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 524
```



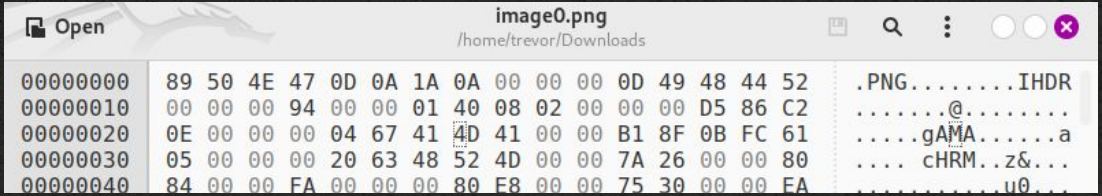
```
→  hideme binwalk -e flag.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 512 x 504, 8-bit/color RGBA, nc
41            0x29            Zlib compressed data, compressed
39739         0x9B3B          Zip archive data, at least v1.0 to extract
et/
39804         0x9B7C          Zip archive data, at least v2.0 to extract
 size: 2858, uncompressed size: 3015, name: secret/flag.png
42897         0xA791          End of Zip archive, footer length: 22

→  hideme ls
```

./forensic_file_analysis

Image Forensic Analysis

- Know the Magic Hex Signature (Header, Trailer, Body)
- https://gist.github.com/leommoore/f9e57ba2aa4bf197ebc5
- https://www.garykessler.net/library/file_sigs.html
- https://asecuritysite.com/forensics/png?file=%2Flog%2Fbasn0g01.png

Example: PNG Image



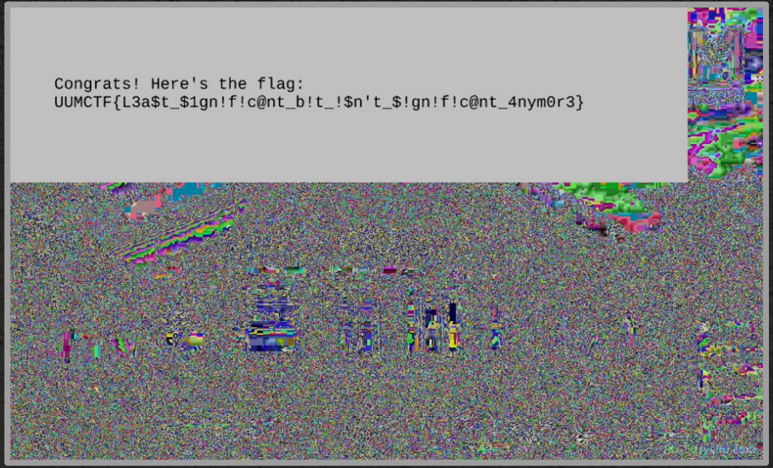
```
00000000  89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  .PNG........IHDR
00000010  00 00 00 94 00 00 01 40 08 02 00 00 00 D5 86 C2  .......@........
00000020  0E 00 00 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61  .....gAMA......a
00000030  05 00 00 00 20 63 48 52 4D 00 00 7A 26 00 00 80  .... cHRM..z&...
00000040  84 00 00 FA 00 00 00 80 E8 00 00 75 30 00 00 EA  ............u0...
```

Header: 89 50 4E 47 (.PNG)
Trailer: AE 42 60 82 (IEND)

For Scanning Signature Analysis:
[PNG file, sig: 89504E470D0A1A0A] → Malware Analysis

./time_for_some_flags

./forensic_steganography



```
Congrats! Here's the flag:
UUMCTF{L3a$t_$1gn!f!c@nt_b!t_!$n't_$!gn!f!c@nt_4nym0r3}
```

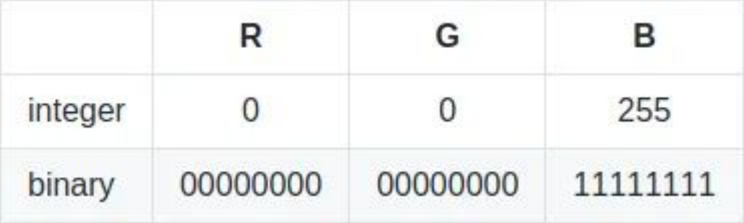
The art of hiding data in images or audio
Popular CTF challenge and it might be a separate category by itself
Common Methods:

- LSB (Least Significant Bit)
- Discrete Fourier Transform (DFT)
- Palette-Based Technique

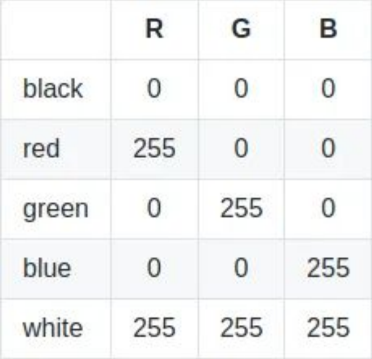
./forensic_steganography

Understanding How LSB Works:

- Each image has pixels with 3 channel of RGB
- Each channel needs 1 byte (8 bits of 1’s and 0’s)

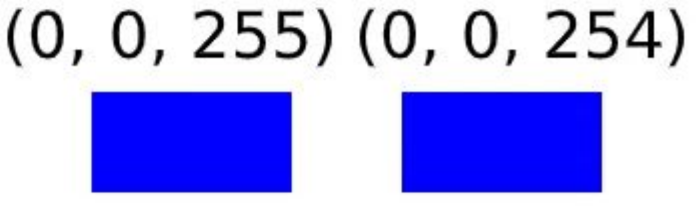


	R	G	B
integer	0	0	255
binary	00000000	00000000	11111111



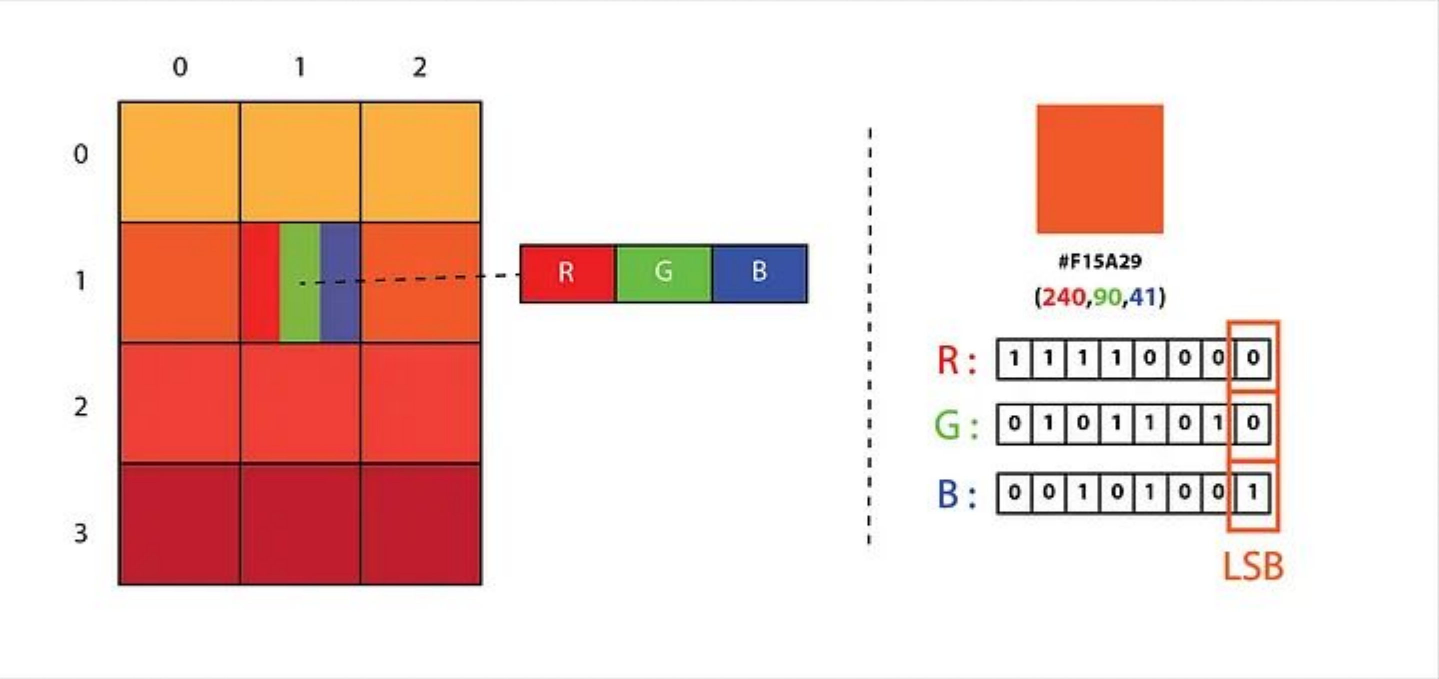
	R	G	B
black	0	0	0
red	255	0	0
green	0	255	0
blue	0	0	255
white	255	255	255

If we change a single bit of the pixel, the last one (LSB), the result doesn't appeal to be very different.



So message are decoded in binary from ASCII:
Example: Letter ‘A’ -> ASCII value 97 -> 01100001
First pixel : 0 1 1; Second pixel: 0 0 0; Third pixel: 0 1

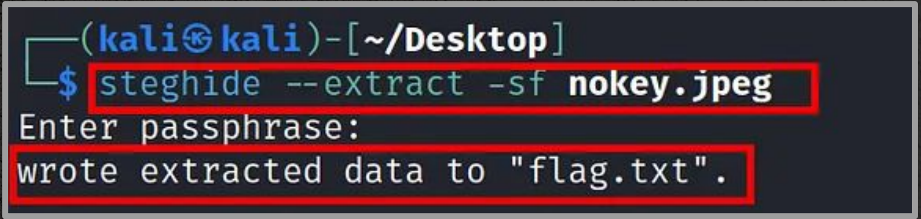
./forensic_steganography



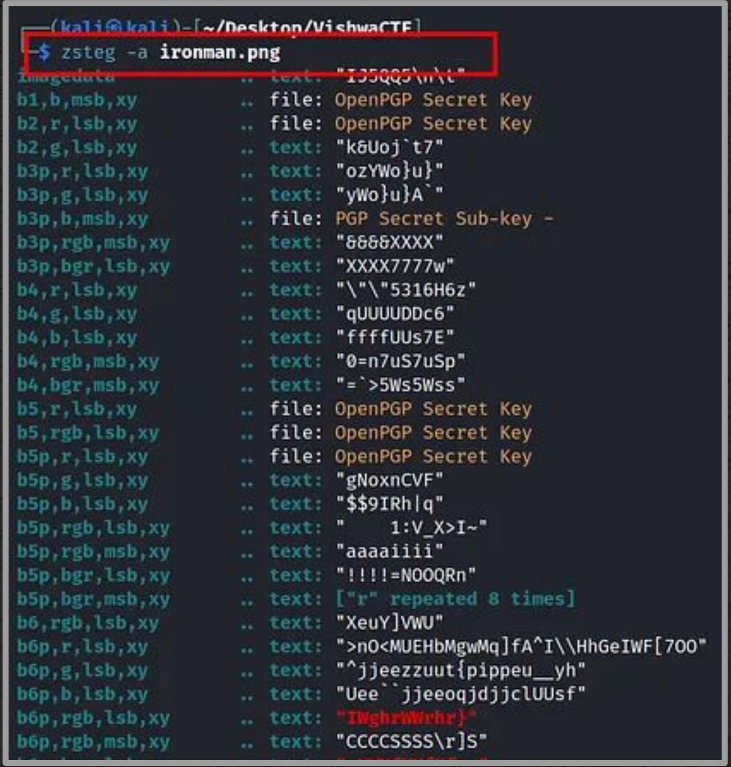
./forensic_steganography

Common tools for steganography challenge:

- Strings
- File
- Exiftool
- Binwalk
- Zsteg
- Steghide
- Sonic Visualizer
- Audacity



```
┌──(kali㉿kali)-[~/Desktop]
└─$ steghide --extract -sf nokey.jpeg
Enter passphrase:
wrote extracted data to "flag.txt".
```



```
┌──(kali㉿kali)-[~/Desktop/VishwaCTF]
└─$ zsteg -a ironman.png
imagedata           .. text: "I35QQ5\n\t"
b1,b,msb,xy         .. file: OpenPGP Secret Key
b2,r,lsb,xy         .. file: OpenPGP Secret Key
b2,g,lsb,xy         .. text: "k&Uoj`t7"
b3p,r,lsb,xy        .. text: "ozYWo}u}"
b3p,g,lsb,xy        .. text: "yWo}u}A`"
b3p,b,msb,xy        .. file: PGP Secret Sub-key -
b3p,rgb,msb,xy      .. text: "&&&&XXXX"
b3p,bgr,lsb,xy      .. text: "XXXX7777w"
b4,r,lsb,xy         .. text: "\"\"5316H6z"
b4,g,lsb,xy         .. text: "qUUUUDDc6"
b4,b,lsb,xy         .. text: "ffffUUs7E"
b4,rgb,msb,xy       .. text: "0=n7uS7uSp"
b4,bgr,msb,xy       .. text: "=`>5Ws5Wss"
b5,r,lsb,xy         .. file: OpenPGP Secret Key
b5,rgb,lsb,xy       .. file: OpenPGP Secret Key
b5p,r,lsb,xy        .. file: OpenPGP Secret Key
b5p,g,lsb,xy        .. text: "gNoxnCVF"
b5p,b,lsb,xy        .. text: "$$9IRh|q"
b5p,rgb,lsb,xy      .. text: "    1:V_X>I~"
b5p,rgb,msb,xy      .. text: "aaaaiiii"
b5p,bgr,lsb,xy      .. text: "!!!!=NOOQRn"
b5p,bgr,msb,xy      .. text: ["r" repeated 8 times]
b6,rgb,lsb,xy       .. text: "XeuY]VWU"
b6p,r,lsb,xy        .. text: ">nO<MUEHbMgwMq]fA^I\\HhGeIWF[7OO"
b6p,g,lsb,xy        .. text: "^jjeezzuut{pippeu__yh"
b6p,b,lsb,xy        .. text: "Uee``jjeeoqjdjjclUUsf"
b6p,rgb,lsb,xy      .. text: "IWghrWWrhr}"
b6p,rgb,msb,xy      .. text: "CCCCSSSS\r]S"
```

./osint_intro

OSINT -> Open Source Intelligence

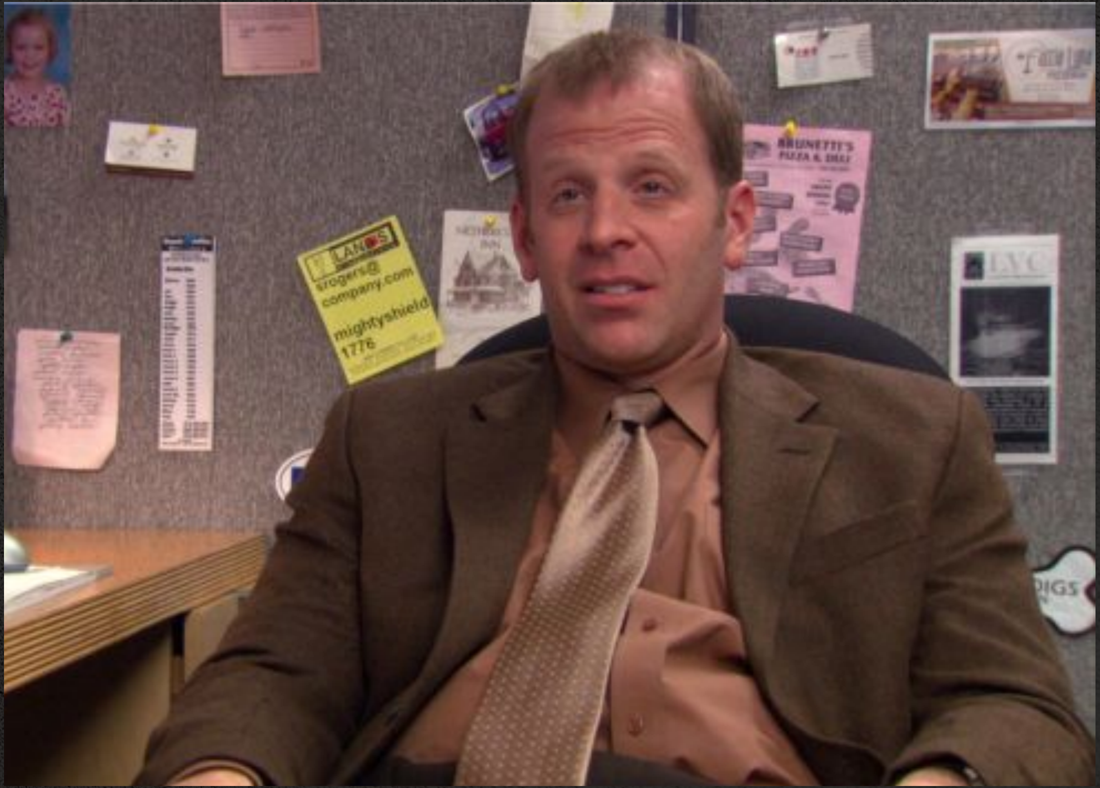
- Gathering information from public sources
- Google, Social Media, company websites and etc.
- In cyber, term “recon” is to collect as much information to perform attack

Not just for ethical hacking, for cybercrime division is useful to:

https://www.youtube.com/watch?v=3xKzuquqvBE&rco=1

From a video, they able to find out which boat is and find out who is responsible for the crime

./osint_intro

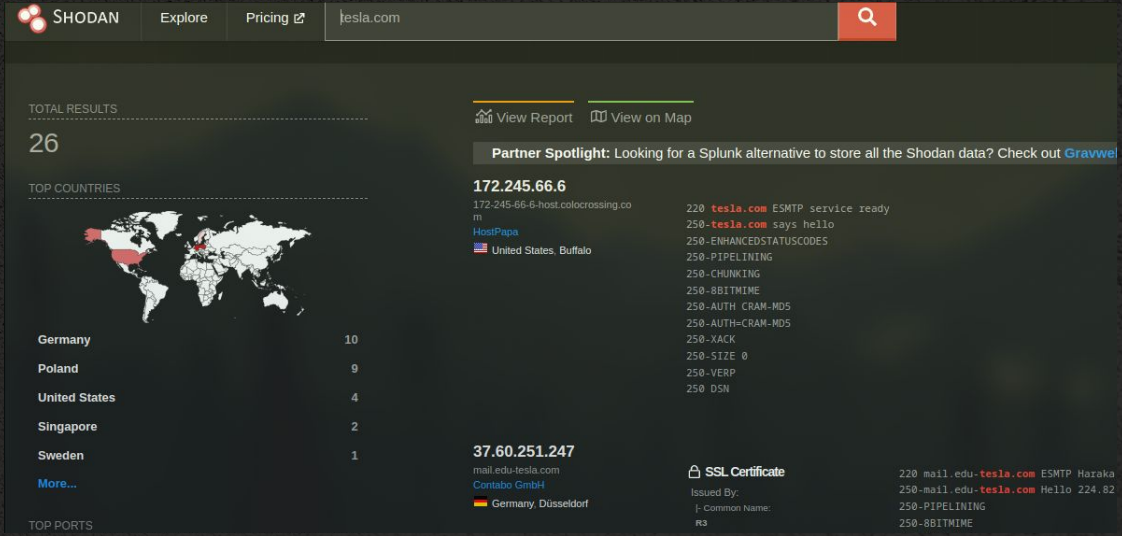


From this image, we can know his email and password, this is how OSINT works

Basically how hackers use information that we as users expose it publicly or unintentionally

./osint_tools

1. osintframework
2. sherlock
3. maltego
4. Shodan
5. Recon-Ng
6. WayBack machine
7. theHarvester



TOTAL RESULTS

26

TOP COUNTRIES

Germany	10
Poland	9
United States	4
Singapore	2
Sweden	1

TOP PORTS

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out Gravwel

172.245.66.6
172-245-66-6-host.colocrossing.com
HostPapa
United States, Buffalo

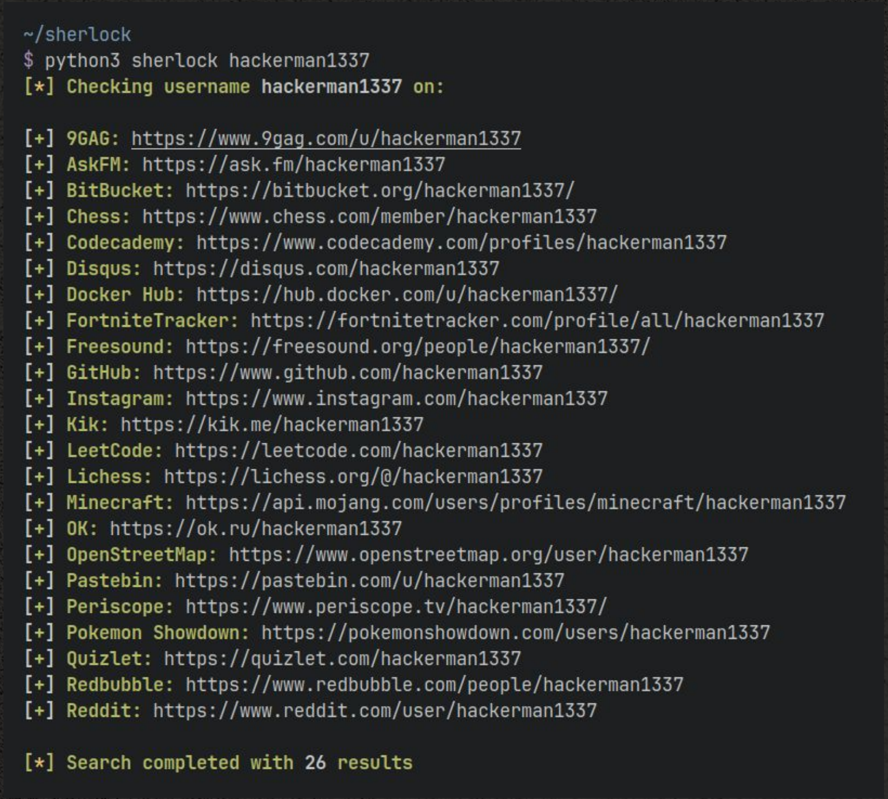
```
220 tesla.com ESMTP service ready
250-tesla.com says hello
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250-8BITMIME
250-AUTH CRAM-MD5
250-AUTH=CRAM-MD5
250-XACK
250-SIZE 0
250-VERP
250 DSN
```

37.60.251.247
mail.edu-tesla.com
Contabo GmbH
Germany, Düsseldorf

SSL Certificate
Issued By:
|- Common Name:
R3

```
220 mail.edu-tesla.com ESMTP Haraka
250-mail.edu-tesla.com Hello 224.82
250-PIPELINING
250-8BITMIME
```

./osint_with_sherlock 🕵️



```
~/sherlock
$ python3 sherlock hackerman1337
[*] Checking username hackerman1337 on:

[+] 9GAG: https://www.9gag.com/u/hackerman1337
[+] AskFM: https://ask.fm/hackerman1337
[+] BitBucket: https://bitbucket.org/hackerman1337/
[+] Chess: https://www.chess.com/member/hackerman1337
[+] Codecademy: https://www.codecademy.com/profiles/hackerman1337
[+] Disqus: https://disqus.com/hackerman1337
[+] Docker Hub: https://hub.docker.com/u/hackerman1337/
[+] FortniteTracker: https://fortnitetracker.com/profile/all/hackerman1337
[+] Freesound: https://freesound.org/people/hackerman1337/
[+] GitHub: https://www.github.com/hackerman1337
[+] Instagram: https://www.instagram.com/hackerman1337
[+] Kik: https://kik.me/hackerman1337
[+] LeetCode: https://leetcode.com/hackerman1337
[+] Lichess: https://lichess.org/@/hackerman1337
[+] Minecraft: https://api.mojang.com/users/profiles/minecraft/hackerman1337
[+] OK: https://ok.ru/hackerman1337
[+] OpenStreetMap: https://www.openstreetmap.org/user/hackerman1337
[+] Pastebin: https://pastebin.com/u/hackerman1337
[+] Periscope: https://www.periscope.tv/hackerman1337/
[+] Pokemon Showdown: https://pokemonshowdown.com/users/hackerman1337
[+] Quizlet: https://quizlet.com/hackerman1337
[+] Redbubble: https://www.redbubble.com/people/hackerman1337
[+] Reddit: https://www.reddit.com/user/hackerman1337

[*] Search completed with 26 results
```

Usage:
$ sherlock <target username>

Easy as it is but be patient

Substitute of sherlocks:
-https://github.com/webbreacher/whatsmyname
-https://github.com/soxoj/maigret

There are many more, here is why Linux is best at, most tools are open-source and develop by community. It can be found in Github

./osint_with_google_dorking

Google Dorking:

- Using advanced search operators to find information
- An efficient way to uncover hidden data with precision
- https://github.com/chr3st5an/Google-Dorking

Common Operators:

site:	Limit search to a specific site
intitle:	Search for pages with a specific title
inurl:	Search for URLs containing a specific string
filetype:	Search for specific file types
cache:	View the cached version of a site
index of:	Search for documents containing direct downloads

./time_for_some_flags

THE END...WEEEEEE
AND HAPPY HACKING 🚩🚩

KEEP TRYING AND GIT GUD AT IT