
EIT
TRAINING

TRAINING PLAN

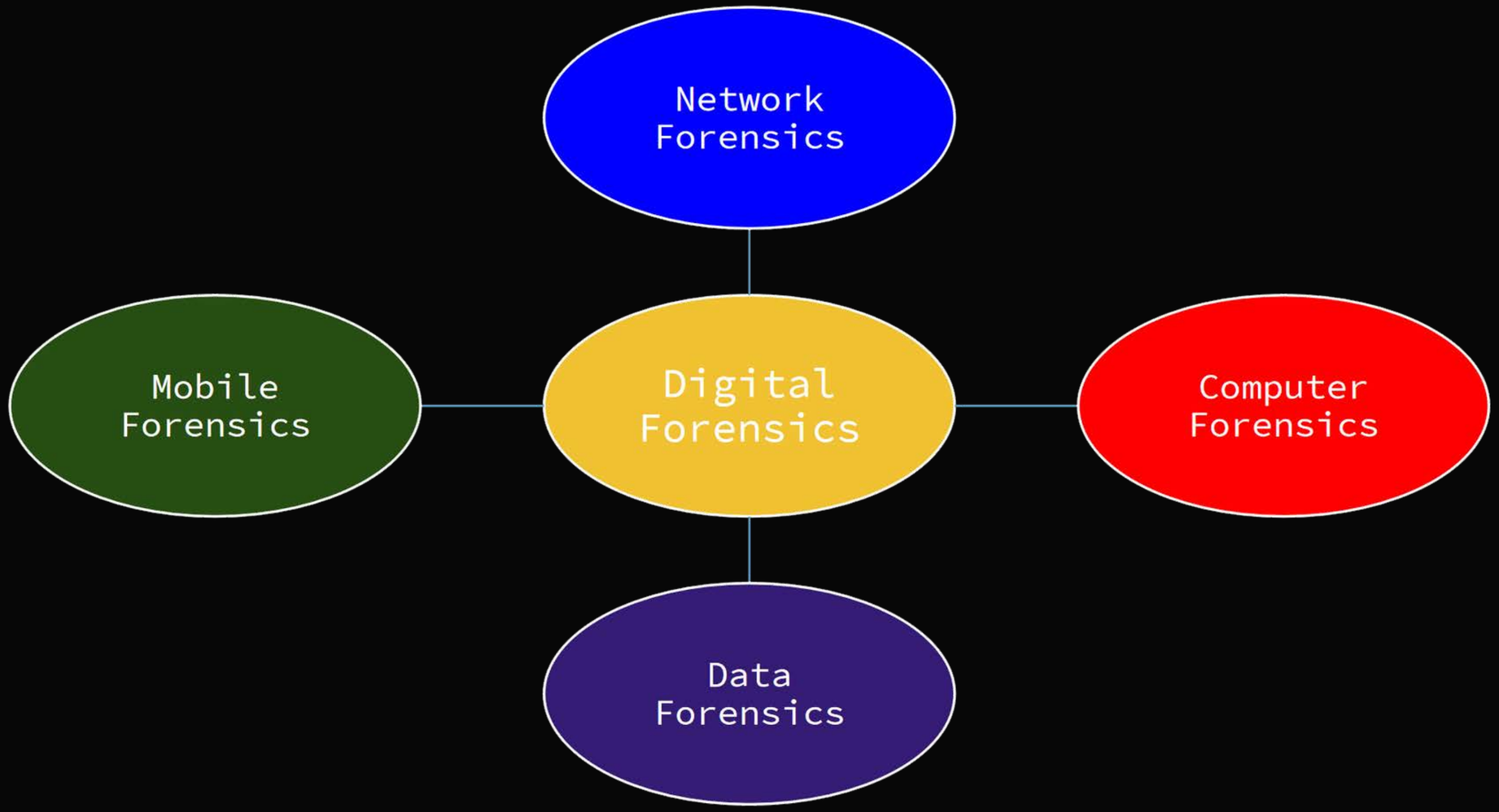
- INTRODUCTION TO LINUX
- **FORENSICS AND OSINT**
- CRYPTOGRAPHY
- WEB EXPLOITATION
- REVERSE ENGINEERING
- BINARY EXPLOITATION

Digital Forensics

A branch of forensic science encompassing the recovery, investigation, examination and analysis of material found in digital devices, often in relation to mobile devices and computer crime.

It is the science of collecting, inspecting, interpreting, reporting, and presenting computer-related electronic evidence

Branches of Digital Forensics



#file

File command is the basic tool to identify the type of any file.

Can be misleading if the file is:

1. Corrupted or manipulated intentionally.
2. Containing another file.

#strings

Searches for all plaintext strings in the file.

May reveal some useful information.

File signatures (magic bytes)

It's a group of HEX numbers in the beginning of a file which is used to identify or verify its type. These signatures are also known as magic numbers.

89 50 4E 47 0D 0A 1A 0A	‰PNG␍␊␚␊

```
└─$ hexdump -C evidence1.png | head
00000000  89 50 4e 47 0d 0a 1a 0a  00 00 00 0d 49 48 44 52  |.PNG........IHDR|
00000010  00 00 03 20 00 00 02 3e  08 06 00 00 00 44 db 6e  |... ...>.....D.n|
```

FF D8 FF E0 00 10 4A 46 49 46 00 01	ÿØÿà␐JFIF␁␀

```
└─$ hexdump -C oof.jpg | head
00000000  ff d8 ff e0 00 10 4a 46  49 46 00 01 02 00 00 01  |......JFIF......|
00000010  00 01 00 00 ff ed 00 9c  50 68 6f 74 6f 73 68 6f  |........Photosho|
```

#hexdump/xxd

Shows the HEX representation of any file, each offset and the corresponding hex numbers.

```
┌──(kali㉿kali)-[~/.local/share/Trash/files]
└─$ hexdump -C evidence1.png | head -2
00000000  89 50 4e 47 0d 0a 1a 0a  00 00 00 0d 49 48 44 52  |.PNG........IHDR|
00000010  00 00 03 20 00 00 02 3e  08 06 00 00 00 44 db 6e  |... ...>.....D.n|

┌──(kali㉿kali)-[~/.local/share/Trash/files]
└─$ xxd evidence1.png | head -2
00000000: 8950 4e47 0d0a 1a0a 0000 000d 4948 4452  .PNG........IHDR
00000010: 0000 0320 0000 023e 0806 0000 0044 db6e  ... ...>.....D.n
```

#hexedit

Edit the raw values of the file in hex.

- CTRL+X to save and exit.
- Backspace to undo last change.

Image Analysis

- #exiftool gives information about an image (dimensions , location, etc.)

pngs being one of the most popular images types in CTFs:

- #pngcheck check if the PNG file is corrupted.
- #zsteg for PNG/BMP Analysis.

General Methodology

When dealing with a file:

- Open the file with a normal text editor (it can be human-readable).
- Identify the file (google the extension and how to open that kind of file).
- Sometimes file extensions are tricky or the file is provided without extension, so try to use its magic bytes or its signature to identify it.
- Don't forget to use `strings` command, it can reveal helpful info.
- Don't forget also to see the file's description (`exiftool` in linux).
- See if the file contains another file (`binwalk` in linux).
- See if the file has a password.

Challenges!

A friend gave me this file. I think there's something hidden inside but I'm not sure what it is.

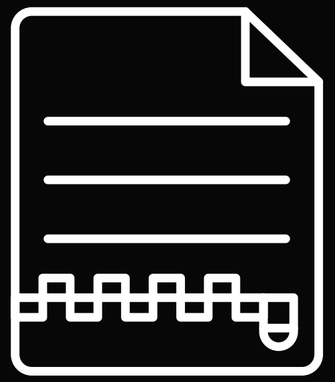
I can't open this picture. Can you help me?

Archive Files

Common Archive formats : zip, 7z, rar, tar or tgz
Usually the goal here is to extract a file from an archive (the archive might be damaged), bruteforce the archive password or use some other methods to unlock the contents of a zip.

Tools for zip cracking : fcrackzip and John The Ripper

- unzip will often output helpful info on why a zip will not decompress.
- zipinfo lists information about the zip file's contents, without extracting it.
- bkcrack is useful for cracking zip files using zipcrypto encryption algorithm through known plaintext attack.



Disk Images

A disk image is an electronic copy of a drive. It's a bit-by-bit or bitstream file that's an exact, unaltered copy of the device being duplicated.

Disk Images extensions:
*.iso *.raw *.dmg *.mdf *.nrg *.bin *.001 *.002 *.aa *.ab *.e01 *.e02 *.vmdk *.vhd

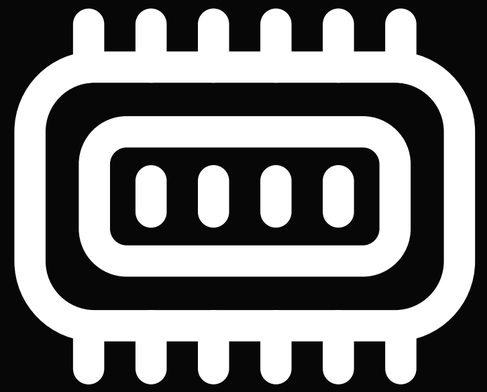
Tools to extract data from disk images:
Autopsy, The Sleuth Kit, testdisk, foremost...

Memory Captures

A memory dump (also known as a core dump or system dump) is a snapshot capture of computer memory data from a specific instant.

Memory image extensions: *.raw *.mem *.vmem...

Tools to extract data from disk images: Volatility...



Volatility Commands

volatility -f image.raw imageinfo #get info about the capture, and get suggested profiles to use. Only one unique profile can be used

volatility -f image.raw --profile=Selected_Profile pslist #to list processes

volatility -f image.raw --profile=Selected_Profile psxview #to view hidden processes

volatility -f image.raw --profile=Selected_Profile netscan #to list all connections

volatility -f image.raw --profile=Selected_Profile ldrmodules #full check on each process, 3 columns appear: InLoad, InInit, InMem. If anyone is false it is likely to be injected

volatility -f image.raw --profile=Selected_Profile apihooks #see processes disassembly

Steganography

It's the art of hiding secret data inside a file, this secret data can be a message or another file, mostly secured by a password to unlock it. It can also be combined with an encryption of the data.

Audio Analysis

The most known trick concerning audio files is to hide messages in its frequency spectrum. You can use audacity, sonic-visualiser, or spek to check up on it. There is also DeepSound.

Steganography Tools

#stegsolve

Shows seperate channels (alpha, red, green, blue) and additional transformations for a given image.

#binwalk

Great for checking out if other files are embedded or appended to a file.

#stegoveritas

exiftool, stegsolve and binwalk combined.

#steghide

One of the most famous tools in the field of Steganography. May require a password to extract information.

Challenges!

le hackeur

skobidobido

Challenges!

inception