CYBER CHALLENGE.IT

UNIVERSITÀ DI TRENTO

# Forensics

Matteo Golinelli

Slides adapted from Veronica Chierzi & Francesco Pasqualini work

UNIVERSITÀ DI TRENTO

# What is Forensics

## Real-world computer forensics

- Recovery, investigation, examination and analysis of material found in digital devices
- Usually related to crimes

## Forensics challenges

- Analysis of files, memory dumps, network packet captures, ...
- **Steganography**: hiding information within another medium (e.g. image, audio) without detection
    - Find **hidden information** in static data files

# Tools

UNIVERSITÀ
DI TRENTO

# Generic

https://github.com/DominicBreuker/stego-toolkit

| Tool | Description | How to use |
|---|---|---|
| file | Check out what kind of file you have | `file stego.jpg` |
| exiftool | Check out metadata of media files | `exiftool stego.jpg` |
| binwalk | Check out if other files are embedded/appended | `binwalk stego.jpg` |
| strings | Check out if there are interesting readable characters in the file | `strings stego.jpg` |
| foremost | Carve out embedded/appended files | `foremost stego.jpg` |
| pngcheck | Get details on a PNG file (or find out is is actually something else) | `pngcheck stego.png` |
| identify | GraphicMagick tool to check what kind of image a file is. Checks also if image is corrupted. | `identify -verbose stego.jpg` |
| ffmpeg | ffmpeg can be used to check integrity of audio files and let it report infos and errors | `ffmpeg -v info -i stego.mp3 -f null -` to recode the file and throw away the result |

# Steganography

https://github.com/DominicBreuker/stego-toolkit

| Tool | File types | Description | How to use |
|---|---|---|---|
| stegoVeritas | Images (JPG, PNG, GIF, TIFF, BMP) | A wide variety of simple and advanced checks. Check out `stegoveritas.py -h`. Checks metadata, creates many transformed images and saves them to a directory, Brute forces LSB, … | `stegoveritas.py stego.jpg` to run all checks |
| zsteg | Images (PNG, BMP) | Detects various LSB stego, also openstego and the Camouflage tool | `zsteg -a stego.jpg` to run all checks |
| stegdetect | Images (JPG) | Performs statistical tests to find if a stego tool was used (jsteg, outguess, jphide, …). Check out `man stegdetect` for details. | `stegdetect stego.jpg` |
| stegbreak | Images (JPG) | Brute force cracker for JPG images. Claims it can crack `outguess`, `jphide` and `jsteg`. | `stegbreak -t o -f wordlist.txt stego.jpg`, use `-t o` for outguess, `-t p` for jphide or `-t j` for jsteg |

# More Tools

- **Bless**: Hex Editor
- **Wireshark**: network packet captures analyser
- **Sonic Visualiser**: audio files analyser

# Least Significant Bit

Embedding information within the least significant bits of a digital file

- Without causing any noticeable change to the file
- LSBs are the bits that have the **least impact** on the overall value of the file

| | |
|---|---|
| R | 11011110 |
| G | 11101011 |
| B | 11101010 |

# Magic Bytes

https://en.wikipedia.org/wiki/List_of_file_signatures: data used to identify or verify the content of a file

| Hex signature | ISO 8859-1 | Offset | Extension | Description |
|---|---|---|---|---|
| FF D8 FF DB | ÿØÿÛ | 0 | jpg<br>jpeg | JPEG raw or in the JFIF or Exif file format[14] |
| FF D8 FF E0 00 10 4A 46 49 46 00 01 | ÿØÿà..JFIF.. | | | |
| FF D8 FF EE | ÿØÿî | | | |
| FF D8 FF E1 ?? ?? 45 78 69 66 00 00 | ÿØÿá??Exif.. | | | |
| FF D8 FF E0 | ÿØÿà | 0 | jpg | JPEG raw or in the JFIF or Exif file format[14] |

# Homework for tomorrow's Lab

**Install**

- stegoveritas
- zsteg
- testdisk
- Bless
- Wireshark
- exiftool
- binwalk

Guide to install the tools

TODO

# Homework for tomorrow's Lab

Optional and probably overkill

- https://github.com/DominicBreuker/stego-toolkit
- Good to keep as a list of tools

# References

- https://trailofbits.github.io/ctf/forensics/
- https://en.wikipedia.org/wiki/Digital_forensics