CCSC
BOOTCAMP TRAINING

Day 3 : Forensics/Osint

~ [CCSC] CIT Cyber Security Cell ~
OUSSAMA RAHALI
OMAR AOUAJ

CLUB INFORMATIQUE & TÉLÉCOM

cat README.md

1. Digital Forensics :
   - 1.1 whatis Forensics
   - 1.2 Types
   - 1.3 Initial analysis
   - 1.4 commands :
     - file
     - strings
   - 1.5 File Signature
     - Hexdump / hexedit
   - 1.6 Archive files
   - 1.7 Image Analysis
   - 1.8 Steganography
     - whatis Steganography
     - Commands
   - 1.9 Audio Analysis

`what are those`

Familiarity (1-10) ?

Digital forensics

`Whatis Forensics`

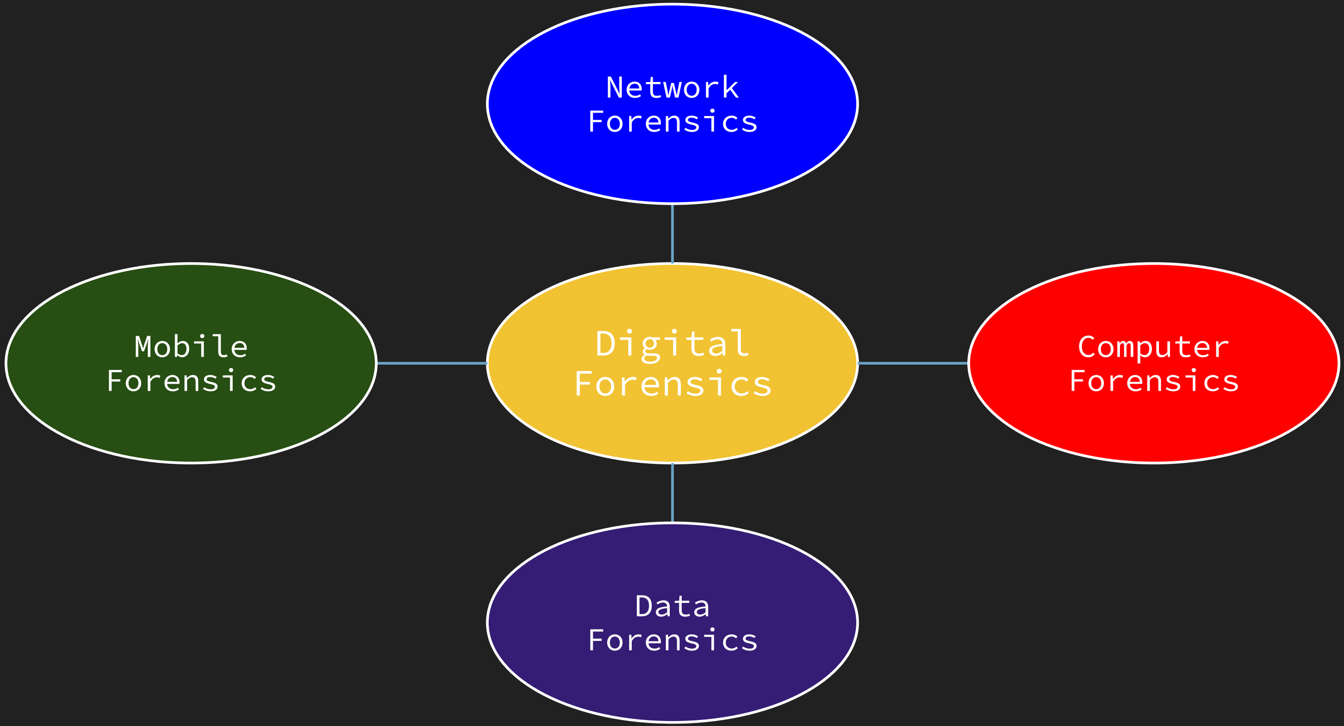
forensics: nothing appropriate.

When an incident happens in the IT domain (and in others too, even irl!!), we should always investigate, search for clues and use them to find other clues, and vice-versa.

In order to do that, we should provide an answer to these questions:

Who did that, where, when, how and why?

Types



Network Forensics

Mobile Forensics

Digital Forensics

Computer Forensics

Data Forensics

`ls -al Initial Analysis`

Hmmm.. Let's begin our analysis !

if a file is provided in a challenge, we can proceed as the following:

- 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 files).
- 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.

$(which file)

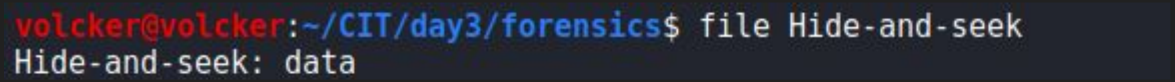
/usr/bin/file

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 (someone has been messy with the signature of the file)

2- containing another file

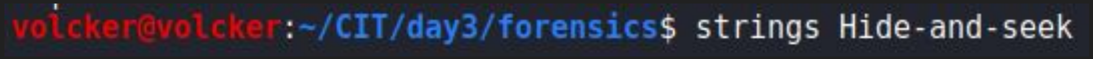


```
volcker@volcker:~/CIT/day3/forensics$ file Hide-and-seek
Hide-and-seek: data
```

# strings

Strings search for all plain-text strings in the file.

Sometimes it may reveal the flag or has some useful information to find it.



```
volcker@volcker:~/CIT/day3/forensics$ strings Hide-and-seek
```

Get your hands dirty

Challenge 1 : Hide and Seek

>> we got hacked by a really sophisticated attack.
Fortunately I was able to recover that file !
Can you "grep" the flag for me :D

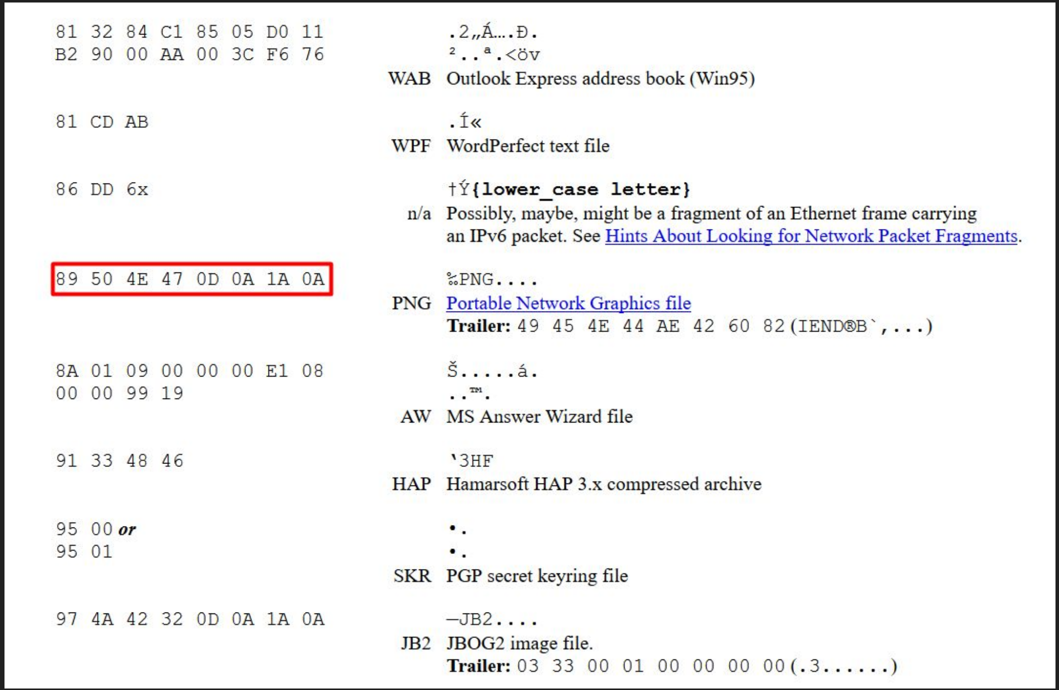
Flag Format : CCSC{.*?}

File Signature aka Magic bytes

It’s a group of HEX numbers in the beginning of a file (open it as hex data) which is used to identify or verify the content of a file. Such signatures are also known as magic numbers.

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

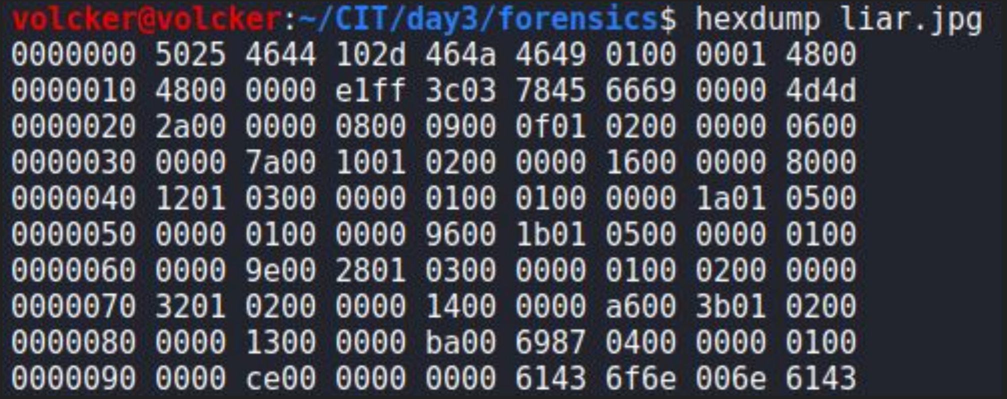
File Signature aka Magic bytes



81 32 84 C1 85 05 D0 11 B2 90 00 AA 00 3C F6 76		.2„Á….Ð. ²..ª.<öv
	WAB	Outlook Express address book (Win95)
81 CD AB		.Í«
	WPF	WordPerfect text file
86 DD 6x		†Ý**{lower_case letter}**
	n/a	Possibly, maybe, might be a fragment of an Ethernet frame carrying an IPv6 packet. See Hints About Looking for Network Packet Fragments.
89 50 4E 47 0D 0A 1A 0A		‰PNG....
	PNG	Portable Network Graphics file **Trailer:** 49 45 4E 44 AE 42 60 82 (IEND®B`,...)
8A 01 09 00 00 00 E1 08 00 00 99 19		Š.....á. ..™.
	AW	MS Answer Wizard file
91 33 48 46		‘3HF
	HAP	Hamarsoft HAP 3.x compressed archive
95 00 ***or*** 95 01		•. •.
	SKR	PGP secret keyring file
97 4A 42 32 0D 0A 1A 0A		—JB2....
	JB2	JBOG2 image file. **Trailer:** 03 33 00 01 00 00 00 00 (.3......)

$ hexdump / hexedit

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



```
volcker@volcker:~/CIT/day3/forensics$ hexdump liar.jpg
0000000 5025 4644 102d 464a 4649 0100 0001 4800
0000010 4800 0000 e1ff 3c03 7845 6669 0000 4d4d
0000020 2a00 0000 0800 0900 0f01 0200 0000 0600
0000030 0000 7a00 1001 0200 0000 1600 0000 8000
0000040 1201 0300 0000 0100 0100 0000 1a01 0500
0000050 0000 0100 0000 9600 1b01 0500 0000 0100
0000060 0000 9e00 2801 0300 0000 0100 0200 0000
0000070 3201 0200 0000 1400 0000 a600 3b01 0200
0000080 0000 1300 0000 ba00 6987 0400 0000 0100
0000090 0000 ce00 0000 0000 6143 6f6e 006e 6143
```

Get your hands dirty

Challenge 2 : Liar

>> a hacker gained access to our system and messed with our files, we're seeking for your help to repair our most important file since we don't know what's wrong with it

Flag starts with : Every....

`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 like known-plaintext attacks to unlock the contents of a zip

$ ZIP Archive

Tools for zip cracking: **fcrackzip** and **John The Ripper**

- **Unzip**: will often output helpful information on why a zip will not decompress.
- **Zipinfo** : lists information about the zip file's contents, without extracting it.

# Image analysis

- **exiftool** Important tools that gives more information about an image (Dimensions, Location,....)
- PNG is one of the most popular images types in CTFs
  - PNG Important Tools:
    - **Pngcheck**: check if the PNG file is corrupted or not
    - **Zsteg** : PNG/BMP analysis.

Steganography

YO DAWG, I HEARD YOU LIKE STEGANOGRAPHY
SO I STEGANOGRAPHED A MEME INTO THIS MEME
memegenerator.net

`Whatis Steganography`

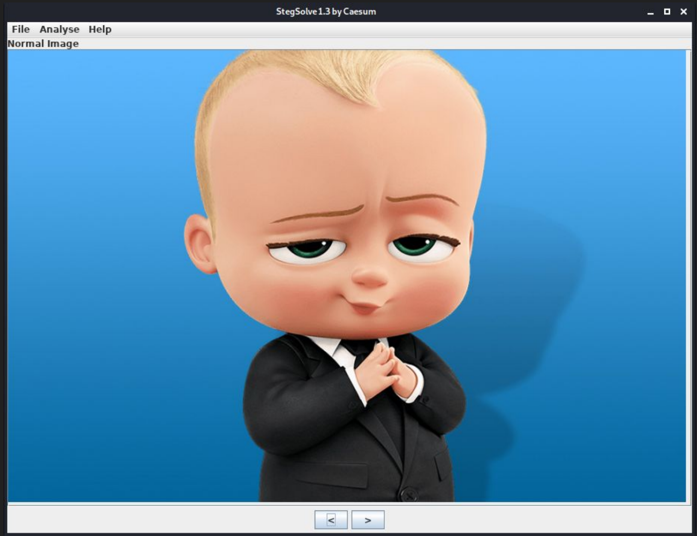
steganography: nothing appropriate.

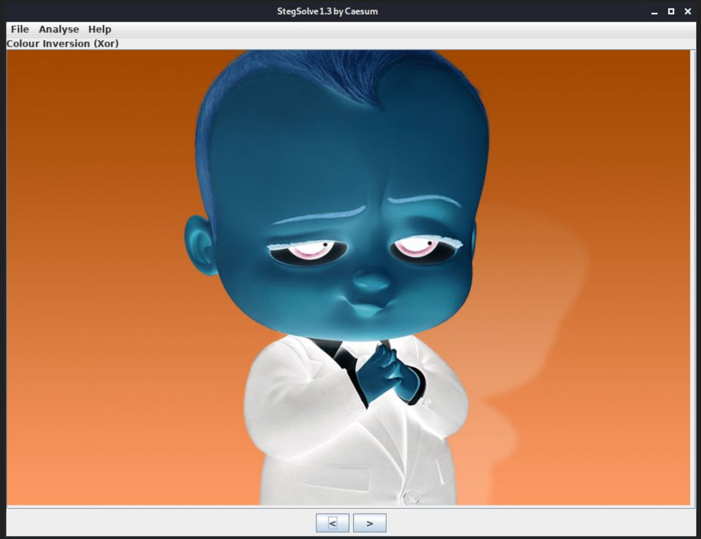
Steganography is the art of hiding secret data inside a file, this secret data can be a message or another file, mostly secured by a password to unlock it. It can also be combined with an encryption of the data.

# cd Tools

$ Stegsolve

It is often used to apply various steganography techniques to image files in an attempt to detect and extract hidden data.

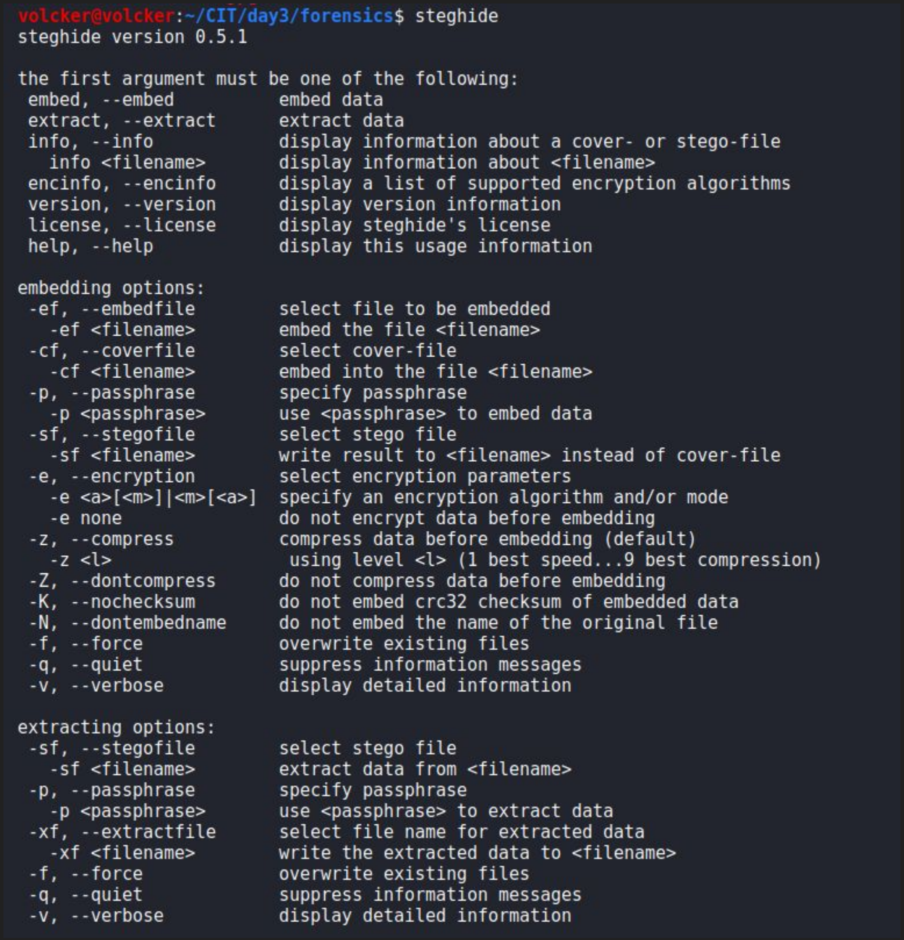




# cd Tools

$ Steghide

- Is one of the most famous tools in the field of Steganography. It may require a password to extract file.



```
volcker@volcker:~/CIT/day3/forensics$ steghide
steghide version 0.5.1

the first argument must be one of the following:
 embed, --embed          embed data
 extract, --extract      extract data
 info, --info            display information about a cover- or stego-file
   info <filename>       display information about <filename>
 encinfo, --encinfo      display a list of supported encryption algorithms
 version, --version      display version information
 license, --license      display steghide's license
 help, --help            display this usage information

embedding options:
 -ef, --embedfile        select file to be embedded
   -ef <filename>        embed the file <filename>
 -cf, --coverfile        select cover-file
   -cf <filename>        embed into the file <filename>
 -p, --passphrase        specify passphrase
   -p <passphrase>       use <passphrase> to embed data
 -sf, --stegofile        select stego file
   -sf <filename>        write result to <filename> instead of cover-file
 -e, --encryption        select encryption parameters
   -e <a>[<m>]|<m>[<a>]  specify an encryption algorithm and/or mode
   -e none               do not encrypt data before embedding
 -z, --compress          compress data before embedding (default)
   -z <l>                 using level <l> (1 best speed...9 best compression)
 -Z, --dontcompress      do not compress data before embedding
 -K, --nochecksum        do not embed crc32 checksum of embedded data
 -N, --dontembedname     do not embed the name of the original file
 -f, --force             overwrite existing files
 -q, --quiet             suppress information messages
 -v, --verbose           display detailed information

extracting options:
 -sf, --stegofile        select stego file
   -sf <filename>        extract data from <filename>
 -p, --passphrase        specify passphrase
   -p <passphrase>       use <passphrase> to extract data
 -xf, --extractfile      select file name for extracted data
   -xf <filename>        write the extracted data to <filename>
 -f, --force             overwrite existing files
 -q, --quiet             suppress information messages
 -v, --verbose           display detailed information
```

Get your hands dirty

Challenge 3 : Scooby-Doo-Bi-Doo

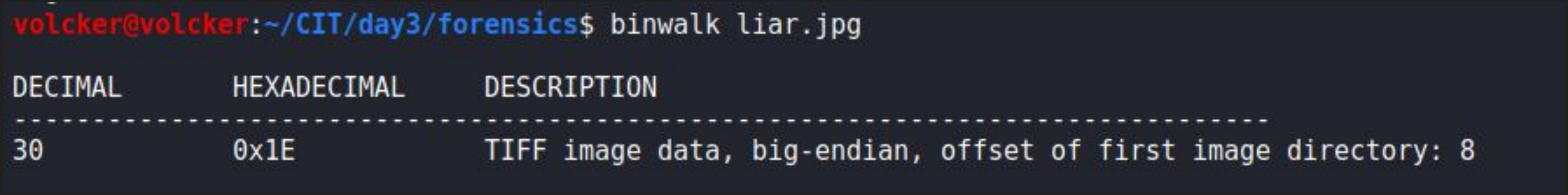
>> can you unveil the secret in this file, It took me ages to realize that I'm just a noob and that secrets fly by my eyes without me finding them !
Remember that I'm the famous (exif) artist of all the time ....

Flag Fromat: CCSC{}

# cd Tools

$ Binwalk

binwalk: is great for checking out if other files are embedded or appended to a file.



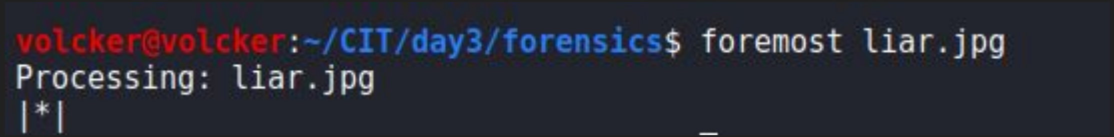
```
volcker@volcker:~/CIT/day3/forensics$ binwalk liar.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
30            0x1E            TIFF image data, big-endian, offset of first image directory: 8
```

# cd Tools

$ Foremost

Foremost is a forensic data recovery program for Linux used to recover files using their headers, footers, and data structures through a process known as file carving.



```
volcker@volcker:~/CIT/day3/forensics$ foremost liar.jpg
Processing: liar.jpg
|*|
```

Get your hands dirty

Challenge 4 : Inception

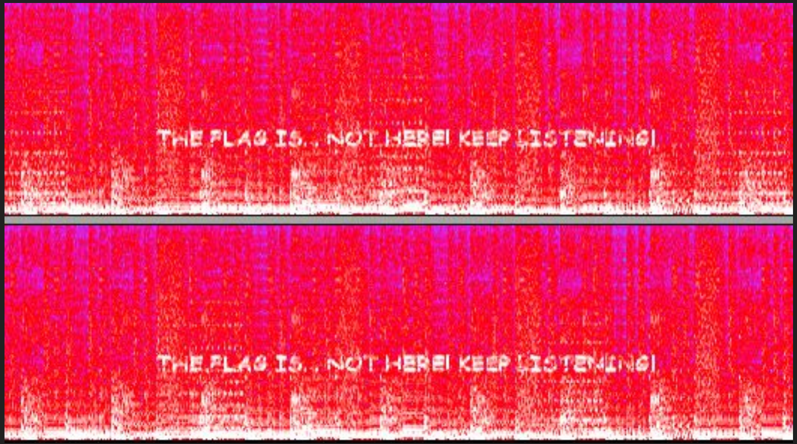
>> I've concatenated two files in a single one to hide an important image and I totally regret it cos I can't recover it. Can you please do that for me?

Flag Format : CCSC{}

# Audio Analysis

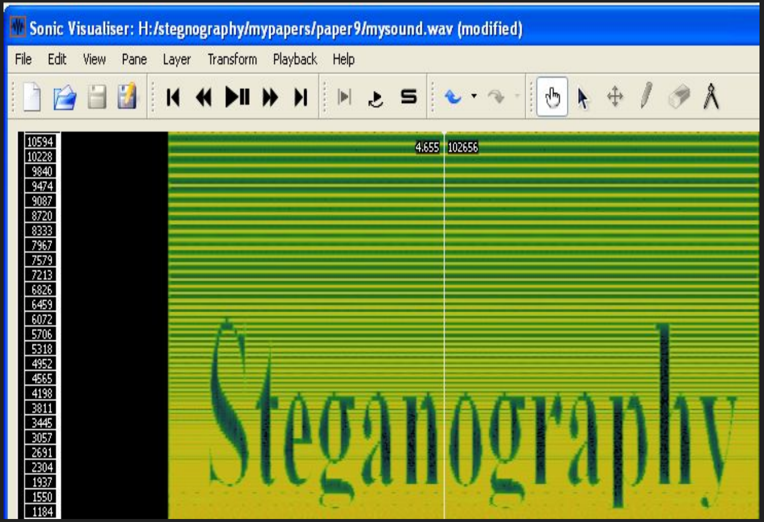
$ Audacity

- One of the famous tricks of Steganography is to hide information in an audio or video file. Audacity can help you recover the hidden data in the spectrogram for example.


THE FLAG IS... NOT HERE! KEEP LISTENING!
THE FLAG IS... NOT HERE! KEEP LISTENING!

# Audio Analysis

$ Sonic Visualizer



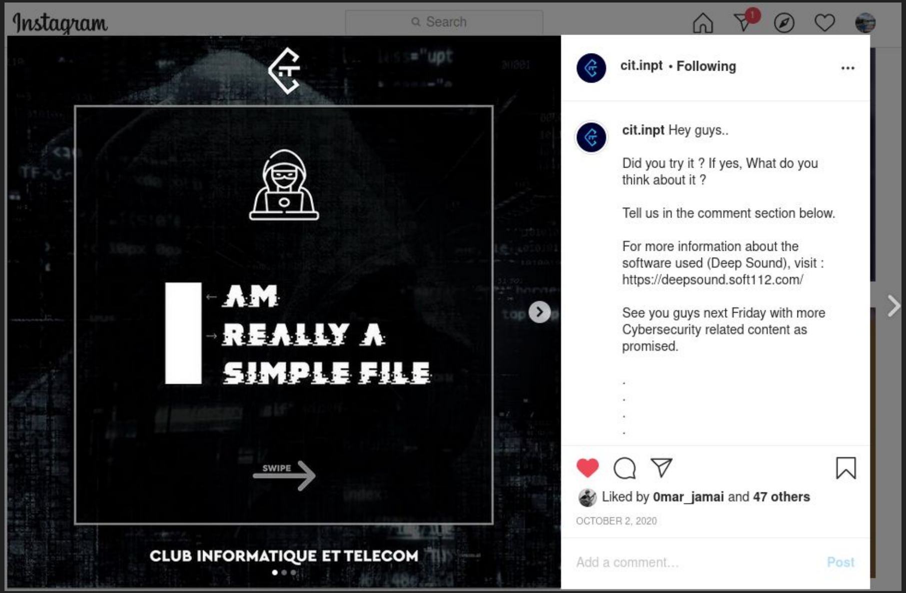
Sonic Visualiser: H:/stegnography/mypapers/paper9/mysound.wav (modified)

https://www.sonicvisualiser.org/

# Audio Analysis

$ Deep Sound

http://insoft.net/DeepSoundInstalled.aspx



cit.inpt Hey guys..

Did you try it ? If yes, What do you think about it ?

Tell us in the comment section below.

For more information about the software used (Deep Sound), visit : https://deepsound.soft112.com/

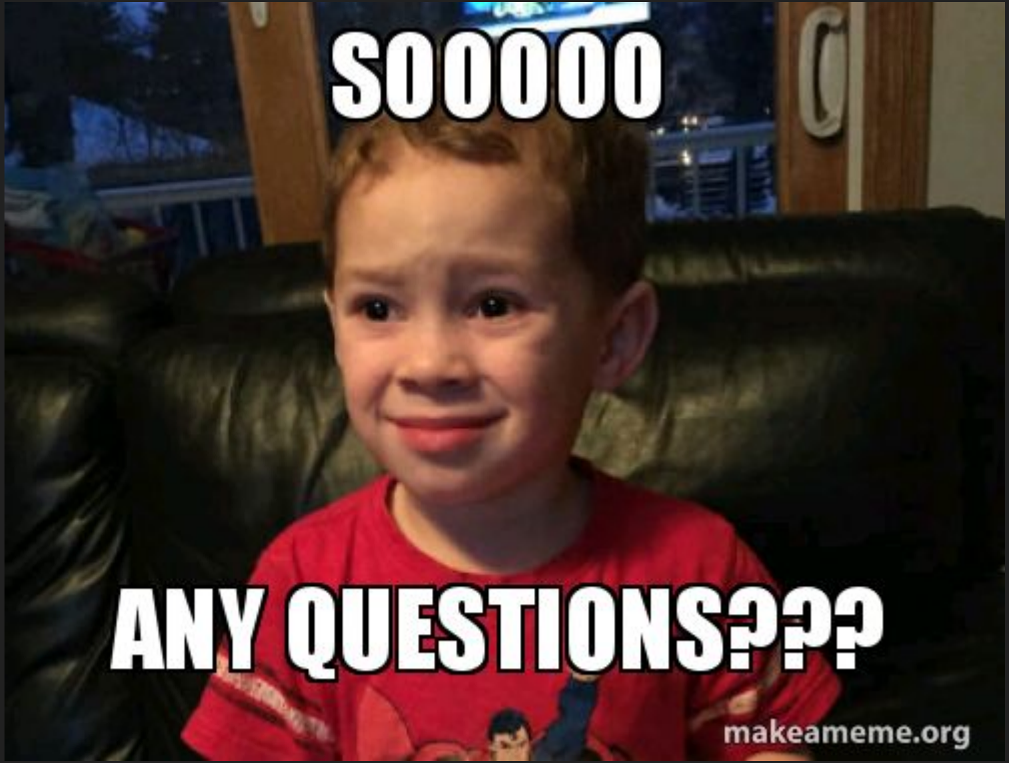
See you guys next Friday with more Cybersecurity related content as promised.

.
.
.
.

Liked by **0mar_jamai** and **47 others**

OCTOBER 2, 2020

shutdown



ls -al .Contact_us

OUSSAMA RAHALI

OMAR AOUAJ

Facebook : /oussama.rahali.925

Facebook : /omar.aouaj.77