\ShellMates:# echo ' Welcome to @workshop '

ART OF STEGANOGRAPHY

PRESENTED BY: MEHDI NACER KERKAR

HACK-INI

$_whoami :

MEHDI NACER KERKAR

- Information Security Student at USDB
- Security Researcher and development at CDTA
- CTF-Player
- Board Member at Shellmates Club

Qu'est-ce que la «Steganographie» !?


1
- Introduction:

Stéganographie

Dans un sens Litairaire

- est dérivé des mots stegos signifie **couverture** et grafia signifie **écriture** la définissant comme écriture couverte.

Dans un sens plus large

- l'art et la science d'ecrire des messages caché, dans la façon que null persone à part les Communiquants Ne suspect l'existance du message.

- Stéganographie Masquer les messages à l'intérieur du support de couverture, porteuse multiple formats.

- La rupture de la stéganographie est connue sous le nom de STÉGANALYSE.

Stéganographie VS Cryptographie

La **cryptographie** est l'art du secret, c'est-à-dire l'art de rendre un message inintelligible à tout le monde sauf à son destinataire ;

la **stéganographie** est l'art de la dissimulation, c'est-à-dire l'art de faire passer inaperçu un message dans un autre.

Objectifs de la Stéganographie

Pas de détection:

- Toute personne non autorisée ne sait pas qu'il existe des données sensibles.

Visibilité:

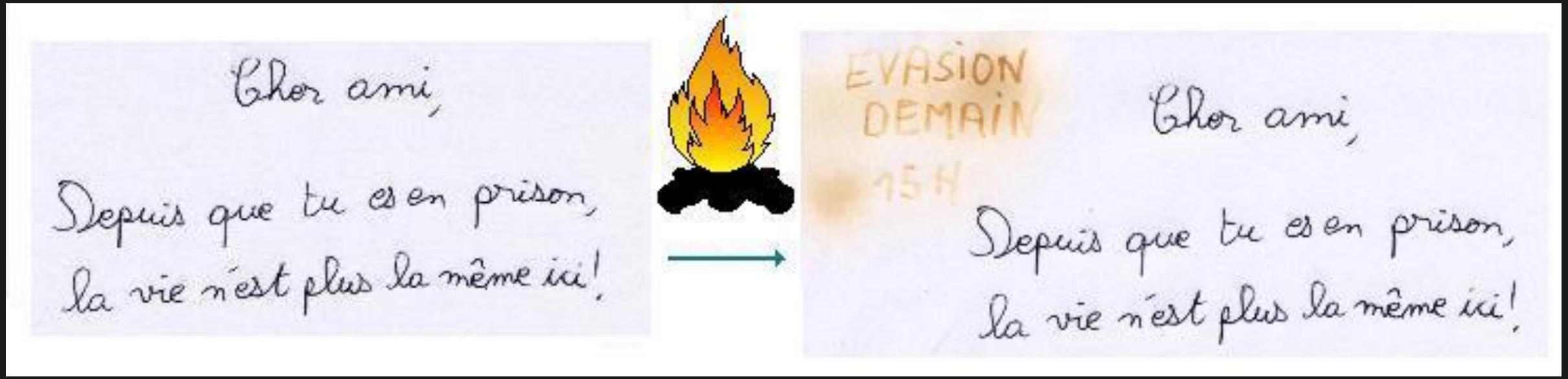
- Les utilisateurs ne peuvent voir aucune modification visible du fichier dans lequel les données sont masquées.

Type de Steganographie

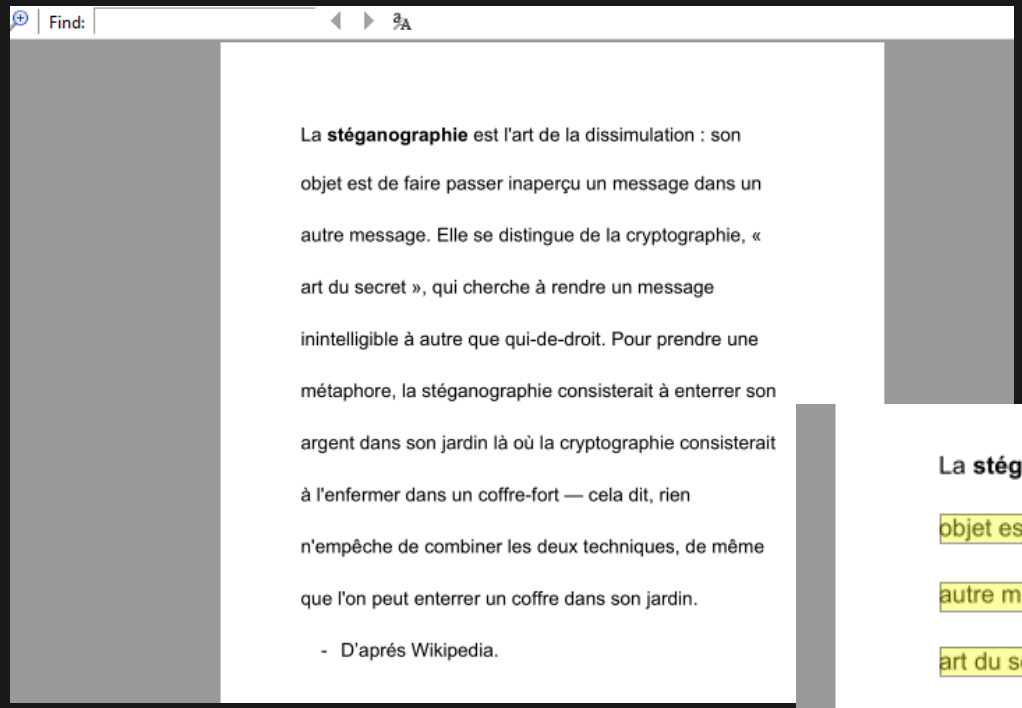
- Text / Image Steganographie
- Audio Steganographie
- Video Steganographie

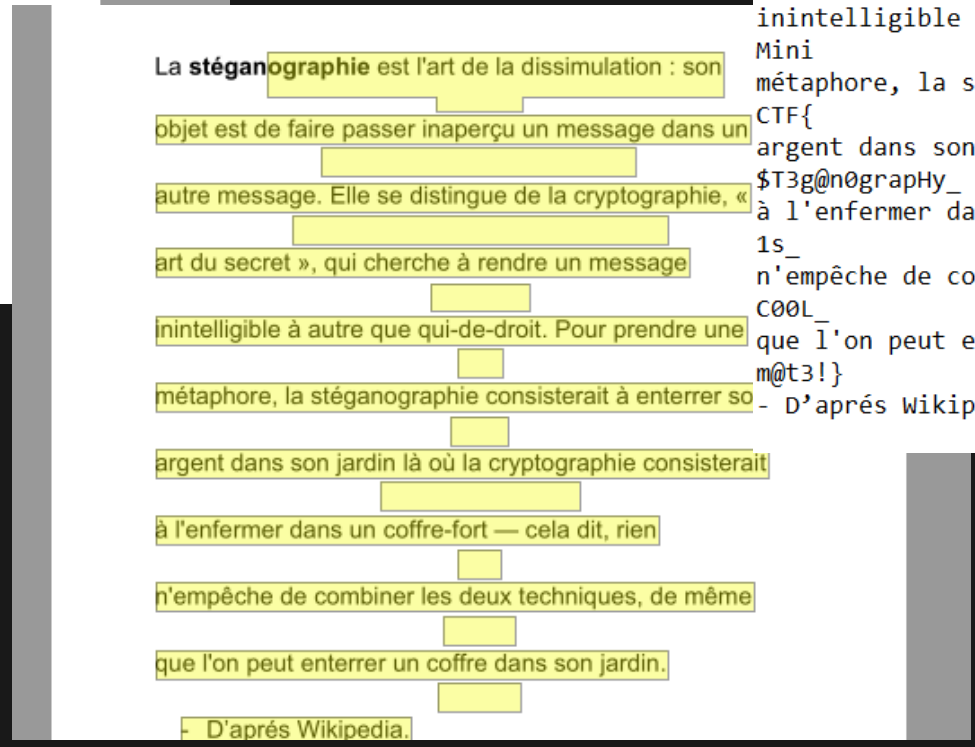
Text Steganographie

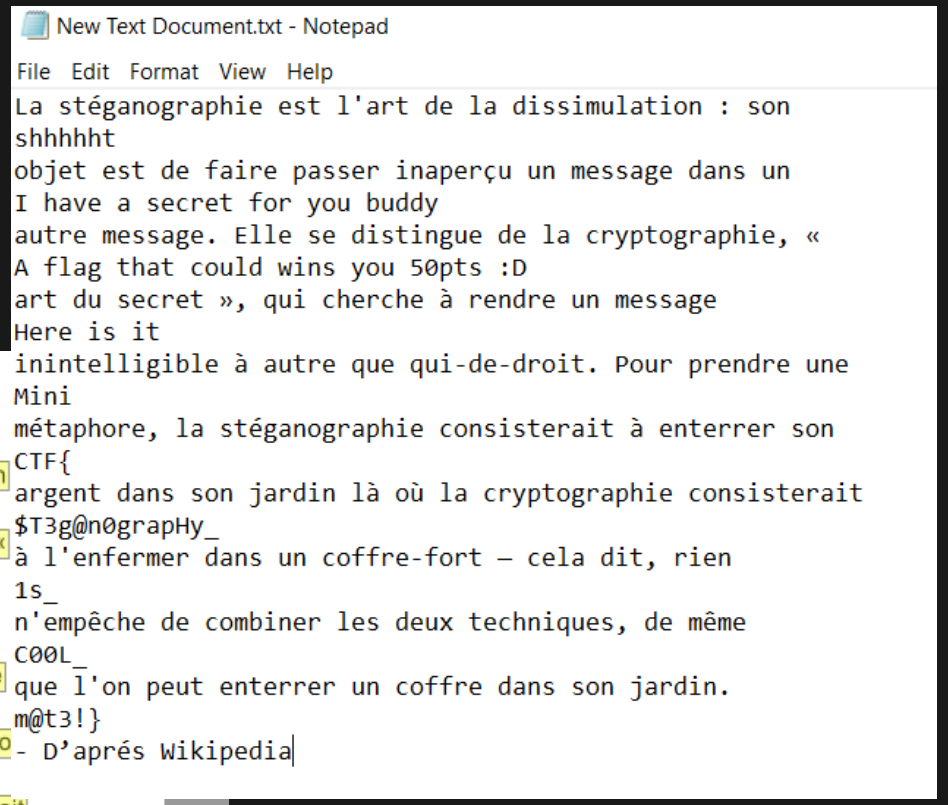
- Cacher de l'info d'un façon que son existance n'est pas suspectible



Dissimulation d'écriture







Ecriture dans écriture

Since **E**veryone **C**an **R**ead, **E**ncoding **T**ext
In **N**eutral **S**entences **I**s **D**oubtfully **E**ffective

'Secret inside'

Image Steganographie

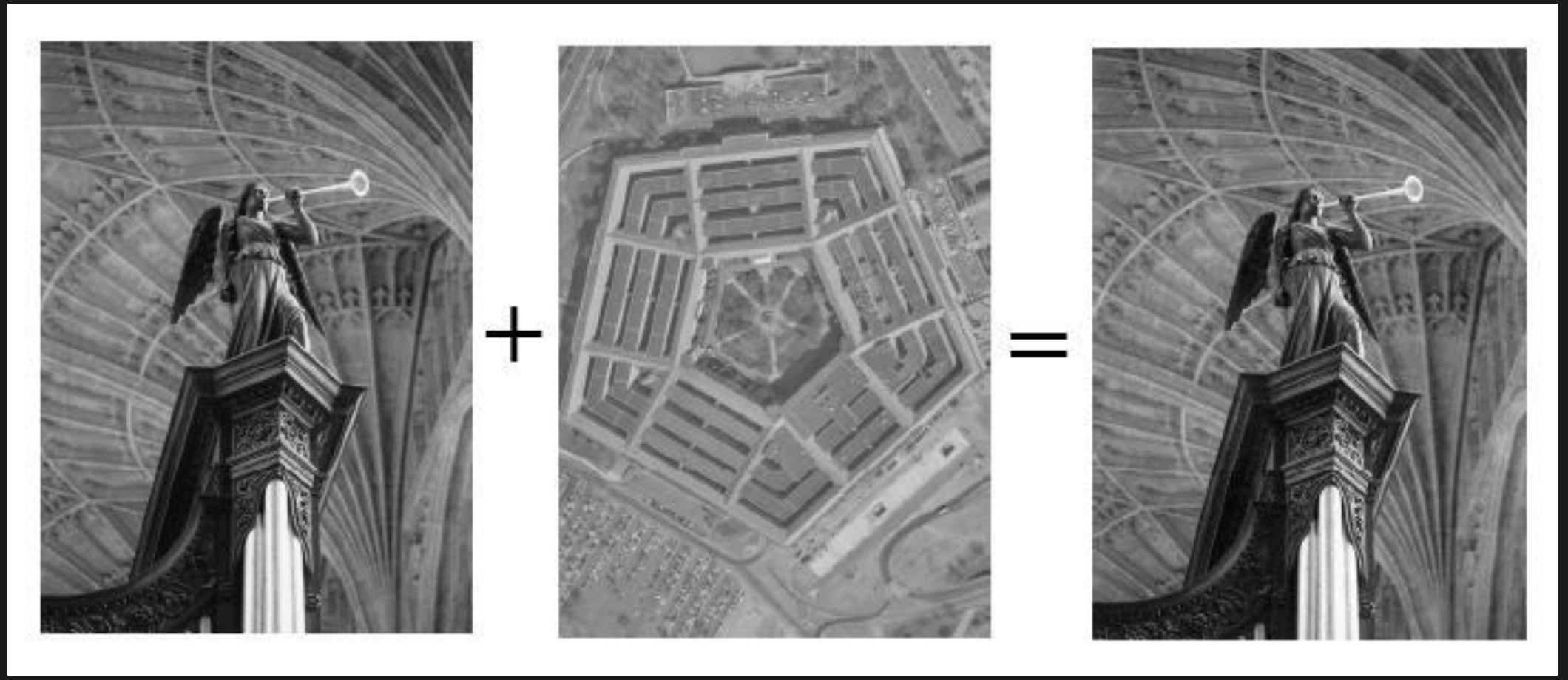
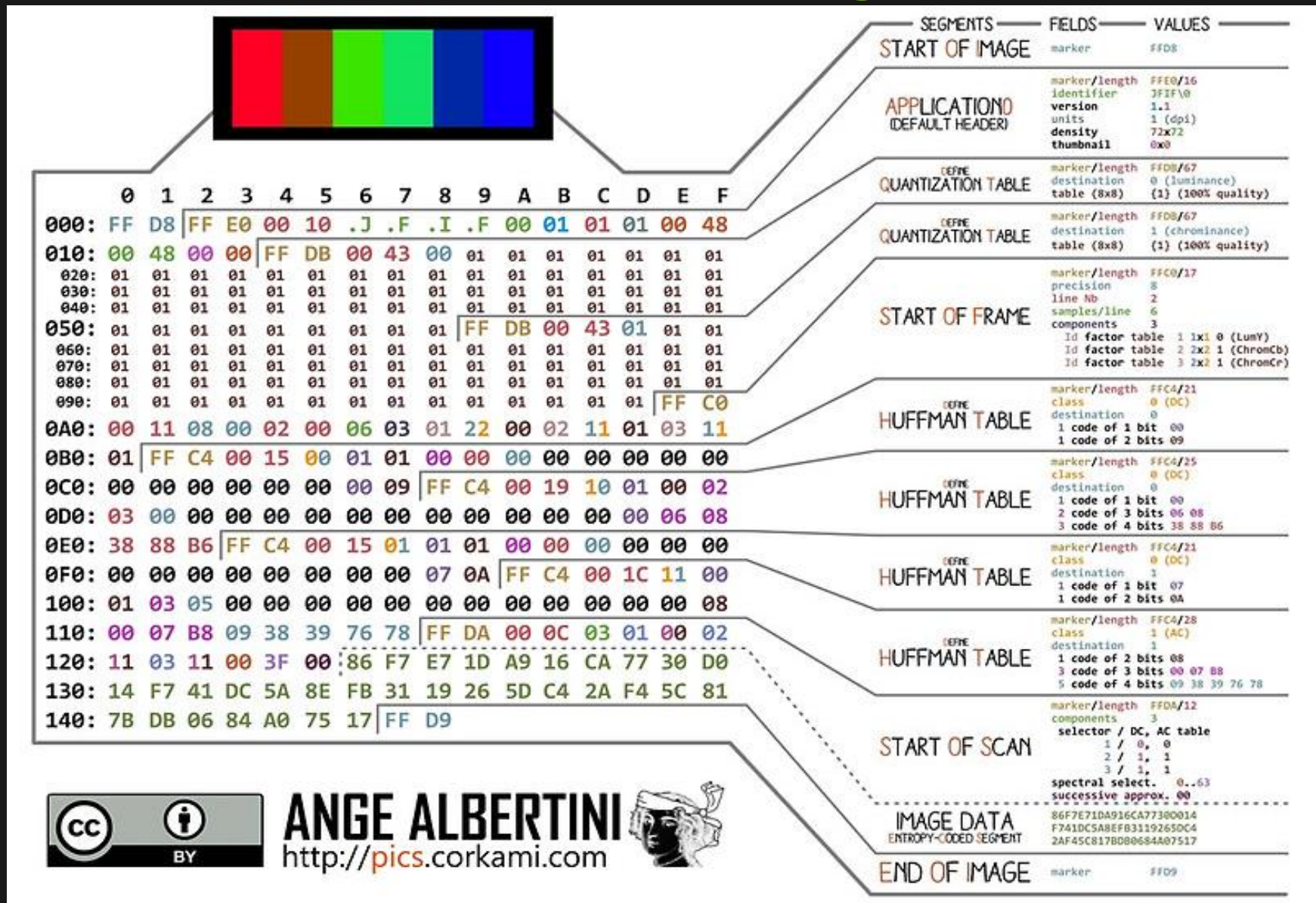


Image cache Images

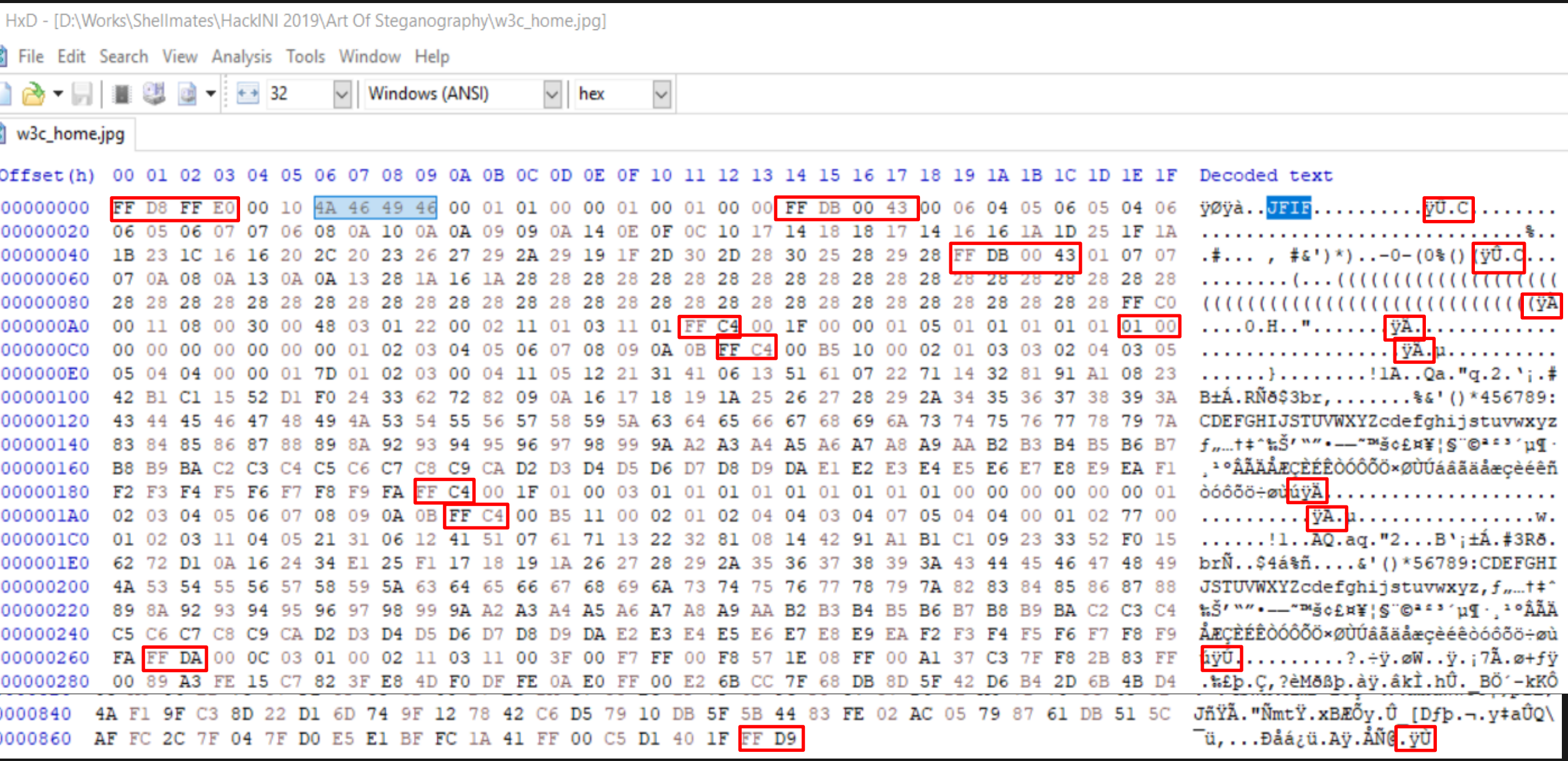
Image Principale

JPEG File Interchange Format



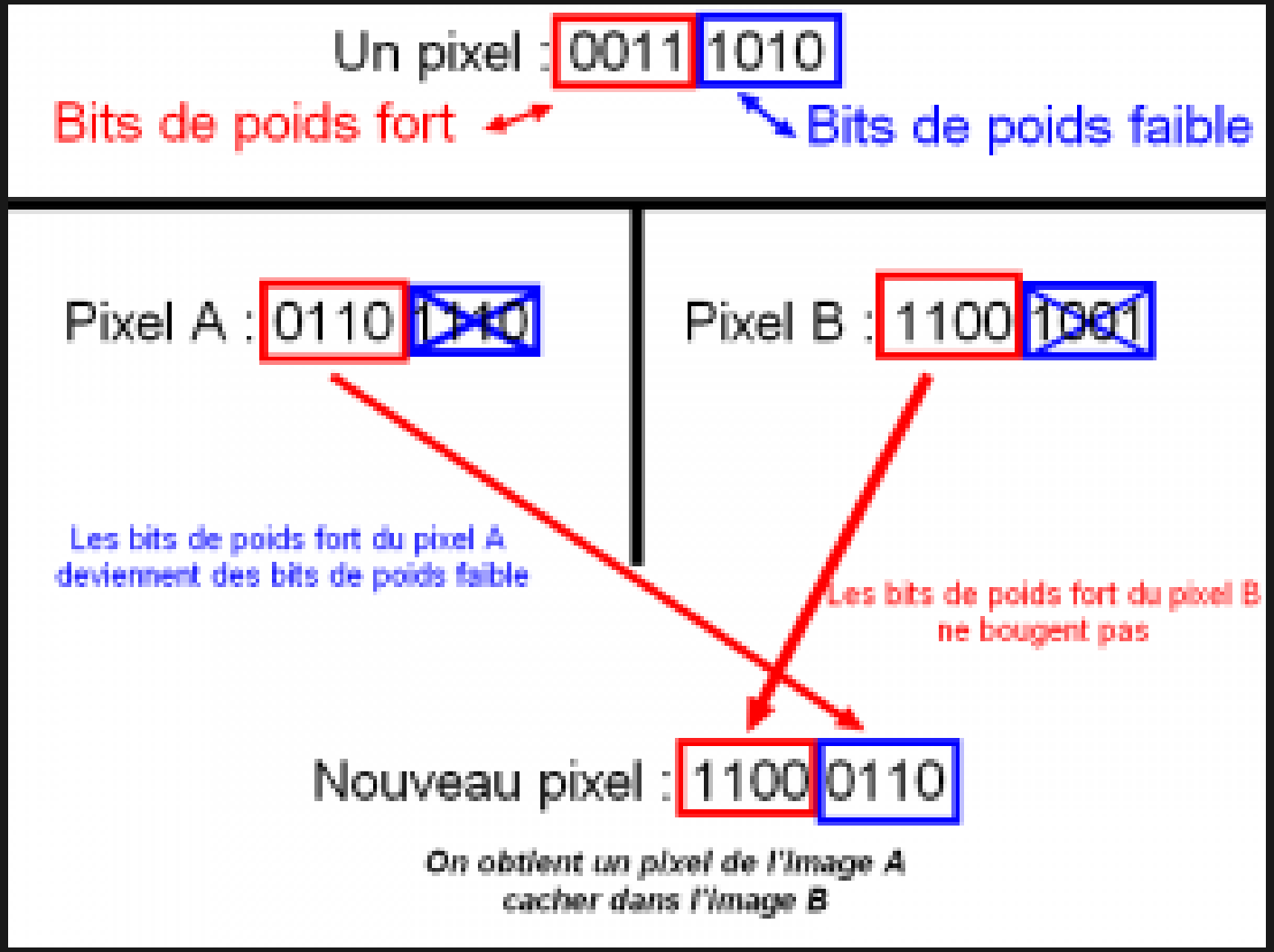
JPEG IS THE ENCODING STANDARD, JFIF IS THE FILE FORMAT

JPEG File Interchange Format Exemple



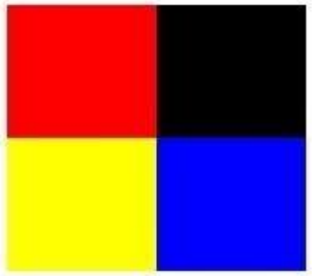
Least Significant Bit

- Parfois abrégé en LSB
- le bit le moins significatif est le bit le plus bas d'une série de nombres en binaire
- le LSB est situé à l'extrême droite d'une chaîne



Least Significant Bit

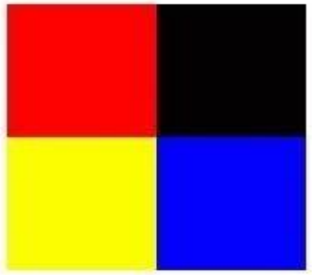
Original Image



```
11111111  00000000
00000000  00000000
00000000  00000000

11111111  00000000
11111111  00000000
00000000  11111111
```

Least Significant Bit Steganography

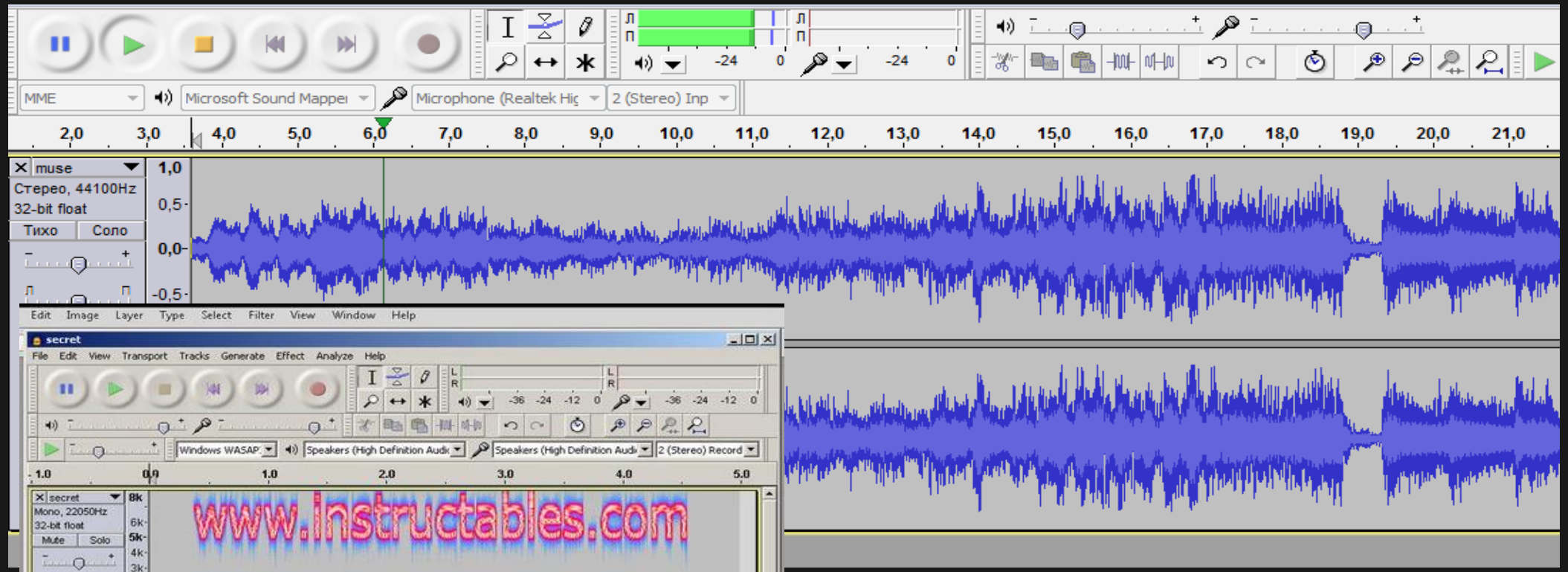
Stego Image



```
11111101  00000011
00000010  00000001
00000000  00000010

11111100  00000011
11111101  00000001
00000001  11111100
```

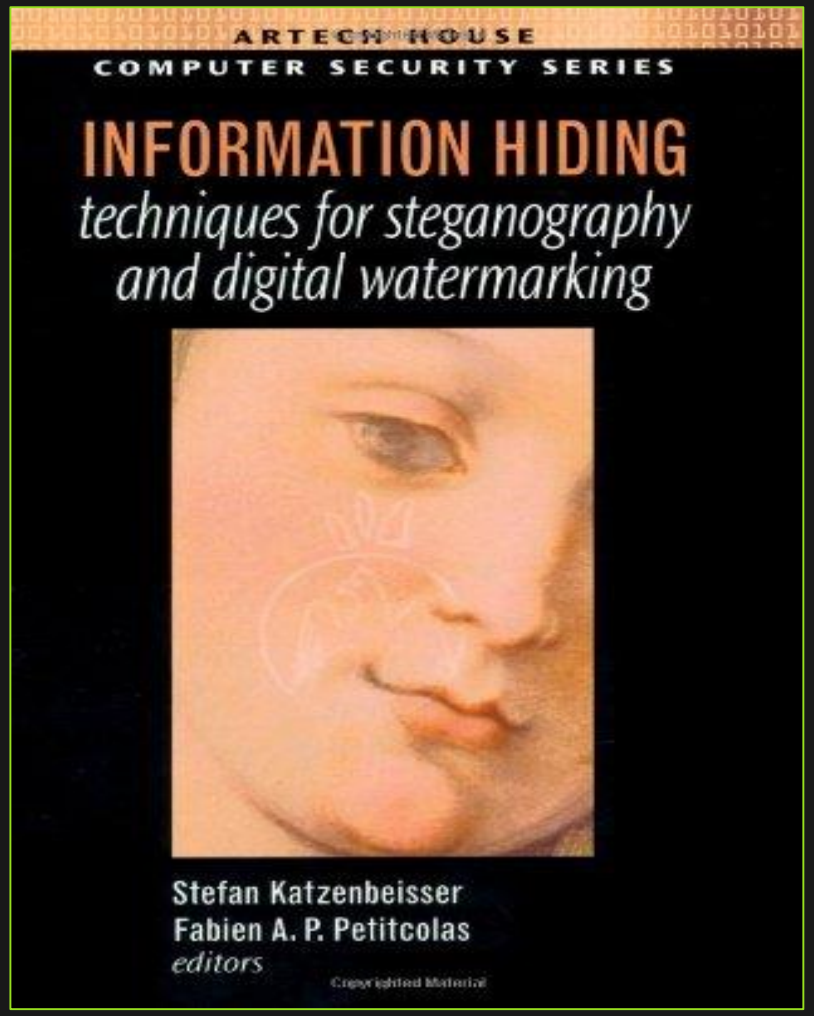
c	a	t
01 10 00 11	01 10 00 01	01 11 01 00

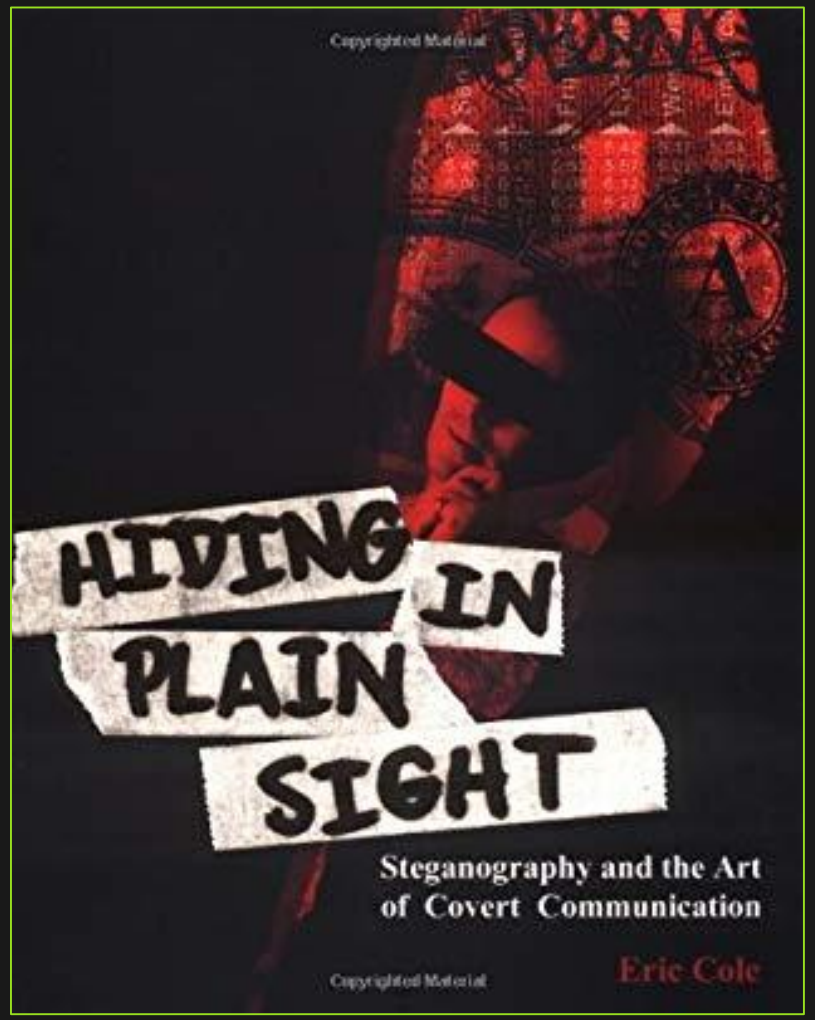
Audio Steganographie



Video Steganographie

Steganographie Resources





Plateformes pour pratiquer

- https://www.root-me.org
- https://www.hackthebox.eu
- https://microcorruption.com

WORKSHOP

ART OF STEGANOGRAPHY

PRESENTED BY: MEHDI NACER KERKAR

HACK-INI

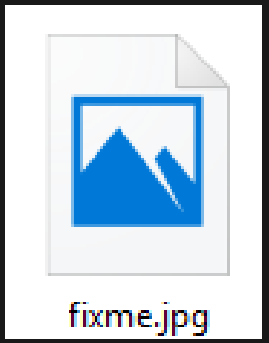
Dissimulation d'écriture

```
# file w3c_home.jpg
w3c_home.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment
length 16, baseline, precision 8, 72x48, frames 3

# cat w3c_home.jpg
▒▒▒▒▒▒ JFIF    ▒▒ C
……
y▒a▒Q\▒▒,••▒▒▒▒▒▒A▒ ▒▒@▒▒

# echo this is my password >> w3c_home.jpg

# cat w3c_home.jpg
▒▒▒▒▒▒ JFIF    ▒▒ C
……
y▒a▒Q\▒▒,••▒▒▒▒▒▒A▒ ▒▒@▒▒this is my password
```

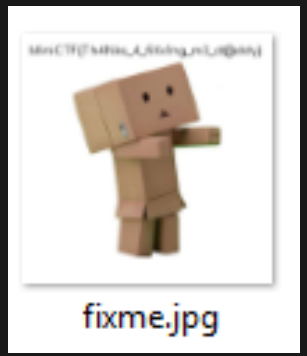
HxD Hex Editor

HxD est un éditeur hexadécimal, un éditeur de disque et un éditeur de mémoire développé par Maël Hörz pour Windows. Il peut ouvrir des fichiers de plus de 4 Gio.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	00	DD	E1	00	56	45	78	69	66	00	00	4D	4D	00	2A	00	.Ýá.VExif..MM.*.
00000010	00	00	08	00	04	01	12	00	03	00	00	00	01	00	01	00	.....
00000020	00	01	1A	00	05	00	00	00	01	00	00	00	3E	01	1B	00	.....>...
00000030	05	00	00	00	01	00	00	00	46	01	28	00	03	00	00	00	.....F.(.....
00000040	01	00	02	00	00	00	00	00	00	00	00	01	2C	00	00	00	.....,...
00000050	01	00	00	01	2C	00	00	00	01	FF	DB	00	43	00	01	01	....,....ÿÛ.C...
00000060	01	01	01	01	01	01	01	01	01	01	01	01	01	02	01	01	.....
00000070	01	01	01	02	01	01	01	02	02	02	02	02	02	02	02	02	.....
00000080	03	03	04	03	03	03	03	03	02	02	03	04	03	03	04	04	.....
00000090	04	04	04	02	03	05	05	04	04	05	04	04	04	04	FF	DB	ÿÛ



Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	D8	E1	00	56	45	78	69	66	00	00	4D	4D	00	2A	00	ÿØá.VExif..MM.*.
00000010	00	00	08	00	04	01	12	00	03	00	00	00	01	00	01	00	.....
00000020	00	01	1A	00	05	00	00	00	01	00	00	00	3E	01	1B	00	.....>...
00000030	05	00	00	00	01	00	00	00	46	01	28	00	03	00	00	00	.....F.(.....
00000040	01	00	02	00	00	00	00	00	00	00	00	01	2C	00	00	00	.....,...
00000050	01	00	00	01	2C	00	00	00	01	FF	DB	00	43	00	01	01	....,....ÿÛ.C...



bibliotheque Python

Utilisation de Stegano, avec la method LSB et exifHeader

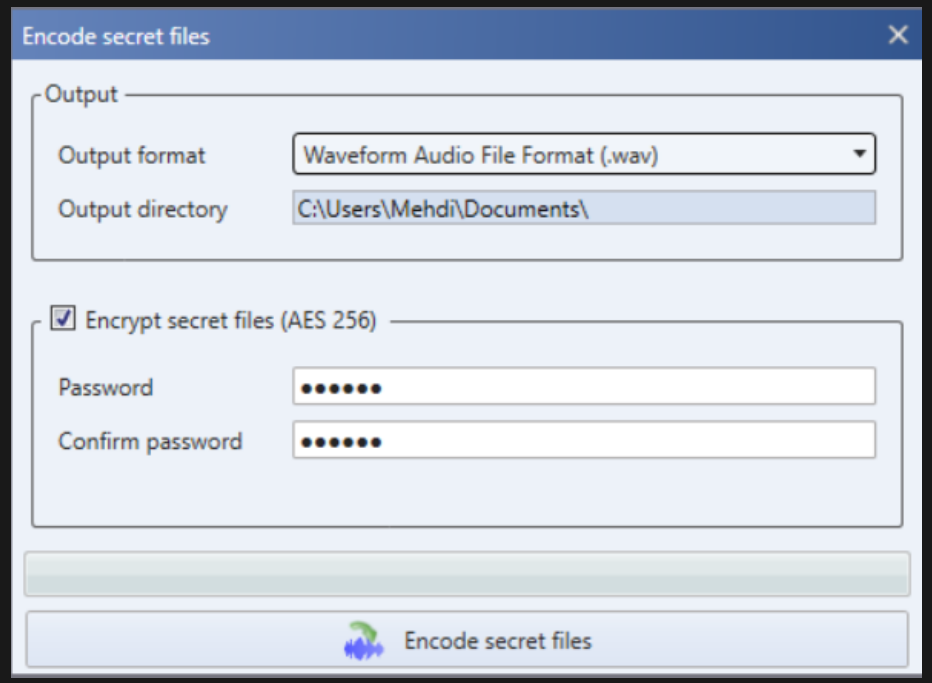
```
# from stegano import lsb
# secret = lsb.hide("./tests/sample-files/Lenna.png", "Secret")
# secret.save("./Lenna-secret.png")
# print(lsb.reveal("./Lenna-secret.png"))
Secret
```

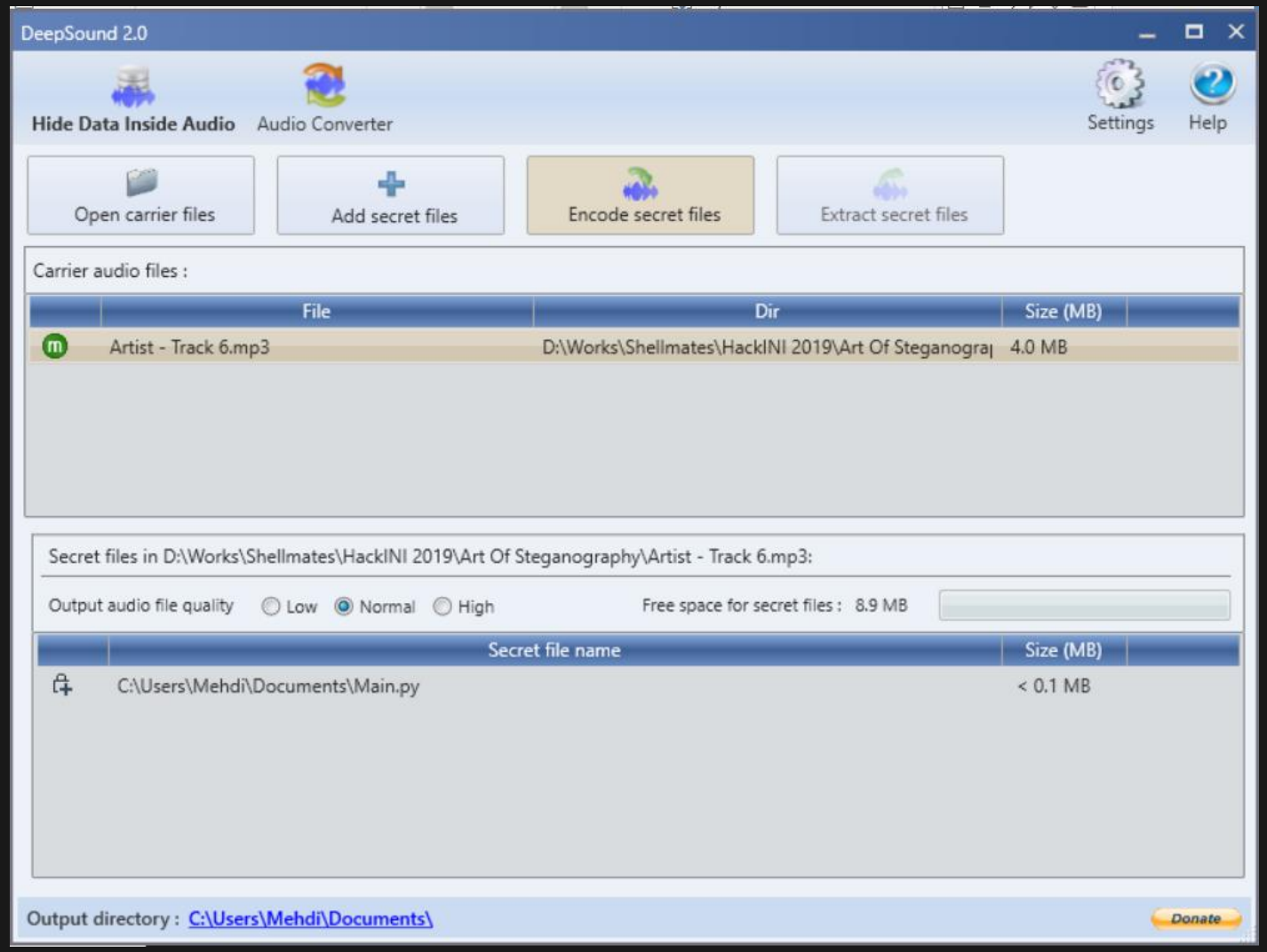
```
# from stegano import exifHeader
# secret = exifHeader.hide(“wéc_home.jpg", "w2c_secret.jpg", secret_message=“This is my password ")
# print(exifHeader.reveal("w2c_secret.jpg "))
```

Je vous conseil la bibliotheque Python Pillow pour toutes gestion sur une image
https://pillow.readthedocs.io/en/latest/handbook/tutorial.html

DeepSound

DeepSound est un outil gratuit de stéganographie et un convertisseur audio qui masque les données secrètes dans des fichiers audio.
http://jpinsoft.net/deepsound/download.aspx





Références

- CS 4953 The Hidden Art of Steganograph
- Cryptography By Mohamed ALLAL
- https://pics.corkami.com

THANKS FOR LISTENING!
HAVE A GOOD **CRACKING** DAY ☺

Website: www.mehdikerkar.keraterra.com

E-mail: mehdi.kerkar@tuta.io

LinkedIn: /in/mehdi-nacer-kerkar/

Twitter: @mehdi_kerkar

SHELLMATES HACK-INI