

```
\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» !?



- Introduction:



Stéganographie

Dans un sens Litéraire

- 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'écrire des **messages caché**, dans la façon que null personne à part les Communiquants Ne suspect **l'existence** 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:

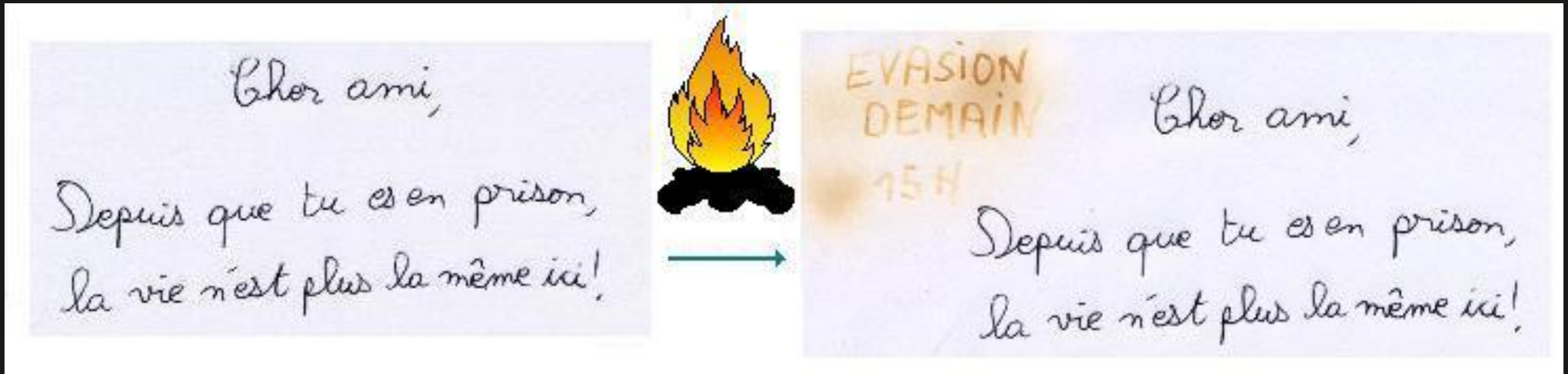
- Les utilisateurs ne peuvent voir aucune modification visible du fichier dans lequel les données sont masquées.

Type de Steganographie

- Text / Image Steganographie
- Audio Steganographie
- Video Steganographie

Text Steganographie

- Cacher de l'info d'un façon que son **existence** n'est pas **susceptible**



Dissimulation d'écriture

La **stéganographie** est l'art de la dissimulation : son objet est de faire passer inaperçu un message dans un autre message. Elle se distingue de la cryptographie, « art du secret », qui cherche à rendre un message inintelligible à autre que qui-de-droit. Pour prendre une métaphore, la stéganographie consisterait à enterrer son argent dans son jardin là où la cryptographie consisterait à l'enfermer dans un coffre-fort — cela dit, rien n'empêche de combiner les deux techniques, de même que l'on peut enterrer un coffre dans son jardin.

- D'après Wikipedia.

La **stéganographie** est l'art de la dissimulation : son objet est de faire passer inaperçu un message dans un autre message. Elle se distingue de la cryptographie, « art du secret », qui cherche à rendre un message inintelligible à autre que qui-de-droit. Pour prendre une métaphore, la stéganographie consisterait à enterrer son argent dans son jardin là où la cryptographie consisterait à l'enfermer dans un coffre-fort — cela dit, rien n'empêche de combiner les deux techniques, de même que l'on peut enterrer un coffre dans son jardin.

- D'après Wikipedia.

New Text Document.txt - Notepad

File Edit Format View Help

La stéganographie est l'art de la dissimulation : son shhhht
objet est de faire passer inaperçu un message dans un I have a secret for you buddy
autre message. Elle se distingue de la cryptographie, « A flag that could wins you 50pts :D
art du secret », qui cherche à rendre un message Here is it
inintelligible à autre que qui-de-droit. Pour prendre une Mini
métaphore, la stéganographie consisterait à enterrer son CTF{
argent dans son jardin là où la cryptographie consisterait \$T3g@n0graphY_
à l'enfermer dans un coffre-fort – cela dit, rien 1s_
n'empêche de combiner les deux techniques, de même C00L_
que l'on peut enterrer un coffre dans son jardin. m@t3!}
- D'après Wikipedia|

Écriture 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 Steganography



+



=



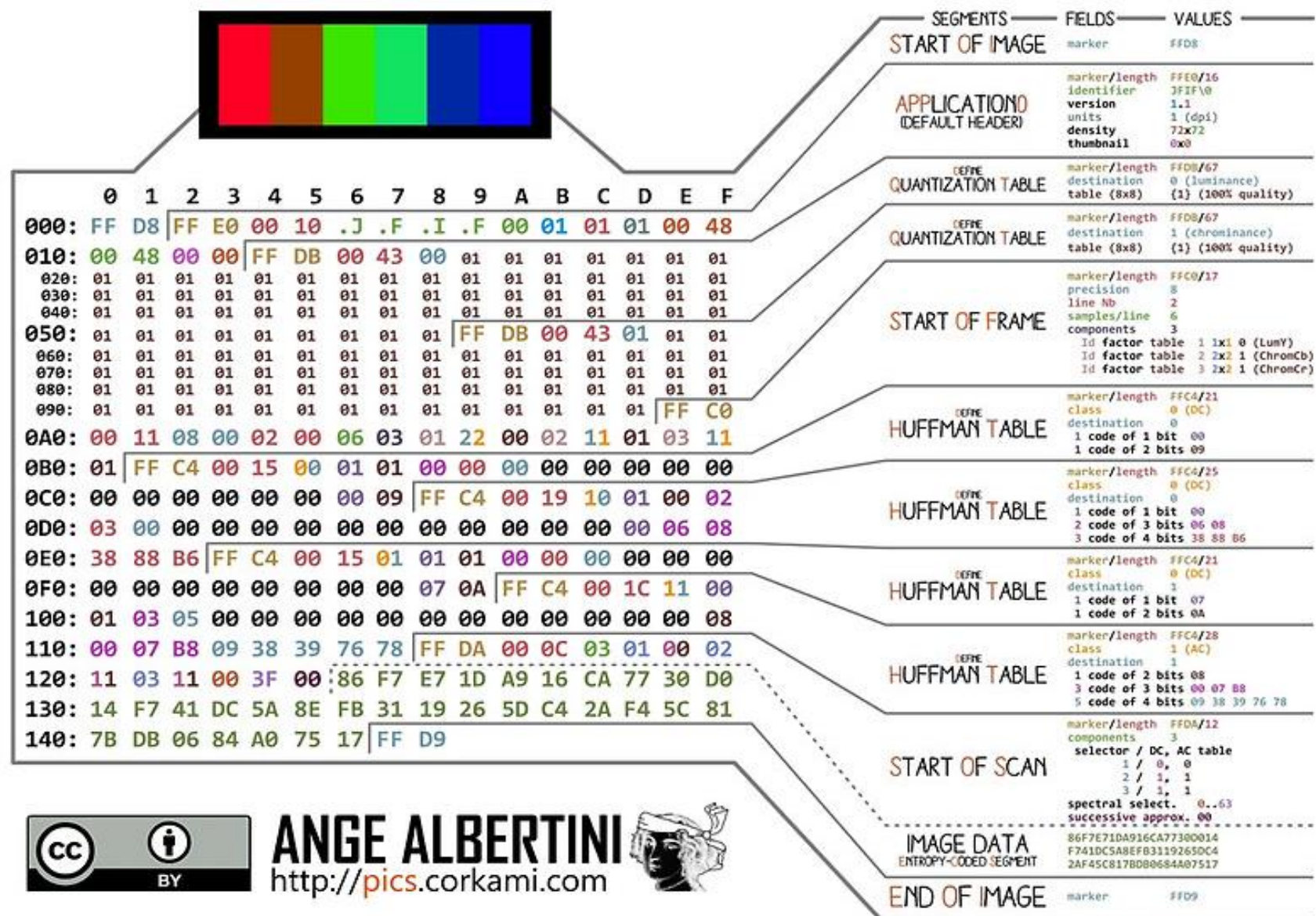
Image cache Images



Image Principale



JPEG File Interchange Format



ANGE ALBERTINI
<http://pics.corkami.com>



JPEG IS THE ENCODING STANDARD, JFIF IS THE FILE FORMAT

JPEG File Interchange Format Example

HxD - [D:\Works\Shellmates\HackINI 2019\Art Of Steganography\w3c_home.jpg]

File Edit Search View Analysis Tools Window Help

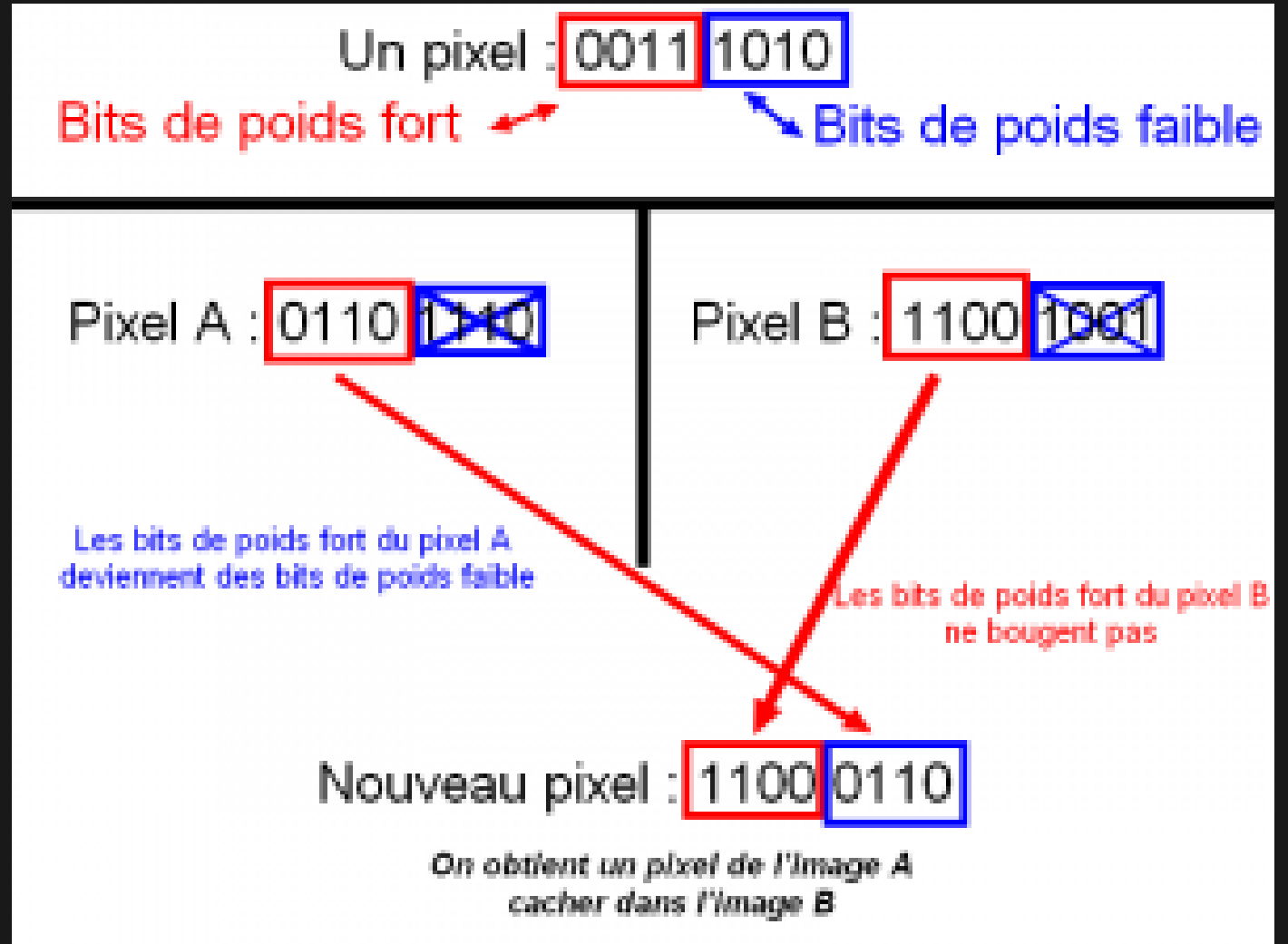
32 Windows (ANSI) hex

w3c_home.jpg

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	Decoded text
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	00	01	00	00	FF	DB	00	43	00	06	04	05	06	05	04	06	yøÿà..JFIF.....ÿÜ.C.....
00000020	06	05	06	07	07	06	08	0A	10	0A	0A	09	09	0A	14	0E	0F	0C	10	17	14	18	18	17	14	16	16	1A	1D	25	1F	1A%
00000040	1B	23	1C	16	16	20	2C	20	23	26	27	29	2A	29	1F	2D	30	2D	28	30	25	28	29	28	FF	DB	00	43	01	07	07	.#... , #&'*)..-0-(0%()ÿÜ.C...	
00000060	07	0A	08	0A	13	0A	0A	13	28	1A	16	1A	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28(((((
00000080	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	(((((
000000A0	00	11	08	00	30	00	48	03	01	22	00	02	11	01	03	11	01	FF	C4	00	1F	00	00	01	05	01	01	01	01	01	01	00O.H..".....ÿÄ.
000000C0	00	00	00	00	00	00	00	01	02	03	04	05	06	07	08	09	0A	0B	FF	C4	00	B5	10	00	02	01	03	03	02	04	03	05ÿÄ.
000000E0	05	04	04	00	00	01	7D	01	02	03	00	04	11	05	12	21	31	41	06	13	51	61	07	22	71	14	32	81	91	A1	08	23}.....!lA..Qa."q.2.';.#
00000100	42	B1	C1	15	52	D1	F0	24	33	62	72	82	09	0A	16	17	18	19	1A	25	26	27	28	29	2A	34	35	36	37	38	39	3A	B±Á.RÑð\$3br,...,%&'()* *456789:
00000120	43	44	45	46	47	48	49	4A	53	54	55	56	57	58	59	5A	63	64	65	66	67	68	69	6A	73	74	75	76	77	78	79	7A	CDEFGHIJSTUVWXYZcdefghijstuvwxyz
00000140	83	84	85	86	87	88	89	8A	92	93	94	95	96	97	98	99	9A	A2	A3	A4	A5	A6	A7	A8	A9	AA	B2	B3	B4	B5	B6	B7	f,,,,+~`%Š'""—™šćłŕ¥;§"©²³´µ¶·,
00000160	B8	B9	BA	C2	C3	C4	C5	C6	C7	C8	C9	CA	D2	D3	D4	D5	D6	D7	D8	D9	DA	E1	E2	E3	E4	E5	E6	E7	E8	E9	EA	FB	,°ÅÃÀÆÇÈÉÊËÔÕÖ×ØÙÚáâãäåæçèéñ
00000180	F2	F3	F4	F5	F6	F7	F8	F9	FA	FF	C4	00	1F	01	00	03	01	01	01	01	01	01	01	01	01	01	00	00	00	00	00	01	óôõö÷øùÿÄ.....
000001A0	02	03	04	05	06	07	08	09	0A	0B	FF	C4	00	B5	11	00	02	01	02	04	04	03	04	07	05	04	04	00	01	02	77	00ÿÄ.
000001C0	01	02	03	11	04	05	21	31	06	12	41	51	07	61	71	13	22	32	81	08	14	42	91	A1	B1	C1	09	23	33	52	F0	15!l..AQ.aq."2...B';±Á.#3Rð.
000001E0																																	

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

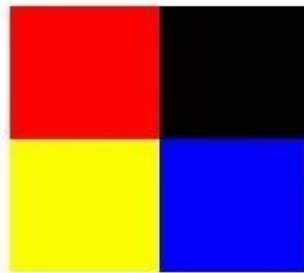
Original Image



11111111	00000000
00000000	00000000
00000000	00000000
11111111	00000000
11111111	00000000
00000000	11111111

Least Significant Bit Steganography

Stego Image



111111 01	000000 11
000000 10	000000 01
000000 00	000000 10
111111 00	000000 11
111111 01	000000 01
000000 01	111111 00



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

Audio Steganographie

The image displays two software interfaces used for audio steganography. The top interface is Audacity, showing a stereo audio waveform with a time scale from 2.0 to 21.0 seconds. The bottom interface is a steganography tool, showing a mono audio waveform with a time scale from 0.0 to 5.0 seconds. The tool's interface includes a menu bar (File, Edit, View, Transport, Tracks, Generate, Effect, Analyze, Help), a toolbar, and a track list. The track list shows a track named 'secret' with a sample rate of 22050 Hz and a 32-bit float format. The waveform in the steganography tool shows a hidden message, which is revealed as a flag in the bottom right corner.

www.instructables.com

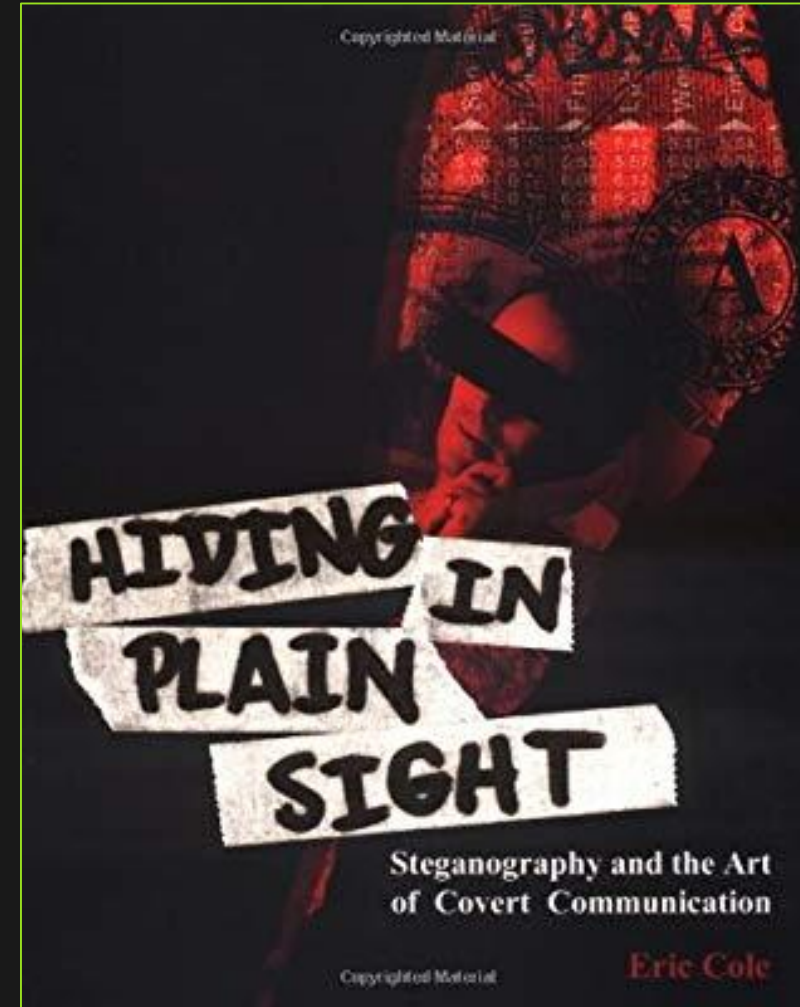
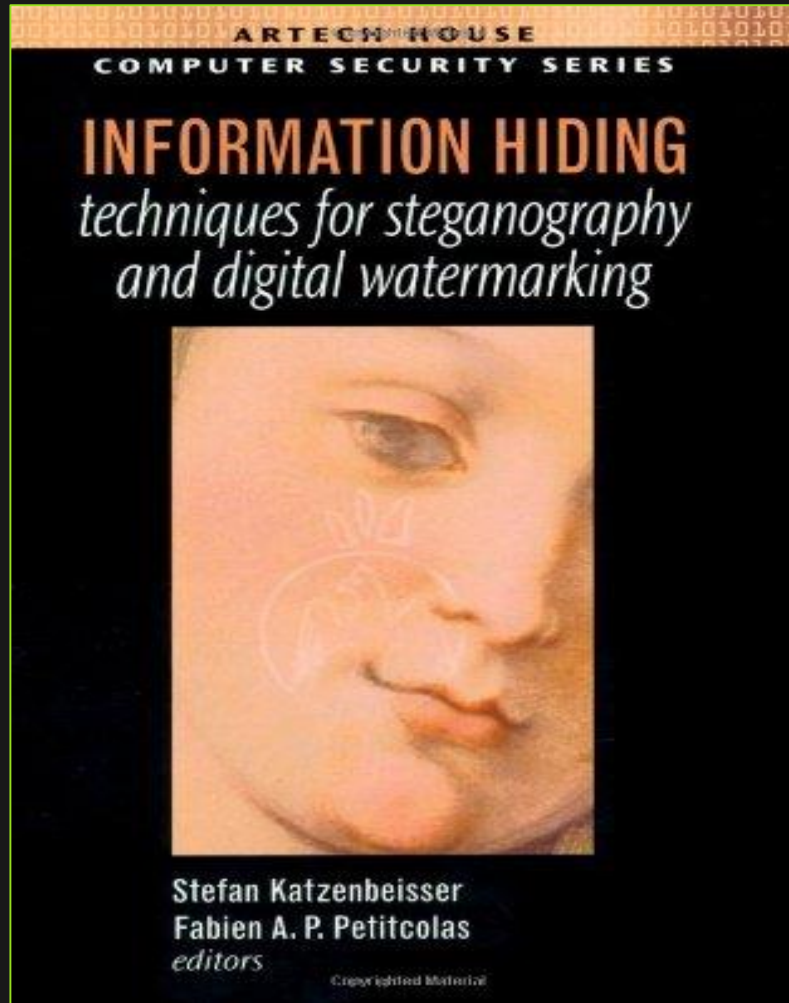
flag: e5353bb7b57578bd4da1c898a8e2d767

flag: e5353bb7b57578bd4da1c898a8e2d767

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
```

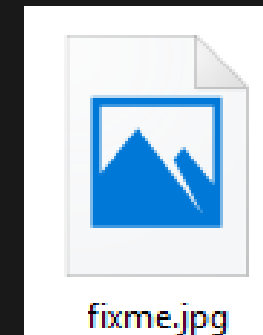
```
.....
```

```
y a Q \ , • • A @ this is my password
```

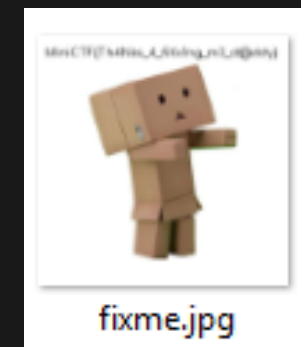
HxD Hex Editor

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	DD	E1	00	56	45	78	69	66	00	00	4D	4D	00	2A	00		..Yá.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	00F.(.....
00000040	01	00	02	00	00	00	00	00	00	00	01	2C	00	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	02	02	03	04	03	03	04	04	
00000090	04	04	04	02	03	05	05	04	04	05	04	04	04	04	FE	DBÿÛ



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FE	D8	E1	00	56	45	78	69	66	00	00	4D	4D	00	2A	00	ÿÛá.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	00F.(.....
00000040	01	00	02	00	00	00	00	00	00	00	01	2C	00	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>

Encode secret files

Output

Output format: Waveform Audio File Format (.wav)

Output directory: C:\Users\Mehdi\Documents\

☒ Encrypt secret files (AES 256)

Password:

Confirm password:

Encode secret files

DeepSound 2.0

Hide Data Inside Audio Audio Converter

Open carrier files Add secret files Encode secret files Extract secret files

Carrier audio files :

	File	Dir	Size (MB)
m	Artist - Track 6.mp3	D:\Works\Shellmates\HackINI 2019\Art Of Steganogra	4.0 MB

Secret files in D:\Works\Shellmates\HackINI 2019\Art Of Steganography\Artist - Track 6.mp3:

Output audio file quality: ☐ Low ☒ Normal ☐ High Free space for secret files : 8.9 MB

	Secret file name	Size (MB)
+	C:\Users\Mehdi\Documents\Main.py	< 0.1 MB

Output directory: C:\Users\Mehdi\Documents\ Donate

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/](https://in/mehdi-nacer-kerkar/)

Twitter: [@mehdi_kerkar](https://twitter.com/mehdi_kerkar)

