Stéganographie

Comment transmettre discrètement une information

Presented by
Alexis El mrini
Président HackIn'TN 2018

Sommaire

1. Définition
2. Types de supports
3. Quelques méthodes

Définition

Définition

- Etymologie : steganós (« étanche ») et graphế (« écriture »).
- But : cacher un message/fichier dans un autre message/fichier = dissimuler une info

Jamais il ne me viendrait à l'esprit d'utiliser ce texte à des fins de dissimulation, ce serait peu utile...

Définition

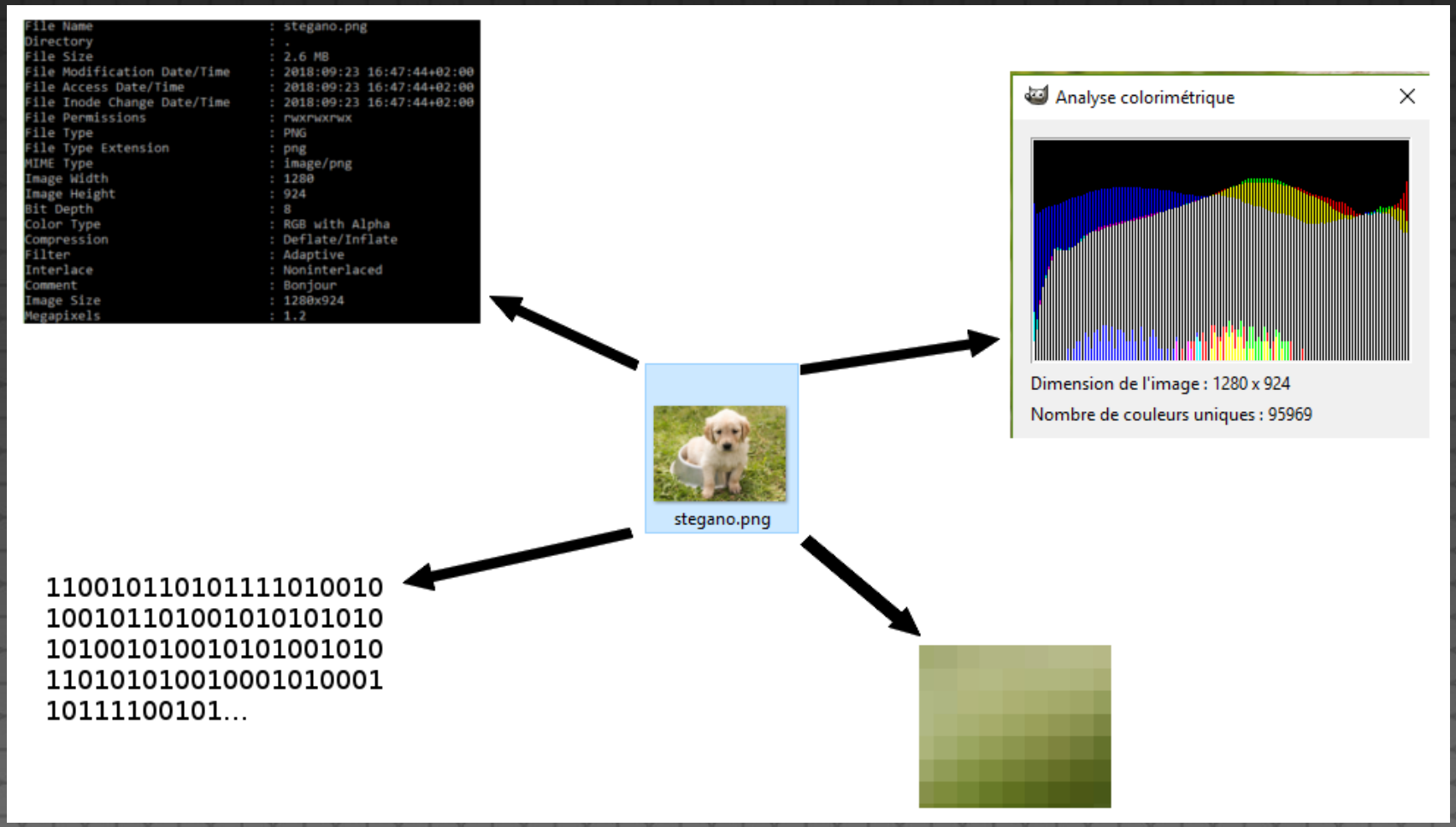
- Bonne stéganographie :
  - Compréhensible pour les destinataires
  - Incompréhensible pour les autres
  - Pas de clé : seulement connaître l’astuce

Quel message se cache dans cette image ?...

Types de supports

Types de supports

- 1 fichier = plein de représentations



Types de supports

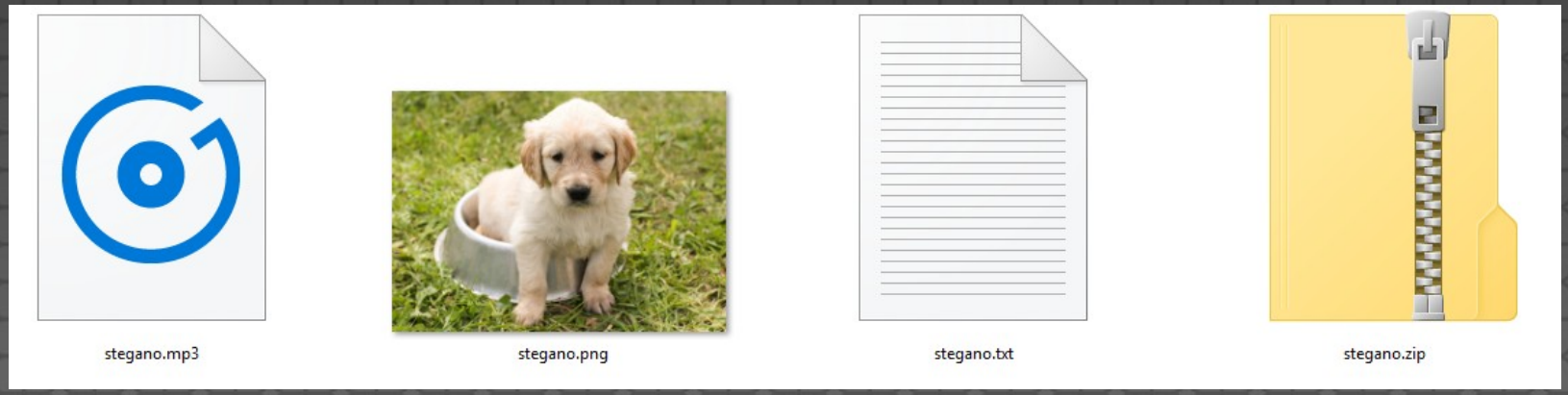
- Information binaire
  - Un fichier informatique = données binaires
  - Découpage : octets (ex : 0b01100001 = 0x61 = 97)
  - Plusieurs significations (encodage, valeur,...)

Types de supports

- Information principale
  - Information support du message
  - Dépend du format :
    - image (jpg, png,...)
    - Audio (mp3, wav,...)
    - Exécutable (bin, exe,...)
    - Code source (c, cpp, java,...)
    - Etc.

Types de supports

- Information principale
  - Lecture différente = information différente
  - Changement de format
  - Changement de mode de lecture



Types de supports

- Informations secondaires
  - En-tête de fichier : format d’origine
  - Données EXIF
  - Peuvent être très utiles !


```
GPS Altitude                    : 202.5 m Above Sea Level
GPS Date/Time                   : 2016:01:11 18:31:45.01Z
GPS Latitude                    : 48 deg 40' 8.13" N
GPS Longitude                   : 6 deg 9' 15.21" E
GPS Position                    : 48 deg 40' 8.13" N, 6 deg 9' 15.21" E
```

exiftool

Il suffit de chercher dans les données EXIF !

Où se trouve cette école ?

Types de supports

- Informations analytiques
  - Analyses des données selon le type
    - Audio : FFT, spectrogramme,...
    - Image : FFT, colorimétrie, histogrammes,...
    - Texte : fréquence des lettres,...

Stégano version Amixem

Quelques méthodes

Quelques méthodes

- De très TRÈS nombreuses méthodes
- Quelques-unes :
  - Least Significant Bit
  - Audio spectrograms
  - Funky File formats
  - EXIF Comment

Quelques méthodes

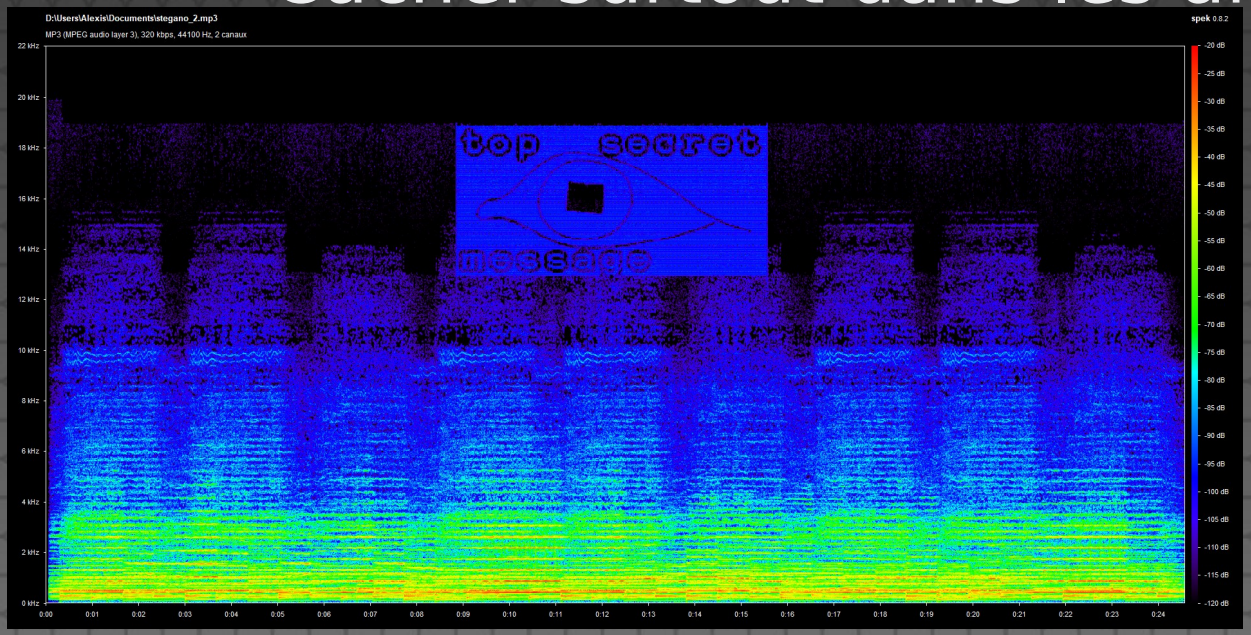
- Least Significant Bit
  - Format image, audio,...
  - Utiliser le bit de poids le plus faible

    → Influe très peu l'image, le son,...
  - 1 bit par pixel pour une image

Je vous laisse trouver le message caché dans cette image ;)

Quelques méthodes

- Audio spectrograms
  - Dessiner dans un spectrogramme audio
  - Répartition intensité selon temps et fréquence
  - Cacher surtout dans les aigus

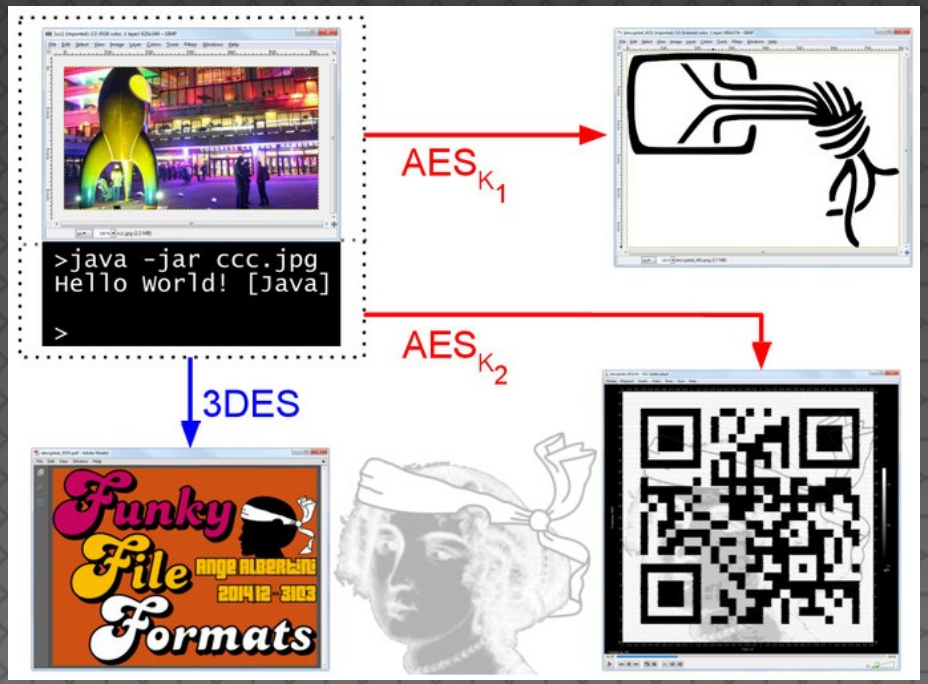


Jouer l’audio

Source : https://solusipse.net/

Quelques méthodes

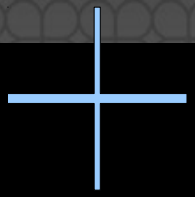
- Funky File Formats
  - Fichier polyglotte : plusieurs fichiers en un
  - Ex : jpeg + java + bmp
  - Transformation par chiffrement (angecryption)

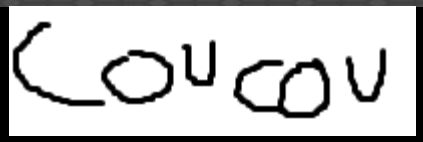


Source : Ange Albertini

Quelques méthodes

- EXIF Comments :
  - Données EXIF : relatives à l’image JPEG
  - Données photographiques, générales, etc.
  - Champ Comment : y mettre n’importe quoi






```
alexis@DESKTOP-U1O8V09:/mnt/d/Users/Alexis/Documents/stegano$ exiftool stegano.png
ExifTool Version Number         : 10.40
File Name                       : stegano.png
Directory                       : .
File Size                       : 2.6 MB
File Modification Date/Time     : 2018:09:24 23:57:29+02:00
File Access Date/Time           : 2018:09:24 23:57:29+02:00
File Inode Change Date/Time     : 2018:09:24 23:57:29+02:00
File Permissions                : rwxrwxrwx
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 1280
Image Height                    : 924
Bit Depth                       : 8
Color Type                      : RGB with Alpha
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Comment                         : BM6(A....XXXhhh```......hhhHHH...hhh...```hhh......   hhh```...```XXX......```   hhh......hhhHHH   ......pppppp000hhh```   ...      XXX......hhh......HHH...```hhh   ...   hhhppp......000   ppp   ...hhh..
.XXX...   PPP```...ppp   ppp......XXX...hhh...   ...XXXhhhppp...hhhHHH...HHH.........HHH......pppppp```hhhXXXppp.................................ppp......   hhh...hhhImage Size              : 1280x924
Megapixels                      : 1.2
```

En bref

- En stéganographie, toute information est utilisable
- Les méthodes sont limitées par l’imagination !

Liens utiles

- Spectrogram steganography
- Funky File Formats
- LSB decoder

Questions?