Le format JPEG en stéganographie

By Strepoetlo

Que faire lorsque l'on tombe fasse a une image de type .jpg lors d'une épreuve de stéganographie?

I. Vérifier le fichier.

Alors tout d'abord le premier réflexe à avoir c'est de vérifier que le document est bien à la base une fichier .JPG, avec la commande "file".

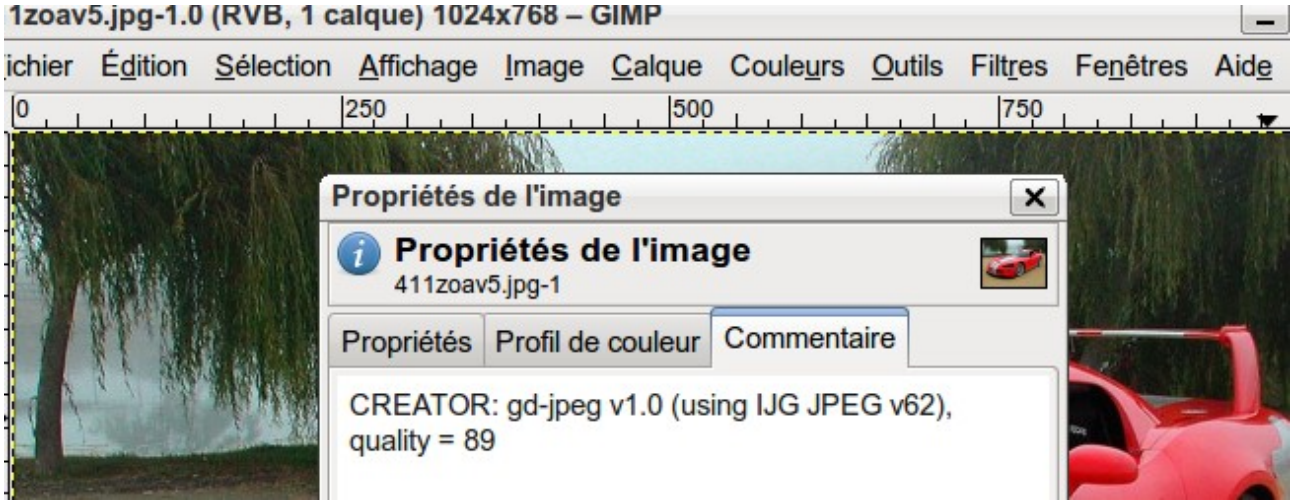
```
strepoetlo@strepoetlo-K50ID:~/Images$ file 411zoav5.jpg
411zoav5.jpg: JPEG image data, JFIF standard 1.01, comment: "CREATOR: gd-jpeg v1.0 (using IJ"
```

Comme on peux le voir, ce fichier est un fichier .jpg, et il possède un commentaire.

II. Les commentaires

Le deuxième point à regarder c'est la présence ou non de commentaires.
Pour cela la commande file est bien aussi, malheureusement si le commentaire est important la commande ne ressort pas le commentaire en entier (comme dans l'exemple précédent).
Donc plusieurs possibilités s'offre à vous, en fait ça dépend de vos habitudes et des logiciels que vous utilisez, personnellement j'utilise GIMP.

Donc j'ouvre l'image avec gimp > Image > Propriétés de l'image > Commentaire.



Le commentaire est ici « CREATOR: gd-jpeg …. quality = 89 »

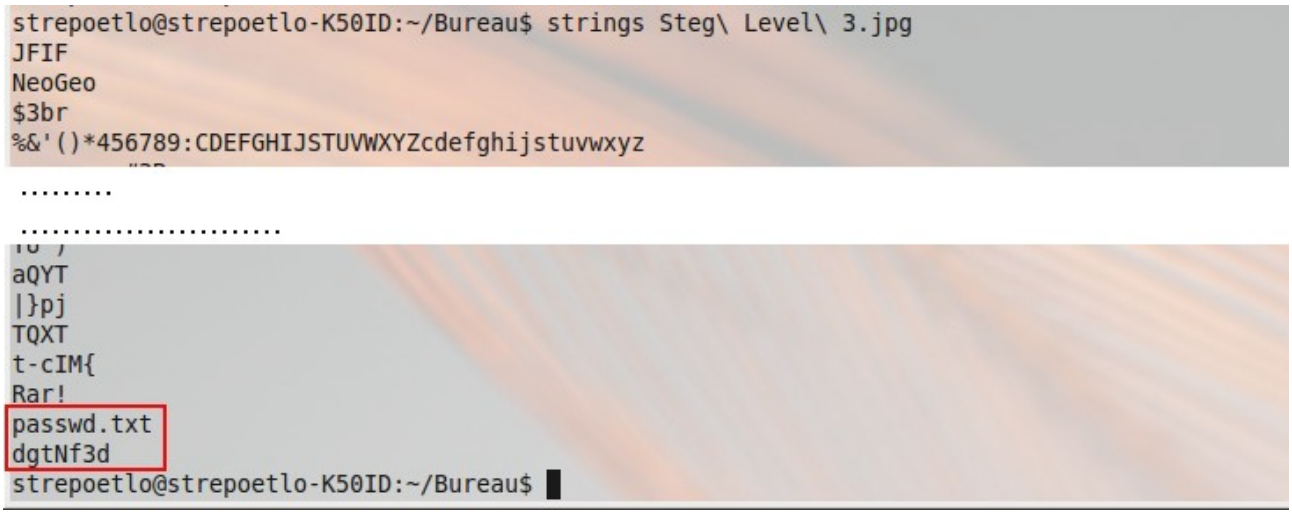
mais vous pouvez aussi utiliser : Phatch, exiv2 (exiv2 -pc l_image.jpg)....

III. Paramètres de l'image

En effet il est possible de modifier les couleurs d'une image ou de seuil pour pouvoir faire apparaitre un message qui est caché dans l'image même,
mais cette technique ne fait pas partie de la stéganographie pure, ce n'est qu'une technique assez simple a mettre en œuvre pour cacher du texte.
Pour cela utiliser des logiciels comme gimp ou photosphop, ou tout autre logiciel de traitement d'image.

IV. Les strings

Il est possible de cacher du texte directement à l'intérieur d'une image en modifiant son code hexadécimal, il est possible de trouver une chaine de caractère dans une image
grâce aux commandes "strings" ou "cat", cependant il en faut pas croire" que toute chaine de caractères donne une informations, au contraire, certaines chaines ce sont créés par hasard.



Là le password est clairement indiqué en bout de fichier.

V. Les en têtes

Dans les en têtes d'une image ce cache tout un tas d'informations qui peuvent nous être utile, comme la taille originale d'une image, ou si un fichier a été caché à l'intérieur de l'image.

En effet le format jpg étant un format a compression si la taille est très grande, un autre fichier peut être caché à l'intérieur.

Par exemple des données exif peuvent nous renseigner sur la présence d'une miniature intégré à l'image, mais différentes de l'image visible.
Pour cela on utilise exif2 : exif2 l_image_de_base -et le_nom_de_la_miniature_a_extraire.
Il ne vous reste plus qu'a regarder la vignette extraite.

Ce paper est incomplet, merci de me contacter pour ajouter des informations.