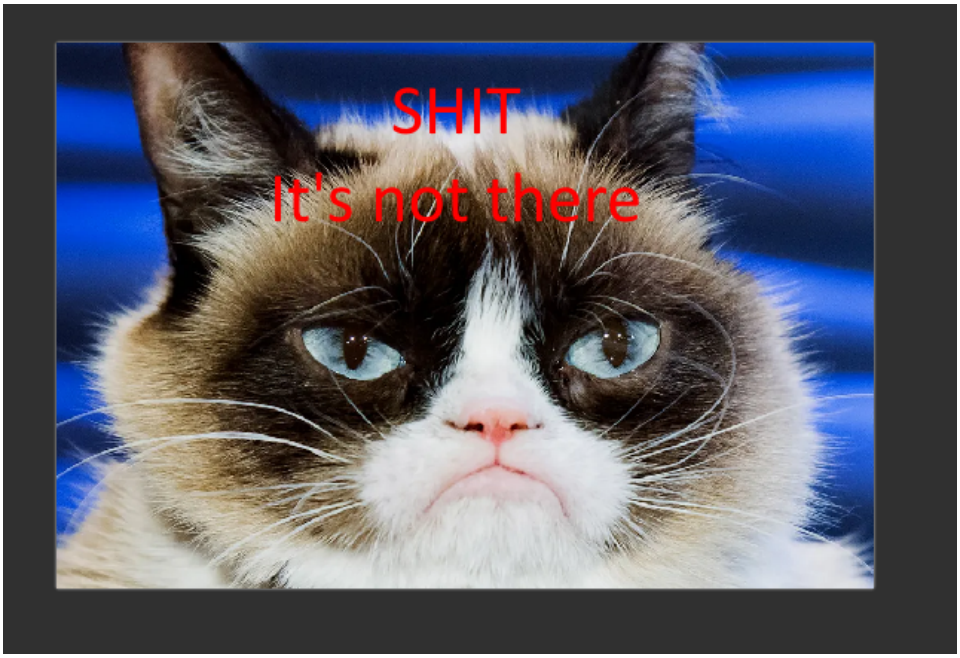
Stéganographie - HiddenHalf - 75 points

Kévin DUVERGER

Table des matières

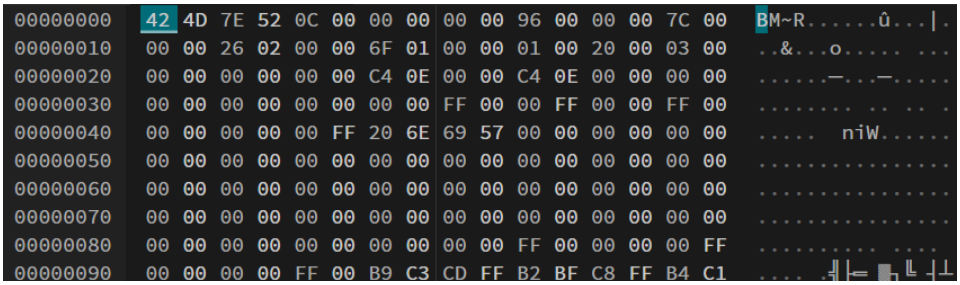
1 Résolution HiddenHalf :

Nous avons donc un fichier `mysteriousImage.png` qui s'affiche de la façon suivante :



Jusque ici, rien de bien remarquable (sauf peut-être la tête du chat).

C'est un fichier BMP, on peut donc tenter d'aller voir un peu les champs de l'en-tête pour nous aider :



Nous pouvons maintenant utiliser la documentation dans `https://en.wikipedia.org/wiki/BMP_file_format` pour tenter de comprendre un peu mieux les différentes valeurs de l'en-tête :

0x42 0x4D	0x7E 0x52 0x0C 0x00	0x00 0x00	0x6F 0x01	0x96 0x00 0x00 0x00
BM	size (LE) = 807550	--	--	addr data = 0x96

hdr. size = 0x7C	width = 0x226 (550)	height = 0x16F (367)

Quelque chose ne matche pas ici, les dimensions indiquées de cette image sont `550*367` et la taille déclarée dans le fichier BMP matche bien également : si chaque pixel est stocké sur 4 octets, on obtient $550 \times 367 \times 4 = 807400$ octets qui est très proche de la bonne valeur (807550). Le problème est que la taille réelle du fichier est 2 fois supérieure, `1 617 950` octets pour être exact.

Il semblerait donc que des données soient cachées dans l'autre partie de l'image, peut être même une autre image. Il faudrait donc arriver à modifier les dimensions de telle sorte à doubler la surface et faire apparaître l'image cachée, mais comment peut-on faire cela ?
L'idée est que les images bitmap sont stockées du pixel en bas à gauche, ligne par ligne, jusqu'au pixel en haut à droite : en cachant des octets on retire donc les lignes en partant du haut !
L'idée sera donc de doubler la hauteur, ce que l'on peut fair directement sur `hexed.it`, la nouvelle valeur étant `0x2DE`, ce qui devrait faire apparaître une nouvelle partie en haut de l'image originale.

Voici le résultat qui nous donne le flag :

D'autres possibilités intéressantes pourraient être de changer l'adresse de début des données, ...