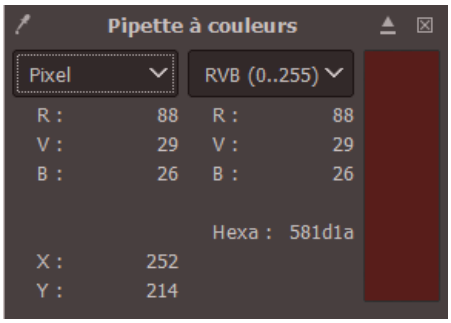
CASALE Pierre 04/10/2022

Cf : stegano2021.pdf

TP Cybersécurité Stéganographie

Q1/ Couleur d'un pixel

Retrouver la couleur du pixel aux coordonnées (252,214) (stega-img0.png).

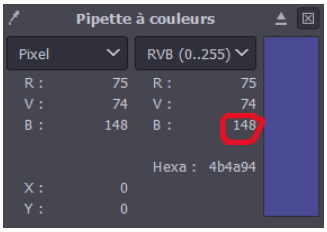


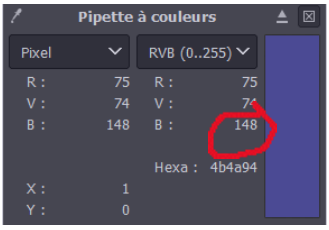
Le pixel est de couleur rouge foncé son code hexa est : #581d1a.

Q2/ Description du procédé stéganographique

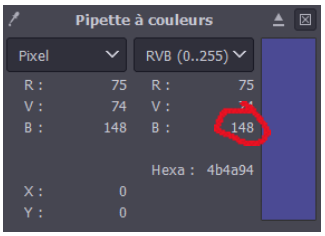
Les deux pixels en position (0,0) et (0,1)

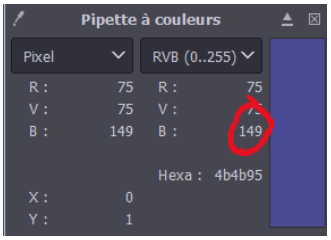
sont de la même couleur.





On n'aperçoit pas de changement à l'œil nu.





Q3/ Retrouver un message

Le message est : TB !

Pour retrouver le message on a déterminé le bit de poids faible des pixels 0 à 7 de la première ligne en se basant sur leur code hexadécimal traduit en binaire puis en décimal ce qui donne 00000100 (Base 2) = 4 (Base 10), Chaque caractère de la table ASCII étant codé sur 8 bits, donc 8x4 = 32, nous devions donc chercher 32 bits, on nous dit que ces bits sont situés sur la ligne suivante.

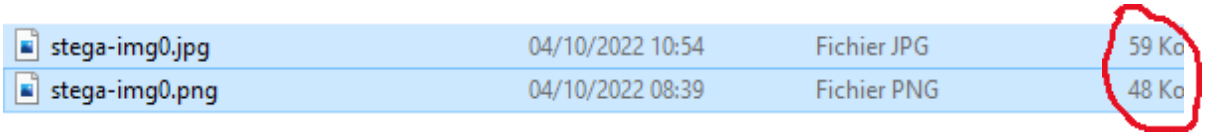
Ce tableau montre les 32 bits trouvés et leur conversion à l'aide de la table ASCII.

0	1	0	1	0	1	0	0	0	1	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1
T								B								[Espace]								!							

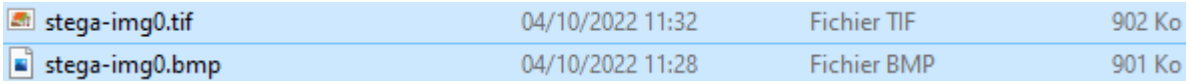
Q4/ Choix du format de sauvegarde

Quand on charge l'image au format .jpg le message est impossible à retrouver car tous les pixels sont à 149/255 pour le code bleu, donc tous les bits de poids faible sont à 1.

On remarque également que le fichier .jpg est plus lourd que le fichier .png.



J'ai testé les formats .bmp et .tif qui sont tous deux bien plus lourd encore mais qui restituent chaque pixel correctement.



On peut donc en déduire que la stéganographie fonctionnera beaucoup moins bien en utilisant le format .jpg.

Q5/ Vers l'infini et au-delà !

La stéganographie peut être utilisé sur une image comme on a pu le voir mais également avec d'autres types de fichiers comme des fichiers audio, url ou script par exemple.

Récemment encore, un malware caché dans un logo Windows :

« Attention à ce malware qui peut se cacher dans ce vieux logo de Windows ! »

« Un groupe de pirates connu sous de multiples appellations utilise un vieux logo pour piéger ses victimes. Bien que cette technique ne soit pas toute récente, elle est rarement utilisée par les groupes de hackers à l'envergure internationale. »

- https://www.phonandroid.com/attention-a-ce-malware-qui-peut-se-cacher-dans-ce-vieux-logo-de-windows.html

Pour se protéger de ce type d'attaques il existe des solutions, notamment des logiciels qui peuvent détecter ces images contenant un potentiel malware.

« Configurer une solution antimalware pour détecter les binders. Les logiciels antimalware doivent être configurés de sorte à pouvoir déceler la présence de binders susceptibles de contenir des stégo-images. »

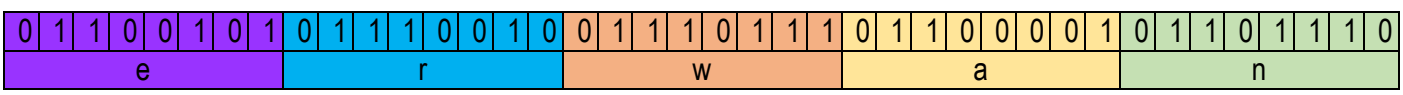
Dans un cadre plus professionnel on peut également envisager de segmenter le réseau.

« Segmenter le réseau. Au cas où votre entreprise serait victime d'une attaque stéganographique, une architecture de virtualisation approuvée associée à une segmentation de réseau adéquate est utile pour endiguer la propagation. En effet, la surveillance continue du trafic et le processus de démarrage sûr et vérifiable que cette architecture utilise permettent de mieux isoler les applications. »

- https://www.mcafee.com/enterprise/fr-ca/assets/solution-briefs/sb-quarterly-threats-jun-2017-2.pdf

Q bonus/ Dissimuler un message

Avec mon voisin Erwan nous avons échangé une image avec un message caché sur la troisième ligne, j'ai retrouvé dans son image 8 octets qui sont : 01100101 ; 01110010 ; 01110111 ; 01100001 ; 01101110 qui équivaut à 101, 114, 119, 97, 110 en décimal puis à l'aide de la table ASCII on obtient « erwan ».



Je lui ai envoyé une image avec comme code binaire à retrouver sur 2 octets = 10100000 ; 10000111 = 80 ; 67 = PC.