GUASTAMACCHIA 20/10/23

Livio

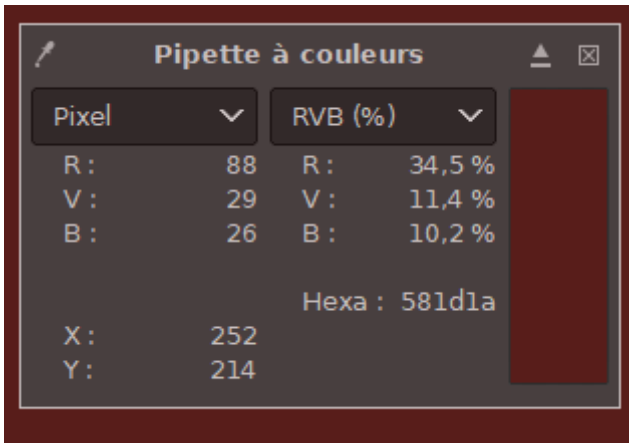
SIO1

TP noté :

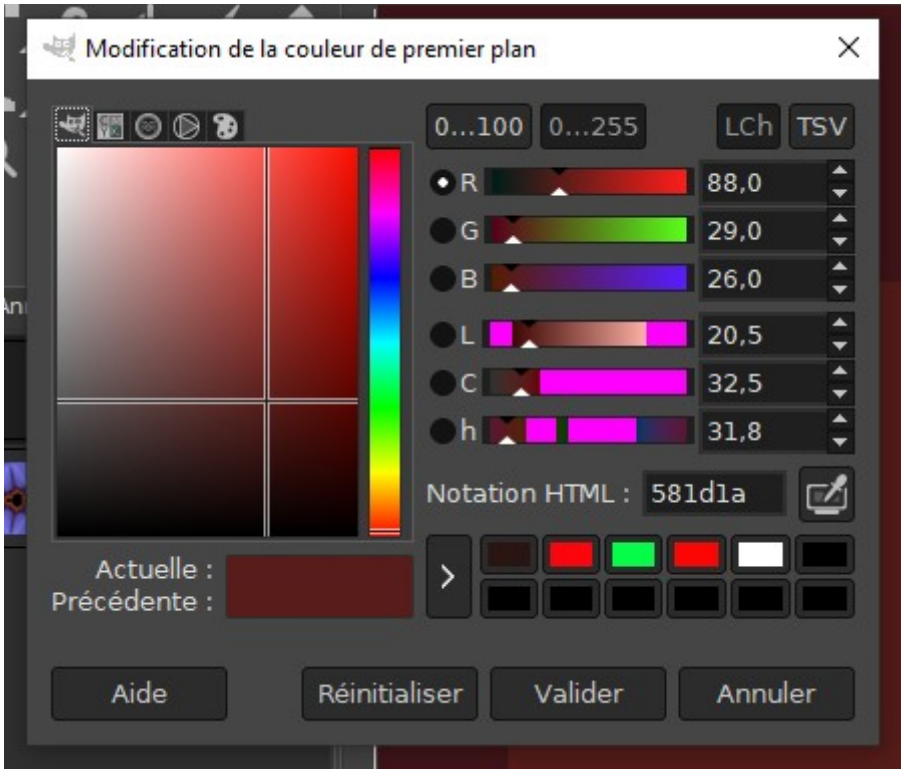
« Image et sécurité informatique » / stéganographie

Couleur d'un pixel :

Pour connaitre le code hexadécimal et html j'ai zoomé sur le pixel demandé (252,214) puis j'ai utilisé l'outil pipette pour prendre d'information du pixel.



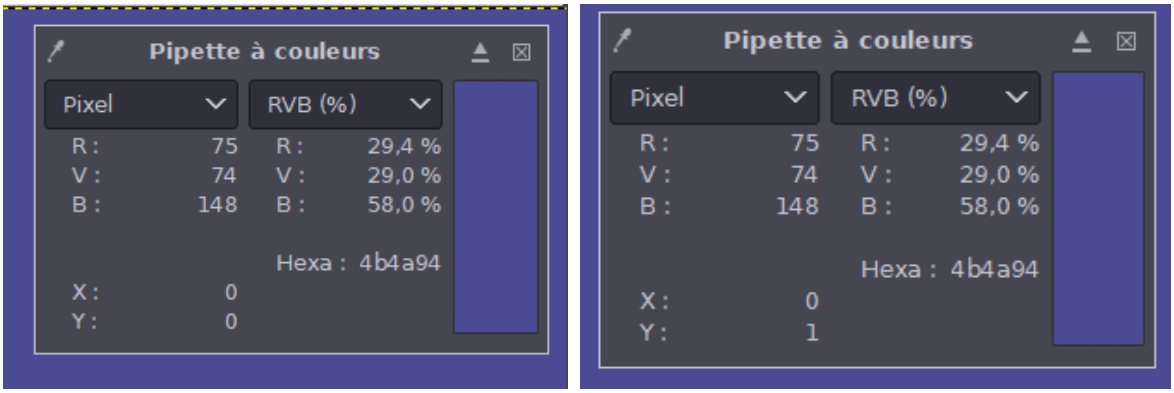
Sur cette capture d'écran de mon gimp on peut voir l'onglet où est marqué le code héxadécimal qui est 581dla.



Et sur celle-ci nous pouvons voir le code html qui est 581dla.

Description du procédé stéganographique :

1/



En utilisant l'outil pipette, j'ai comparé les deux pixels et nous pouvons voir que les valeurs R V et B sont les mêmes donc les deux pixels sont de même couleur.

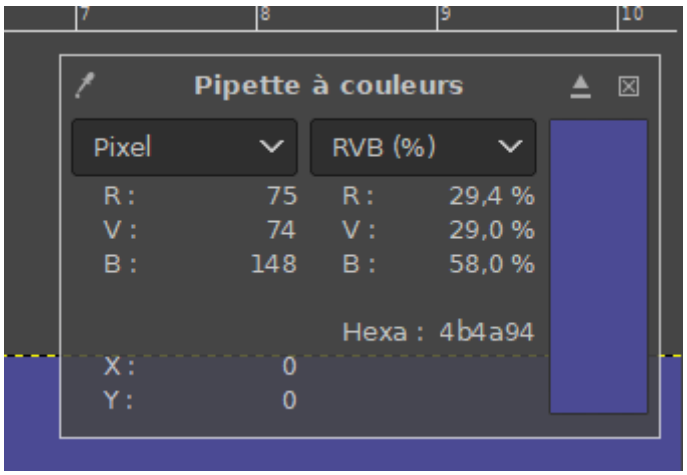
2/ Pour modifier la couleur du pixel (0,0) j'ai ouvert la fenêtre « couleur de premier plan » puis modifié la valeur du bleu de 1 pour ensuite prendre l'outil crayon, modifié sa taille à 1 pixel pour qu'il n'affecte que 1 pixel puis modifié la couleur du pixel demandé.

3/ En observant le pixel modifié et son pixel voisin, à l'œil nu on ne voit aucune différence.

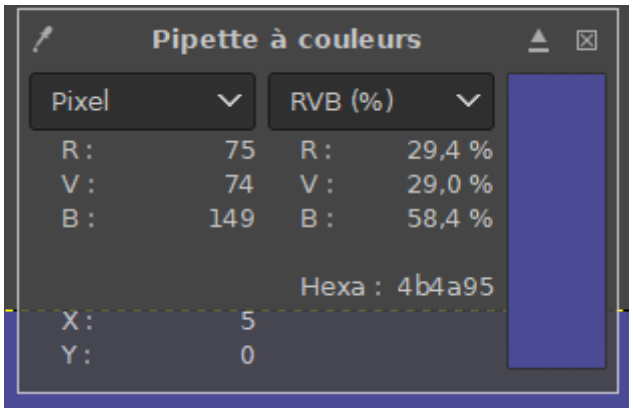
Retrouver un message :

1/ Pour la première ligne des abscisses :

Les valeurs du bleu, des pixels 0, 1, 2, 3, 4, 6 et 7 est de 148



Mais la valeur du bleu du pixel 5 est de 149



2/ Vu que nous somme en binaire les bits de point faible des nombres pairs seront en toute logique équivalent à 0 et ceux des nombres impairs équivalent à 1.

Donc pour la première ligne, leurs bits de point faible sont :

Pixel :

0 1 2 3 4 5 6 7

Bit de point faible :

0 0 0 0 0 1 0 0

3/ En prenant le paquet de 8 bits de point faible en regardant sur le tableau ASCII on obtient 4 donc 8x4= 32.

La longueur du message de la ligne deux est donc de 32 pixels.

Codes binaires des caractères cachés :

Pour obtenir le message caché je vais marquer à la suite les bits de point faible. Lorsque la valeur bleue est égale à 148 je noterai 0 et lorsqu'elle est égale a 149 je noterai 1.

Donc le code binaire est :

01010100010000100010000000100001

Que l'on divise par 4 pour donner des paquets de 8

01010100 01000010 00100000 00100001

4/ avec la table ASCII le code binaire correspond donc au message

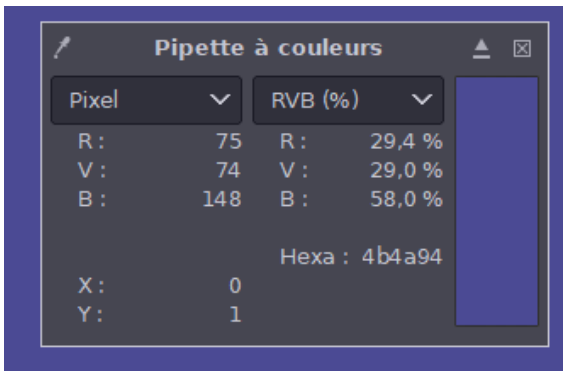
T B SP !

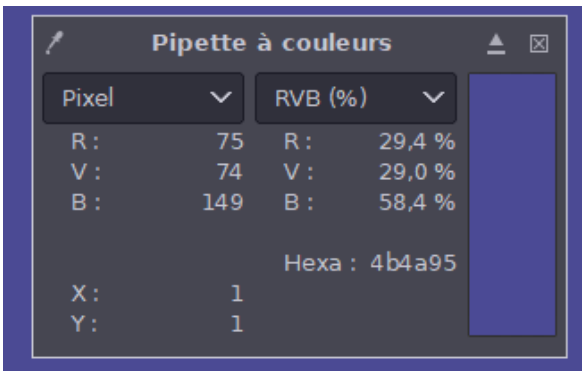
Choix du format de sauvegarde du fichier :

1/ premièrement pour enregistrer le fichier en format jpg il faut aller dans l'onglet fichier puis « exporter sous » pour enfin modifier le format du fichier et l'enregistrer.

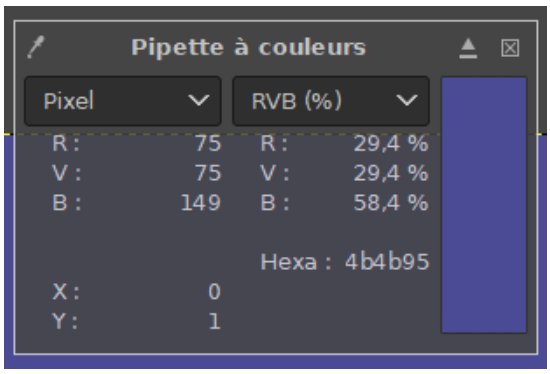
2/ en chargeant cette image dans Gimp on remarque que lorsque l'on essaye de retrouver les informations cachées on ne les retrouve plus

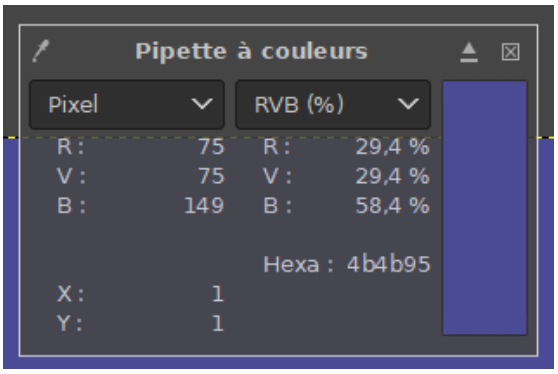
Avant enregistrement au format jpg :





Après enregistrement au format jpg :





3/ Pour voir le poids du fichier j'ai fait un clic droit sur le fichier de mon image et j'ai fait « propriété ».

Taille format jpg :

Taille :	55,6 Ko (56 993 octets)
Sur disque :	56,0 Ko (57 344 octets)

Taille format png :

Taille :	47,2 Ko (48 398 octets)
Sur disque :	48,0 Ko (49 152 octets)

On remarque qu'avec le fichier jpg la qualité de l'image est détériorée et en plus elle prend plus de place.

4/ pour cette question je vais tester plusieurs formats de fichier que j'aurai vu sur google et évoqué mon point de vue par rapport à ces formats de fichiers, les raisons de pourquoi ils sont bien ou pas bien pour la sténographie.

Sur google j'ai appris qu'il y avait 2 types de format, le format matricielle et vectorielle.

Format matricielle : format de fichier avec un nombre de pixel défini

Format vectorielle : format de fichier avec un nombre modulable de pixels

Maintenant je vais procéder à l'analyse des différents formats de fichiers :

JPEG :

Le format JPEG est un format de fichier qui compresse un document, mais a son désavantage il supprime les détails non visibles a l'œil nu ce qui rend la lecture de message caché impossible car il a été supprimé, en plus le poids du fichier devient supérieur par rapport au poids de base de l'image. Ce format n'est donc pas bon pour une utilisation sténographique.

Taille :	55,6 Ko (56 993 octets)
Sur disque :	56,0 Ko (57 344 octets)

BMP :

Le format BMP est un format de fichier qui compresse le fichier de base sans supprimer les détails non visibles à l'œil nu mais en contre partie il rend le fichier beaucoup trop lourd par rapport au format de base. Ce fichier est donc bon pour la sténographie mais pas rentable niveau poids comparé à d'autres

Taille :	900 Ko (921 722 octets)
Sur disque :	904 Ko (925 696 octets)

GIF :

Le format GIF est un format de fichier qui compresse le fichier de base sans supprimer les détails non visibles à l'œil nu, le format est encore d'actualité. Ce format est donc bon pour la sténographie.

Taille :	25,5 Ko (26 212 octets)
Sur disque :	28,0 Ko (28 672 octets)

TIFF :

Le format TIFF est un format de fichier qui compresse le fichier de base sans supprimer les détails non visibles à l'œil nu mais en contre partie il rend le fichier énormément plus lourd que le format de base. Ce fichier est donc bon pour la sténographie mais il n'est pas rentable niveau poids comparé à d'autres.

Taille :	1,02 Mo (1 070 354 octets)
Sur disque :	1,02 Mo (1 073 152 octets)

Conclusion :

En résumé le format de fichier le plus approprié à la sténographie, de ceux que j'ai testé, est le format GIF. Celui-ci est capable de garder les informations contenues dans le fichier tout en le compressant d'une façon rentable en réduisant son poids. Comparé aux autres, qui eux compressent le fichier en le rendant plus lourd comme les formats BMP et TIFF ou encore en supprimant les informations non visibles à l'œil nu comme le format JPEG.

Vers l'infini et au-delà :

Sur le site IT-connect.fr, j'ai trouvé une attaque à base de stéganographie le 22/03/2022 qui s'est abattu sur la France, les pirates s'y sont pris de la manière suivante :

Premièrement les pirates ont utilisé la technique du phishing en envoyant des mails contenant un document Word pour une campagne du RGPD qui intégrait lui-même une macro malveillante. Lorsque que l'on ouvrait le fichier Word et que nous donnait accès au contenu, le document installait une image de chipeur de Dora l'exploratrice qui contenait un script PowerShell grâce a la stéganographie, la macro exécutait ensuite le script qui a pour but d'installer le gestionnaire de paquet Chocolatey (sert à installer des logiciels) sur le pc, qui ensuite a pour but d'installer deux paquets : Python et PIP. Vu que les services informatiques utilisent souvent Chocolatey, il y avait beaucoup de chance qu'on le laisse effectuer l'installation. C'est de cette manière que les pirates on réussis a intégré le Malware dans les pc.

Conclusion :

Grâce à cet article j'ai remarqué que la stéganographie est utiliser pour le mal mais le principal problème et d'intégrer et d'exécuter l'image dans le pc de l'autre c donc pour sa que la stéganographie a été mélangé avec le phishing dans cet article.