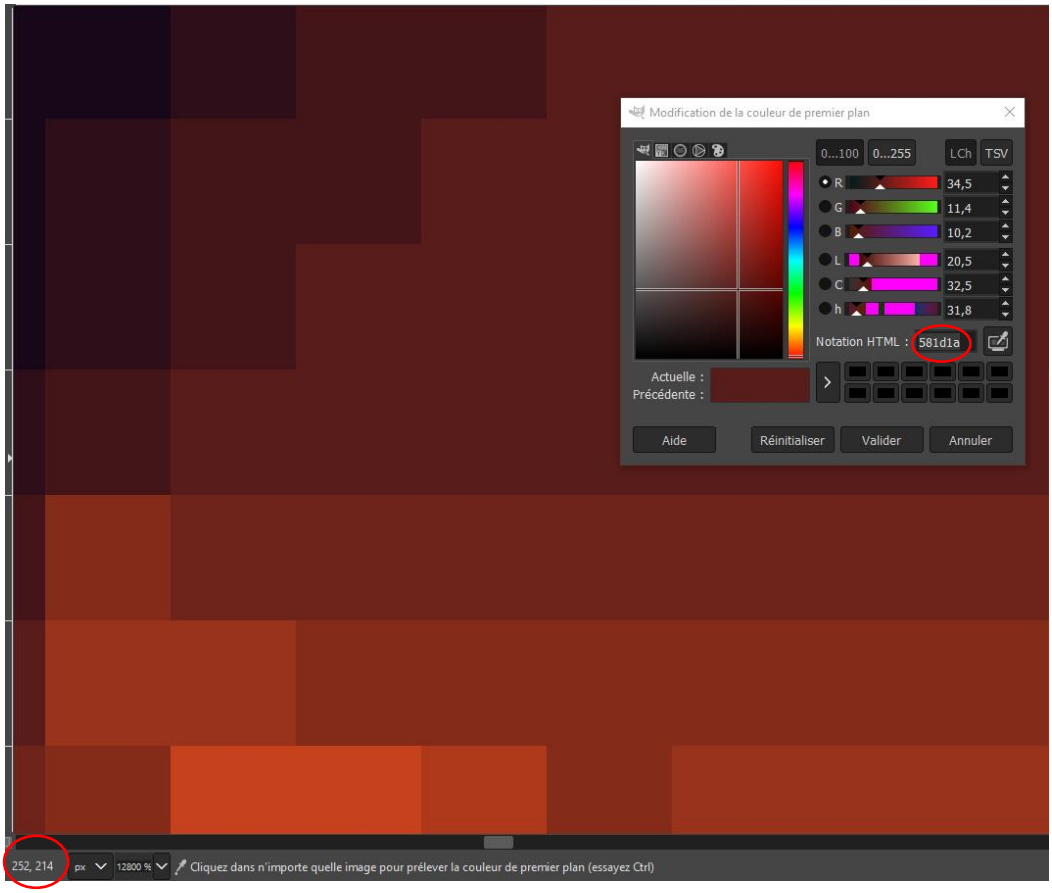
DERRUAU
Roméo

TP noté « Images et sécurité informatique » / Stéganographie

Couleur d'un pixel (2pts)

Quel est le code hexadécimal, celui utilisé en html, pour cette couleur ?

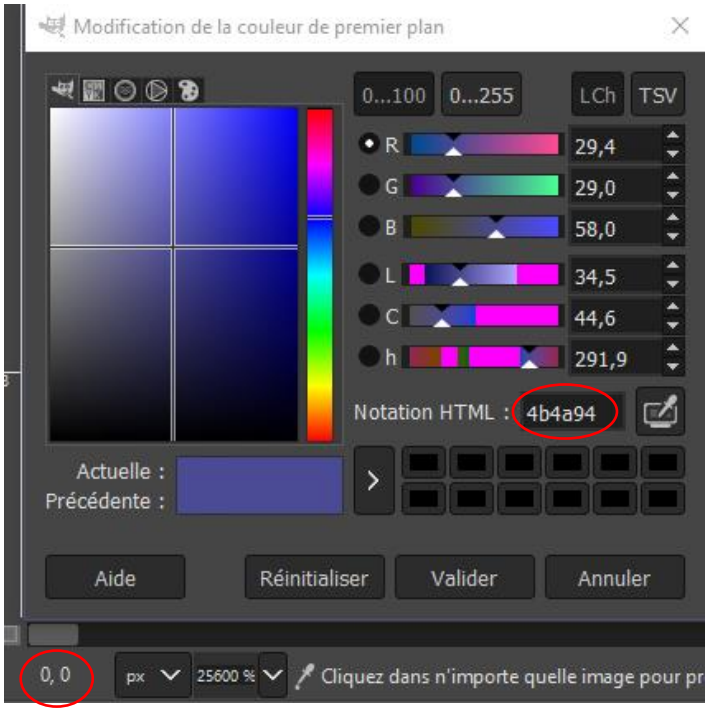


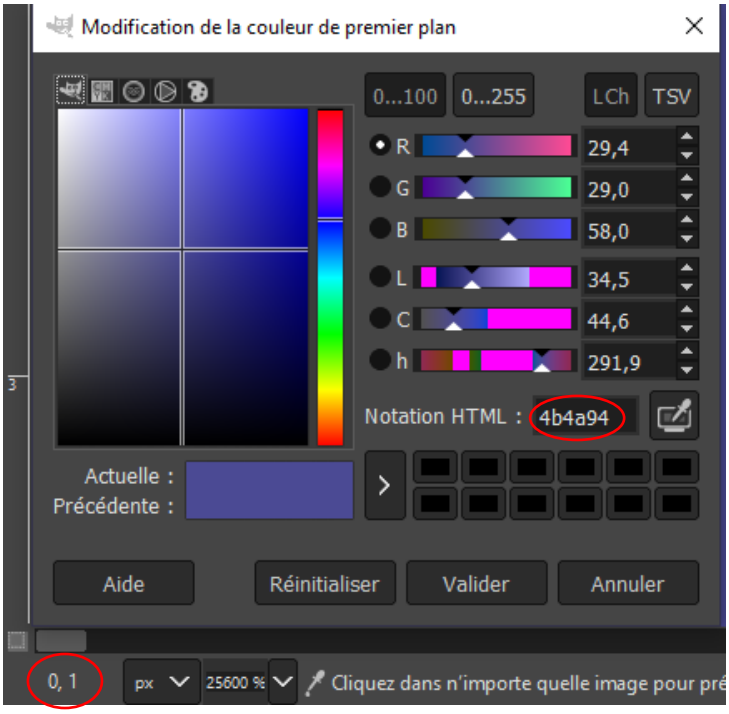
Le code hexadécimal du pixel "252,214" est 581d1a, pour le trouver j'ai utilisé l'outil pipette directement sur le pixel concerné.

Description du procédé stéganographique (4pts)

1. **Vérifiez que les deux points de coordonnées (0,0) et (0,1) (tout en haut à gauche de l'image) sont exactement de la même couleur.**

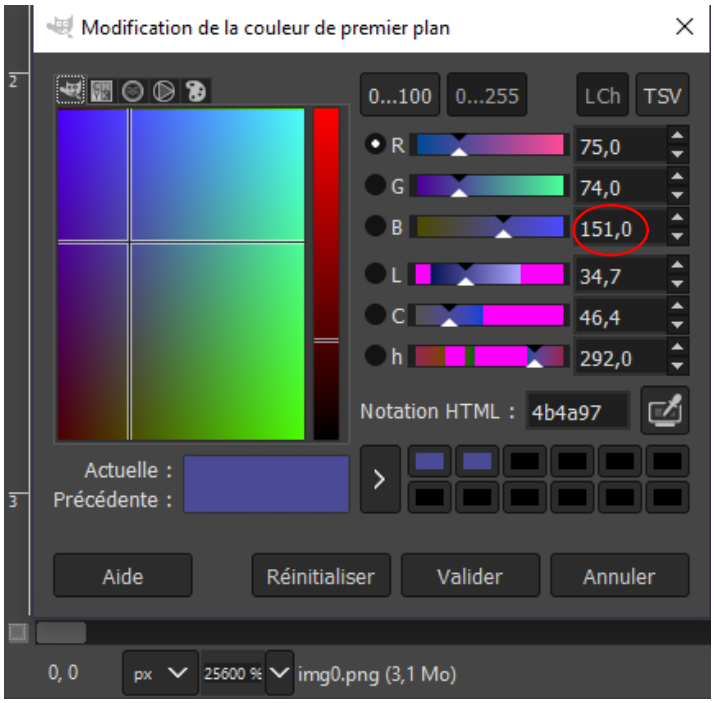
> Les deux points de coordonnées sont de la même couleur, dans les deux cas le code hexadécimal





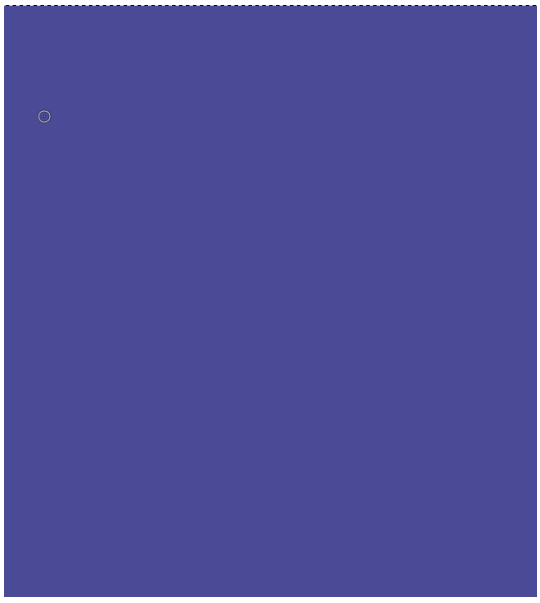
2. Modifiez la couleur du pixel de coordonnées (0,0) en ajoutant 1 à la composante bleue de sa couleur : dans la "Boîte à outils", après avoir sélectionnée la couleur du pixel avec la pipette cliquez sur la couleur de premier plan, vous pouvez alors modifier la composante bleue puis faites la modification à l'aide de l'outil rayon que vous aurez réglé pour qu'il n'affecte qu'un seul pixel. Attention à rester sur une grille de type « RGB (0..255) » !

> J'ai ajouté 1 à la composante bleue.



3. Voyez-vous une différence de couleur avec le pixel voisin ? N'hésitez pas à zoomer au maximum.

> Sur le screen ci-dessous, il a deux pixels différents, on se rend compte qu'on ne voit pas la différence.



Retrouver un message (8pts)

1. **Commencez par noter les valeurs de composantes bleues.**

Pixel	0.0	1.0	2.0	3.0	4.0	5.0	6.0	7.0
Valeur	148	148	148	148	148	149	148	148

2. **Déterminez les valeurs de leur bit de poids faible.**

Pixel	0.0	1.0	2.0	3.0	4.0	5.0	6.0	7.0
Valeur	148	148	148	148	148	149	148	148
Bit	0	0	0	0	0	1	0	0

Les valeurs des bits sont :
Pour 148 : 0
Pour 149 : 1

3. **Trouvez les codes binaires des caractères cachés,**

A l'aide du tableau suivant et des valeurs trouvées plus haut, on trouve "0100" qui vaut 4 en hexadécimal.

Décimal	Hexadécimal	Binaire
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Donc en suivant la consigne, on peut trouver que le message est fait sur 32 bits.
Les valeurs de ces 32 bits sont "01010100 01000010 00100000 00100001"

4. **En vous aidant de la table du codage ASCII sur Wikipedia révélez le message.**

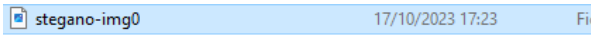
   Grace à toutes les informations récoltées dans les questions précédentes et en traduisant la valeur trouvée dans la question 3, on trouve le message “TB !”.

   J’ai utilisé un traducteur binaire vers texte.

Choix du format de sauvegarde du fichier (4pts)

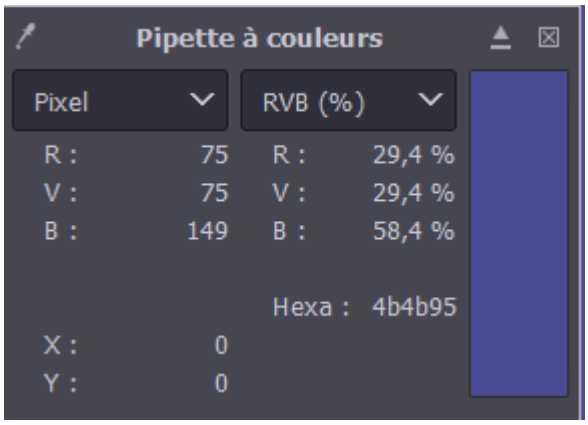
1. **Reprenez l’image de laquelle vous avez extrait le message qui y était dissimulé. En utilisant Gimp, enregistrez-la sur disque au format jpg. Laissez inchangés les paramètres par défaut.**

Sur la version PDF on ne voit pas le format de l’image mais elle est bien en JPG sur le screen ci-dessous.



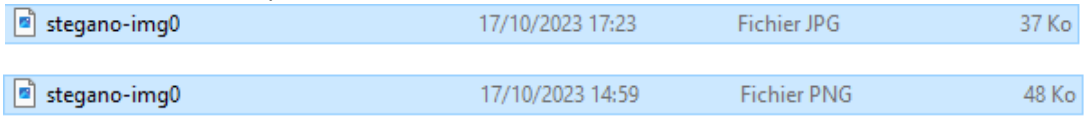
2. **Chargez cette image au format jpg avec Gimp et tentez de retrouver l'information dissimulée. Que constatez-vous ?**

> La valeur de la bleue est à 149 sur tous les pixels, donc impossible de récupérer les informations dissimulées.



3. **Comparez la taille des deux fichiers aux formats jpg et png. Qu'en pensez-vous ?**

La version PNG est un peu plus lourde que la version JPG, sûrement dû aux différentes valeurs de couleur en plus.



4. **Examinez d'autres formats possibles. Lesquels conviennent pour notre procédé stéganographique ?**

(Tableau fait avec Victor)

Type de fichier d'image	Est-ce qu'on peut stéganographié avec
PNG	Oui
JPG	Non
BMP	Oui
TIF	Oui
EPS	Non

Vers l'infini et au-delà ! (2pts)

Quels autres types de fichiers pourraient être concernés par cette technique ?

D'après Kaspersky, il existe 5 principaux types de stéganographie :

- Stéganographie de texte

Modification du format d'un texte existant, le changement de mots dans un texte, l'utilisation de grammaires hors contexte pour générer des textes lisibles ou encore la génération de séquences de caractères aléatoires.

- Stéganographie d'images

Cette technique consiste à cacher des informations dans les fichiers image.

- Stéganographie vidéo

Permet de cacher de grandes quantités de données dans un flux continu d'images et de sons.

- Stéganographie audio

Intégration de messages cachés dans un fichier audio, modifiant ainsi la séquence binaire du fichier audio correspondant.

- Stéganographie réseau

Technique dissimulation d'informations dans les protocoles de contrôle de réseau utilisés pour la transmission de données, tels que TCP, UDP, ICMP, etc.

Des utilisations récentes de ce processus ont-elles eu lieu ?

On peut relever plusieurs utilisations malveillantes de ce processus récemment, en voici quelques-unes.

Sources : *https://www.bleepingcomputer.com/tag/steganography/*

- Le groupe "Worok" cache des logiciels malveillants dans des images PNG pour infecter les machines des victimes avec des logiciels malveillants.

- Une campagne malveillante du groupe de piratage "Witchetty", qui utilise la stéganographie pour cacher un malware de porte dérobée dans un logo Windows.

- Les analystes des menaces ont repéré une nouvelle campagne de malware baptisée « GO#WEBBFUSCATOR » qui s'appuie sur des e-mails de phishing, des documents malveillants et des images spatiales du télescope James Webb pour propager des malwares.

Conclusion :

Ce TP m'a appris les bases de la stéganographie, ce que ce processus permet, les différents formats sous lesquels on peut le retrouver. J'ai également pu découvrir plusieurs attaques utilisant cette technique pour diffuser des logiciels malveillants.