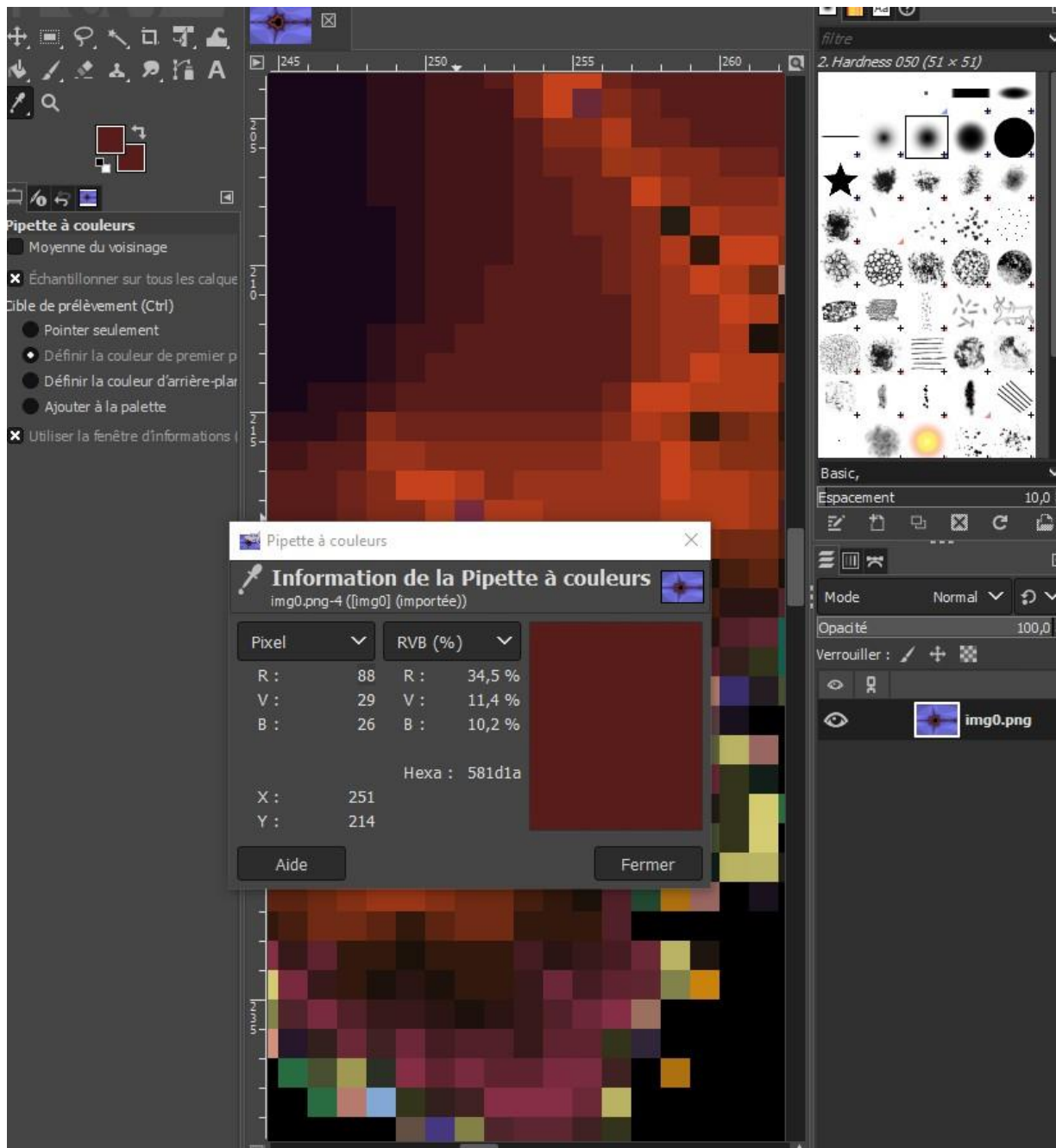


TP 1 : ITURRIA Victor

Couleur d'un pixel

Couleur du pixel :



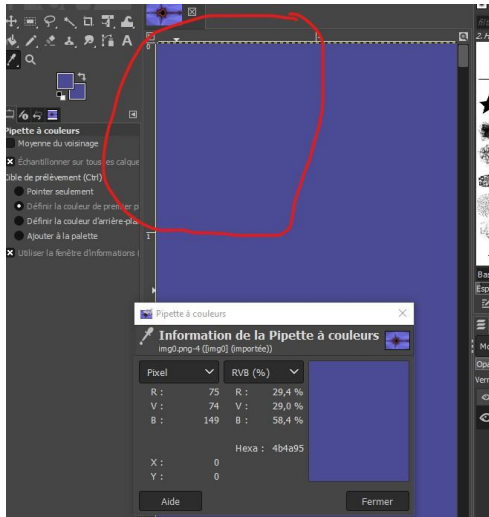
Le code hexa utilisé est #581d1a

Description procédé stéréographique

Code couleur de (0 ; 0) : 4b4a94

Code couleur de (0 ; 1) : 4b4a94

Je ne vois aucune différence entre les deux pixels à l'œil nu après modification de la couleur.



Le pixel modifié est en rouge (son code hexa a été augmenté de 1)

Retrouver un message

Valeur de la couleur bleue des 8 premiers pixels (trouvée en utilisant la pipette MAJ + clic gauche) :

Pixels	1	2	3	4	5	6	7	8
Valeur du bleu	148	148	148	148	149	148	148	148
Nombre de bit en +	0	0	0	0	0	1	0	0

Soit un bit de valeur 0000 0100 ce qui correspond à 4 selon le tableau binaire

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

La première ligne nous à donnée 4, donc le message est sur 4 octets (victor m'a aidé)

Le message sera donc sur les (4 x 8) pixels de la deuxième ligne

Pixel du 1ere octets	1	2	3	4	5	6	7	8
Valeur du bleu	148	149	148	149	148	149	148	148
Nombre de bit en +	0	1	0	1	0	1	0	0

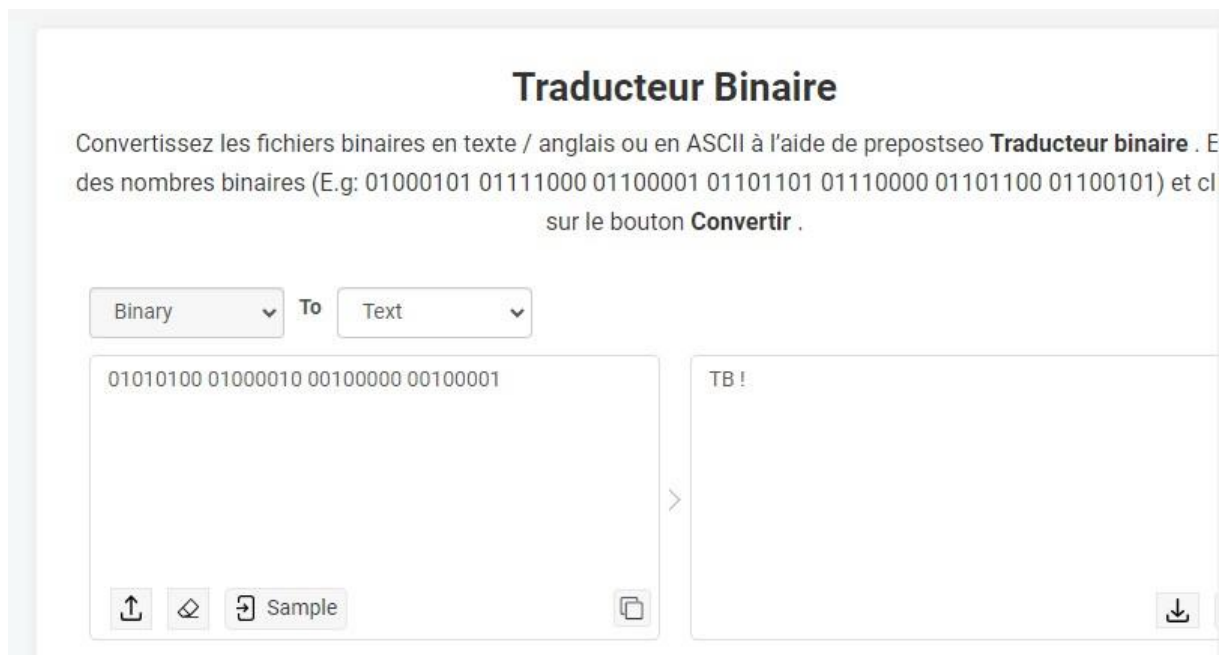
Pixel du 2eme octets	1	2	3	4	5	6	7	8
Valeur du bleu	148	149	148	148	148	148	149	148
Nombre de bit en +	0	1	0	0	0	0	1	0

Pixel du 3eme octets	1	2	3	4	5	6	7	8
Valeur du bleu	148	148	149	148	148	148	148	148
Nombre de bit en +	0	0	1	0	0	0	0	0

Pixel du 4eme octets	1	2	3	4	5	6	7	8
Valeur du bleu	148	148	149	148	148	148	148	149
Nombre de bit en +	0	0	1	0	0	0	0	1

Donc le code est 01010100 01000010 00100000 00100001

Selon un traducteur de binaire le message est « TB ! »



Choix de sauvegarde du fichier

Tous les pixels de la première et deuxième ligne du fichier au format jpg ont une valeur bleue de 149

Le fichier JPG est plus lourd (54Ko contre 48ko pour le PNG)

Tableau fait avec roméo

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

Vers l'infini et l'au-delà

La stéganographie pourrait également concerner les fichier vidéo, les fichiers texte ainsi que les fichiers audios. (Source : Kaspersky)

C'est une technique de défense contre la censure particulièrement efficace, elle peut être également très pratique pour créer des filigrammes ainsi que pour sécuriser une information de tiers indésiré. (Source : Kaspersky)

Cependant, elle souvent utilisé pour déployer des malwares, le cas le plus récent est celui du groupe « worok » qui à infecter des images PNG avec des malwares voleurs d'information, opération ayant touchée des personnes haut-placé tel que des agents du gouvernement américain. (bleepingcomputer.com)

Dans cette activité j'ai donc appris à détecter de la stéganographie sur une image et à en extraire le message ainsi qu'en créer un moi-même, j'ai également renseigné les différents types de fichiers compatibles avec cette méthode.