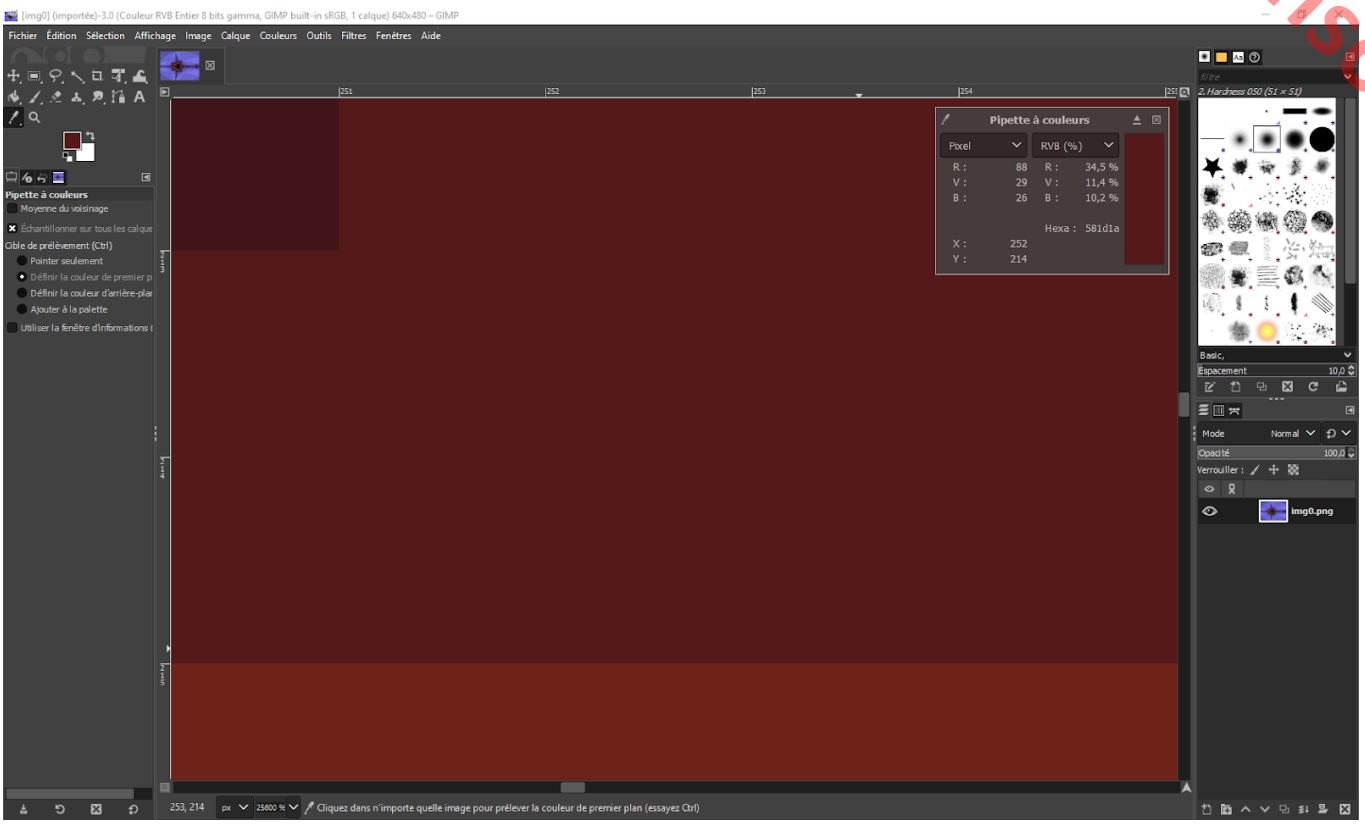
2024.11.19 - Bloc 3 - TP1 Stéganographie

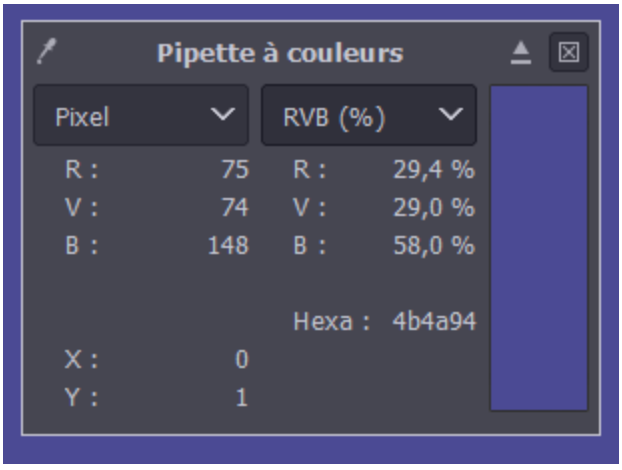
Couleur d'un pixel

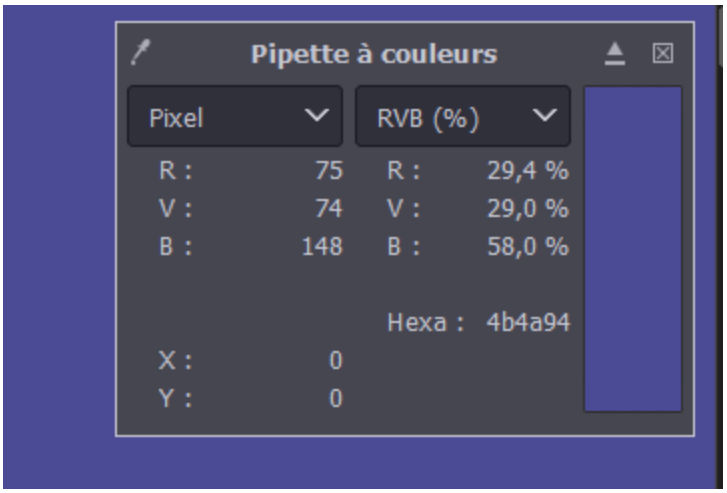
Le code hexadécimal (en html) de la couleur du pixel de coordonnées (252,214) est `#581d1a`.



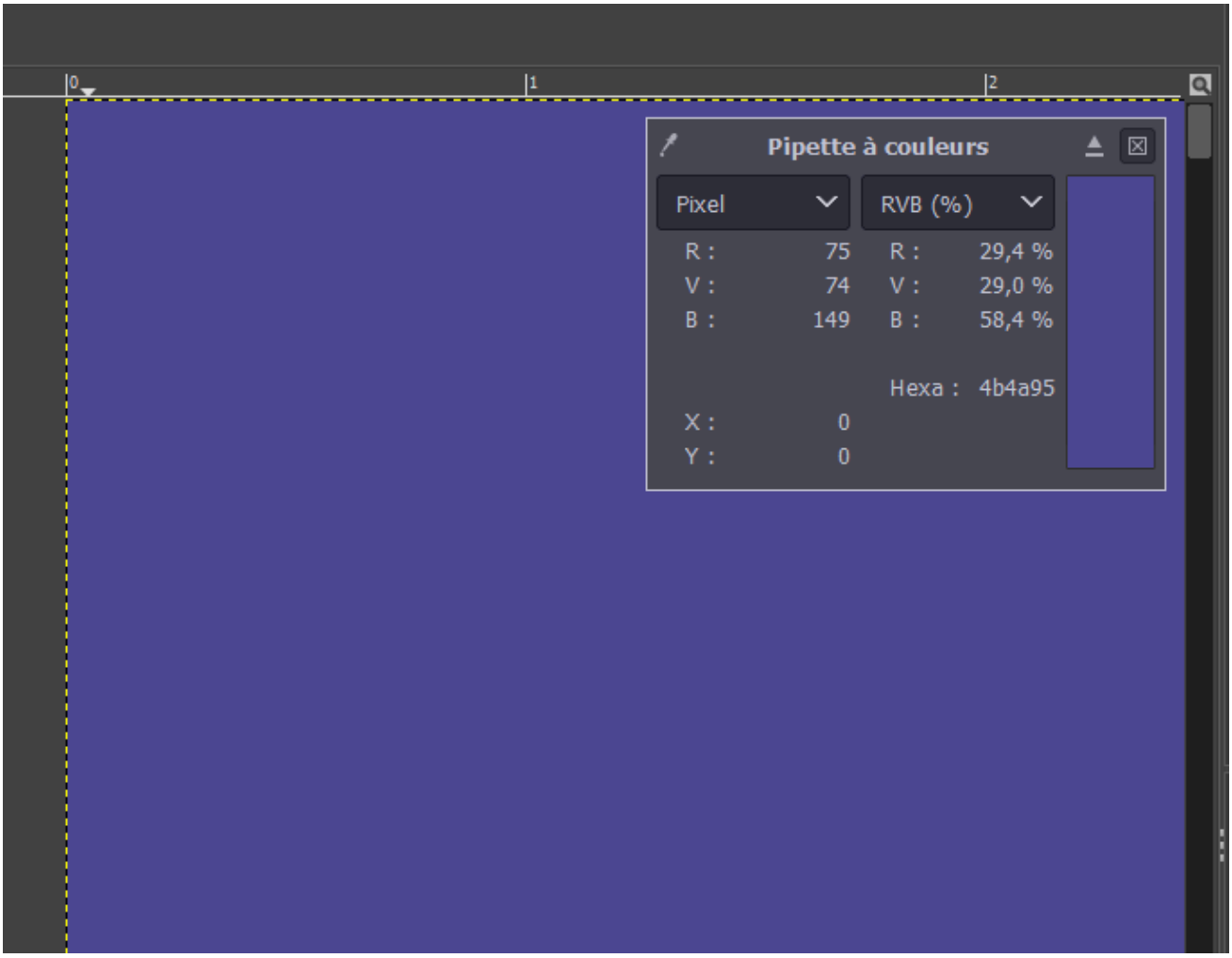
Description du procédé stéganographique

1. Oui, les deux points de coordonnées (0,0) et (0,1) sont exactement de la même couleur.





2. Dans la boîte à outils =>Pinceau à pixel en taille 1 => cliquer sur les coordonnées (0,0) => modifier la couleur bleue sur la grille RGB en ajoutant 1 à 148 et valider.



3. A l'œil nu, nous n'observons pas de différence avec le pixel voisin.

Retrouver un message

Pour trouver le nombre de caractères du message dissimulé dans l'image, on regarde la valeur de 8 derniers pixels (poids faibles) de :

1. La première ligne.

Ligne	Valeur	Binaire
0,0	148	10010100
1,0	148	10010100
2,0	148	10010100
3,0	148	10010100
4,0	148	10010100
5,0	149	10010101
6,0	148	10010100
7,0	148	10010100

1. En sélectionnant les bits de poids faible, nous obtenons donc le nombre binaire 00000100

27	26	25	24	23	22	21	20
128	64	32	16	8	4	2	1
0	0	0	0	0	1	0	0
0	0	0	0	0	4	0	0

1. Ce codage codant chaque caractère sur 8 bits, le nombre de pixels dissimulant un bit du message est donc égal à 8xl. Donc, 8x4 = 32 bits. Le message caché se trouve donc dans les 32 premiers bits de la deuxième ligne.

Ligne	Valeur	Binaire
0,1	148	10010100
1,1	149	10010101
2,1	148	10010100
3,1	149	10010101
4,1	148	10010100
5,1	149	10010101
6,1	148	10010100
7,1	148	10010100
8,1	148	10010100
9,1	149	10010101

10,1	148	10010100
11,1	148	10010100
12,1	148	10010100
13,1	148	10010100
14,1	149	10010101
15,1	148	10010100
16,1	148	10010100
17,1	148	10010100
18,1	149	10010101
19,1	148	10010100
20,1	148	10010100
21,1	148	10010100
22,1	148	10010100
23,1	148	10010100
24,1	148	10010100
25,1	148	10010100
26,1	149	10010101
27,1	148	10010100
28,1	148	10010100
29,1	148	10010100
30,1	148	10010100
31,1	149	10010101

1. Voici le message caché ; En reprenant les bits de poids faibles de chacune de ces valeurs et en les séparant par 4 octets (de 8 bits chacun) nous retrouvons : 01010100 01000010 00100000 00100001. Et en utilisant la table ACSII nous obtenons ce message :
   TB (SP = espace) !

Dissimuler un message

Pour retrouver le nombre de bits de mon message, se rendre ligne 0.

Il faut regarder les 8 premiers pixels de la ligne 0 et nous retrouverons ce binaire :
00000010

27	26	25	24	23	22	21	20
128	64	32	16	8	4	2	1
0	0	0	0	0	0	1	0

Donc le message se cache dans 16 bits. (à retrouver Sur la ligne 4)

Message caché (sur la ligne 4).

Mon message : ok 01101111 01101011

Le nombre de pixels dissimulant un bit du message est égal 16 pixels

Ligne	Valeur	Binaire
0.3	148	10010100
1.3	149	10010101
2.3	149	10010101
3.3	148	10010100
4.3	149	10010101
5.3	149	10010101
6.3	149	10010101
7.3	149	10010101
8.3	148	10010100
9.3	149	10010101
10.3	149	10010101
11.3	148	10010100
12.3	149	10010101
13.3	148	10010100
14.3	149	10010101
15.3	149	10010101

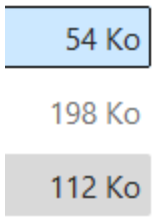
En prenant les bits de poids faibles de chacune des valeurs obtenues.
Nous trouvons donc les 2 octets (16 bits)
Voici le binaire 01101111 01101011 (et en utilisant la table de codage ASCII on obtient le message : ok)

(les lettres en gras sont uniquement pour l'esthétique)

- J’ai envoyé mon message caché à Amandine AUGUSTIN.

Choix du format de sauvegarde du fichier

1. Je constate que toutes les valeurs sont en 149 et non en 148, le message n’est donc plus dissimulé.
2. Je constate que la taille du deuxième fichier est deux fois plus lourde.
   La compression d’un fichier PNG se fait sans perte contrairement au JPG, il contient plus d’informations que le JPG. Il n’y a pas forcément de meilleur format mais il faut évidemment s’assurer de garder une certaine qualité. (Trouver un article pour le citer).



1. Les autres formats possibles pour la stéganographie

Les formats compatibles : BMP, GIF, TIG, PDF, ICO, EPS (Il y a un décalage au niveau des lignes)
Les formats non compatibles : HEIF

- J’ai reçu le message caché d’Amandine AUGUSTIN

Pour trouver le message qu’Amandine a dissimulé, j'ai effectué les mêmes étapes que dans l’exercice précédent. J’ai regardé les 8 premiers pixels de la quatrième ligne. En sélectionnant les bits de poids faible j'obtiens le nombre binaire : 00000011.

8*3 = 24 bits ; le message qu’Amandine à caché se trouve dans les 24 premiers bits de la troisième ligne.

J'obtiens 3 octets : 01100010 01101001 01110000 et j'obtiens grâce à la table ACSII le message : bip.

(les lettres en gras sont uniquement pour l'esthétique)

Vers l’infini et l’au-delà !

La stéganographie peut être concerné de différentes façons, dans les images (comme nous avons pu le faire lors de cet exercice) mais aussi comme dans d’autres types de fichiers :

- Fichiers Audio : Des chevaux de Troie cachés dans des fichiers audio WAV
- Fichier Vidéo : Dissimulation dans des fichiers vidéo MP4, des cybercriminels ont utilisé des fichiers vidéo pour cacher des commandes d'un malware. Chaque image de la vidéo contenait des fragments de code qui, une fois assemblés, exécutent des actions malveillantes sur le système infecté.
- Word ou Excel : Des documents Word et Excel avec des macros activées ont été utilisés pour installer des logiciels malveillants.
- Fichiers PDF : Un fichier Zip peut être caché dans un fichier PDF, il est téléchargé lorsque le PDF s'ouvre.
- Fichiers réseau et protocoles : Dans ces attaques, des données cachées sont insérées dans des paquets de réseau TCP/IP.

Malgré le fait que la stéganographie peut être utilisé pour la cybercriminalité, l'espionnage et la communication secrète, elle peut tout de même s'avérer utile dans des pays où la liberté d'expression est limitée, elle permet de contourner les mécanismes de censure en dissimulant des messages dans des fichiers courants (comme ceux mentionné plus haut).

Voici quelques-unes des dernières cyberattaques notables utilisant la stéganographie :

- Cyberattaque ; Malware caché dans des images : Un ransomware récent appelé SyncCrypt utilise des images apparemment innocentes pour dissimuler des fichiers malveillants. Elles sont téléchargées à partir d'e-mails spam qui contiennent en réalité des archives ZIP.
- Attaque contre l'opérateur télécom Kyivstar en Ukraine : En décembre 2023, l'opérateur mobile ukrainien Kyivstar a été victime d'une cyberattaque attribuée au groupe russe Sandworm, qui a visé ses 24 millions d'abonnés.
- Ransomwares ciblant les sauvegardes : En Finlande, une campagne d'attaques utilisant le ransomware Akira a été identifiée fin 2023, avec des attaques qui visaient directement les dispositifs de sauvegarde NAS et les bandes magnétiques.

Par ailleurs, dans l'entreprise où j'effectue mon apprentissage (Ministère des Armées et des Anciens Combattants) Il nous est fortement interdit, sous peine d'amendes et d'emprisonnement de télécharger quoi que ce soit qui provient d'Internet, d'installer un logiciel étranger à l'Intradef ou de simplement brancher une clé USB ou un Téléphone. Chaque logiciel souhaité est obligatoirement demandé à la DIRISI (via un ticket), une fois validé et vérifié, ils nous font l'installation à distance.

Si nous souhaitons apporter un fichier, ou de simples photos personnelles sur clé USB, la clé devra obligatoirement passer par ce qu'on appelle une machine blanche.

(Sources : Google ; simplilearn.com ; nomios.fr ; ledecodeur.ch ; l'Intradef « uniquement consultable dans mon entreprise »)
Utilisation partielle de ChatGPT pour corriger certaines fautes d'orthographe.**