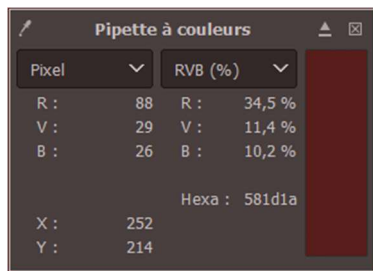


# TP1 : Cybersécurité de systèmes d'informations

## Stéganographie

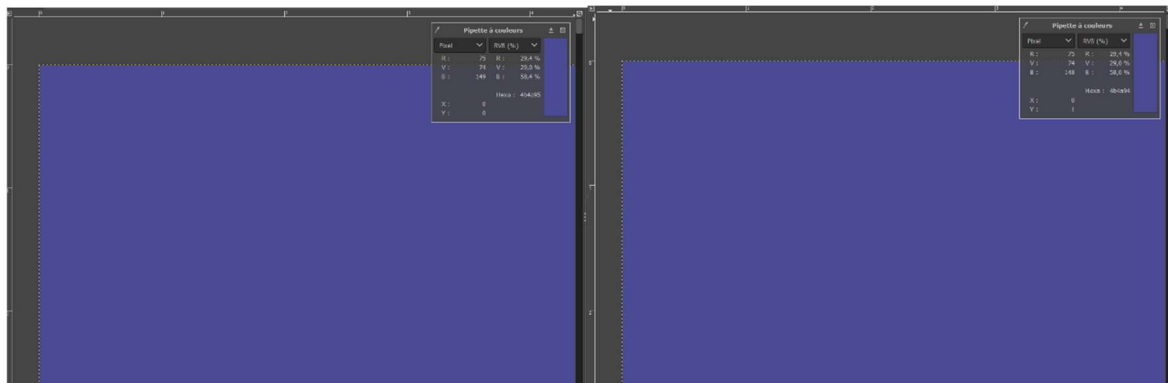
### Question 1 : Couleur d'un pixel

Le code hexadécimal en html du pixel est ; 581d1a. J'ai pu trouver cette réponse en utilisant la pipette à couleur.



### Question 2 : Description du procédé sténographiques

On voit bien ici qu'après modification du pixel en rajoutant +1 en bleu (149 et 148). On voit bien qu'il n'y a aucune différence à l'œil nu mais on voit bien que dans le code HTML (4b4a95 et (4b4a94) et dans le bleu qu'il y a une différence.



### Question 3 : Retrouver un message

- Les valeurs de la composante bleu dans la première ligne sur les 8 premiers pixels (8 pixels = 1 octet) sont : 148 ;148 ;148 ;148 ;148 ;149 ;148 ;148 (148 équivalents à 0 et 149 à 1 grâce au leur bit de poids faible, ici en rouge) ce qui équivaut en binaire à 00000100 ce qui équivaut en décimal à 4. Mon message caché sur la deuxième ligne sera donc sur 4 octets. (4 octets équivalent à 4\*8bits et 1 bit équivaut à 1 pixel).
- Ensuite sur la deuxième ligne j'ai pu trouver que pour :
  - o Le premier octet, la valeur en binaire est 01010100 qui est égal à 84 en décimal.
  - o Le second octet, la valeur en binaire est de 01000010 ce qui en décimal vaut 66.
  - o Le troisième octet, la valeur en binaire est de 00100001 qui est égal à 33 en décimal.

- Le quatrième octet, le binaire est égal à 00100000 ce qui vaut 32 en décimal.
- Enfin en comparant avec le tableau ASCII avec les valeurs en décimal trouvé ci-dessus (84, 66, 33, 32). Nous trouvons le message caché : <TB !>

#### Question 4 : Choix du format de sauvegarde du fichier

On constate qu'on ne peut pas retrouver notre message caché dans le format JPG car il n'y a plus de différence dans le bleu. En comparant la taille des deux fichiers jpg = 54Ko / png = 47Ko, on constate qu'il n'y a pas une grande différence.

Après une rapide recherche sur internet, le format BMP et TIF apparaît souvent ([Wikipédia](#)). Après un test, on s'aperçoit que le procédé stéganographique fonctionne toujours. Cependant les fichiers compressés ne marcheront pas tel que le JPG, JPEG ainsi que le PDF car en compressant ils perdront des informations.

#### Question 5 : Vers l'infini et au-delà !

Enfin, on peut également utiliser ce procédé dans les fichiers audio, vidéo et notamment des fichiers textes. Cette méthode permet de dissimuler des informations « basiques », mais aussi du code malveillant, des URL pour permettre à un malware de recevoir des instructions ou encore des fichiers de configurations. On peut prendre pour exemple une « récente » attaque en janvier 2019, avec ce procédé, les utilisateurs des ordinateurs Mac ont été victimes d'une campagne de publicité malveillante. La pub contenait des images qui à l'intérieur cachaient du code JavaScript, il redirigeait l'utilisateur vers des fausses mises à jour pour Adobe qui en réalité étaient des malwares.

A la suite de ce TP, on réalise donc que ce procédé existe depuis très longtemps avant même l'apparition des ordinateurs et de l'informatique. C'est un moyen très efficace pour faire des attaques envers des utilisateurs lambda car c'est une méthode très difficile à remarquer, comme nous avons pu le voir avec les pixels de couleur bleus précédemment, à l'œil nu on ne voit aucune différence.