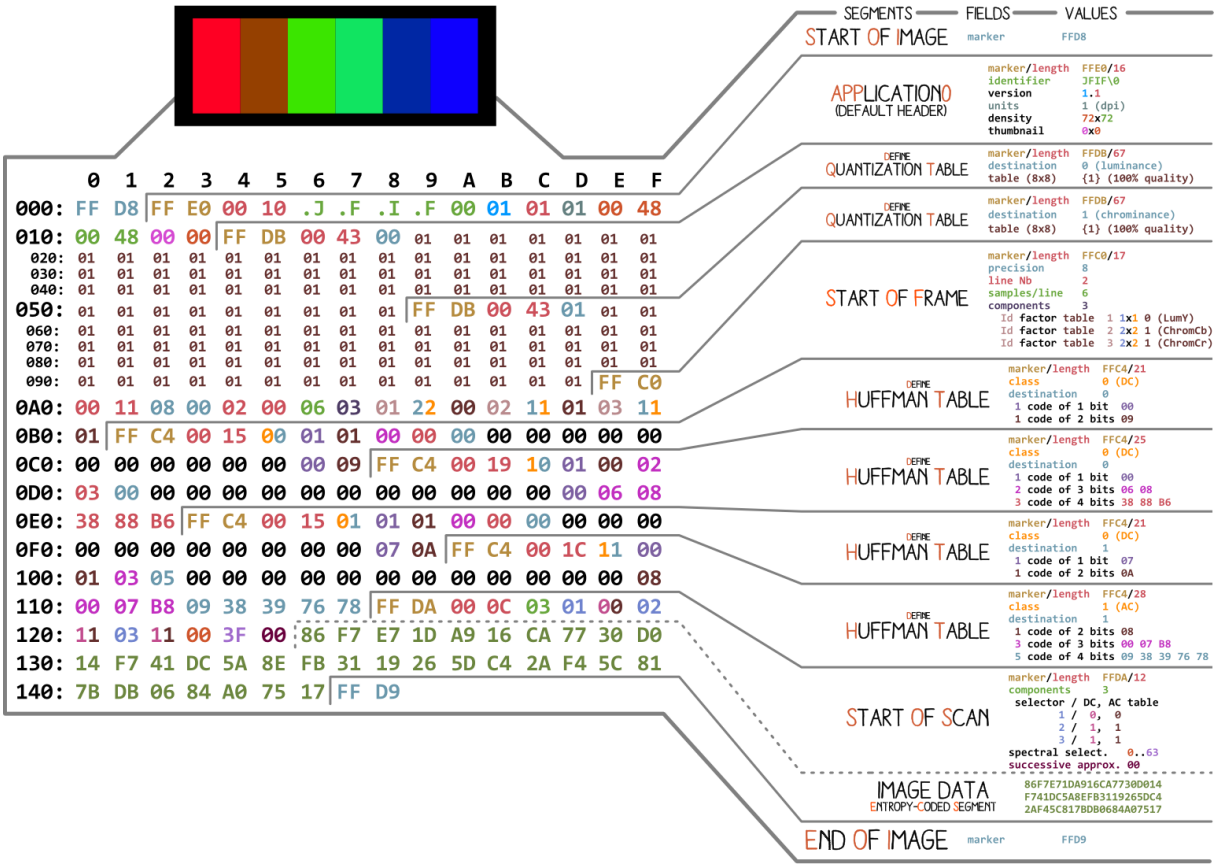
[Utiliser un éditeur capable de changer la Valeur hexadécimale des octets d'un fichier (HxD editor).]



L'observation des propriétés du fichier montre une grande taille pour la simple image de petit format.

En fait, il y a beaucoup plus de pixels qu'en apparence dans cette image et on le détecte à la taille.

Il s'agit d'analyser le contenu en modifiant la taille pour faire apparaître des données non affichées.

JPEG SIZE : FFC0 : sauter 3 octets (non pertinents) : il y a la largeur et la hauteur sur 2 octets chacun.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texte Décodé
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	60	ÿØÿà..JFIF.....`
00000010	00	60	00	00	FF	DB	00	43	00	03	02	02	03	02	02	03	.`..ÿÛ.C........
00000020	03	03	03	04	03	03	04	05	08	05	05	04	04	05	0A	07	....
00000030	07	06	08	0C	0A	0C	0C	0B	0A	0B	0B	0D	0E	12	10	0D	....
00000040	0E	11	0E	0B	0B	10	16	10	11	13	14	15	15	15	0C	0F	....
00000050	17	18	16	14	18	12	14	15	14	FF	DB	00	43	01	03	04	.........ÿÛ.C...
00000060	04	05	04	05	09	05	05	09	14	0D	0B	0D	14	14	14	14	....
00000070	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	....
00000080	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	....
00000090	14	14	14	14	14	14	14	14	14	14	14	14	14	FF	C0	.....	.............ÿÀ
000000A0	00	11	08	00	DD	01	6A	03	01	22	00	02	11	01	03	11	....Ý.j.."......
000000B0	01	FF	C4	00	1F	00	00	01	05	01	01	01	01	01	01	00	.ÿÄ.............
000000C0	00	00	00	00	00	00	00	01	02	03	04	05	06	07	08	09	....
000000D0	0A	0B	FF	C4	00	B5	10	00	02	01	03	03	02	04	03	05	..ÿÄ.µ..........

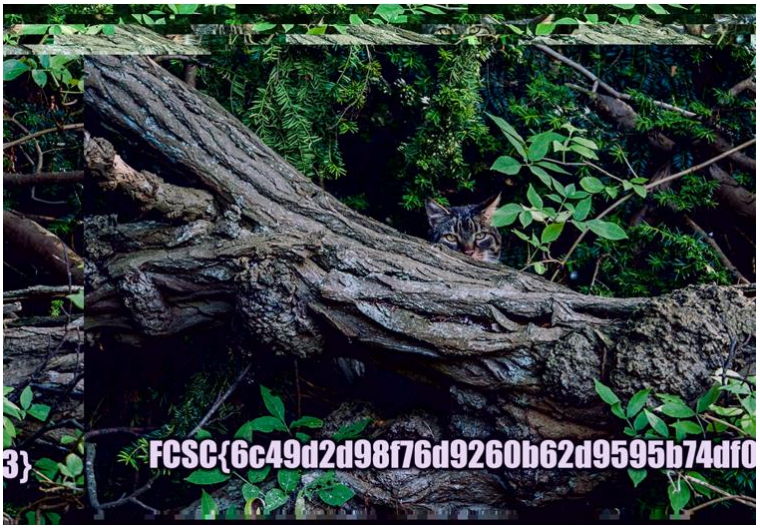
Pour trouver le segment suivant après le SOF, vous devez continuer à lire jusqu'à ce que vous trouviez un octet 0xFF qui n'est pas immédiatement suivi de 0x00 (voir "bourrage d'octets"). Normalement, ce sera le segment EOI qui se trouve à la fin du fichier.

Si FF est suivi de 00, il s'agit d'un marqueur de donnée et non pas de trames. Repérer les marqueurs.

Les secteurs identifiés en segments commencent par FF mais NON suivis de 00. (bourrage d'octets).

Et quel que soit le fichier JPEG, celui-ci se termine systématiquement par le marqueur de type FFD9.

Le réglage de taille 04 2A 04 AB modifiée à adapter dans l'image JPEG parviennent à montrer le flag.



Le flag à trouver est interprétable en direct : FCSC{6c49d2d98f76d9260b62d9595b74df03}