4.6 Images

Je ne vous apprends rien en vous disant que tout le monde est équipé d'un APN (Appareil Photo Numérique). À une époque où le téléphone devient plus une option de son smartphone, tous nos petits appareils en sont pourvus.

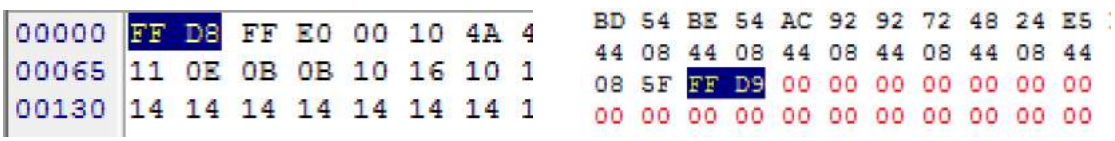
Il n'est donc pas anormal de devoir en faire des analyses, car elles peuvent nous apprendre beaucoup de choses. Des photos de vacances qui indiquent le lieu de séjour, des images à caractère pédopornographique qui une fois analysée pourront révéler s'il s'agit d'un montage, d'un téléchargement, des informations sur l'utilisateur et/ou le matériel utilisé. Et encore bien d'autres renseignements potentiellement utiles.

4.6.1 Recherche par extension et/ou signature numérique

Commençons par les réunir, une simple recherche par extension « *.jpg » ou « *.jpeg) avec les outils précédemment cités (§4.4) permet de faire sortir un grand nombre d'image sur un disque dur. Il s'agit là de l'extension la plus répandue, mais il existe une multitude de formats (PNG ; GIF ; BMP ; …).

Un peu plus complexe, on peut faire une recherche par signature de fichier. Chaque type de fichier est défini par un format. On sait qu'un fichier image peut être un « JPG ». Mais que se passe-t-il si je change l'extension « *.jpg » par un « *.tst ». Le système ne connaissant pas se format met une icône neutre et en double cliquant dessus demande avec quelle application il doit l'ouvrir. Bref, on se retrouve avec une image illisible par le système.

Hors un fichier quel qu'il soit, conserve sa structure. Avec un éditeur hexadécimal, on affiche la structure du fichier. On se rend compte que nos deux fichiers différents par leur format ne le sont pas de par leur structure. En effet, tous deux commencent par FF D8 et se terminent par FF D9.



En hexadécimal, ces deux fichiers sont identiques. La modification de l'extension ne modifie pas la structure du fichier. Dès lors que l'on connaît la structure d'une image, il devient aisé de faire une recherche en spécifiant une analyse Hexa avec comme début FF D8 et comme Fin FF D9.

4.6.2 Analyse photo et des métadonnées

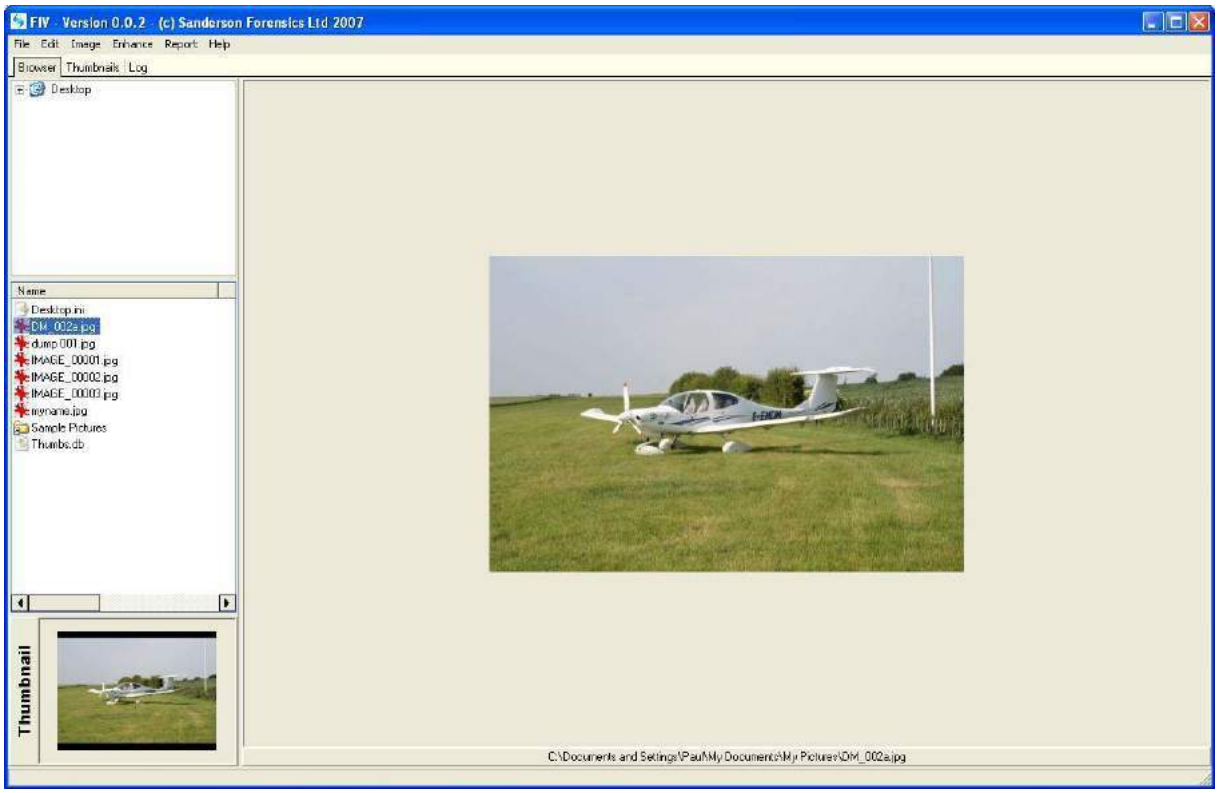
À l'époque de la photographie argentique, les plus méticuleux des photographes tenaient un carnet de bord dans lequel ils inscrivaient tout un tas d'informations et notamment les principaux paramètres de prise de vues (date, vitesse, diaphragme, mémorisation d'exposition, etc..) dans une optique de progression.

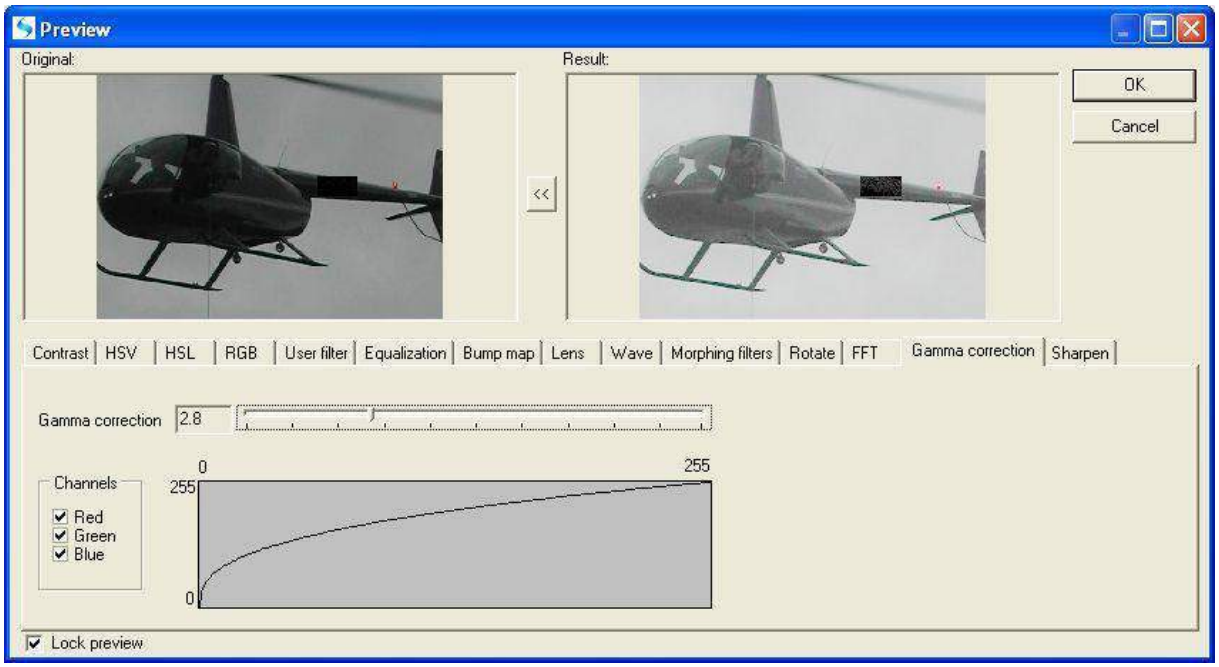
Ces carnets ont bien évidemment disparu le jour où les APN sont arrivés, car une bonne partie de ces informations est enregistrée automatiquement lors de la prise de la photo. Toujours avides d'information, maintenant nos clichés vont même à enregistrer leur position géographique. Une mine d'or d'information que l'on nomme « donnée EXIF ».

Sur un ordinateur, lorsque vous faites un clic droit + propriétés, les informations communiquées par le système sont les données EXIF de l'image, mais condensées. Il existe de nombreux outils sur la toile qui permettent d'extraire ces informations et d'en faire l'analyse :

- Exifer
- Exif Jpeg Header Manipulation Tools (jhead)
-
- Forensics Image Viewer
- ExifProbe

Exemple avec l'outil FIV (Forensics Image Viewer disponible sur la distribution DEFT)





Pour une meilleure compréhension, rien ne vaut un cas pratique. Ci-après, nous avons été mandatés afin d'expertiser une photographie dans le but de vérifier sa datation.

Cas Pratique : Monsieur XY

Nous avons été mandatés par XX, et Maître YY, Avocat, son conseil avec mission de :

- Recevoir copie du fichier numérique dénommé :
  « ***2014 05 14 Photographie de Monsieur XY en date du 1er janvier 2009.jpg*** »,
- Analyser l'ensemble des datations disponibles de ce fichier numérique,
- Réaliser toutes les investigations susceptibles de permettre de confirmer ou d'infirmer la date alléguée de la prise de vues de cette photographie.

Le fichier « ***2014 05 14 Photographie de Monsieur XY en date du 1er janvier 2009.jpg*** ».

a. Préalable

En préalable, nous rappelons quelques éléments techniques qui, insérés aux données digitales d'une photographie numérique, permettent de la qualifier.

Propriété EXIF : **EXIF** est l'abréviation d'**Exchangeable Image File Format**.

Les données EXIF constituent un remplacement commode du petit carnet qui accompagnait, à l'époque de la photographie chimique, les photographes méticuleux pour leur permettre de conserver toutes une série d'information comme la date, le lieu, les conditions de prise de vue, les réglages choisis, etc.

Sur un appareil numérique, ces informations sont enregistrées et conservées automatiquement avec chaque photo, et incluses au fichier lui-même.

L'**Exchangeable Image File Format** est une spécification normalisée utilisée par les appareils photographiques numériques. Les balises de métadonnées définies dans le format EXIF standard couvrent un très large éventail de données, notamment : Date ; Heure ; Réglage de l'appareil ; Géo localisation ; Description et Droits d'Auteur…

Elément THUMBNAIL : littéralement « ongle de pouce » en référence à sa taille.

Un THUMBNAIL est une version d'une image dont la taille est réduite par rapport à l'original. Son utilité principale est similaire à celle d'un index ou d'une table des matières pour du texte : permettre la construction de galeries d'images. Les thumbnails sont aujourd'hui souvent intégrés par l'appareil de prise de vues au fichier de l'image originale lors de son enregistrement.

En cas de retouche ou recadrage ultérieur de la photo originale, le thumbnail n'est pas systématiquement mis à jour.

b. Description et structure du fichier

Le fichier : « 2014 05 14 Photographie de Monsieur XY en date du 1er janvier 2009.jpg » présente l'apparence et les caractéristiques suivantes :

Ses caractéristiques affichées par l'explorateur Windows, comme le ferait toutes applications de traitement de l'image sont les suivantes :

On remarquera notamment :

. Le type de l'appareil photo : SONY DSC-V1

. La date de prise de vue : 01/01/2009 12:10

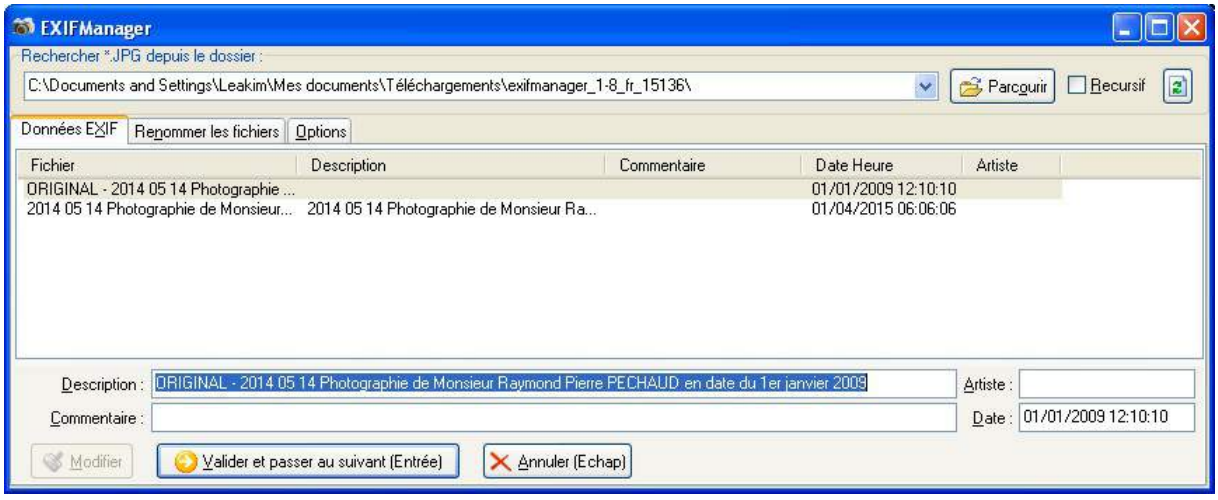
. Les réglages de l'appareil photo

Largeur	1660 pixels
Hauteur	1197 pixels
Résolution horizontale	72 ppp
Résolution verticale	72 ppp
Profondeur de couleur	24
Nombre de trames	1
Fabricant de l'équipement	SONY
Modèle d'appareil photo	DSC-V1
Représentation des cou...	sRGB
Mode flash	
Longueur de la focale	12 mm
Point-F	F/3,2
Temps d'exposition	1/60 secondes
Vitesse ISO	ISO-100
Mode de contrôle	Motif
Source de la lumière	Inconnu
Programme d'exposition	normal
Compensation de l'expo...	0 étape
Date du cliché	01/01/2009 12:10

c. Modification de l'intégrité du fichier

Nous venons de rappeler qu'un fichier de photo numérique contient dans ses métadonnées les propriétés EXIF. Comme pour tout fichier informatique, il est évidemment possible de modifier ces métadonnées.

Dans notre exemple nous avons analysé le fichier de la photographie en cause. À l'aide d'un outil téléchargeable gratuitement sur Internet nommé « EXIFManager.exe » il est aisé de modifier les informations contenues dans les propriétés EXIF :



Une fois le bouton « Modifier » activé, il est possible de modifier à titre d'exemple la « Date du cliché ». Ici la photo est datée du « **01/01/2009 à 12h10** ».
Nous avons remplacé cette date par « **01/04/2015 à 06h06** ».

Largeur	1660 pixels
Hauteur	1197 pixels
Résolution horizontale	72 ppp
Résolution verticale	72 ppp
Profondeur de couleur	24
Nombre de trames	1
Fabricant de l'équipement	SONY
Modèle d'appareil photo	DSC-V1
Représentation des cou...	sRGB
Mode flash	
Longueur de la focale	12 mm
Point-F	F/3,2
Temps d'exposition	1/60 secondes
Vitesse ISO	ISO-100
Mode de contrôle	Motif
Source de la lumière	Inconnu
Programme d'exposition	normal
Compensation de l'expo...	0 étape
Date du cliché	01/04/2015 06:06

Nous précisons qu'il est possible de modifier l'ensemble des données EXIF à l'aide d'un ou plusieurs outils et ce, inclus le type et la marque de l'appareil photo utilisé.

Après enregistrement de cette donnée, nous avons vérifié les propriétés ainsi modifiées de la photo et nous constatons que la « date du cliché » affichée est bien **01/04/2015 06:06.**

Dans cet exemple, nous n'avons modifié que la date du cliché.

d. Exportation du THUMBNAIL de la photo inclus au fichier

À l'aide d'un autre utilitaire « EXIFER », nous avons réalisé l'exportation des données de la THUMBNAIL (vignette créée lors de la prise de vues à l'origine de la photo) sous forme d'un fichier numérique autonome. Ce dernier, directement issu des métadonnées de l'image elle-même, ne comporte aucune propriété propre à l'exception de celles créées par le système d'exploitation Windows lors de la création du fichier par l'exportation ainsi réalisée.

Le THUMBNAIL extrait est la suivante :

Nous constatons que sur cette dernière apparaissent des éléments ne figurant pas sur la photographie original « 2014 05 14 Photographie de Monsieur XY en date du 1er janvier 2009.jpg ».

Cette vignette fait notamment apparaitre :

Sur le bord gauche, un rideau maintenu par une sangle de couleur rouge.
Sur la partie inférieure, un premier plan (table avec un magazine et une coupelle ou cendrier).

Ces éléments démontrent qu'un recadrage de la photographie originale a été réalisé :

e. Analyse des logs EXIF et Méthode E.L.A

JPEGsnoop est un logiciel, libre en téléchargement, qui permet d'analyser en détail le contenu EXIF d'une photographie et de déterminer si elle a été retouchée.

JPGsnoop répertorie 4 classes :

- class 1 : photo retouchée *(image is processed/edited)*
- class 2 : photo avec une grande probabilité d'avoir été retouchée *(image has high probability of being processed/edited)*
- class 3 : photo avec une grande probabilité d'être originale *(image has high probability of being original)*
- class 4 : incertitude entre photo originale ou retouchée *(uncertain if processed or original)*

Ce logiciel a cependant des limites.

. Il ne permet pas de faire la différence entre une amélioration de photo : couleur, contraste et un photomontage,
. Il considère une image au format Raw convertie en Jpeg comme une image retouchée,
. En dépit de sa base de données importantes, il affecte certaines photos en class 4, c'est-à-dire « incertitude ».

L'extrait du log édité par le logiciel JPGsnoop (ci-après), fait apparaitre l'utilisation de l'application « Adobe Photoshop » ainsi que l'indice « Class1 » confirmant la modification de la photo originale.

…
*** Searching Compression Signatures ***

Signature: 01B7D42A6678B6F1F20EB05FFC2A8EB9
Signature (Rotated): 01B7D42A6678B6F1F20EB05FFC2A8EB9
File Offset: 0 bytes
Chroma subsampling: 2x2
EXIF Make/Model: OK [SONY] [DSC-V1]
EXIF Makernotes: OK
EXIF Software: NONE

Searching Compression Signatures: (3347 built-in, 0 user(*))

EXIF.Make / Software	EXIF.Model	Quality	Subsamp Match?
SW :[Adobe Photoshop]		[Save As 05]	

NOTE: Photoshop IRB detected
Based on the analysis of compression characteristics and EXIF metadata:

ASSESSMENT: Class 1 - Image is processed/edited
…

Enfin, nous avons effectué le test « ELA » (Error Level Analysis).

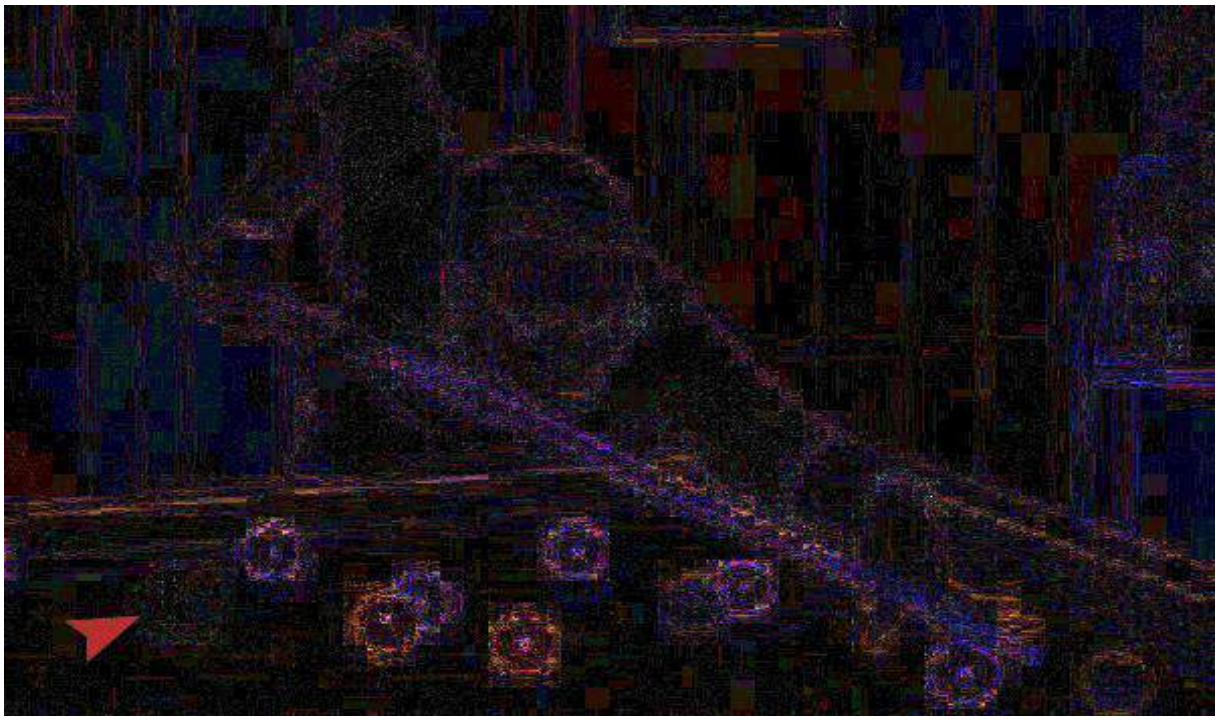
Ce procédé consiste à analyser les différentes couches de compression de l'image et d'en faire une représentation pixélisée. De ce fait, toutes modifications sur l'image sont représentées par une non-homogénéité des pixels.

À titre d'exemple, nous avons procédé à la suppression d'une bille rouge à gauche du tapis dans la photo ci-dessous :

Photo originale

Photo modifiée (bille rouge à gauche)

Traitement E.L.A sur l'image modifiée :



On constate très clairement en bas à gauche de l'image (flèche rouge), une zone arrondie différente de la partie sombre du fond (tapis).

Nous avons réalisé cette même analyse sur la photographie de Monsieur XY en cause :

On ne constate aucune anomalie de pixel sur l'ensemble de l'image.

Cette analyse semble confirmer que cette photographie de Monsieur XY n'a fait l'objet que du recadrage déjà identifié et d'aucun photomontage autre.

III - CONCLUSIONS

Nous avons démontré, dans un premier temps, qu'il est très fac facilement possible de modifier les informations EXIF contenues dans tout fichier de photographie numérique et en particulier sa date de prise de vues.

Une seconde analyse nous a permis d'exporter les données du THUMBNAIL inclus au fichier original dénommé « *2014 05 14 Photographie de Monsieur XY en date du 1er janvier 2009.jpg* ».

La comparaison de ce THUMBNAIL avec l'original nous permet d'affirmer que celle-ci a fait l'objet à minima d'un recadrage ultérieurement à la prise de vues.

Le log du logiciel JPGsnoop fait apparaitre l'utilisation du logiciel de retouche « Adobe Photoshop ».

Enfin, le test E.L.A semble démontrer que la photographie n'a pas subi d'autre modification que le recadrage identifié.