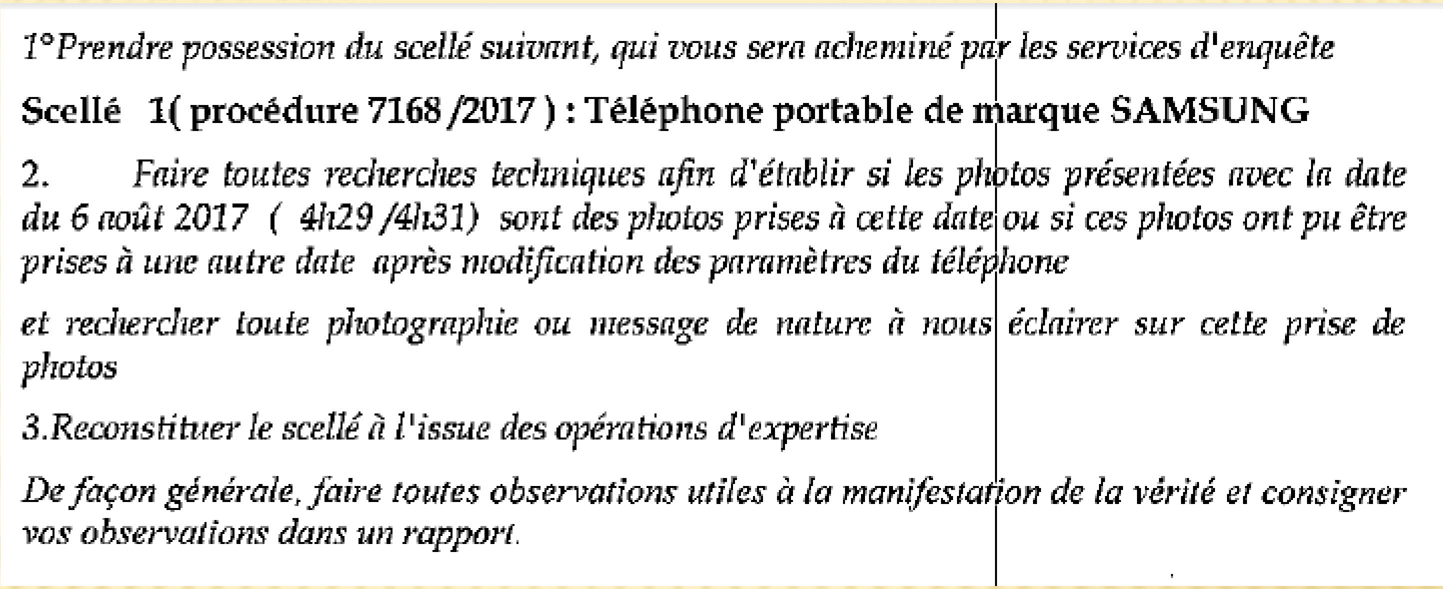
JEAN-ARNAUD CAUSSE
EXPERT DE JUSTICE

J-T
25 SEPTEMBRE 2018

FALSIFICATION DE L'HORODATAGE DE PHOTOS SUR SMARTPHONE

LA MISSION



1°Prendre possession du scellé suivant, qui vous sera acheminé par les services d'enquête

Scellé 1(procédure 7168 /2017) : Téléphone portable de marque SAMSUNG

2. *Faire toutes recherches techniques afin d'établir si les photos présentées avec la date du 6 août 2017 (4h29 /4h31) sont des photos prises à cette date ou si ces photos ont pu être prises à une autre date après modification des paramètres du téléphone*

et rechercher toute photographie ou message de nature à nous éclairer sur cette prise de photos

3.Reconstituer le scellé à l'issue des opérations d'expertise

De façon générale, faire toutes observations utiles à la manifestation de la vérité et consigner vos observations dans un rapport.

En quelques mots

- **SAMSUNG SM-G925F - Android 6.0.1 sans carte SD**
- **Un auteur présumé aux cheveux BRUN reconnu sur une vidéo surveillance**
- **Il produit des photos datées au moment des faits avec une chevelure DECOLOREE**
- **Enquêteur constate horodatage des photos sauvegardées sur GOOGLE DRIVE**
- **Technicien n’a pas pu déterminer la validité de l’horodatage des photos sur le Tél**

LES FICHIERS

Analyse des fichiers photo

- **Les fichiers photo sont nommés d'après l'horloge interne**

  (et non avec un compteur comme sur les iPhone)

  20170806_043048.jpg

- **L'horodatage EXIF de la prise de vue est cohérent avec le nom du fichier**

  06/08/2017

- **Le modèle d'appareil photo EXIF est cohérent du boitier téléphonique**

- **Les métadonnées EXIF ne contiennent pas de données GPS**

Pas de possibilité de trouver d'erreur de chronologie par le nom, la date ou les métadonnées

LES DOSSIERS

Analyse des dossiers et DB photo

- **L'album photo ne contient plus aucune photo sauf les 4 images**

  /data/media/0/DCIM/

- **Deux DB qui n'apportent aucune date intéressante**

  (26/04/2016) /data/com.android.providers.media/databases/external.db

  (18/09/2017) /data/com.android.providers.media/databases/external.db

- **Ces photos ont été sauvegardées sur Google Drive puis rechargées sur le téléphone lorsque produit devant les enquêteurs**

  → Le dossier de stockage /data/media/0/DCIM/Restored/

  → Les fichiers sont datées du 18/09/2017

- **Le dossier standard des clichés pris avec le tél est (pas de carte SD ici)**

  /data/media/0/DCIM/Camera

Pas de possibilité de conclure sur la réalité de la prise de vue avec ce téléphone précisément

LES VIGNETTES

Analyse des vignettes Photo

- **Deux DB contenant les vignettes des photos dans le dossier (analyse XWAYS)**
  - **(15/09/2017 – 15/09/2017)** **/data/media/0/DCIM/.thumbnails/.thumbdata3-1763508120**
  - **(14/09/2017 – 19/09/2017)** **/data/media/0/DCIM/.thumbnails/.thumbdata3--1967290299**

→ **nombreuses vignettes datées mais les photos correspondantes supprimées**

→ **seule la deuxième DB contient les vignettes des 4 photos**

→ **les vignettes des 4 photos en plusieurs exemplaires sont datées**

18/09/2017 **jour où le téléphone est montré aux enquêteurs**
19/09/2017 **jour de l'analyse par le NTECH**

✗ Pas de possibilité de conclure d'après les vignettes

LES ENVOIS/RECEPTIONS DE PHOTO

Recherche de copie des photos dans les APP

- **MMS - pièces attachées**
  - **/data/com.android.providers.telephony/app_parts/**
- **SNAPCHAT**
  - **/data/com.snapchat.android/cache/**
- **INSTAGRAM**
  - **/data/com.instagram.android/cache/image/**
- **FACEBOOK**
  - **/data/com.facebook.katana/cache/image/**
- **GOOGLE +**
  - **/data/com.google.android.apps.plus/files/**
  - **/data/com.google.android.apps.plus/cache/**
- **HANGOUTS**
  - **/data/com.google.android.talk/files/**
  - **/data/com.google.android.talk/cache/**

Aucune trace d’envoi / réception ou copie de ces photos

LES LOGS

Analyse des Logs

- **Nécessite au moins une extraction système de fichiers**

  19/09/2017 : extraction logique par enquêteur

  14/10/2017 : extraction physique par moi même

→ les logs ne remontent que 7 jours après les faits

→ une extraction physique le 19/09 aurait permis de préserver les logs couvrant la période des faits (et de la falsification …)

DOSSIER .FACE

Reconnaissance de visage

- **Constat de plusieurs centaines de vignettes de visages**
  - **→ ressemblent aux photos des comptes FACEBOOK**
  - **→ mais aussi visages extraits des photos recherchées !**

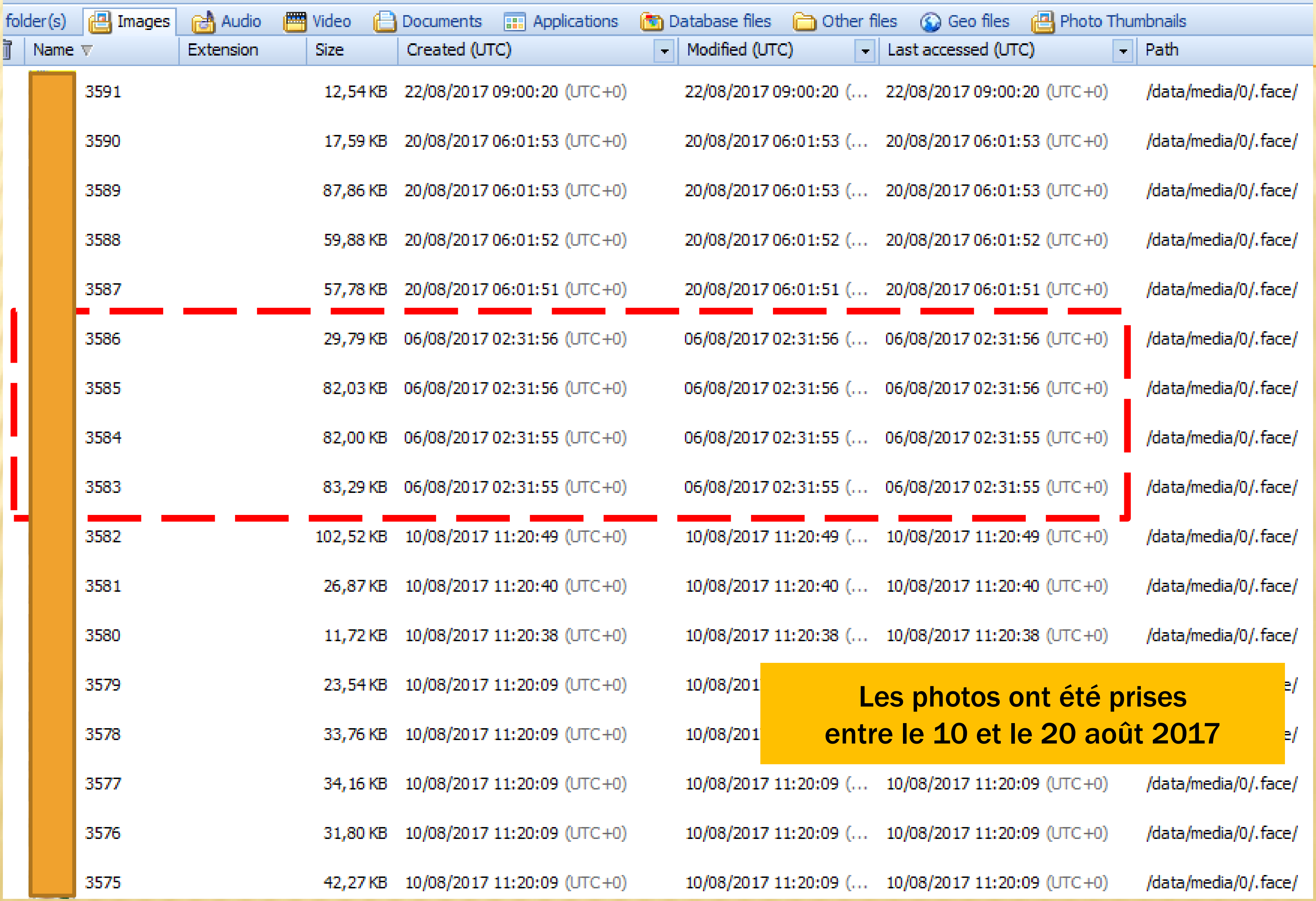
- **Une fonction en standard de recherche de visages**
  - **→ Extrait chaque visage dans un fichier nommé automatiquement sans extension**

/data/media/0/.face/3585

/data/media/0/.face/3586

…

Le tri des fichiers selon leur nom a permis de trouver une seule anti-chronologie
Celle des visages extraits des photos du soir des faits



Name	Extension	Size	Created (UTC)	Modified (UTC)	Last accessed (UTC)	Path
[redacted] 3591		12,54 KB	22/08/2017 09:00:20 (UTC+0)	22/08/2017 09:00:20 (...	22/08/2017 09:00:20 (UTC+0)	/data/media/0/.face/
[redacted] 3590		17,59 KB	20/08/2017 06:01:53 (UTC+0)	20/08/2017 06:01:53 (...	20/08/2017 06:01:53 (UTC+0)	/data/media/0/.face/
[redacted] 3589		87,86 KB	20/08/2017 06:01:53 (UTC+0)	20/08/2017 06:01:53 (...	20/08/2017 06:01:53 (UTC+0)	/data/media/0/.face/
[redacted] 3588		59,88 KB	20/08/2017 06:01:52 (UTC+0)	20/08/2017 06:01:52 (...	20/08/2017 06:01:52 (UTC+0)	/data/media/0/.face/
[redacted] 3587		57,78 KB	20/08/2017 06:01:51 (UTC+0)	20/08/2017 06:01:51 (...	20/08/2017 06:01:51 (UTC+0)	/data/media/0/.face/
[redacted] 3586		29,79 KB	06/08/2017 02:31:56 (UTC+0)	06/08/2017 02:31:56 (...	06/08/2017 02:31:56 (UTC+0)	/data/media/0/.face/
[redacted] 3585		82,03 KB	06/08/2017 02:31:56 (UTC+0)	06/08/2017 02:31:56 (...	06/08/2017 02:31:56 (UTC+0)	/data/media/0/.face/
[redacted] 3584		82,00 KB	06/08/2017 02:31:55 (UTC+0)	06/08/2017 02:31:55 (...	06/08/2017 02:31:55 (UTC+0)	/data/media/0/.face/
[redacted] 3583		83,29 KB	06/08/2017 02:31:55 (UTC+0)	06/08/2017 02:31:55 (...	06/08/2017 02:31:55 (UTC+0)	/data/media/0/.face/
[redacted] 3582		102,52 KB	10/08/2017 11:20:49 (UTC+0)	10/08/2017 11:20:49 (...	10/08/2017 11:20:49 (UTC+0)	/data/media/0/.face/
[redacted] 3581		26,87 KB	10/08/2017 11:20:40 (UTC+0)	10/08/2017 11:20:40 (...	10/08/2017 11:20:40 (UTC+0)	/data/media/0/.face/
[redacted] 3580		11,72 KB	10/08/2017 11:20:38 (UTC+0)	10/08/2017 11:20:38 (...	10/08/2017 11:20:38 (UTC+0)	/data/media/0/.face/
[redacted] 3579		23,54 KB	10/08/2017 11:20:09 (UTC+0)	10/08/201	[illegible]	e/
[redacted] 3578		33,76 KB	10/08/2017 11:20:09 (UTC+0)	10/08/201	[illegible]	e/
[redacted] 3577		34,16 KB	10/08/2017 11:20:09 (UTC+0)	10/08/2017 11:20:09 (...	10/08/2017 11:20:09 (UTC+0)	/data/media/0/.face/
[redacted] 3576		31,80 KB	10/08/2017 11:20:09 (UTC+0)	10/08/2017 11:20:09 (...	10/08/2017 11:20:09 (UTC+0)	/data/media/0/.face/
[redacted] 3575		42,27 KB	10/08/2017 11:20:09 (UTC+0)	10/08/2017 11:20:09 (...	10/08/2017 11:20:09 (UTC+0)	/data/media/0/.face/

**Les photos ont été prises
entre le 10 et le 20 août 2017**

DB GOOGLE PHOTO

Photos sauvegardées sur GOOGLE DRIVE

- **DB SQLite contenant l’activité Google Photo**

  /data/com.google.android.apps.photos/databases/gphotos0.db

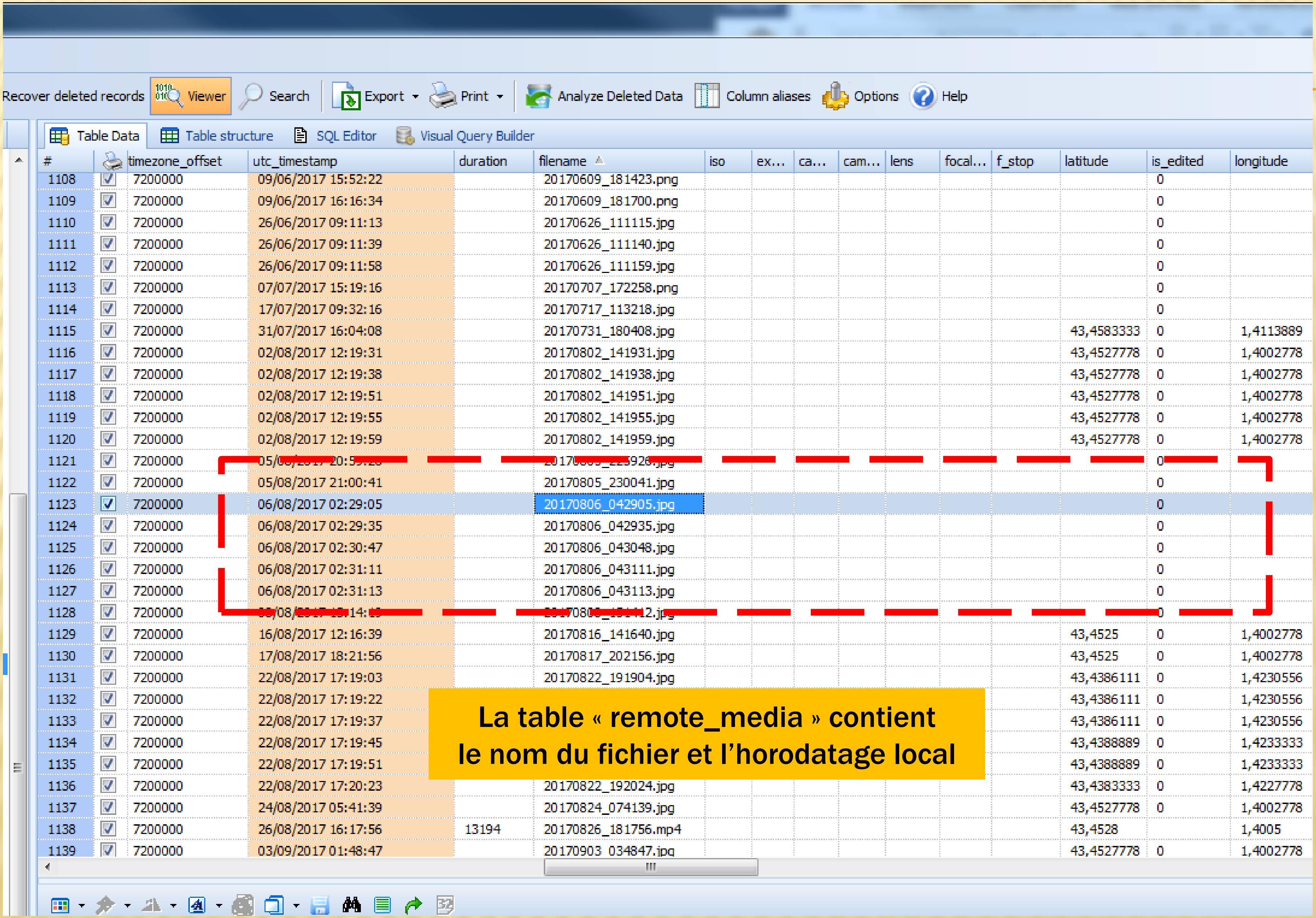
- **Table « remote_media »**

  → **Horodatage du 1ier téléchargement de chaque photo vers GOOGLE**

  → **Horodatage donnée par GOOGLE**

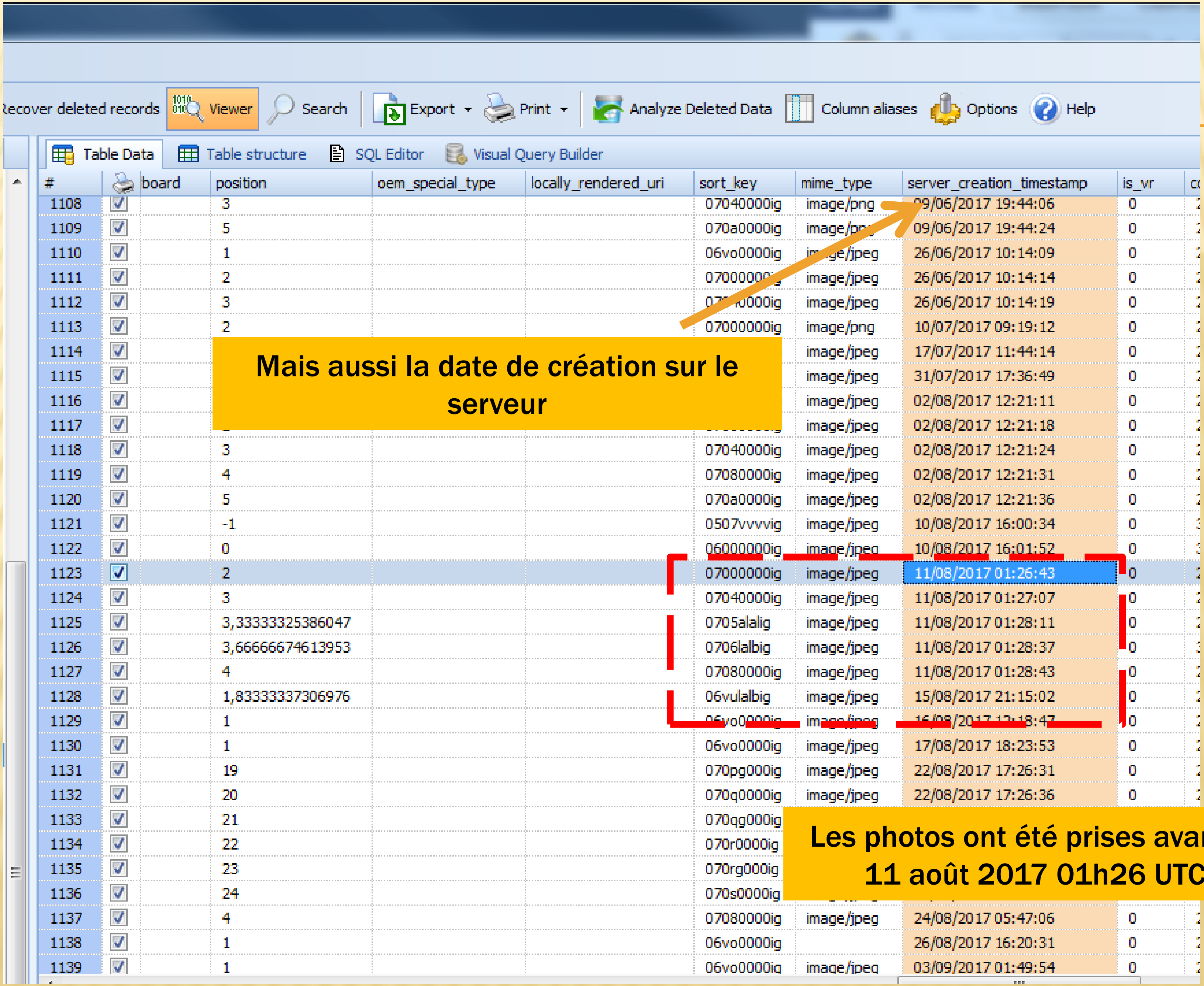
  Les 4 fichiers ont été envoyés le 11/08/2017

La base de données GOOGLE PHOTO contient une référence horaire externe
non modifiable par l’utilisateur



#		timezone_offset	utc_timestamp	duration	filename	iso	ex...	ca...	cam...	lens	focal...	f_stop	latitude	is_edited	longitude
1108	☑	7200000	09/06/2017 15:52:22		20170609_181423.png									0	
1109	☑	7200000	09/06/2017 16:16:34		20170609_181700.png									0	
1110	☑	7200000	26/06/2017 09:11:13		20170626_111115.jpg									0	
1111	☑	7200000	26/06/2017 09:11:39		20170626_111140.jpg									0	
1112	☑	7200000	26/06/2017 09:11:58		20170626_111159.jpg									0	
1113	☑	7200000	07/07/2017 15:19:16		20170707_172258.png									0	
1114	☑	7200000	17/07/2017 09:32:16		20170717_113218.jpg									0	
1115	☑	7200000	31/07/2017 16:04:08		20170731_180408.jpg								43,4583333	0	1,4113889
1116	☑	7200000	02/08/2017 12:19:31		20170802_141931.jpg								43,4527778	0	1,4002778
1117	☑	7200000	02/08/2017 12:19:38		20170802_141938.jpg								43,4527778	0	1,4002778
1118	☑	7200000	02/08/2017 12:19:51		20170802_141951.jpg								43,4527778	0	1,4002778
1119	☑	7200000	02/08/2017 12:19:55		20170802_141955.jpg								43,4527778	0	1,4002778
1120	☑	7200000	02/08/2017 12:19:59		20170802_141959.jpg								43,4527778	0	1,4002778
1121	☑	7200000	05/0[illegible] 20:5[illegible]		2017[illegible]_2[illegible]926.jpg									0	
1122	☑	7200000	05/08/2017 21:00:41		20170805_230041.jpg									0	
1123	☑	7200000	06/08/2017 02:29:05		20170806_042905.jpg									0	
1124	☑	7200000	06/08/2017 02:29:35		20170806_042935.jpg									0	
1125	☑	7200000	06/08/2017 02:30:47		20170806_043048.jpg									0	
1126	☑	7200000	06/08/2017 02:31:11		20170806_043111.jpg									0	
1127	☑	7200000	06/08/2017 02:31:13		20170806_043113.jpg									0	
1128	☑	7200000	[illegible]/08/[illegible]:14:[illegible]		20170[illegible]_[illegible]412.jpg									0	
1129	☑	7200000	16/08/2017 12:16:39		20170816_141640.jpg								43,4525	0	1,4002778
1130	☑	7200000	17/08/2017 18:21:56		20170817_202156.jpg								43,4525	0	1,4002778
1131	☑	7200000	22/08/2017 17:19:03		20170822_191904.jpg								43,4386111	0	1,4230556
1132	☑	7200000	22/08/2017 17:19:22		[illegible]								43,4386111	0	1,4230556
1133	☑	7200000	22/08/2017 17:19:37		[illegible]								43,4386111	0	1,4230556
1134	☑	7200000	22/08/2017 17:19:45		[illegible]								43,4388889	0	1,4233333
1135	☑	7200000	22/08/2017 17:19:51		[illegible]								43,4388889	0	1,4233333
1136	☑	7200000	22/08/2017 17:20:23		20170822_192024.jpg								43,4383333	0	1,4227778
1137	☑	7200000	24/08/2017 05:41:39		20170824_074139.jpg								43,4527778	0	1,4002778
1138	☑	7200000	26/08/2017 16:17:56	13194	20170826_181756.mp4								43,4528		1,4005
1139	☑	7200000	03/09/2017 01:48:47		20170903_034847.jpg								43,4527778	0	1,4002778

La table « remote_media » contient le nom du fichier et l’horodatage local



#		board	position	oem_special_type	locally_rendered_uri	sort_key	mime_type	server_creation_timestamp	is_vr
1108	☑		3			07040000ig	image/png	09/06/2017 19:44:06	0
1109	☑		5			070a0000ig	image/png	09/06/2017 19:44:24	0
1110	☑		1			06vo0000ig	image/jpeg	26/06/2017 10:14:09	0
1111	☑		2			0700000[illegible]	image/jpeg	26/06/2017 10:14:14	0
1112	☑		3			07[illegible]0000ig	image/jpeg	26/06/2017 10:14:19	0
1113	☑		2			07000000ig	image/png	10/07/2017 09:19:12	0
1114	☑		[illegible]	[illegible]	[illegible]	[illegible]	image/jpeg	17/07/2017 11:44:14	0
1115	☑		[illegible]	[illegible]	[illegible]	[illegible]	image/jpeg	31/07/2017 17:36:49	0
1116	☑		[illegible]	[illegible]	[illegible]	[illegible]	image/jpeg	02/08/2017 12:21:11	0
1117	☑		[illegible]	[illegible]	[illegible]	[illegible]	image/jpeg	02/08/2017 12:21:18	0
1118	☑		3			07040000ig	image/jpeg	02/08/2017 12:21:24	0
1119	☑		4			07080000ig	image/jpeg	02/08/2017 12:21:31	0
1120	☑		5			070a0000ig	image/jpeg	02/08/2017 12:21:36	0
1121	☑		-1			0507vvvvig	image/jpeg	10/08/2017 16:00:34	0
1122	☑		0			06000000ig	image/jpeg	10/08/2017 16:01:52	0
1123	☑		2			07000000ig	image/jpeg	11/08/2017 01:26:43	0
1124	☑		3			07040000ig	image/jpeg	11/08/2017 01:27:07	0
1125	☑		3,33333325386047			0705alalig	image/jpeg	11/08/2017 01:28:11	0
1126	☑		3,66666674613953			0706lalbig	image/jpeg	11/08/2017 01:28:37	0
1127	☑		4			07080000ig	image/jpeg	11/08/2017 01:28:43	0
1128	☑		1,83333337306976			06vulalbig	image/jpeg	15/08/2017 21:15:02	0
1129	☑		1			06vo0000ig	image/jpeg	16/08/2017 12:18:47	0
1130	☑		1			06vo0000ig	image/jpeg	17/08/2017 18:23:53	0
1131	☑		19			070pg000ig	image/jpeg	22/08/2017 17:26:31	0
1132	☑		20			070q0000ig	image/jpeg	22/08/2017 17:26:36	0
1133	☑		21			070qg000ig	[illegible]	[illegible]	[illegible]
1134	☑		22			070r0000ig	[illegible]	[illegible]	[illegible]
1135	☑		23			070rg000ig	[illegible]	[illegible]	[illegible]
1136	☑		24			070s0000ig	[illegible]	[illegible]	[illegible]
1137	☑		4			07080000ig	image/jpeg	24/08/2017 05:47:06	0
1138	☑		1			06vo0000ig		26/08/2017 16:20:31	0
1139	☑		1			06vo0000ig	image/jpeg	03/09/2017 01:49:54	0

Mais aussi la date de création sur le serveur

Les photos ont été prises avant le 11 août 2017 01h26 UTC

Les quatre clichés ont été pris entre le 10 et le 11 août 2017 et non le 06 août 2017

Il m’a fallu

• un bon outil d’extraction	UFED
• un bon outil d’analyse d’arborescence et de DB	Oxygen Forensics

CNEJITA
EXPERTS

JEAN-ARNAUD CAUSSE
EXPERT DE JUSTICE

J-T
25 SEPTEMBRE 2018

FALSIFICATION DE L'HORODATAGE DE PHOTOS SUR SMARTPHONE

FIN