

iPhone / Photos effacées

Retour d'expérience

Sommaire

- Le contexte, la mission
- Première approche avec l'UFED Touch
- Logiciel « appareil photo » : principe de fonctionnement
- Comment faire ?
- Exemple concret

Le contexte

- La nuit du nouvel an (vers 05:00), la victime est endormie sur son lit.
- Le mis en cause aurait déshabillé la victime pendant son sommeil avant de la prendre plusieurs photos avec son iPhone.
- La victime se réveille
- L'agresseur part quelques instants aux toilettes avec son iPhone
- Lorsqu'il en sort le petit ami de la victime consulte l'iPhone et ne trouve rien
- Le téléphone est saisi par les enquêteurs vers 14:00

La mission

- Restaurer les photos effacées et déterminer les heures de prises de vues.

Première approche : UFED Touch

- C'est un iPhone 4 avec mot de passe
- Découverte du mot de passe avec Physical Analyzer
- Suivi d'un dump mémoire toujours avec PA
- Analyse du dump avec PA et Adroït
- Aucune photo présente ou effacée aux horaires indiqués par la victime.

Logiciel « Appareil Photo »

- Règles de nommage des photos et vidéos :
 - IMG_YYYY.JPG
 - IMG_XXXX.MOV
 - IMG_ZZZZ.PNG
- Les photos, vidéo et copies d'écran sont conservées dans un même dossier

Exemple 1

- La dernière photo réalisée se nomme :
 - IMG_0100.JPG
- Lorsque l'opérateur prendra 2 prochaines photos puis une vidéo suivie d'une autre photo alors les nouveaux fichiers créés seront nommés :
 - IMG_0101.JPG, IMG_0102.JPG, IMG_0103.MOV, IMG_0104.JPG
- Si l'utilisateur supprime le fichier 103 et/ou 104 puis prend une nouvelle photo, cette-ci se nommera :
 - IMG_0105.JPG

Les numéros des photos effacées ne sont jamais réutilisés

Numérotation

- Le dernier numéro utilisé est conservé dans un fichier système (DCIM_APPLE.plist) **non accessible à l'utilisateur**
- A chaque nouvelle photo, ce numéro est augmenté de 1 puis affecté à la nouvelle photo puis enregistré dans le fichier DCIM_APPLE.plist
- Quand une photo (vidéo, copie d'écran) est supprimée, ce numéro reste inchangé dans le fichier DCIM_APPLE.plist.

Numérotation (suite)

- La différence entre le dernier numéro de photo et le numéro présent dans le fichier DCIM_APPLE.plist permet de connaître le nombre de photos effacées
- Si la dernière photo présente se nomme : IMG_0800.JPG et que le n° 810 est inscrit dans DCIM_APPLE.plist alors 10 photos ont été prises puis effacées après la photo IMG_0800.JPG .

Horodatage des photos

- Les métadatas (EXIF) conservent dans la photo la date et l'heure de la prise de vue.
- Cette information n'est pas accessible à l'utilisateur
- Le fichier contenant la photo est également horodaté avec notamment la date de création
- Lors de la création d'une photo, ces 2 dates sont identiques (ou presque)
- Si ces 2 dates ne sont pas identiques, c'est qu'il y a eu manipulation.
- Si la date de modification du fichier n'est pas identique à celle de création, c'est que le fichier a été retouché après sa création.

Horodatage des photos

- Les métadatas (EXIF) conservent dans la photo la date et l'heure de la prise de vue.
- Cette information n'est pas accessible à l'utilisateur
- Le fichier contenant la photo est également horodaté avec notamment la date de création
- Lors de la création d'une photo, ces 2 dates sont identiques (ou presque)
- Si ces 2 dates ne sont pas identiques, c'est qu'il y a eu manipulation.
- Si la date de modification du fichier n'est pas identique à celle de création, c'est que le fichier a été modifié après sa création. La date de création ne change pas.

Résumé

- Date de prise de vue inscrite dans l'image : UTC
- Date de création du fichier contenant l'image : UTC+1 ou UTC+2
- Date de dernière modification du fichier contenant l'image : UTC+1 ou UTC+2

Les 2 dates de création ne sont pas modifiables par les logiciels présents en standard dans l'iPhone.

Autres fichiers concernés

- Chaque fois qu'une photo est réalisée, les dates des fichiers et dossiers suivants sont modifiées :
 - Fichier « Photos.sqlite-wal »
 - Fichier « changes-wal »
 - Dossier « MISC »
 - Fichier « DCIM_APPLE.plist » contenu dans le dossier « MISC »
- La date et l'heure des 4 éléments ci-dessus correspondent au moment où a été pris le dernier cliché.
- Un fichier nommé « PreviewWellImage.tiff » est créé dans le dossier « MISC » s'il n'existe pas déjà. S'il existe, c'est sa date de modification qui est changée

Horodatage des vidéos

- Principe identique pour les fichiers vidéo à la différence qu'une date de création n'est conservée dans la vidéo elle-même.
- La création d'une vidéo entraîne la création automatique de vignettes conservées dans un dossier système non accessible à l'utilisateur.

Synthèse

- Tout fichier portant un numéro plus grand qu'un autre fichier.
- Exemple avec IMG_XXXX.JPG et IMG_YYYY.JPG. Si YYYY est supérieur à XXXX alors le fichier IMG_YYYY.JPG a été créé après IMG_XXXX.jpg.
- A chaque nouveau cliché le contenu et la date de création du fichier « DCIM_APPLE.plist » devient celle de la création du dernier cliché.
- Pour connaître la date de création du dernier cliché réalisé avec un iPhone il suffit de regarder la date de modification du fichier « DCIM_APPLE.plist »

Suppression d'une photo

- Lorsqu'une photo est supprimée, les dates de modification des fichiers suivants sont modifiées :
 - Fichier « Photos.sqlite-wal »
 - Fichier « changes-wal »
 - Dossier « MISC »
- Le fichier « PreviewWellImage.tiff » (situé dans le dossier « MISC ») est supprimé s'il ne reste plus de photo une fois celle-ci supprimée. S'il reste des clichés une fois cette photo supprimée alors c'est la date de modification du fichier « PreviewWellImage.tiff » qui est modifiée et qui devient celle du moment de la suppression de la photo.

Formatage des dates

- La date de création stockée dans l'image est au format UTC (ex GMT)
- Les dates de création et modification des fichiers contenant les photos sont au format UTC+1 (ou +2) en fonction de la période de l'année.

Comment faire concrètement ?

- Pas besoin d'un iPhone jailbreaké
- Télécharger et lancer l'application Mac/PC : explorer 3 (anciennement PhoneDisk) sur le site <http://www.macroplant.com/phonedisk/>
- Le contenu du filesystem de l'iPhone apparaît sur le bureau.
- Ouvrir l'iPhone puis accéder au dossier « / var / mobile / Media / PhotoData / »
- Copier les 2 fichiers suivants depuis l'iPhone sur votre disque dur :
 - Photos.sqlite-wal
 - changes-wal

Comment faire concrètement ?

- Copier le dossier « MISC » et son contenu (fichiers « DCIM_APPLE.plist » et « PreviewWellImage.jpg ») depuis l'iPhone sur votre disque dur
- Si les dates de modification des fichiers « Photos.sqlite-wal » et « DCIM_APPLE.plist » sont identiques alors une photo, une vidéo ou une copie d'écran a été réalisée en dernier lieu.
- Si par contre la date de « DCIM_APPLE.plist » est antérieure à celle de « Photos.sqlite-wal » alors la dernière opération réalisée est une suppression.
- Si la date de modification de « DCIM_APPLE.plist » est postérieure à celle de « Photos.sqlite-wal » alors les fichiers ont été manipulés manuellement et doivent être considérés avec précaution.

Comment faire concrètement ?

- Ouvrir le fichier « DCIM_APPLE.plist » à l'aide d'un éditeur de texte pour identifier le dernier numéro utilisé pour nommer la dernière photo.
- Ouvrir le fichier « Photos.sqlite » à l'aide d'un éditeur hexa et rechercher tous les noms de photos. A proximité de chacun d'eux se trouve la date de création.

Exemple concret

Nom	Date de création	Date de modification
IMG_0561.JPG	8 septembre 2012 10:54	8 septembre 2012 10:54
IMG_0562.JPG	8 septembre 2012 11:59	8 septembre 2012 11:59
IMG_0563.JPG	8 septembre 2012 11:59	8 septembre 2012 11:59
IMG_0564.JPG	8 septembre 2012 12:50	8 septembre 2012 12:50
IMG_0565.JPG	8 septembre 2012 12:50	8 septembre 2012 12:50
IMG_0566.JPG	8 septembre 2012 12:50	8 septembre 2012 12:50
IMG_0567.JPG	8 septembre 2012 12:50	8 septembre 2012 12:50
IMG_0568.JPG	8 septembre 2012 12:50	8 septembre 2012 12:50
IMG_0569.JPG	8 septembre 2012 15:47	8 septembre 2012 15:47
IMG_0570.JPG	8 septembre 2012 19:51	8 septembre 2012 19:51
IMG_0578.PNG	16 septembre 2012 04:00	16 septembre 2012 04:00
IMG_0616.MOV	9 octobre 2012 23:54	9 octobre 2012 23:54
IMG_0617.PNG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0629.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0633.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0641.MOV	20 octobre 2012 22:16	20 octobre 2012 22:16
IMG_0647.PNG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0663.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0670.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0671.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0675.PNG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0676.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0678.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0682.PNG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0683.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0684.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0691.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0692.PNG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0699.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0700.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0706.PNG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0707.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0708.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0709.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0711.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0712.MOV	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0713.MOV	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0714.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33

Exemple concret

Nom	Date de création	Date de modification
IMG_0561.JPG	8 septembre 2012 10:54	8 septembre 2012 10:54
IMG_0562.JPG	8 septembre 2012 11:59	8 septembre 2012 11:59
IMG_0563.JPG	8 septembre 2012 11:59	8 septembre 2012 11:59
IMG_0564.JPG	8 septembre 2012 12:50	8 septembre 2012 12:50
IMG_0565.JPG	8 septembre 2012 12:50	8 septembre 2012 12:50
IMG_0566.JPG	8 septembre 2012 12:50	8 septembre 2012 12:50
IMG_0567.JPG	8 septembre 2012 12:50	8 septembre 2012 12:50
IMG_0568.JPG	8 septembre 2012 12:50	8 septembre 2012 12:50
IMG_0569.JPG	8 septembre 2012 15:47	8 septembre 2012 15:47
IMG_0570.JPG	8 septembre 2012 19:51	8 septembre 2012 19:51
IMG_0578.PNG	16 septembre 2012 04:00	16 septembre 2012 04:00
IMG_0616.MOV	9 octobre 2012 23:54	9 octobre 2012 23:54
IMG_0617.PNG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0629.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0633.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0641.MOV	20 octobre 2012 22:16	20 octobre 2012 22:16
IMG_0647.PNG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0663.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0670.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0671.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0675.PNG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0676.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0678.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0682.PNG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0683.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0684.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0691.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0692.PNG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0699.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0700.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0706.PNG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0707.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0708.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0709.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0711.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0712.MOV	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0713.MOV	21 janvier 2012 19:33	21 janvier 2012 19:33
IMG_0714.JPG	21 janvier 2012 19:33	21 janvier 2012 19:33