JFC du 21/6/2016
Expertise pénale

Les outils d'analyse de disques durs…

Gilles GRIMAULT (expert CA Colmar)

Introduction

Quand nous démarrons notre activité d'expert en tant qu'ingénieur, nous sommes prêts pour les dossiers au Civil.

Quand nous abordons le Pénal, c'est une autre affaire...

Mon histoire…

- (2006-2007) 1ères affaires avec des outils "gratuits" (CD-live Knoppix, grep...).
- (2007) 1ères sueurs froides (montage en RO, formats des fichiers Office, Unicode, viewers, carving, masse d'images et de vidéos à analyser...).
- (lente montée en charge en 2009)
- (2009) Achat d'un duplicateur Tableau (pour ne plus travailler avec l'original).
- (2009) Achat de "XWays-Trace" (spécifique Internet-Explorer) et de "XWays-Forensics" (+ 2 semaines d'auto-formation minimum !)
- (2010) Achat de bloqueurs Tableau (eSata - Sata/IDE).
- (2010) Achat de "Internet Evidence Finder" (aux coûts très variables !).

Ce qu'on peut attendre d'un outil d'analyse de disques durs…

(Liste non exhaustive, largement inspirée des principales fonctions de XWF + IEF)

- Création, ouverture d'un « Case ».
- Interface ayant une ergonomie efficace, qui ne change pas trop...
- Multi-partitions (FAT, NTFS, ext, HPFS…).
- Différentes vues (Partition, File, Preview, Details, Gallery, Calendar).
- Tris et filtrages du contenu des répertoires.
- Mettre de côté des contenus intéressants. Extraire ces contenus.
- Extraction de métadonnées.
- Extraction des « File types » avec entêtes et signatures.
- Hash code, emails, skin tone…
- Notion de « carving ».
- Recherche à base de mots-clés. Expressions régulières…
- Extraction des données de navigation web : multi-browsers, recherches, tchats…
- Extraction de données de synchros de téléphone (Android, iOS).

De l'intérêt d'acheter des solutions inforensiques professionnelles :

- Éviter de multiplier les outils logiciels.
- Aller plus vite (et donc facturer au plus juste).
- Ne pas se laisser dépasser par les technos.
- Avoir la garantie d'une certaine qualité (exemple : format Encase ".E01" adopté par tous les grands logiciels).
- Avoir un support technique.
- Éviter d'avoir à justifier des protocoles...

- **Aujourd'hui :** le HW est assez standard, les OS sont standards, mais nos "clients" utilisent de plus en plus des téléphones et tablettes...

JFC du 21/6/2016
Expertise pénale

Les outils d'analyse de téléphones…

Gilles GRIMAULT (expert CA Colmar)

Suite de mon histoire :

- (2009) Essais d'extractions de téléphones avec des logiciels / câbles "gratuits".
- (2010) Achat de "Oxygen Forensic Suite 2010".
- (2011) Achat de "Mobiledit Forensic" (avec sa petite mallette de câbles).
- (marre de passer mon temps à chercher des drivers, des câbles, à reconfigurer mes PC...)
- (2012) Achat de "XRY logical" (avec sa grosse mallette de câbles).
- (2014) 4ème achat : XRY physical (avec sa 2ème mallette de câbles).

- **Aujourd'hui :** les câbles sont presque standards, les OS sont presque standards.
- On demande de plus en plus des extractions avec « carving »...
- La concurrence fait rage (XRY, Cellebrite...), on doit se méfier des effets d'annonce.
- On dépend de failles logicielles de plus en plus rares (et rapidement corrigées)...

- **Demain :** on va nous demander de plus en plus d'extraire des données du Cloud...