Retour sur les JFIN (Journées Francophones de l'Investigation Numérique)

10-12 octobre 2012

Olivier Perret

AFSIN

OSSIR

Plan

Les JFIN sont aux experts judiciaires informatique ce que les JRES sont aux administrateurs réseaux du CNRS.

- Rappel sur le rôle des investigateurs;
- Cadre de la conférence: invités, exposants, ...
- Présentations techniques.

C'est un éco-système à part réunissant experts, universitaires, enquêteurs et magistrats.

N'étant pas juriste, je ne peux pas juger !

Oubliez ça !

- La justice n'est pas réservées aux spécialistes;
- Seul l'avis du juge fait autorité;
- Il s'appuie autant que possible sur des citoyens.

En tant qu'expert non-déclaré votre avis compte sans doute plus que vous ne le pensez...

Quelques règles

- Les experts sont assermentés et interviennent en leur nom propre;
- Indépendance des parties...et de l'employeur;
- Respect des autres intervenants enquêteurs (police, huissiers, gendarmes,...);
- Toujours référer au juge.

Conséquence visible au niveau des participants: une certaine discrétion,...

Les missions de l'expert

- **Investigation**;
- **Vulgarisation**;
- **Respect du débat contradictoire**;
- **Témoignage au procès**.

Pas forcément les mêmes qualités que pour être DSI...

Le parcours de l'expert

- Candidature en début d'année (1er mars);
- Inscription en fin d'année;
- 8 demi-journées de formation en cas de succès;
- Serment.

A moins d'une recommandation directe d'un juge, prévoir deux ou trois tentatives.

Les outils de l'expert

Par ordre d'expertise croissante

- Récupération de fichiers: PhotoRec/Testdisk, Recuva, PC Inspector
- Boite à outils: Glary Utilities
- Production de rapports: Encase forensics, Digital Forensics, X-Ways Forensics
- licence, nationalité: DFF

L'expert n'a jamais peur d'en ramasser trop,

Les exposants/sponsors

- Gold: Cellebrite et Tracip (local)
- Silver: Micro Systemation (mobiles), Guidance Software (Tableau/Encase), Synerese (Fr)
- Bronze: Cabinet d'expert
- Intervenants: Arxsys

Une frontière toujours difficile à cerner.

Le Programme

- Labo: virus, monitoring réseau, traitement d'images, mémoires flash
- Nouvelles pistes: artefacts windows, machines virtualisées,
- Légal: CNIL, Cloud,...
- Sponsors et exposants.

Loria: (Jean-Yves MARION/ Guillaume BONFANTE)

La virologie: amie ou ennemie de l'investigation numérique

- Analyse morphologique;
- Réalignement de code;
- Application vedette: Stuxnet == Duqu;
- Pas encore mûr pour les antivirus (coût en temps), mais pourquoi pas dans l'investigation numérique ?

Loria: monitoring réseau (Laurent CIARLETTA)

Le monitoring réseau.

- Réseau de surveillance des malwares;
- Capitalise des données depuis plusieurs années;
- Associé à d'autres réseaux de surveillance;
- Ouvert aux investigations.

Exploit notable: avoir réussi à créer une enclave sécurisée dans un monde de chercheurs.

OBS / Inria (Jacques FELD-MAR)

Traitement et amélioration d'images fixes et dynamiques

- éclaircir les zones sombres
- sans être accusé de falsification...

Quand la preuve est un fichier image qu'on aimerait améliorer...

La CNIL (Thomas DAUTIEU)

L'Expert judiciaire et la CNIL

- Discours classique, peut-être un peu plus précis sur les modalités d'intervention;
- Plutôt rassurant pour un public exposé...
- Mais pas passioné par ces problèmes.

Aucun expert interviewé n'a eu à travailler sur des affaires se revendiquant de la loi Informatique et Libertés.

Etude de cas originale (Lemmy FONTAINE)

Analyse des bornes de jeux et surf Internet

- Comment auditer ce type de matériel très particulier;
- Conçu justement pour ne pas être interfacé;
- Attaque par contenu connu...
- ...ou destiné à être récupéré (infos de paiement).

Les botnets (Eric FREYSSINET)

Description d'un nouveau phénomène et conséquences pour l'investigation

- Diversifié dans ses cibles;
- Mondialisé, donc nécessitant une coopération;
- Générateur de traces à l'insu du propriétaire;
- Pistes: coopération, détection, mitigation au niveau des grands réseaux.

DGA/MI (Bruno DAVENEL)

Intervention numérique sur mémoire flash.

- Nouveau media, nouveaux problèmes;
- Phénomème: non reproductibilité de l'image-disque;
- Problème: pas sérieux face à la défense;
- Réponse: se positionner comme le médecin-légiste.

C'est le labo d'investigation de la DGA; ils embauchent.

Démo (Emmanuel BON-HEURE)

Développement d'un outil d'analyse des artefacts sous Windows

- Détournement de l'horloge;
- Effacement de fichiers dont il reste des traces réelles;
- Intégration dans les outils d'analyse.

Evolution probable/souhaitable des logiciels d'analyse.

Analyse Cloud (Patrick ROUSSEL)

Le cloud c'est surtout Facebook !

- Le conseil de l'Europe encourage les pays à ratifier le gel des données (cf. liste est publiée);
- La téléperquisition nécessite l'accord de la victime;
- Si seulement les utilisateurs lisaient les CLUF...

Outils: Facebook Forensics, (K.Wong, Valkyrie-X), Encase le fait aussi.

Arxsys (Frédéric BAGUELIN)

Analyse de machine virtualisée

- Licence libre;
- API Python/C++;
- Virtualisation.

Place aux jeunes !

Conclusion JFIN

La justice n'est pas épargnée par les évolutions techniques récentes.

- Beaucoup de moyens (DGA, jeunes pousses,...)
- Encore beaucoup d'obstacles rébarbatifs: (formation des juges, mondialisation des des délits, ...)
- Paradoxe: besoin de transparence et impératifs de discrétion.

7ème édition en 2013 à Neufchâtel.

Conclusion pour l'OSSIR

Les JFIN sont un lieu où trouver les réponses juridiques qu'on ne trouve pas a l'OSSIR;

- Intéressante ne serait-ce que par son programme (aucune intervention sur HADOPI :-);
- Milieu plus dynamique techniquement qu'on ne pouvait le craindre;
- Mériterait d'être ajoutée dans la liste des confs (cf. site)...