JFC 28/11/17
Constats:outils

Michel Leclerc, Vianney Genet

Plan

- Groupe de travail Constat
- Principes pour la caisse à outils
- Nature de clés
- Structure des clés
- Types d’outils
- Comment se procurer les clés ?

Groupe de travail constat

- Le groupe de travail constat s'est réuni en 2017, en moyenne 1 fois par mois. Il a produit les outils.
- Il est constitué d'experts + Société Appliweb représentée par Vianney Genet
- les membres experts:
- Patrice Bajon - Michel Cappelli – Jean-Arnaud Causse- Fabien Cleuet - Michel Entat - Jean-Marie Ferrières - Antoine Laureau - Michel Leclerc - Franck Leroy
-

Principes pour la caisse à outils

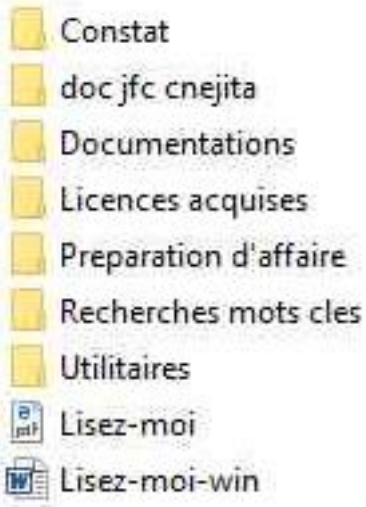
- Les outils sont gratuits ou peu chers (entre 40 et 100 euros)
- Ils s'exécutent sur une clé USB
- Sur la clé, pour chaque outil, une documentation pratique d'utilisation dans le cadre du constat
- Si l'outil est gratuit, il est présent sur la clé.
- Si l'outil est payant, il est absent de la clé mais on précise le lieu de téléchargement pour acquérir une licence.

Nature des clés

- Clé N°1 : des outils windows. La clé est introduite après que le poste à analyser a démarré. Bootable avec un outil de contournement mot de passe (konboot)
- Clé N°2 : des outils windows (version light). Par rapport à la clé N°1, on retire les outils qui occasionnent des alertes anti-virus
- Clé N°3 : des outils Mac. Bootable avec un outil de copie disque (osfclone).
- Clé N°4 : outils à utiliser sans démarrer le poste à analyser. La clé est bootable après production par l'expert.

Structure des clés

- Dépend de la clé
- A la source : le module bootable
- Exemple de la clé Windows :



Types d'outils

- Clés Windows
  - Recherche de documents avec mots clés
  - Recherche de fichiers effacés
  - Copie de disque en fichier image
  - Récupérer des emails sous webmail et mettre au format *eml, en triant les emails.
  - Faire des impressions écran
  - Nombreux utilitaires réseau et de connaissance des environnements
  - Outil d'empreinte de fichiers récupérés
  - Audit du poste (HW et Soft)
  - Contournement de mot de passe de poste

Types d'outils

- Clé Mac
  - Recherche de fichiers en batch et en temps réel
  - Outil de clonage de disque avec empreinte
  - Récupération de fichiers effacés
  - Recherche de mails
  - Création d'un OSX sur un support bootable
  - Audit de poste
  - Bloquage du montage des disques
  - Utilitaires natifs du Mac
  - Contournement du mot de passe de poste

Types d'outils

- Clé support bootable
  - Contient 4 packages multi-utilitaires
  - Caine,Deft,Paladin,Hiren (à télécharger sur liens)
  - Fiches sur quelques utilitaires utiles
    - Monter des disques (mounter-disks)
    - Copier des disques (guymager-Ddrescue-DC3DD,cyclone)
    - Faire l'empreinte (hash) (quick hash-dhash2)
    - Extraire des mails (readdbx-undbx-readpst)
    - Analyse de registre (fred-regripper)
    - Analyse base de données (sqlite)
    - Extraction de fichiers (bulk extractor viewer)

Comment se procurer les clés

- 4 fichiers ZIP. Un pour chaque clé
  - USB CNEJITA Mac V1.01
  - USB CNEJITA Win V1.04
  - USB CNEJITA Win Light V1.04
  - USB CNEJITA SUPPORTS BOOTABLES V1.00

  - Il faut dézipper pour que la clé soit opérationnelle et exécuter le module qui la rend bootable : konboot ou osfclone. (konboot est le même module pour l'environnement windows et l'environnement Mac)
  - Téléchargement à demander à Michel Entat
  - Taille clé : 32 gigas minimum

Questions

- Pour participer au groupe Outils et méthodes de constats : contacter Michel Entat