



OUTILS D'ANALYSE DISQUE DUR

POINT SUR L'OFFRE

Patrice BAJON
Expert Informatique
Cour d'Appel de Toulouse

JT du 21 juin 2016

L'ACQUISITION DES DONNEES :

Les bloqueurs hard :

- Marque phare : TABLEAU (T35x, T8, TD2U)
- Moins connu WEIBETECH.

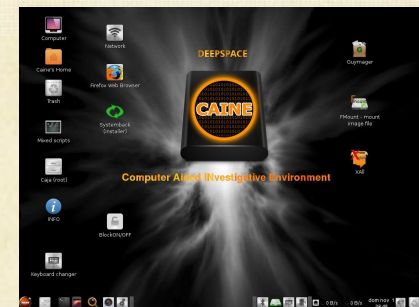




L' ACQUISITION DES DONNEES :

Les bloqueurs Soft :

- LIVE DVD USB principalement des distributions Linux





L' ACQUISITION DES DONNEES : LES LOGICIELS

Tous les logiciels « standards », les Live DVD proposent des logiciels « graphiques » permettant de gérer l'acquisition.

L'utilitaire FTK Imager peut être très utile.

Sinon les commandes `dd`, `ddrescue`, `dcfl` ... sont toujours nos amis.



L' ACQUISITION DES DONNEES :

CAS PARTICULIER : DISQUE SOUDÉ

Les Live USB/DVD sont l'alternative pour faire une image du disque.

Pensez à un CCC (Carbon Copy Cloner) pour les MAC OSX. Il permettent un démarrage dans l'environnement de l'ordinateur saisi.

Inconvénient il faut un mac pour faire l'image.



LES OUTILS STANDARD DU MARCHE :



Sleuth Kit, Autopsy (Windows, Linux)

EnCase® Forensic

Tous les utilitaires contenus dans les lives





L'ANALYSE DES RESULTATS (1 / 2):

- Deux formats très courant pour les images : RAW et E01 (compressé) – nette préférence E01 pour les transfert et tous les outils l'intègre.
- Il existe une partie d'analyse et de travail sur l'image avant l'exploitation des résultats (temps non négligeable).
- Des utilitaires sympas : Xtract, Wfra, Periscope



L'ANALYSE DES RESULTATS (2/2):

- Tous les outils standards font à peu près le même travail – Backlight non testé.
- Un outil intégré permet d'avoir toutes les grandes fonctions dans une même interface. (carving, exploration...)
- Pour l'analyse trafic internet : **IEF indispensable.**

CONCLUSION : 2 OUTILS OBLIGATOIRES DONT IEF



RETOUR D'EXPERIENCE

- Couplage analyse téléphone, tablette/disque dur potentialise les résultats.
- Au début on peut commencer avec des logiciels libres et se faire prêter IEF.
- Cas des données chiffrées deux solutions:
 - Passware Kit (tenter de casser !!!)
 - Nos amis du CTA (peines encourus plus de deux ans)

Coût : Attention en plus du coût d'acquisition entre 600 et 2500 € outil d'analyse + IEF (1500 €) : la maintenance annuelle.

Formation: peut être intéressant, mais à un coût financier/temps, la certification à l'outil.....