Analyses forensiques post-mortem et outils libres

La présentation s'est articulée selon les grandes lignes d'une analyse forensique, qu'elle soit réalisée dans le cadre d'une expertise judiciaire ou non :

- acquisition des données
- analyse de celles-ci

M. Roukine, expert près la cour d'appel de Grenoble, a présenté comment de nombreux outils classiques des environnements libres permettent de réaliser une grande partie d'une analyse. Ainsi, dd et netcat permettent facilement d'obtenir une image du support à analyser (facilement ne signifiant pas forcément rapidement). D'autres outils, comme dcfldd ou sdd, ont aussi été évoqués.

Les bloqueurs de lecture, pour ne pas altérer le disque originel dont on fait une image, et leur intérêt dans ce genre de situation ont été abordés.

L'analyse d'une image peut être faite en montant celle-ci, comme s'il s'agissait d'une partition classique (le montage sera préférablement fait en lecture uniquement). De là, toutes les recherches habituelles sur un système de fichiers et son contenu visible peuvent être réalisées avec les outils que l'on connaît bien (find, strings, grep, etc.). Ces recherches sur une partition montée ne pourront toutefois pas détecter des fichiers cachés dans des blocs non alloués, effacés ou autres.

D'autres outils, dont Sleuthkit et son interface Autopsy, ont été présentés. Ils permettent de procéder à une recherche et une analyse plus approfondies, notamment en examinant aussi les fichiers effacés, en procédant à des recherches "larges" sur l'image analysée (comme strings peut le faire sur une image non montée ou sur un descripteur de périphérique), et en dressant la chronologie des accès au système de fichiers (création, accès, modification de fichiers).

Quelques autres outils (fatback, foremost, galleta, pasco, rifiuti) ont été évoqués. Les trois derniers peuvent être téléchargés sur le site openforensics.org.

La réunion s'est terminée par une démonstration de Sleuthkit/Autopsy.

Auteur : Pierre-Yves Bonnetain — py.bonnetain@ba-cst.com