Travaux pratiques

Digital forensics

Objectifs

Nous allons nous intéresser à l'analyse de disque afin de rechercher/retrouver toutes sortes d'information. Quand nous utilisons un système informatique beaucoup de fichiers sont créés et modifiés. Ils sont souvent une mine d'informations et pour la plupart des gens ils sont impossibles à supprimer. C'est d'autant plus intéressant que ous les objets qui nous entourent sont connectés et sont riches en données personnelles. Nous verrons toute la démarche à suivre pour inspecter un disque et préserver ces données.

Keywords and phrases Incident, hachage, collisions, inspection, récupération, *carving*.
Digital Object Identifier TP2

1 Principe

Forensics est le terme anglais utilise pour décrire tous les activités scientifiques ayant des fins lors d'une enquête judiciaires. Le terme *digital forensics* est restreint à l'étude de tous ce qui est capable de stocker des données numériques.

2 Hachage

Exercice 1: recherche de collision

On peut voir les commandes `sum -s` et `cksum` comme permettant de calculer une fonction de hachage.

Question 1 Construire un fichier `2preimage` tel que `sum -s 2preimage` et `sum -s target` donne la même sortie.

Question 2 Trouver deux fichiers qui provoquent une collision pour la commande `cksum`. Vous pouvez vous inspirer du fichier `collision.bash`

Question 3 Que faut-il conclure pour `sum -s` et `cksum` ?

Question 4 Regardez le contenu des fichiers `l1.ps` et `l2.ps`. Calculer l'empreinte de ces deux fichiers avec `md5sum`. Que faut-il en conclure sur la fonction de hachage MD5 (soyez le plus précis possible dans votre réponse) ?

3 Analyse de système de fichiers

Cette analyse est faites à différents niveaux. A sommet on trouve les **disques** qui sont les matériels qui contiennent physiquement les données. La nature des disques permet quand on dispose d'un bon équipement d'inspecter directement les disques sans passer par une couche

logiciel. Ensuite, un disque peut être composé de différents **volumes** ou **partitions**. Mais un volume peut aussi s'étendre sur plusieurs disques. Il s'agit d'une organisation logique la mémoire. Les volumes sont indépendants les uns des autres.

Une partition dispose d'un système de fichier qui décrit comment les fichiers et leur métadonnées sont organisés. Au plus bas de l'échelle, on trouve les blocs qui sont la plus petite unité de données qu'il est possible d'allouer dans un système de fichiers. Historiquement, la plus petite taille de bloc était de 512 octets. On trouve maintenant principalement des systèmes de fichiers qui travaillent avec des blocs de 4096 octets.

4 Sleuthkit

Le Sleuthkit est un ensemble de 40 commandes qui permettent d'explorer des partitions. On pourrait réaliser l'intégralité de ces commandes avec des scripts qui utiliserait intensivement la commande `dd`. Il y a 6 catégories de commandes:

1. les commandes commençant par `mm` qui permettent d'inspecter les métadonnées des volumes. On trouve parmi ces commandes: `mmcat`, `mmls` et `mmstat`.
2. les commandes commençant par `fs` inspectant les systèmes de fichiers (`fsstat`).
3. les commandes commençant par `blk` permettent de travailler au niveau des blocs. Il s'agit des commandes: `blkstat`, `blkls`, `blkcalc`, `blkcat`.
4. l'exploration du contenu peut être fait de deux façons:
   - en travaillant directement avec les inodes (`ils`, `icat` et `ifind`);
   - en travaillant avec les noms de fichier (`fls`, `fcat` et `ffind`).
5. Enfin, il existe d'autres outils dans le Sleuthkit tel que `jpeg_extract`, `img_stat` ou encore `tsk_recover`.

4.1 Principe

A la racine du répertoire `TP2`, vous disposez d'un fichier `demo.dd` qui contient une partition FAT. Vous pouvez monter cette partition dans le répertoire local `mnt` en utilisant les commande ci-dessous:

```
mkdir mnt
sudo mount demo.dd mnt/
```

Pour enlever le point de montage, il suffit de taper:

```
sudo umount  mnt/
```

On peut maintenant inspecter les métadonnées de ce volume avec:

```
fsstat demo.dd
```

Pour inspecter le contenu du système de fichier:

```
fls demo.dd
ils -e demo.dd
```

`fls` va donner la vision tandis que `ils -e` va vous montrer toutes les inodes du système de fichier. Si on tape seulement `ils demo.dd`, on obtient toutes les inodes des fichiers effacés. Pour obtenir les métadonnées associées à une inode, il vous suffit de faire.

```
istat demo.dd 7
```

Enfin pour extraire un fichier particulier par son numéro d'inode:

```
icat demo.dd 7
```

Vous pouvez bien sur essayer toutes les commandes indiquées précédemment.
En dernier recours, vous pouvez utiliser la commande `foremost` qui permet de récupérer tout ce qui peut l'être mais attention cela peut prendre du temps et il faudra être capable de traiter la masse de données récupérées.

Exercice 2: échauffement

Question 5 Explorer les possibilités offertes par `system.dd.bz2` dans le répertoire `EX2`.