

[Forensic] Collecte de données

Introduction

Avant votre analyse, il vous faudra collecter les données de votre disque ou votre périphérique. Vous pouvez effectuer une copie physique avec un bloqueur d'écriture de disque mais aussi lancer une distribution en live tel que **Tsurugi Linux** ou **Paladin Linux** pour monter les périphériques en lecture seule.

DD

```
sudo dd if=/dev/sdX of=tmp/myusb.raw bs=512M status=progress
```

Ou pour créer une image d'un système distant :

```
ssh root@192.168.122.33 "dd if=/dev/sda bs=512M" | dd of=/root/vm-debian.dd bs=512M
```

EWF Tools

Cette suite d'outils sur Linux permet de faire une copie bit à bit de votre périphérique au format E01.

Pour cela, lancez **ewfacquire** :

```
ewfacquire /dev/sd<X>
```

Tout un tas de question vous sera posé. Laissez par défaut pour la plupart mais faite en sorte de n'avoir qu'un seul segment si possible (c'est plus pratique après pour ne pas à avoir à gérer plusieurs fichiers).

Vous pouvez afficher les informations de votre nouveau conteneur :

ewfinfo myusb.E01

Vous pouvez aussi vérifier l'intégrité de votre conteneur :

ewfverify myusb.E01

Revision #2

Created 4 March 2025 15:19:59 by Elieroc

Updated 13 March 2025 14:53:05 by Elieroc