TRAVAUX PRATIQUES : ANALYSE D'UN SUPPORT DE STOCKAGE

Ressources :

- Arsenal image mounter
- Exiftool
- PhotoREC
- Binwalk
- Veracrypt
- Steghide

Pré-requis :

Nombreuses sont les solutions permettant de réaliser une investigation numérique, c'est pourquoi un système d'exploitation tel que Windows est à privilégier. En effet, celui-ci vous permettra de lancer des exécutables et grâce à l'émulation d'une machine Linux avec WSL vous pourrez lancer du code aisément.

Contexte :

Vous êtes un enquêteur et vous devez analyser une clé USB retrouvé dans la fuite d'un suspect accusé d'un cambriolage.

Questions :

- Retrouver la position GPS du lieu photographié grâce aux métadonnées de l'image ?
- Le suspect possède-t-il une arme ?
- Qu'a fait le suspect et a-t-il un alibi ?