Forensics (Informatique légal)

Le forensics informatique est l'ensemble des techniques utilisées pour collecter, analyser et préserver des preuves numériques dans le cadre d'une enquête. Cela inclut les disques durs, réseaux, mémoires vives, appareils mobiles, et tout autre support contenant des données numériques.

Avant toute analyse, il est crucial de déterminer quels éléments (logs, fichiers, disque dur, etc.) sont pertinents pour l'enquête.

Les preuves doivent être préservées dans leur état original afin qu'elles soient admises en justice. Cela implique souvent la création de copies forensiques (hashing) et l'isolement des systèmes.

L'analyse consiste à extraire, examiner et interpréter les données pertinentes pour découvrir ce qu'il s'est passé.

Outils courants :

Autopsy : Interface graphique pour l'analyse forensique des disques.

FTK Imager : Outil pour créer des images disques et analyser des fichiers.

Wireshark : Analyse réseau pour découvrir des échanges suspects.

Volatility : Outil d'analyse de la mémoire vive (RAM).

X1 Social Discovery : Analyse des données provenant des réseaux sociaux.

Types d'analyse :

Analyse des fichiers système (dossiers, logs)

Récupération de fichiers effacés (notamment avec des outils de récupération de fichiers)

Analyse des connexions réseau (recherche de comportements anormaux)

Analyse de la mémoire vive (recherche de processus malveillants actifs)

Après l'analyse, un rapport détaillant les étapes de l'enquête, les résultats obtenus et les preuves découvertes est créé.

A noté qu'il existe plusieurs types de forensics :

- Disk Forensics (Forensique de disque dur)

Cela consiste à analyser des disques durs, des clés USB, ou tout autre support de stockage pour y retrouver des preuves telles que des fichiers supprimés, des logs ou des traces d'accès non autorisés.

Exemple : Un disque dur d'un employé a été saisi après qu'il ait quitté l'entreprise. L'analyse peut révéler des fichiers volés ou des communications malveillantes.

- Network Forensics (Forensique réseau)

Cette analyse concerne la surveillance et l'analyse des paquets réseau pour déterminer si une attaque a eu lieu via le réseau (ex : exfiltration de données, trafic malveillant).

Exemple : Une entreprise détecte une activité réseau suspecte (augmentation du trafic sortant). Le Network Forensics permettra de retrouver l'origine de l'attaque et ce qui a été exfiltré.

- Memory Forensics (Forensique de mémoire)

C'est l'analyse de la mémoire vive (RAM) d'un ordinateur. La mémoire peut contenir des informations très sensibles (processus en cours, fichiers ouverts, malwares actifs) qui ne sont pas enregistrées sur disque dur.

Exemple : Lors d'une analyse après une intrusion, Volatility peut être utilisé pour extraire des informations de la RAM et y découvrir des traces de malware non détectées sur le disque.

- Mobile Forensics (Forensique mobile)

L'analyse des smartphones ou tablettes pour retrouver des informations supprimées, des messages, ou des activités malveillantes.

Exemple : Un appareil mobile saisi lors d'une enquête peut contenir des communications cryptées, des mots de passe ou des logins de comptes utilisés pour commettre une fraude.

Les challenges en forensics sont :

Volatilité des données : Certaines informations disparaissent rapidement (ex : mémoire vive).

Cryptage et anonymisation : Les malfaiteurs utilisent souvent le cryptage pour cacher leurs actions.

Faux positifs : Il peut être difficile de distinguer les vrais indices des simples données normales ou les traces de fonctionnement.

Volume de données : Gérer des volumes de données massifs, particulièrement pour les attaques à grande échelle.