

Fiche Synthèse : Phases d'une Investigation Forensique

Cette fiche présente les étapes essentielles d'une investigation forensique numérique. Elle permet de structurer l'enquête tout en assurant la rigueur, la traçabilité et l'intégrité des preuves recueillies.

1. Préparation

Définir les politiques, procédures et outils nécessaires. Mettre en place une équipe d'intervention formée et préparer l'environnement technique.

2. Identification

Détecter les signes d'un incident. Identifier les systèmes, données ou utilisateurs concernés. Déterminer la portée et la nature de l'événement.

3. Collecte

Rassembler les preuves numériques (images disques, fichiers journaux, mémoire vive, etc.) en assurant la traçabilité et la chaîne de conservation.

4. Analyse

Examiner les données collectées pour comprendre le déroulement de l'incident, identifier les auteurs potentiels, les techniques utilisées et les impacts.

5. Documentation

Consigner chaque étape, action, résultat et preuve dans un rapport structuré, clair et juridiquement admissible.

6. Présentation

Communiquer les conclusions de l'enquête aux parties prenantes (direction, justice, RSSI). Fournir des recommandations concrètes et exploitables.