

Module 02

Cybersecurity 3

Fiche Récapitulative : Outils de Collecte et Recommandations

Objectif

Cette fiche présente les principaux outils utilisés pour la **collecte de preuves numériques** en investigation forensique, ainsi que les **bonnes pratiques** à respecter lors de cette phase cruciale.

Outils de collecte

Outil	Description	Cas d'utilisation
FTK Imager	Création d'images disques (bit à bit), export de fichiers.	Collecte de disques durs et périphériques.
dd	Outil Unix classique pour la copie brute de données.	Imagerie de partitions/disques physiques.
dc3dd	Version améliorée de dd avec fonctions de hachage intégrées.	Collecte forensique avec vérification d'intégrité.
Guymager	Interface graphique Linux pour la capture disque.	Collecte rapide et fiable sous Linux.
Magnet ACQUIRE	Outil gratuit de Magnet Forensics pour images disque et appareils mobiles.	Imagerie disque, support USB, mobiles, cloud.
X-Ways Forensics	Suite professionnelle avec fonctions d'acquisition et d'analyse.	Contextes judiciaires et enquêtes complexes.
Memoryze	Capture et analyse de la mémoire vive (RAM).	Enquête sur les malwares et rootkits actifs.
FTK Imager Live	Version portable pour acquisition sans arrêt du système.	Collecte à chaud sur machines critiques.

Outil	Description	Cas d'utilisation
Belkasoft RAM Capturer	Outil léger pour capturer la mémoire vive (Windows).	Collecte rapide de RAM sur systèmes en production.

✅ Bonnes pratiques de collecte

1. Intégrité des preuves

- Toujours générer un **hachage (MD5, SHA256)** avant et après la collecte.
- Comparer les valeurs pour confirmer la non-altération.

2. Travailler sur des copies

- Ne jamais manipuler l'original.
- Toujours analyser une **copie forensique**.

3. Documentation rigoureuse

- Noter **heure, date, outil, opérateur, équipement** utilisé.
- Utiliser une **fiche de chaîne de conservation**.

4. Utiliser des outils reconnus

- Préférer les outils validés par la communauté forensique ou reconnus légalement.

5. Sécuriser les supports de stockage

- Chiffrement des disques de stockage (ex : VeraCrypt).
- Sauvegarde dans un environnement isolé ou coffre-fort numérique.

🛡️ Recommandations complémentaires

- Réaliser un **test d'outils** sur un environnement de test avant une opération réelle.
- Toujours garder un **environnement propre**, hors réseau, pour la collecte.
- Éviter toute interaction avec les fichiers originaux en lecture/écriture.