AYI NEDJIMI Consultants

Forensique Disque : Acquisition d'Image et Analyse avec

Catégorie : Forensics Lecture : 9 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide pratique de forensique disque : acquisition d'image forensique, analyse avec Autopsy et FTK Imager, récupération de données, artefacts Windows.

Chaque action effectuée sur un système informatique laisse des traces sur le disque. L'exécution d'un programme génère un fichier Prefetch sous Windows. L'ouverture d'un document crée une entrée dans les Jump Lists et les fichiers LNK. La suppression d'un fichier ne fait que marquer l'espace comme disponible dans le système de fichiers, les données restant physiquement présentes jusqu'à leur écrasement. Même les techniques complexes de living-off-the-land qui tentent de minimiser les artefacts disque laissent des traces dans la MFT (Master File Table), le journal USN ou les bases de registre. Guide pratique de forensique disque : acquisition d'image forensique, analyse avec Autopsy et FTK Imager, récupération de données, artefacts Windows. Ce guide couvre les aspects essentiels de forensique disque autopsy ftk acquisition : méthodologie structurée, outils recommandés et retours d'expérience opérationnels. Les professionnels y trouveront des recommandations directement applicables.

L'analyse forensique de disque est donc une discipline fondamentale du DFIR (Digital Forensics and Incident Response). Elle permet de répondre aux questions essentielles d'une investigation : **Qui** a effectué **quoi**, **quand**, **comment** et avec **quel impact**. Que l'incident soit un ransomware, une exfiltration de données, une compromission par rootkit kernel-mode ou un abus interne, le disque recèle les preuves nécessaires à la compréhension de l'attaque et à la constitution du dossier judiciaire.

Guymager est un outil d'acquisition graphique open source intégré aux distributions forensiques CAINE, SIFT et Tsurugi. Il se distingue par son moteur d'acquisition multi-thread qui exploite tous les coeurs du processeur, offrant des vitesses d'acquisition significativement supérieures à dd. Il produit des images E01, AFF et Raw avec calcul de hash SHA-256 et MD5 simultané.

Formats d'image forensique

Format	Extension	Compression	Métadonnées	Utilisation
Raw / dd	.raw, .dd, .img	Non	Non	Universel, compatible avec tous les outils
E01 (Expert Witness)	.E01, .E02...	Oui (zlib)	Oui (case info, hash)	Standard industriel, FTK/EnCase
AFF4	.aff4	Oui	Oui (RDF)	Open source, extensible, efficace
SMART	.s01	Oui	Oui	ASR Data (historique)

Live vs Dead acquisition

Choix du mode d'acquisition
L'**acquisition dead** (machine éteinte, disque connecté via write blocker) offre la meilleure garantie d'intégrité et constitue la méthode préférée. L'**acquisition live** (machine allumée) est nécessaire lorsque :

- Le disque est chiffré (BitLocker, LUKS, FileVault) et la clé est en mémoire.
- Des volumes chiffrés sont montés (VeraCrypt).
- Les données volatiles (RAM, connexions) sont critiques.
- Un ransomware est en cours d'exécution et la clé peut être extraite de la mémoire.
- Le serveur ne peut pas être éteint (serveur de production critique).

En acquisition live, capturer la RAM en premier (ordre de volatilité RFC 3227), puis réaliser l'image disque. Documenter l'état du système (processus, connexions, utilisateurs connectés) avant toute action.

.

Vos journaux d'événements sont-ils conservés suffisamment longtemps pour une investigation ?

ext4 (Linux) : le système de fichiers ext4 utilise des inodes pour stocker les métadonnées. Le journal (journal=data ou journal=ordered) enregistre les modifications. Les fichiers supprimés voient leur inode marqué comme libre mais les données persistent. L'outil `extundelete` permet la récupération. Les permissions Unix (uid, gid, mode) sont des artefacts forensiques utiles.

APFS (Apple) : le système de fichiers d'Apple (macOS 10.13+, iOS 10.3+) utilise un conteneur avec un ou plusieurs volumes. Les fonctionnalités de snapshot intégrées permettent de récupérer des états antérieurs du système de fichiers. La persistance sur macOS et Linux fait l'objet de techniques spécifiques documentées dans notre article sur la persistence macOS/Linux.

FAT32 : système de fichiers hérité encore présent sur les clés USB et les cartes SD. La suppression d'un fichier remplace le premier caractère du nom par 0xE5 dans l'entrée de répertoire. La récupération est souvent triviale. FAT32 ne stocke pas de permissions, ce qui limite les artefacts forensiques disponibles.

.

```
# Analyse SRUM avec SrumECmd (Eric Zimmerman)
SrumECmd.exe -f "C:\Windows\System32\sru\SRUDB.dat" \
  -r "C:\Windows\System32\config\SOFTWARE" \
  --csv C:\output\ --csvf srum.csv

# Sous Linux avec srum-dump
python srum_dump.py -i SRUDB.dat -r SOFTWARE -o srum_output.xlsx
```

Jump Lists, fichiers LNK et Recycle Bin

Jump Lists (`%AppData%\Microsoft\Windows\Recent\AutomaticDestinations\` et `CustomDestinations\`) enregistrent les fichiers récemment ouverts par chaque application. Chaque entrée contient le chemin complet du fichier, les timestamps d'accès et le numéro de série du volume. Ils révèlent quels documents ont été consultés, même sur des partages réseau ou des clés USB.

Fichiers LNK (raccourcis Windows, `%AppData%\Microsoft\Windows\Recent\`) contiennent des métadonnées précieuses : chemin cible, taille du fichier, timestamps MACB, adresse MAC de l'interface réseau (si le fichier était sur un partage réseau), numéro de série du volume. Ils persistent même après la suppression du fichier cible.

Recycle Bin (`C:\$Recycle.Bin\{SID}\`) : lorsqu'un fichier est supprimé via l'Explorateur, il est déplacé dans la Corbeille. Le fichier `$I` contient les métadonnées (chemin original, date de suppression, taille) tandis que le fichier `$R` contient les données. L'analyse de la Corbeille révèle les fichiers que l'utilisateur ou l'attaquant a tenté de supprimer.

Thumbcache et USN Journal

Thumbcache (`%LocalAppData%\Microsoft\Windows\Explorer\thumbcache_*.db`) stocke les miniatures générées par l'Explorateur Windows pour les images, vidéos et documents. Même après la suppression d'une image, sa miniature peut persister dans le thumbcache, fournissant une preuve visuelle de son existence passée. L'outil `Thumbcache Viewer` permet d'extraire ces miniatures.

Le **USN Journal** ($Extend\$UsnJrnl:$J) enregistre chaque modification du système de fichiers NTFS : créations, suppressions, renommages, modifications de contenu et d'attributs. Chaque entrée contient un timestamp, le nom du fichier, le type de modification et la référence MFT. Le journal USN est crucial pour reconstituer la chronologie des actions d'un attaquant, notamment la dépose de fichiers malveillants, leur exécution et leur suppression ultérieure.

.

Récupération de données

File carving : récupération par signatures

Le **file carving** est une technique de récupération de fichiers basée sur leurs signatures (magic bytes) plutôt que sur les métadonnées du système de fichiers. Cette méthode est particulièrement efficace lorsque le système de fichiers est endommagé, que les entrées de répertoire ont été écrasées ou que le disque a été intentionnellement reformaté.

Le principe est simple : scanner le disque (ou l'espace non alloué) à la recherche de séquences d'octets connues correspondant aux en-têtes et pieds de page des formats de fichiers. Par exemple, un fichier JPEG commence par `FF D8 FF` et se termine par `FF D9`. Un fichier PDF commence par `%PDF` et se termine par `%%EOF`.

```
# File carving avec Photorec (open source, très efficace)
photorec /evidence/disk.raw

# File carving avec Scalpel (configurable)
scalpel -b -o /output/carved/ /evidence/disk.raw

# File carving avec foremost
foremost -t jpg,pdf,docx,xlsx -o /output/carved/ -i /evidence/disk.raw

# Carving ciblé sur l'espace non alloué uniquement
# 1. Extraire l'espace non alloué avec blkls (TSK)
blkls /evidence/disk.raw > unallocated.raw

# 2. Carver l'espace non alloué
photorec unallocated.raw
```

Récupération de fichiers supprimés

La suppression d'un fichier dans la plupart des systèmes de fichiers ne fait que marquer les clusters comme libres et modifier l'entrée de répertoire. Les données restent physiquement sur le disque jusqu'à leur écrasement par de nouvelles données. La récupération est possible tant que les secteurs n'ont pas été réutilisés.

Dans Autopsy, les fichiers supprimés sont automatiquement détectés et affichés dans la section "Deleted Files". L'outil les identifie par l'analyse de la MFT (entrées marquées comme non allouées), du journal USN et de l'espace non alloué. Le taux de récupération dépend du temps écoulé depuis la suppression et de l'activité du système (écriture de nouvelles données).

```
# Lister les fichiers supprimés avec TSK
fls -rd /evidence/disk.raw

# Récupérer un fichier supprimé par son numéro d'inode
icat /evidence/disk.raw 67890 > recovered_file.xlsx

# Récupération massive avec tsk_recover
tsk_recover -e /evidence/disk.raw /output/recovered/

# Sur ext4 avec extundelete
extundelete --restore-all /evidence/disk.raw

# Sur NTFS avec ntfsundelete
ntfsundelete /evidence/disk.raw -t 7d -p '*.docx' -d /output/
```

Analyse avancée

Détection de stéganographie

La **stéganographie** est l'art de dissimuler des informations dans un fichier porteur (image, audio, vidéo) de manière invisible. Un attaquant peut exfiltrer des données en les cachant dans des images apparemment anodines. La détection repose sur l'analyse statistique des fichiers :

- **Analyse chi-carré** : détecte les anomalies dans la distribution des bits de poids faible (LSB).
- **Comparaison de taille** : un fichier image anormalement volumineux par rapport à ses dimensions peut contenir des données cachées.
- **Outils spécialisés** : `StegDetect`, `Stegsolve`, `zsteg` (PNG/BMP), `steghide` (JPEG).

```
# Détection stéganographie dans les images PNG
zsteg -a image_suspecte.png

# Analyse stéganographique JPEG
stegdetect image_suspecte.jpg

# Extraction de données cachées (si mot de passe connu)
steghide extract -sf image.jpg -p "password"

# Analyse en masse des images du disque
find /mnt/evidence/ -name "*.jpg" -exec stegdetect {} \; > steg_results.txt
```

Volumes chiffrés et conteneurs

La détection de volumes chiffrés est une étape critique de l'analyse. Les indicateurs incluent :

- **BitLocker** : signature `-FVE-FS-` dans le Boot Sector, métadonnées BitLocker dans les 3 premiers secteurs.
- **VeraCrypt / TrueCrypt** : absence de signature identifiable (conception anti-forensique), entropie élevée uniforme sur tout le volume.
- **LUKS** (Linux) : signature `LUKS\xba\xbe` en début de partition.
- **FileVault 2** (macOS) : structure Core Storage détectable.

L'accès au contenu chiffré nécessite la clé de déchiffrement. En acquisition live, les clés peuvent être extraites de la mémoire RAM. En acquisition dead, les clés de récupération BitLocker peuvent être trouvées dans l'Active Directory, le compte Microsoft ou un fichier de sauvegarde. Pour les bootkits UEFI, la compromission du processus de démarrage peut également compromettre le chiffrement de disque.

Détection d'anti-forensics

Les attaquants aboutis utilisent des techniques d'**anti-forensics** pour entraver l'investigation. L'analyste doit être capable de les détecter :

Technique anti-forensics	Indicateurs de détection	Outils de détection
Timestomping	Incohérence $SI vs $FN dans MFT	analyzeMFT, MFTECmd, Autopsy
Wiping (sdelete, cipher)	Patterns de zéros dans slack space, entrées USN sans données	Autopsy, EnCase, analyse entropie
Log clearing	Event ID 1102 (Security log cleared), trous dans les Event Logs	Chainsaw, hayabusa, EvtxECmd
File renaming	Extension ne correspondant pas au magic bytes	File Type ID module (Autopsy)
ADS hiding	Données dans Alternate Data Streams	fls (TSK), Autopsy, dir /r
Encrypted volumes	Entropie élevée uniforme, absence de FS reconnu	Entropy analysis, Autopsy Encryption Detection

Les infostealers modernes incluent souvent des routines de nettoyage automatique après l'exfiltration des données, rendant l'analyse de ces artefacts anti-forensics particulièrement importante.

Reporting : génération de rapport

Rapport Autopsy

Autopsy intègre un module de génération de rapports qui produit des documents structurés au format HTML, Excel ou texte. Le rapport inclut automatiquement les artefacts identifiés (fichiers marqués, résultats de recherche par mots-clés, hash matches), les propriétés du cas et les métadonnées des sources de données. L'analyste peut personnaliser le rapport en sélectionnant les modules à inclure et en ajoutant des commentaires sur les artefacts importants (fonctionnalité de tagging).

Timeline export et corrélation

L'export de la timeline au format CSV permet une corrélation avec d'autres sources de données : logs SIEM, logs réseau, alertes EDR. En important la timeline dans un tableur ou un outil de visualisation (Timeline Explorer d'Eric Zimmerman, Kibana, Splunk), l'analyste peut filtrer, trier et croiser les événements pour reconstituer la séquence complète de l'attaque.

```
# Export complet de la super timeline
psort.py -o l2tcsv timeline.plaso \
  "date > '2026-02-10 00:00:00' AND date < '2026-02-15 23:59:59'" \
  > incident_timeline.csv

# Filtrage des événements pertinents
psort.py -o l2tcsv timeline.plaso \
  "source_short == 'FILE' AND filename contains 'mimikatz'" \
  > mimikatz_timeline.csv

# Génération de rapport HTML Autopsy (ligne de commande)
# Via l'interface graphique : Generate Report > HTML Report
# Sélectionner les modules et artefacts à inclure
```

Checklist du rapport forensique disque

- Informations du cas (numéro, date, examinateur).
- Description des sources de données (disques, images, hash).
- Méthodologie d'acquisition (outils, write blockers, vérification hash).
- Résumé des constatations principales.
- Timeline chronologique des événements clés.
- Artefacts identifiés avec captures d'écran et contexte.
- Fichiers récupérés (carving, fichiers supprimés).
- Analyse des techniques anti-forensics détectées.
- Conclusions et recommandations.
- Annexes techniques (hash complets, commandes exécutées, outils et versions).

Pour approfondir ce sujet, consultez notre outil open-source network-forensics-tool qui facilite l'analyse forensique du trafic réseau.

Questions frequentes

Comment mettre en place Forensique Disque dans un environnement de production ?

La mise en place de Forensique Disque en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

Pourquoi Forensique Disque est-il essentiel pour la securite des systemes d'information ?

Forensique Disque constitue un element fondamental de la securite des systemes d'information car il permet de reduire significativement la surface d'attaque, d'ameliorer la detection des menaces et de renforcer la posture globale de securite de l'organisation face aux cybermenaces actuelles.

Quels outils open source utiliser pour Forensique Disque : Acquisition d'Image et Analyse avec ?

Les incontournables sont Autopsy, Volatility 3, Plaso/log2timeline et RegRipper. Ils couvrent l'analyse disque, mémoire, timeline et registre sans coût de licence.

Sources et références : SANS SIFT · MITRE ATT&CK

> Points clés à retenir
>
> • Récupération de données
> • Analyse avancée
> • Reporting : génération de rapport
> • Questions frequentes
> • Conclusion

Conclusion

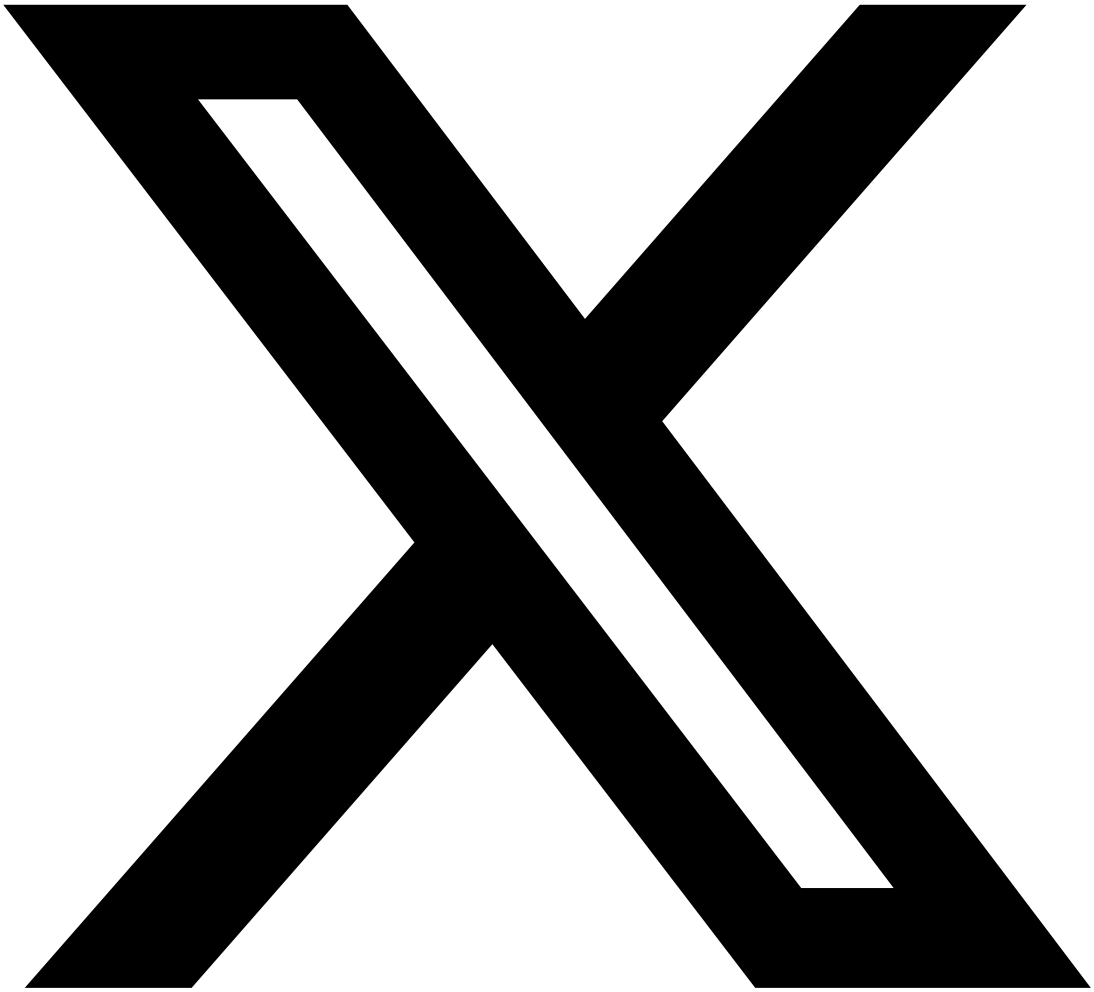
La forensique disque constitue le socle de toute investigation numérique. La rigueur de l'acquisition -- write blocker, vérification des hash, procès-verbal détaillé -- conditionne la recevabilité des preuves. La puissance des outils modernes comme Autopsy et la suite d'Eric Zimmerman permet d'automatiser l'extraction et la corrélation des artefacts, mais l'expertise de l'analyste reste irremplaçable pour interpréter les résultats et reconstituer le récit de l'attaque.

Les artefacts Windows -- Prefetch, Amcache, ShimCache, SRUM, Jump Lists, USN Journal -- forment un écosystème d'indices convergents qui, correctement exploités, permettent de répondre avec précision aux questions fondamentales de l'investigation. La récupération de données par file carving et l'analyse de l'espace non alloué étendent le champ d'investigation aux données que l'attaquant pensait avoir détruites.

Face à des attaquants qui déploient des techniques de ransomware, de persistance avancée par bootkits UEFI ou de persistence cross-platform, la maîtrise de la forensique disque est une compétence stratégique. Elle permet non seulement de comprendre l'incident et d'y remédier, mais aussi de constituer le dossier probatoire nécessaire aux actions judiciaires et aux obligations de notification réglementaire.

La formation continue, la veille sur les nouveaux artefacts introduits par les mises à jour de Windows et la pratique régulière sur des cas d'étude sont les clés de l'excellence en forensique disque.

Partagez cet article

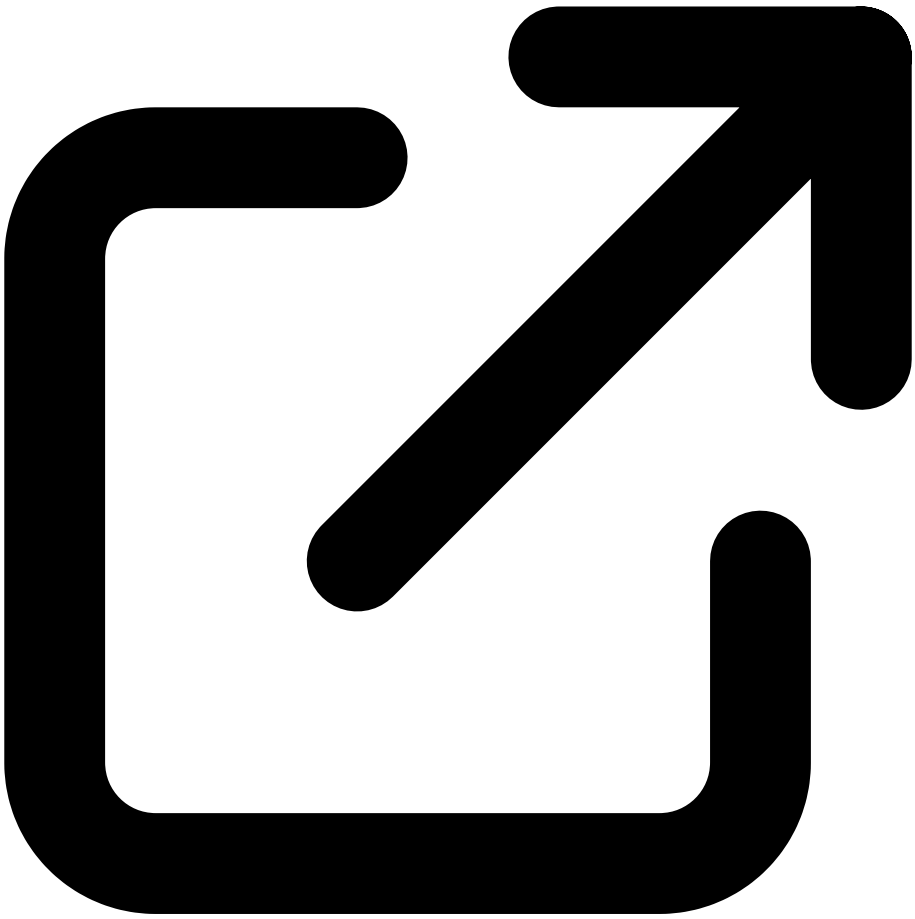


Partager sur X

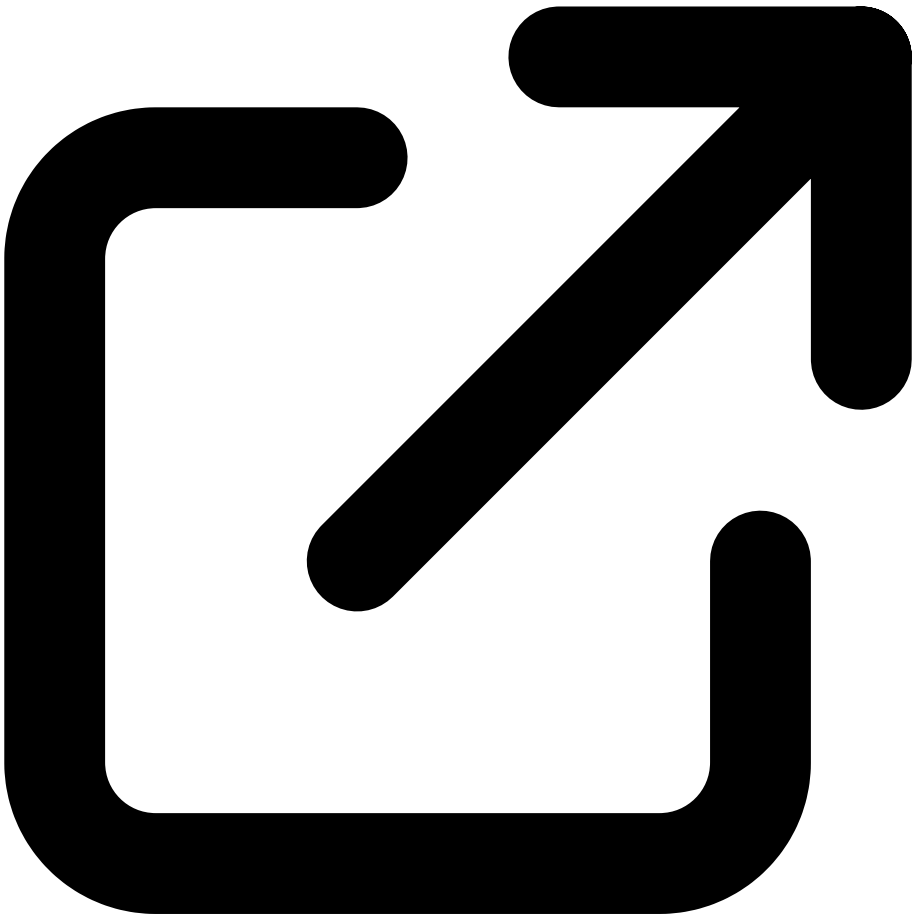
Partager sur LinkedIn

Ressources et Références Officielles

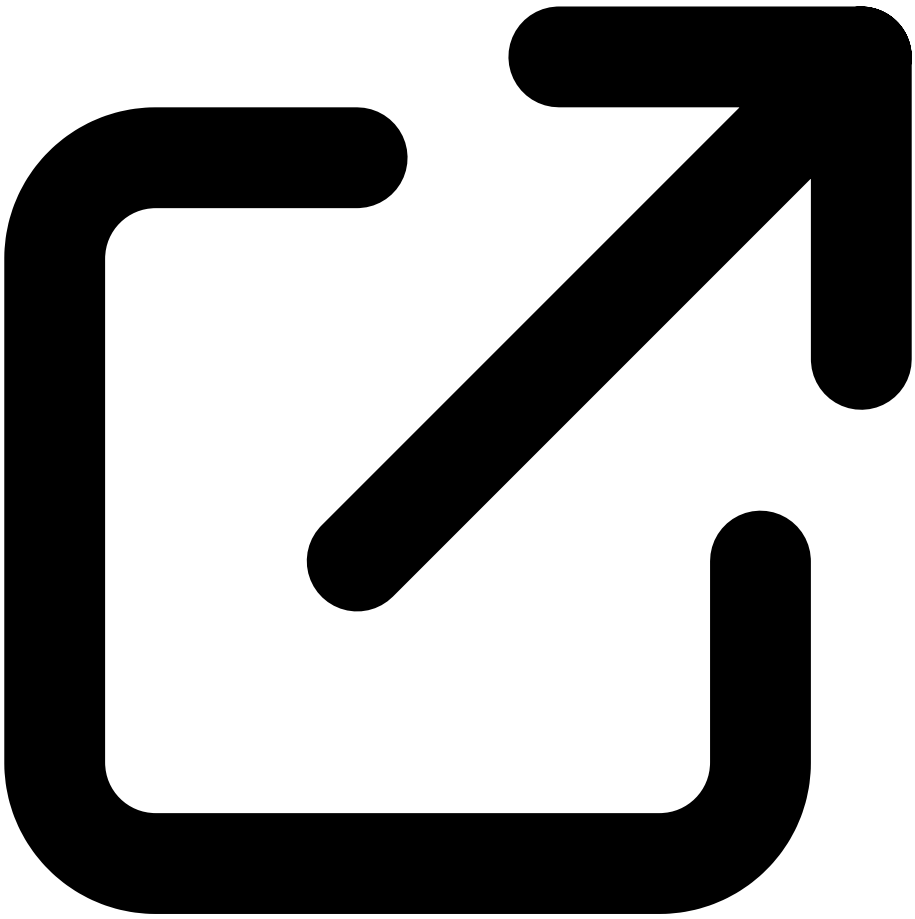
Documentations officielles, outils reconnus et ressources de la communauté DFIR



Autopsy - Digital Forensics Platform
autopsy.com



Eric Zimmerman Tools - DFIR Toolkit
ericzimmerman.github.io



SANS Windows Forensic Analysis Poster
sans.org

Ayi NEDJIMI

Expert en Cybersécurité & Intelligence Artificielle

Consultant senior avec plus de 15 ans d'expérience en sécurité offensive, audit d'infrastructure et développement de solutions IA. Certifié OSCP, CISSP, ISO 27001 Lead Auditor et ISO 42001 Lead Implementer. Intervient sur des missions de pentest Active Directory, sécurité Cloud et conformité réglementaire pour des grands comptes et ETI.

LinkedIn Profil complet Tous ses articles

Références et ressources externes

- Autopsy Documentation -- Guide officiel d'utilisation d'Autopsy
- The Sleuth Kit Wiki -- Documentation de la suite TSK pour l'analyse forensique
- Eric Zimmerman Tools -- Suite d'outils DFIR pour Windows (PECmd, MFTECmd, etc.)
- SANS Digital Forensics Blog -- Articles et recherches en forensique numérique
- NIST CFTT -- Programme de test des outils forensiques du NIST

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr