AYI NEDJIMI Consultants

Forensique Mémoire : Guide Pratique Volatility 3 en 2026

Catégorie : Forensics Lecture : 3 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide pratique forensique mémoire avec Volatility 3 : acquisition de dumps, analyse processus, détection malware, extraction d'artefacts et.

Fichiers et Registry

```
# filescan -- Scanne les structures FILE_OBJECT en mémoire
vol -f memdump.raw windows.filescan

# dumpfiles -- Extrait des fichiers depuis la mémoire
vol -f memdump.raw windows.dumpfiles --pid 1234
vol -f memdump.raw windows.dumpfiles --virtaddr 0xFA8001234560

# registry.hivelist -- Liste les ruches de registre en mémoire
vol -f memdump.raw windows.registry.hivelist

# registry.printkey -- Affiche les clés de registre
vol -f memdump.raw windows.registry.printkey --key
"Software\Microsoft\Windows\CurrentVersion\Run"

# hashdump -- Extrait les hashs NTLM depuis la SAM
vol -f memdump.raw windows.hashdump

# lsadump -- Extrait les secrets LSA
vol -f memdump.raw windows.lsadump

# cachedump -- Extrait les credentials cached domain
vol -f memdump.raw windows.cachedump
```

Extraction de credentials avec Mimikatz

L'un des artefacts les plus critiques en forensique mémoire est l'extraction des **credentials en clair** stockés dans le processus `lsass.exe`. Le plugin `windows.hashdump` extrait les hashs NTLM, mais pour obtenir les mots de passe en clair (WDigest, Kerberos tickets, DPAPI keys), il faut extraire le processus lsass et l'analyser avec Mimikatz ou pypykatz. C'est directement lié aux techniques d'infostealers utilisées par les attaquants : Guide pratique forensique mémoire avec Volatility 3 : acquisition de dumps, analyse processus, détection malware, extraction d'artefacts et. L'investigation numérique exige rigueur et méthodologie. Forensique Mémoire : Guide Pratique Volatility 3 en 2026 couvre les aspects pratiques que les analystes forensics rencontrent sur le terrain. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

```
# Méthode 1 : Extraire le minidump de lsass depuis le dump mémoire
# Identifier le PID de lsass.exe
vol -f memdump.raw windows.pslist | grep lsass
# => lsass.exe  PID: 756

# Dumper la mémoire du processus lsass
vol -f memdump.raw windows.memmap --pid 756 --dump

# Méthode 2 : pypykatz (Python, analyse offline)
pip3 install pypykatz
pypykatz volatility3 -f memdump.raw

# Résultat : credentials en clair si WDigest activé (défaut sur < Win10)
# username: admin  domain: CORP  NTLM: 31d6...  password: P@ssw0rd123
```

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

La mise en place de Forensique Mémoire 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 Mémoire est-il essentiel pour la securite des systemes d'information ?

Forensique Mémoire 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 Mémoire : Guide Pratique Volatility 3 ?

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

Pour approfondir, consultez les ressources de CERT-FR et de NIST Cybersecurity.

Sources et références : SANS SIFT · MITRE ATT&CK

Conclusion

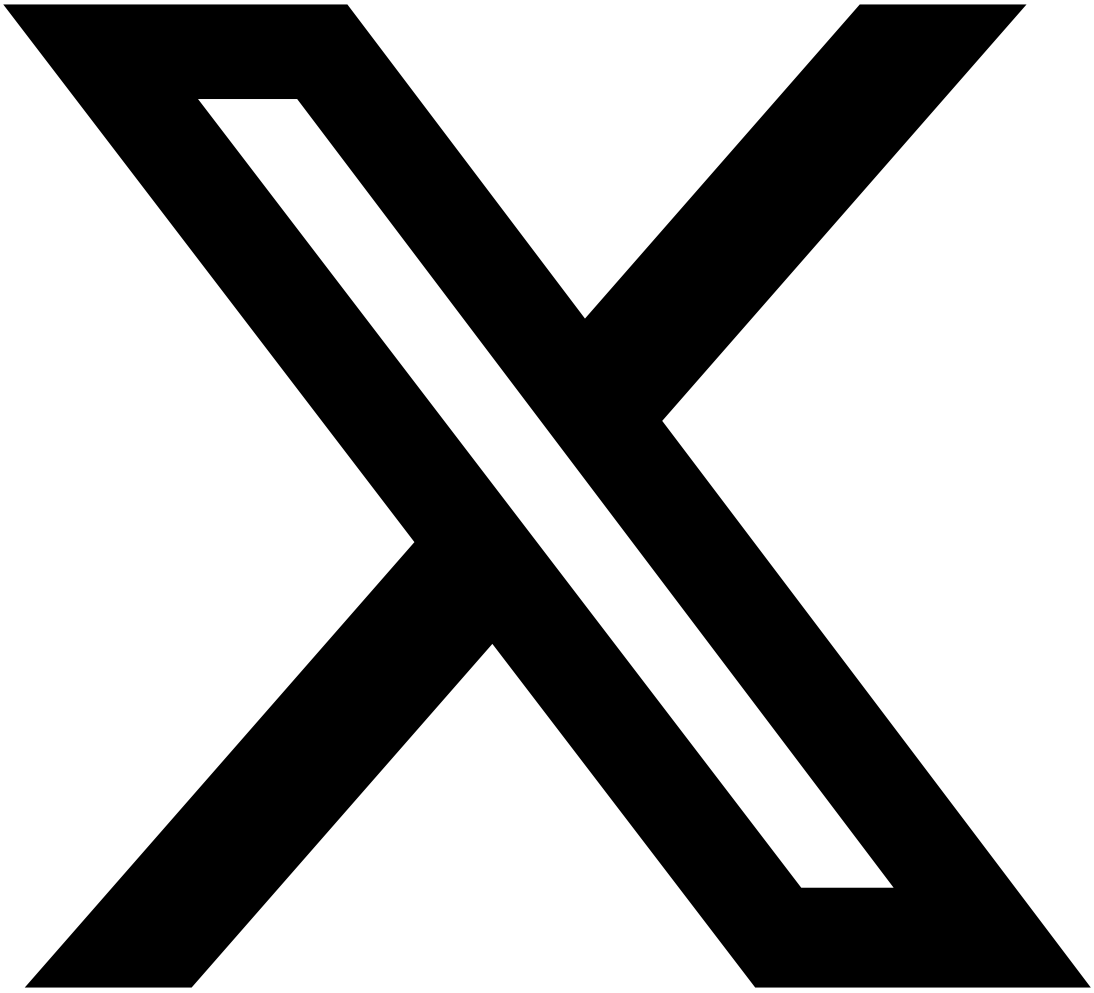
La forensique mémoire avec Volatility 3 est une compétence essentielle pour tout professionnel DFIR. La mémoire vive contient des artefacts que le disque ne peut pas fournir : processus en cours, connexions actives, code injecté, credentials en clair, clés de chiffrement éphémères. Maitriser Volatility 3, c'est gagner en profondeur d'analyse et en rapidité de réponse lors d'incidents critiques.

Les points clés à retenir :

- **L'acquisition est critique** : un dump mal réalisé compromet l'intégralité de l'analyse. Utilisez des outils éprouvés (WinPmem, LiME) et respectez la chaîne de preuve
- **Volatility 3 > Volatility 2** : la migration vers v3 est indispensable pour les systèmes modernes (Windows 11, Server 2022, Linux 6.x)
- **malfind est votre meilleur allié** pour détecter les injections de code et les process hollowing
- **La corrélation est la clé** : croisez processus + réseau + registre + fichiers pour reconstruire la kill chain complète
- **YARA amplifie vos capacités** : maintenez une bibliothèque de règles à jour pour détecter les menaces connues et leurs variantes
- **Pratiquez régulièrement** : utilisez des challenges CTF forensiques (MemLabs, CyberDefenders) pour affiner vos réflexes

Pour compléter votre boite à outils forensique, explorez les analyses de techniques d'évasion EDR/XDR, la compréhension des exploits kernel Windows et le reverse engineering de rootkits. La forensique mémoire ne s'exerce pas en isolation -- elle s'intègre dans un processus complet d'investigation numérique et de réponse aux incidents.

Partager cet article

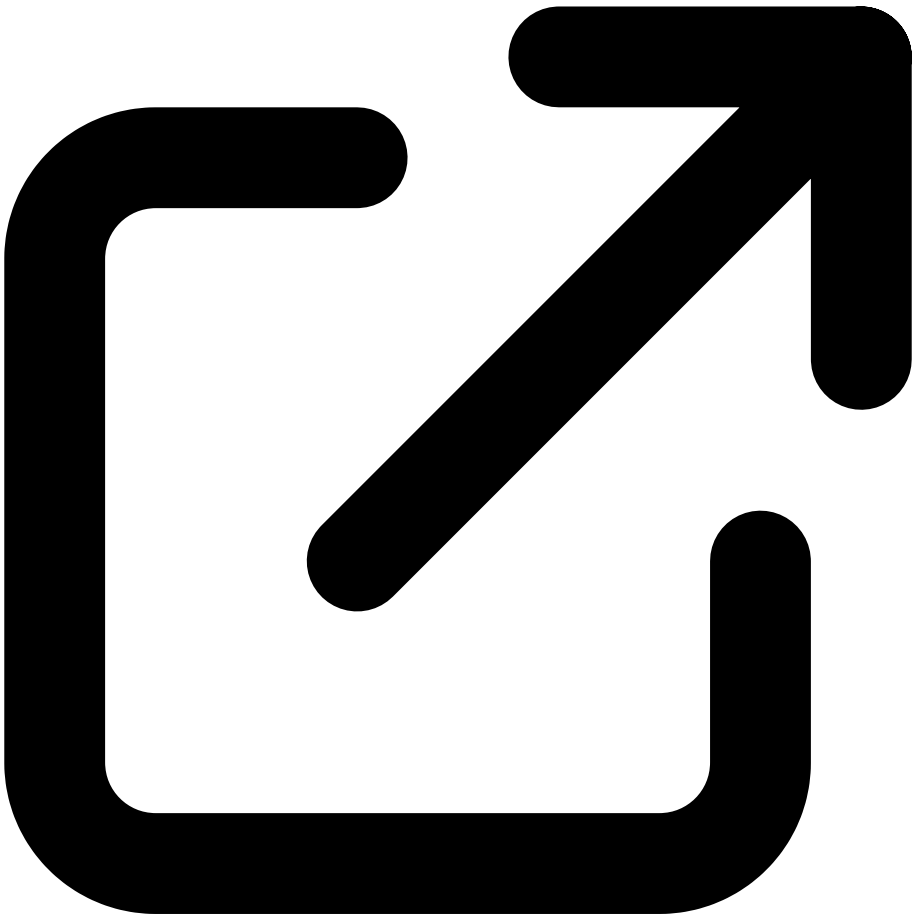


Partager sur X

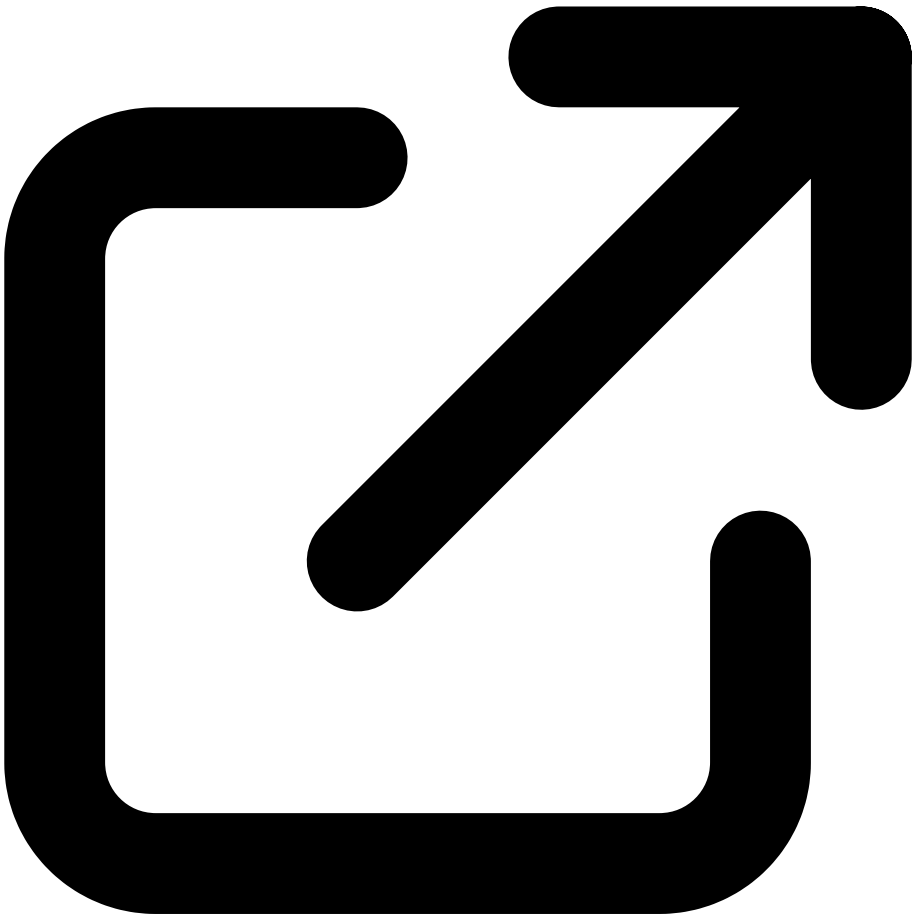
Partager sur LinkedIn

Ressources et Références Officielles

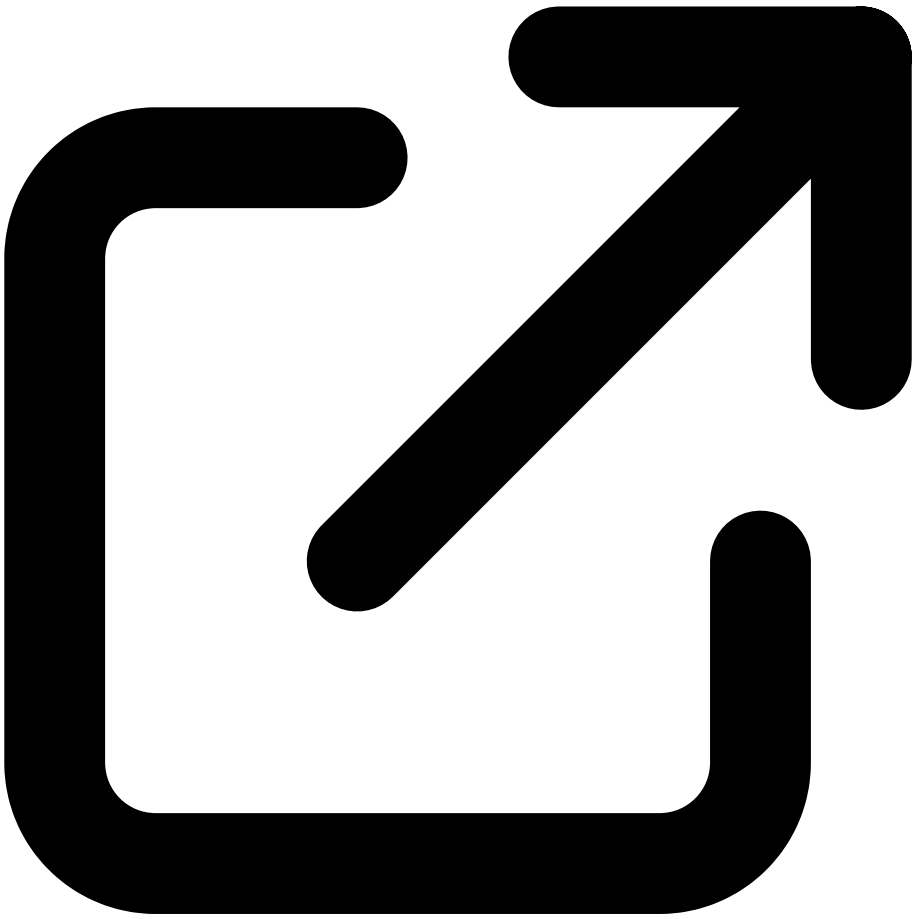
Documentation Volatility, outils et formations DFIR



Volatility 3 - GitHub
github.com/volatilityfoundation



Volatility 3 Documentation
volatility3.readthedocs.io



CyberDefenders - DFIR Challenges
cyberdefenders.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

> Points clés à retenir
>
> - Fichiers et Registry
> - Extraction de credentials avec Mimikatz
> - Conclusion
> - Partager cet article

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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