AYI NEDJIMI Consultants

Timeline Forensique : Reconstituer Pas à Pas une : Guide

Catégorie : Forensics Lecture : 8 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide de timeline forensique : reconstituer la chronologie d'une cyberattaque avec Plaso, log2timeline, MFT, événements Windows, journaux et.

Les timestamps MACB du système de fichiers NTFS

Le système de fichiers NTFS stocke pour chaque fichier et répertoire un ensemble de quatre timestamps connu sous l'acronyme **MACB** : **Modified** (dernière modification du contenu), **Accessed** (dernier accès), **Changed** (dernière modification des métadonnées dans la MFT) et **Birth** (date de création). Ces timestamps sont enregistrés dans deux attributs distincts de la Master File Table (MFT) : `$STANDARD_INFORMATION` (SI) et `$FILE_NAME` (FN). Guide de timeline forensique : reconstituer la chronologie d'une cyberattaque avec Plaso, log2timeline, MFT, événements Windows, journaux et. L'investigation numérique exige rigueur et méthodologie. Timeline Forensique : Reconstituer Pas à Pas une : Guide 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.

La distinction entre ces deux attributs est cruciale pour la forensique. L'attribut `$STANDARD_INFORMATION` peut être modifié par des appels API Windows standard (comme `SetFileTime()`), ce qui en fait une cible privilégiée pour le timestomping. En revanche, l'attribut `$FILE_NAME` ne peut être modifié que par le driver NTFS du noyau, ce qui le rend beaucoup plus fiable. La comparaison entre ces deux attributs constitue l'une des méthodes principales de détection du timestomping.

La MFT elle-même constitue un artefact forensique de premier ordre. Chaque entrée MFT occupe 1024 octets et contient non seulement les timestamps, mais aussi le nom du fichier, sa taille, ses attributs de sécurité et, pour les fichiers de petite taille (inférieur à environ 700 octets), le contenu du fichier lui-même (fichier résident). L'analyse de la MFT permet de retrouver des fichiers supprimés dont l'entrée n'a pas encore été réallouée, offrant une fenêtre sur l'activité historique du système.

Attention : résolution temporelle
Les timestamps NTFS ont une résolution de 100 nanosecondes, mais Windows ne met à jour le timestamp d'accès (A) par défaut que toutes les heures depuis Windows Vista (paramètre `NtfsDisableLastAccessUpdate`). Cette limitation doit être prise en compte lors de l'interprétation des timelines.

Windows Event Logs

Les journaux d'événements Windows sont la source de données temporelles la plus riche pour la forensique. Stockés au format EVTX dans `C:\Windows\System32\winevt\Logs\`, ils enregistrent avec précision les actions du système, des utilisateurs et des applications. Pour la timeline forensique, les journaux les plus pertinents sont :

Journal	Event IDs clés	Intérêt forensique
Security.evtx	4624, 4625, 4648, 4672, 4688, 4697, 4720, 4732	Authentifications, création de processus, élévation de privilèges
System.evtx	7034, 7036, 7045, 104	Services installés, arrêtés, effacement de logs
PowerShell/Operational	4103, 4104	Script block logging, commandes exécutées
Sysmon/Operational	1, 3, 7, 8, 10, 11, 13, 22, 25	Création processus, réseau, chargement DLL, accès registre
TaskScheduler/Operational	106, 140, 141, 200, 201	Tâches planifiées créées, modifiées, exécutées
TerminalServices-LocalSessionManager	21, 22, 23, 24, 25	Sessions RDP entrantes et sortantes

L'Event ID **4688** (Process Creation) mérite une attention particulière. Lorsque l'audit de création de processus est configuré avec la ligne de commande (GPO "Include command line in process creation events"), chaque lancement de processus génère un log contenant le chemin de l'exécutable, la ligne de commande complète, le SID de l'utilisateur et le processus parent. Cette source seule peut suffire à reconstituer une grande partie de l'activité d'un attaquant.

Prefetch, AmCache et ShimCache

Notre avis d'expert
L'analyse de la mémoire vive est devenue incontournable dans les investigations modernes. Les malwares fileless, les attaques living-off-the-land et les techniques d'injection en mémoire ne laissent souvent aucune trace sur le disque. Ignorer la RAM, c'est passer à côté de 60% des preuves.

Vos preuves numériques seraient-elles recevables devant un tribunal ?

Le **Prefetch** (`C:\Windows\Prefetch\`) enregistre les huit dernières dates d'exécution de chaque programme ainsi que la liste des fichiers et répertoires accédés lors du lancement. Chaque fichier `.pf` contient un hash du chemin de l'exécutable, ce qui permet de distinguer des instances du même binaire lancées depuis des emplacements différents. La présence d'un fichier Prefetch pour `PSEXEC.EXE` ou `MIMIKATZ.EXE` constitue un indicateur fort de compromission.

L'**AmCache** (`C:\Windows\AppCompat\Programs\Amcache.hve`) est une ruche de registre qui enregistre les métadonnées des programmes exécutés : hash SHA1, taille, éditeur, version et date de première exécution. Contrairement au Prefetch qui peut être désactivé sur les serveurs, l'AmCache est présent sur toutes les versions de Windows depuis Windows 8 et Server 2012 R2.

Le **ShimCache** (Application Compatibility Cache) est stocké dans la clé de registre `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache`. Il enregistre le chemin, la taille et la date de dernière modification de chaque exécutable rencontré par le système. Un point important : la présence dans le ShimCache ne garantit pas l'exécution effective du programme, car le cache est mis à jour lors du parcours de répertoire. Cependant, un flag "Executed" est présent sous Windows XP/2003, et la position dans le cache (les entrées les plus récentes en premier) fournit un indice temporel précieux.

Registre Windows, historique navigateur et SRUM

Le **registre Windows** contient de nombreuses sources temporelles. Les clés `UserAssist` enregistrent les programmes lancés via l'interface graphique avec un compteur et un timestamp (encodé en ROT13). Les clés `MRU` (Most Recently Used) gardent trace des fichiers récemment ouverts. Les `ShellBags` enregistrent les préférences de dossier de l'utilisateur, révélant quels répertoires ont été parcourus, y compris sur des partages réseau et des supports amovibles. Les timestamps de dernière modification des clés de registre (key last write time) constituent eux-mêmes un artefact temporel exploitable.

KAPE (Kroll Artifact Parser and Extractor), également développé par Eric Zimmerman, est un outil de triage forensique qui combine collecte d'artefacts et traitement automatisé. KAPE utilise des "Targets" pour définir les fichiers à collecter et des "Modules" pour les parser. Pour la construction de timeline, KAPE peut être configuré pour collecter automatiquement les fichiers EVT, le Prefetch, la MFT, le registre, l'AmCache et d'autres artefacts, puis lancer log2timeline et les parsers EZ Tools (outils d'Eric Zimmerman) pour produire une timeline consolidée.

```
# Collecte et traitement KAPE en une commande
kape.exe --tsource C: --tdest E:\collection --target KapeTriage --msource E:\collection --
mdest E:\processed --module !EZParser,MFTECmd,PECmd,AmcacheParser,EvtxECmd

# Structure de sortie KAPE
E:\processed\
├── Timeline/
│   ├── MFTECmd_Output.csv
│   ├── PECmd_Output.csv
│   └── AmcacheParser_Output.csv
├── EventLogs/
│   └── EvtxECmd_Output.csv
└── Registry/
    └── RECmd_Output.csv
```

Axiom : l'approche commerciale

Magnet Axiom est une solution commerciale qui automatise l'ensemble du processus de timeline forensique avec une interface graphique. Axiom ingère des images disque, des captures mémoire et des dumps cloud, et produit une timeline interactive avec des fonctionnalités de filtrage avancées, de tagging et de reporting. Sa fonctionnalité "Relative Time

Filter" permet de visualiser l'activité autour d'un événement spécifique. Axiom est particulièrement apprécié pour sa capacité à corréler automatiquement les artefacts Windows avec les données cloud (Microsoft 365, Google Workspace) et mobiles.

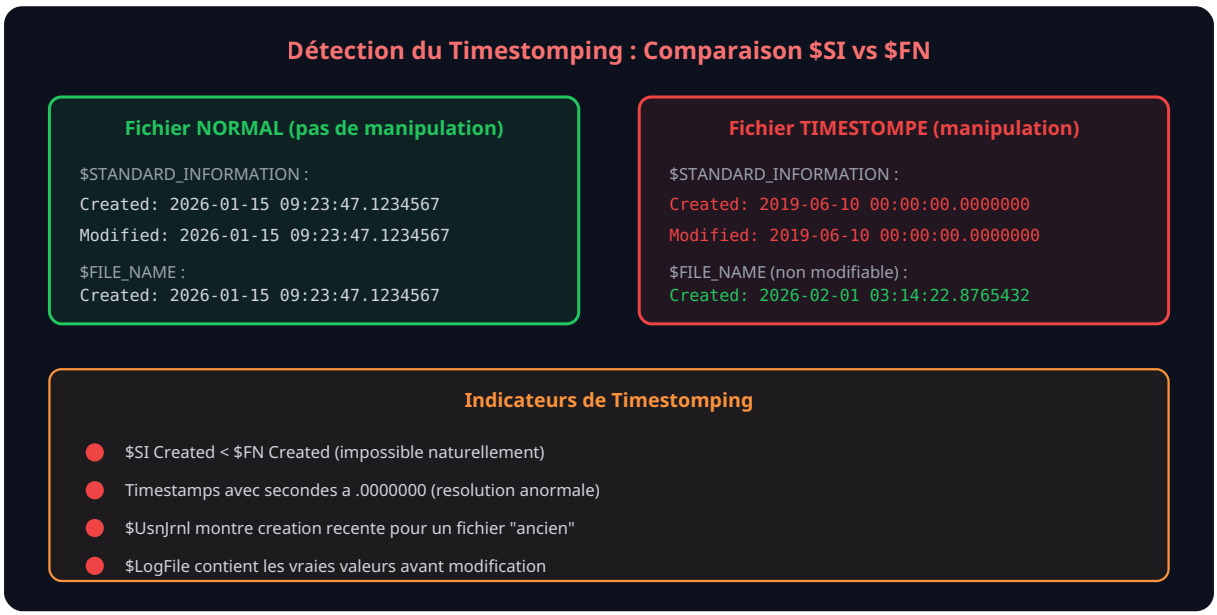
Recommandation : approche en couches
Pour les investigations complexes, utilisez une approche en couches : **KAPE** pour la collecte rapide et le triage initial, **Plaso** pour la construction de la super timeline complète, et **Timeline Explorer** pour l'analyse visuelle. Cette combinaison offre le meilleur rapport entre vitesse, exhaustivité et flexibilité.

Gaps et effacement de logs : un intervalle anormal dans les journaux d'événements Windows -- par exemple, aucune entrée dans Security.evtx pendant une période de 30 minutes alors que les journaux System et Application continuent -- peut indiquer un effacement ciblé. L'Event ID 1102 dans Security.evtx et l'Event ID 104 dans System.evtx enregistrent respectivement l'effacement du journal de sécurité et des autres journaux. Paradoxalement, l'acte d'effacement crée lui-même une entrée dans la timeline.

Détection du timestomping

Le **timestomping** est une technique anti-forensique (MITRE ATT&CK T1070.006) par laquelle l'attaquant modifie les timestamps d'un fichier pour le faire passer pour un fichier système légitime ou pour le rendre antérieur à la fenêtre d'investigation. La détection du timestomping repose sur plusieurs indicateurs convergents :

- **Divergence SI/FN :** si le timestamp de création dans `$STANDARD_INFORMATION` est antérieur à celui de `$FILE_NAME`, c'est une anomalie car le FN ne peut être modifié par les API standard. Un fichier dont le SI indique 2019 mais dont le FN indique 2026 a probablement été timestompé.
- **Timestamps arrondis :** les outils de timestomping comme `timestomp` de Metasploit ou `Set-MACETimestamp` produisent souvent des timestamps avec des secondes arrondies à zéro ou avec une résolution anormalement faible (pas de fraction de seconde) alors que NTFS enregistre normalement des fractions de seconde.
- **Incohérence avec le $UsnJrnl :** le journal USN (`$UsnJrnl:$J`) enregistre les modifications apportées aux fichiers avec ses propres timestamps. Si un fichier apparaît dans le journal USN à une date récente mais affiche un timestamp de création ancien dans la MFT, c'est un indicateur de timestomping.
- **Incohérence avec le $LogFile :** le fichier `$LogFile` (journal de transactions NTFS) peut contenir les valeurs originales des timestamps avant modification, permettant de confirmer le timestomping.




```
# Détection de timestomping avec MFTECmd (Eric Zimmerman)
MFTECmd.exe -f "$MFT" --csv E:\output --csvf mft_output.csv

# Recherche des anomalies SI/FN dans la sortie CSV (PowerShell)
Import-Csv E:\output\mft_output.csv | Where-Object {
    [datetime]$_.'SI_Created' -lt [datetime]$_.'FN_Created' -and
    $_.'InUse' -eq 'True'
} | Select-Object FileName, SI_Created, FN_Created, SI_Modified |
Export-Csv E:\output\timestomping_suspects.csv

# Analyse du journal USN pour corroborer
MFTECmd.exe -f "$UsnJrnl:$J" --csv E:\output --csvf usnjrnl_output.csv
```

Jour J-10, 02h40 UTC -- Le Prefetch révèle l'exécution de `SHARPHOUND.EXE` (collecteur BloodHound). Les ShellBags montrent la navigation vers un répertoire `C:\Users\user042\Documents\loot\` où des fichiers JSON de collecte BloodHound sont stockés temporairement.

Phase 3 : Mouvement latéral et élévation (J-7 à J-3)

Jour J-7, 01h20 UTC -- Sur le contrôleur de domaine DC01, l'Event ID 4624 (Logon Type 3 - réseau) est suivi d'un Event ID 4672 (privilèges spéciaux) pour le compte `svc_backup` depuis l'adresse IP de WORKSTATION-042. Ce compte de service dispose de privilèges `SeBackupPrivilege`, permettant la lecture de la base NTDS.dit. L'exécution de `ntdsutil.exe` est confirmée par le Prefetch de DC01 à J-7, 01h25 UTC.

Jour J-5, 02h00 UTC -- Les Event Logs de quatre serveurs supplémentaires (SRV-FILE01, SRV-FILE02, SRV-APP01, SRV-DB01) montrent des authentifications successives avec le compte `Administrator` depuis DC01. L'Event ID 7045 enregistre l'installation d'un service nommé `BTOBTO` sur chaque machine -- signature caractéristique de PsExec avec le paramètre par défaut.

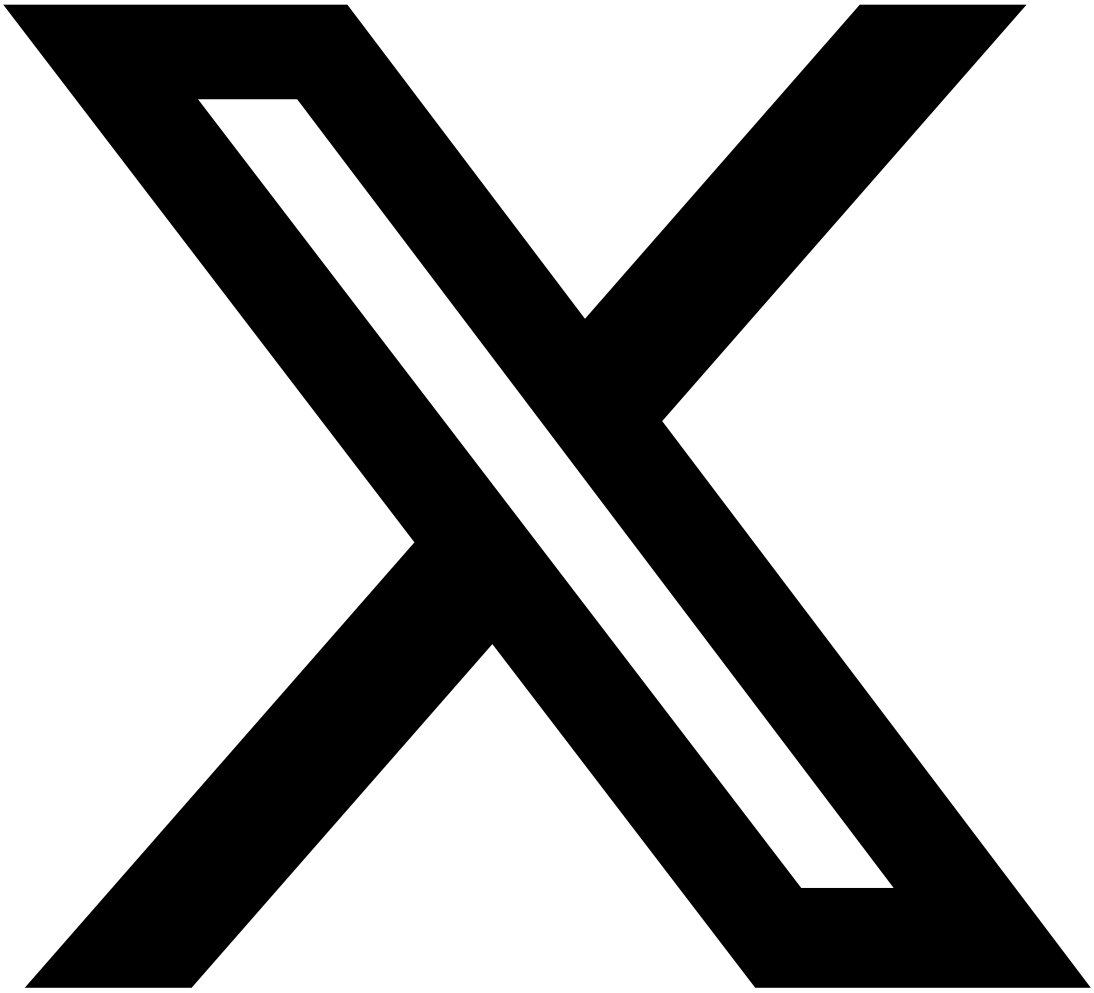
Phase 4 : Exfiltration et déploiement ransomware (J-3 à J-0)

Jour J-3, 22h00 à J-2, 04h00 UTC -- Le SRUM de SRV-FILE01 montre une activité réseau sortante anormale : 47 Go envoyés par un processus `rclone.exe` vers un service de stockage cloud. Les logs du proxy confirment des connexions HTTPS vers `mega.nz`. L'exfiltration des données sensibles est confirmée.

Jour J-0, dimanche 23h45 UTC -- Sur DC01, l'Event ID 4698 (tâche planifiée créée) enregistre la création d'une tâche nommée `WindowsUpdate` exécutant `C:\Windows\Temp\locker.exe` à 00h00 UTC via une GPO s'appliquant à toutes les machines du domaine. Le chiffrement commence à minuit et est découvert par les premiers utilisateurs arrivant le lundi matin.

```
# Timeline résumée de l'incident (format simplifié)
2026-01-15 14:32 UTC | WS-042  | Phishing - visite URL malveillante
2026-01-15 14:34 UTC | WS-042  | Execution payload ISO + LNK + PowerShell
2026-01-15 14:35 UTC | WS-042  | Cobalt Strike beacon deployed (svchost32.exe)
2026-01-15 14:38 UTC | WS-042  | Persistence - Registry Run key created
2026-01-17 03:15 UTC | WS-042  | AD Recon - net group, nltest, net view
2026-01-19 02:40 UTC | WS-042  | BloodHound collection (SharpHound.exe)
2026-01-22 01:20 UTC | DC01    | Lateral movement - svc_backup logon
2026-01-22 01:25 UTC | DC01    | NTDS.dit extraction via ntdsutil
2026-01-24 02:00 UTC | 4 SRVs  | PsExec propagation (service BTOBTO)
2026-01-26 22:00 UTC | FILE01  | Data exfiltration begins (rclone → mega.nz)
2026-01-27 04:00 UTC | FILE01  | Exfiltration complete (~47 GB)
2026-01-28 23:45 UTC | DC01    | Scheduled task created via GPO
2026-01-29 00:00 UTC | Domain  | Ransomware encryption begins
2026-01-29 07:15 UTC | Domain  | Discovery by employees
```

Cet article vous a été utile ? Partagez-le avec votre réseau professionnel !

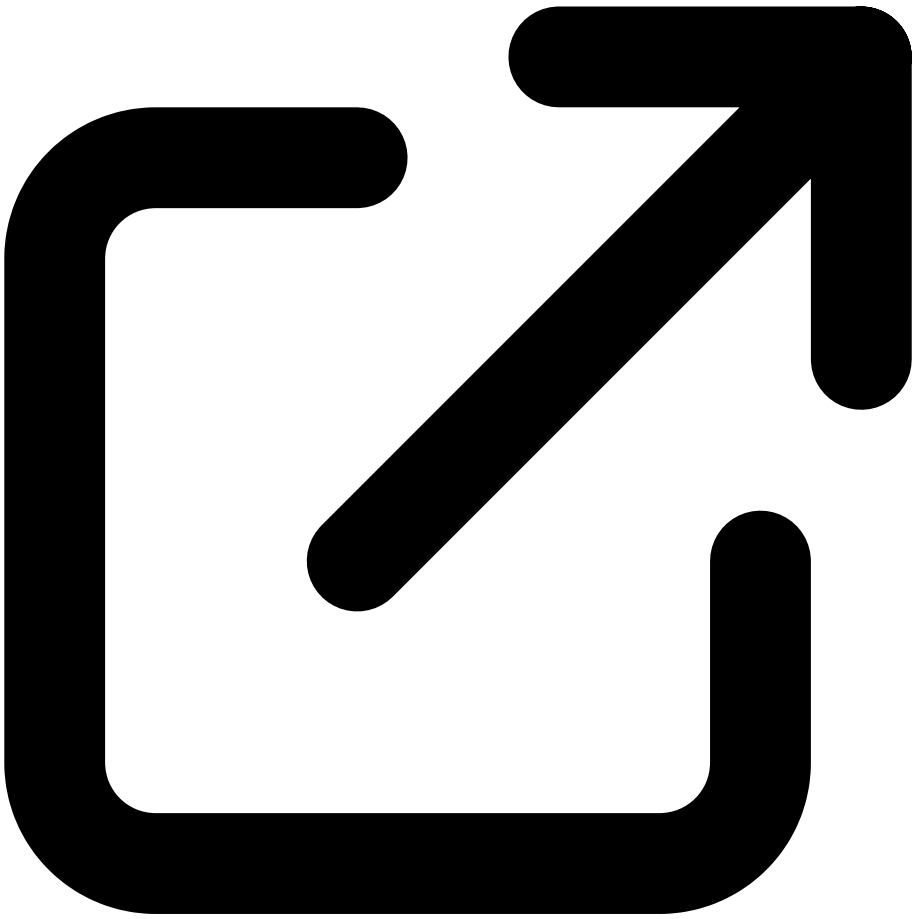


Partager sur X

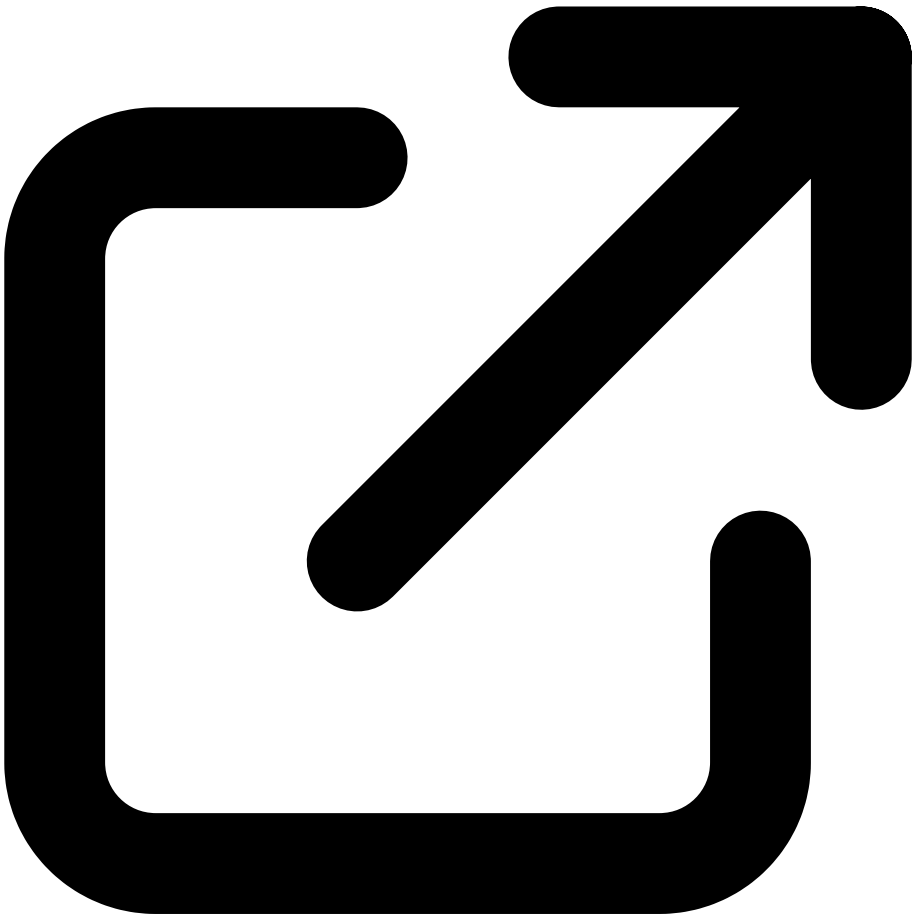
Partager sur LinkedIn

Ressources & Références Officielles

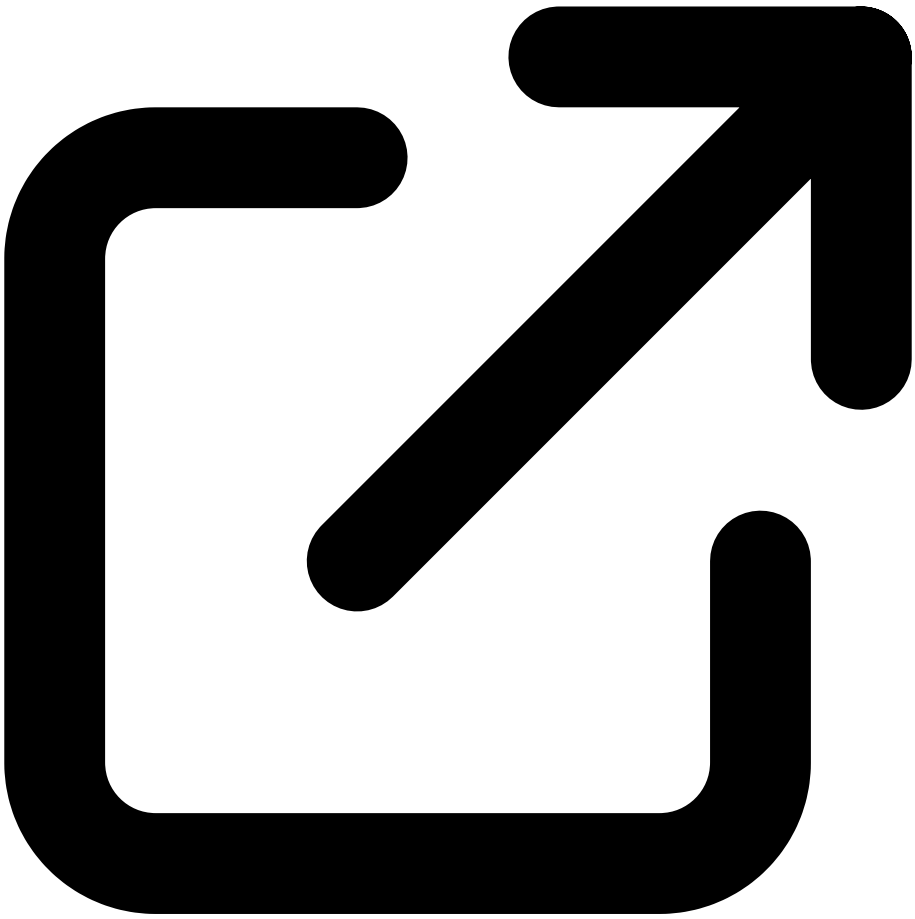
Documentations officielles, outils reconnus et ressources de la communauté



Plaso (log2timeline)
github.com/log2timeline/plaso



Eric Zimmerman's Tools (KAPE, Timeline Explorer)
ericzimmerman.github.io



MITRE ATT&CK - Indicator Removal
attack.mitre.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

- Plaso / log2timeline — Framework de construction de super timelines forensiques
- Eric Zimmerman's Tools — Suite d'outils forensiques (MFTECmd, PECmd, Timeline Explorer, KAPE)
- MITRE ATT&CK T1070.006 — Indicator Removal: Timestomp
- Timesketch — Outil open source de timeline collaborative (Google)
- SANS Windows Forensic Analysis Poster — Référence rapide des artefacts Windows

Sources et références : SANS SIFT · MITRE ATT&CK

Articles connexes

- DFIR Cloud : Investigation Logs AWS CloudTrail en 2026
- Telemetry Forensics - Guide Pratique Cybersecurite
- ETW & WPR : Guide Complet et Bonnes Pratiques pour Experts
- NTFS Advanced : Methodologie et Recommandations de Securite

FAQ

Qu'est-ce que Timeline Forensique ?

Timeline Forensique désigne l'ensemble des concepts, techniques et méthodologies abordés dans cet article. Les fondamentaux sont détaillés dans les premières sections du guide.

Pourquoi timeline forensique chronologie intrusion est-il important ?

La maîtrise de timeline forensique chronologie intrusion est devenue essentielle pour les équipes de sécurité. Les enjeux et le contexte opérationnel sont développés tout au long de l'article.

Comment appliquer ces recommandations en entreprise ?

Chaque section de cet article propose des méthodologies et des outils directement utilisables. Les recommandations tiennent compte des contraintes d'environnements de production réels.

> Points clés à retenir
>
> • Timeline Forensique : Reconstituer Pas à Pas une : Guide

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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