

PAGE DE GARDE

Projet : Investigation numérique sur clé USB suspecte

Auteur : Fatima LY , Aminata Ndiaye

Encadrant : Mr cissé

Année académique : 2025 – 2026

Établissement : BEMTECH

RAPPORT FORENSIC – Analyse d'une clé USB suspecte

1. Contexte de l'incident

Le service informatique a été informé qu'un employé a introduit une **clé USB potentiellement infectée** dans un **poste de travail sensible**. Une analyse forensic complète a été initiée afin d'identifier d'éventuels fichiers malveillants, déterminer le mode d'infection et évaluer les risques encourus.

2. Tableau de bord (Synthèse de l'analyse)

Élément analysé	Résultat	Commentaire
Type de support	Clé USB 16 Go	Support externe non autorisé
Copie bit-à-bit (dd)	Succès	Image sauvegardée sans altération
Analyse Autopsy / FTK	Anomalies détectées	Présence d'exécutables cachés
Fichiers suspects trouvés	3 exécutables + 1 script autorun	Indicateurs de malveillance
Vecteur d'infection probable	exécution automatique / double extension	Tactique fréquente dans les attaques USB
Risque	Élevé	Possibilité de compromission du poste

RAPPORT DE PROJET : ANALYSE DE LOGS

2. Objectifs de l'enquête

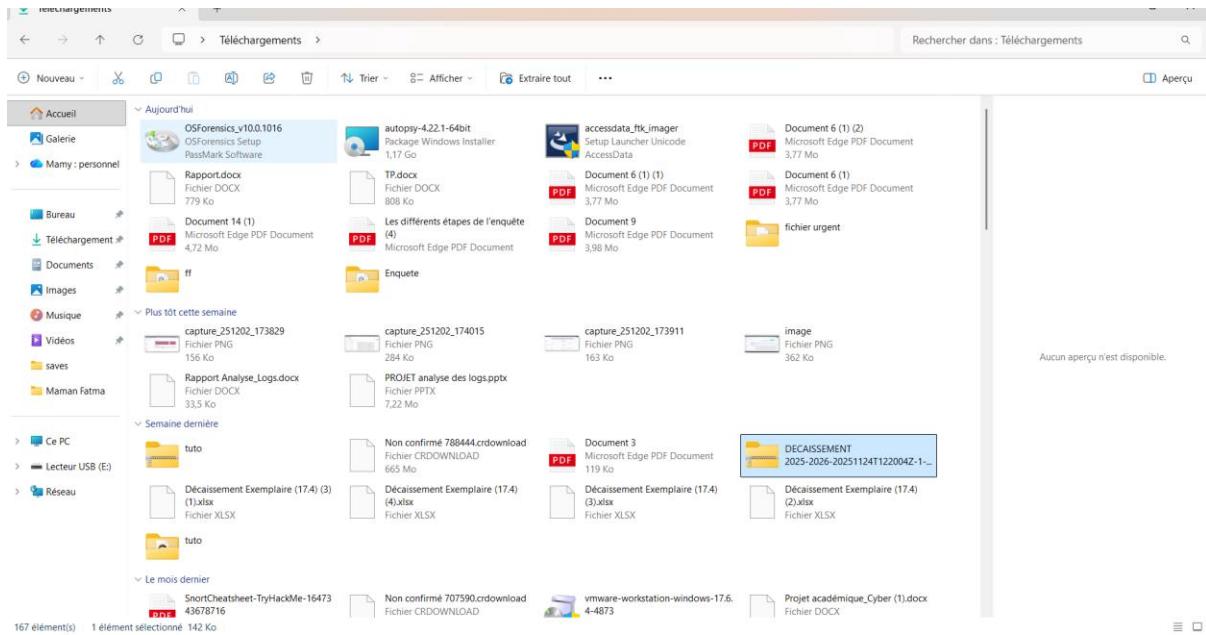
- Réaliser une **copie bit-à-bit** de la clé USB pour préserver l'intégrité des preuves.
- Analyser l'image avec **OSForensics**.
- Identifier les **fichiers exécutables suspects**.
- Déterminer le **vecteur d'infection**.
- Produire un **rapport forensic détaillé**.

1. Introduction

Ce projet consiste à analyser différents fichiers de logs afin d'identifier les anomalies, les événements critiques et les potentielles menaces de sécurité. L'analyse de logs est une étape essentielle pour comprendre le comportement des systèmes informatiques, détecter des activités suspectes et améliorer la performance globale du réseau.

1. IDENTIFICATION DES PREUVES

- Isoler l'environnement concerné : Si possible, isolez les appareils utilisés par l'employé soupçonné (ordinateur, téléphone portable, etc.) pour éviter toute altération des preuves.
- Créer une copie forensique des disques durs et des autres supports de stockage



❖ Nous avons ici une clé USB d'un employé soupçonné pour éviter toute altération, nous allons d'abord faire la copie de la clé USB pour prouver des preuves et tracer les fichiers supprimés

2. Analyse des systèmes

❖ Traçage des activités réseau : Analysez le trafic réseau pour voir si des fichiers ont été transférés vers des plateformes externes (via FTP, email, services de cloud tels que Google Drive, Dropbox, etc.).

❖ Analyse des fichiers téléchargés ou copiés : Utilisez des outils de suivi pour identifier si des fichiers ont été copiés sur des périphériques de stockage externes (clé USB, disque dur externe)

3. Procédure technique réalisée

3.1. Copie bit-à-bit avec dd

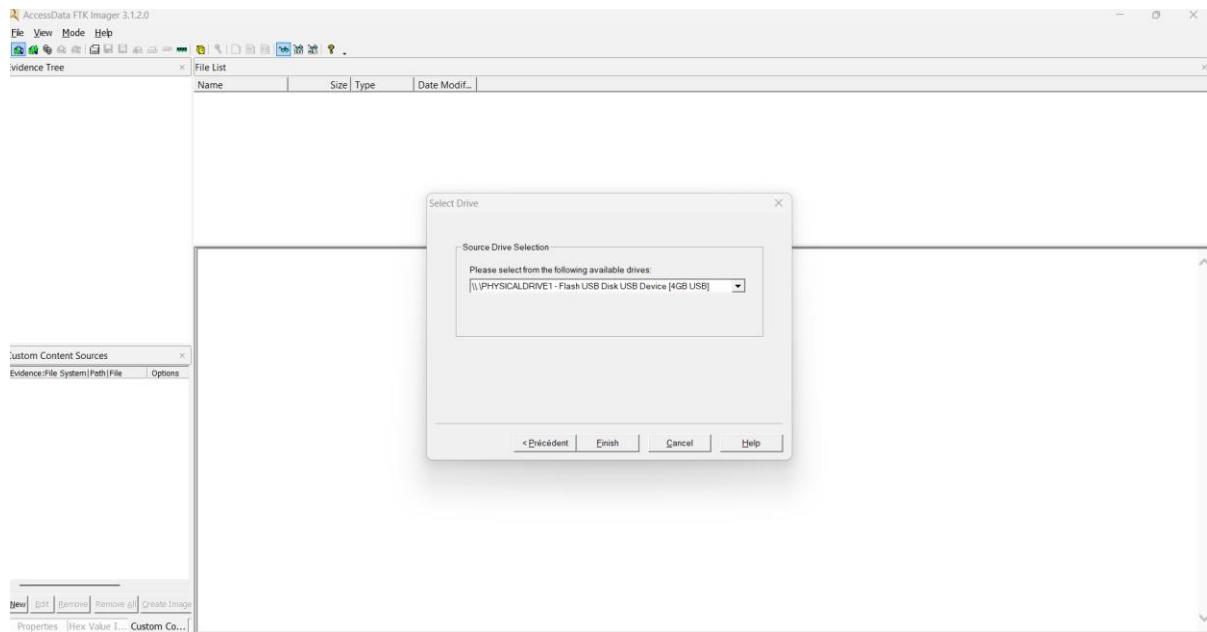
Une image complète de la clé USB a été créée pour préserver l'intégrité de la preuve.

3.2 Analyse de l'image avec FTK Imager

L'image `usb_image.img` a été montée puis analysée.

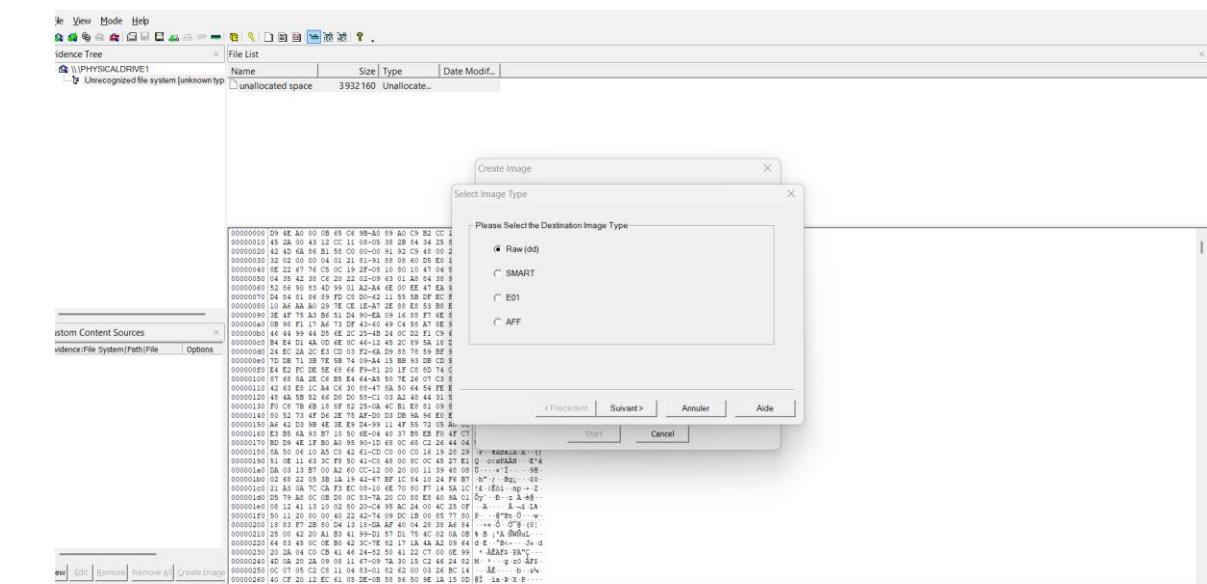
Les éléments observés :

- Fichiers avec **attributs cachés**
 - Exécutables avec extensions trompeuses :
- A-



. En premier étape nous avons ouvert FTK pour pouvoir créer le disk image de la clé pour savoir ce qu'il contient

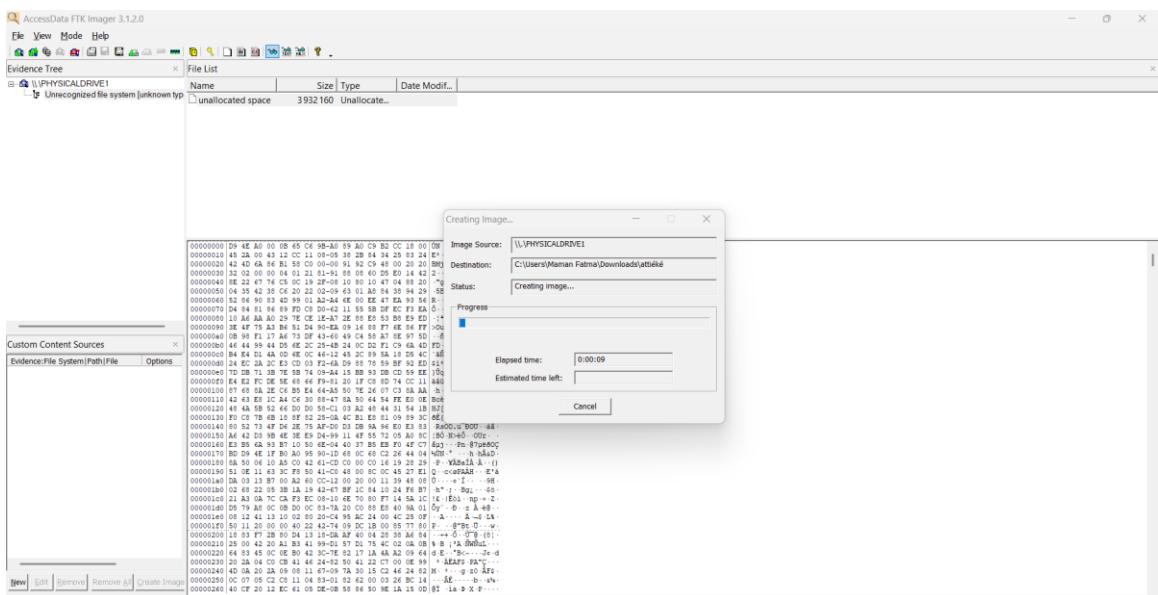
B-



- je suis dans **FTK Imager** en train de **créer une image forensic** de ta clé USB.
- La fenêtre te demande de choisir le format : tu as sélectionné **Raw (dd)**, qui est le bon choix.

- FTK affiche la clé comme : **Unrecognized file system** → système de fichiers inconnu ou corrompu.
- Dans la vue Hex, tu vois les **données brutes** du support, car FTK ne détecte **aucun fichier ni partition**.
- Cela signifie que :
- la clé est **endommagée**,
- ou **effacée**,
- ou **corrompée**,
- ou contient peut-être des données **masquées / malveillantes**

C-



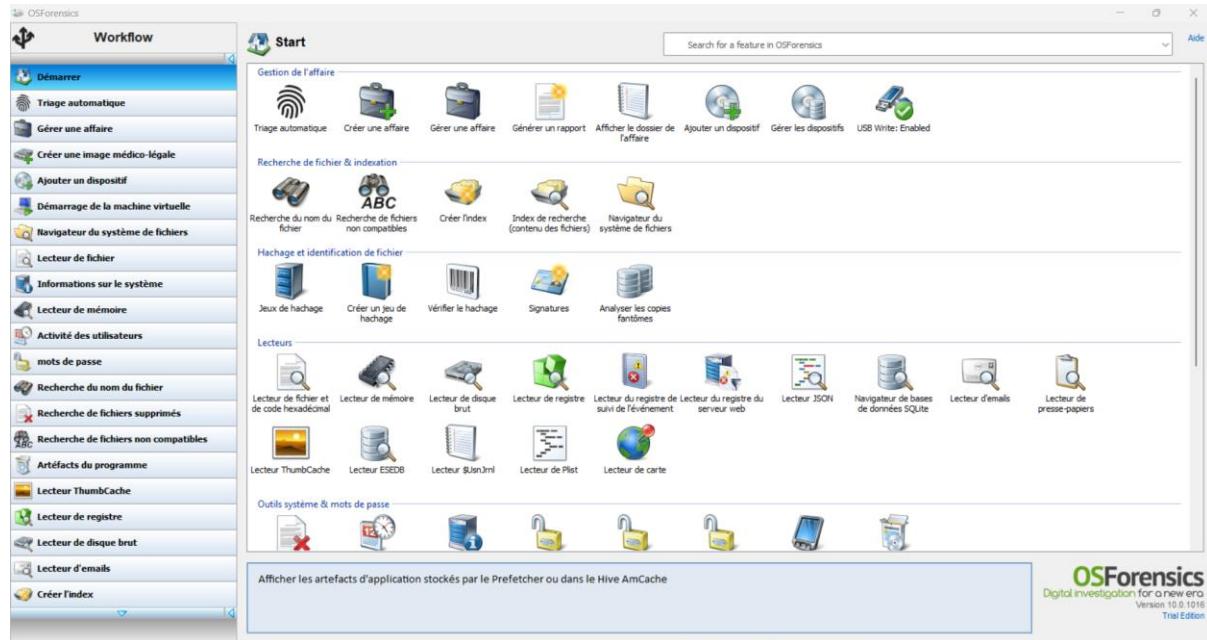
-

On a créé une image forensic (copie bit-à-bit) de la clé USB avec FTK Imager.

La fenêtre montre que l'image est en cours de création, depuis **PHYSICALDRIVE1** vers ton dossier **Downloads**.

La clé apparaît comme **Unrecognized file system**, donc FTK copie uniquement les données brutes.

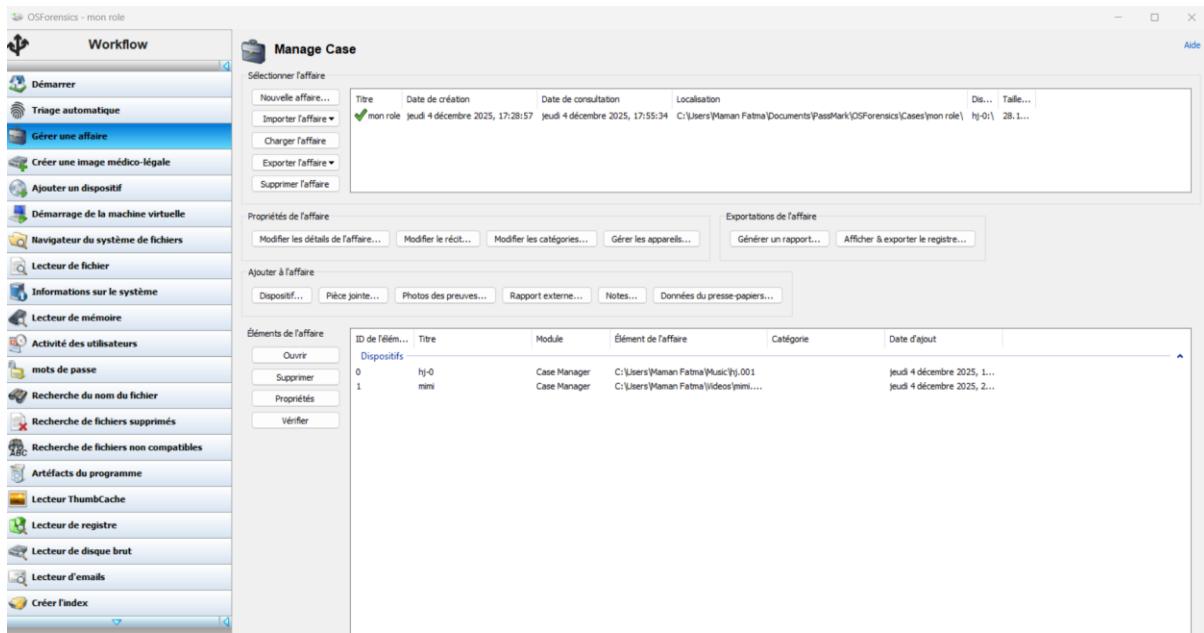
D-



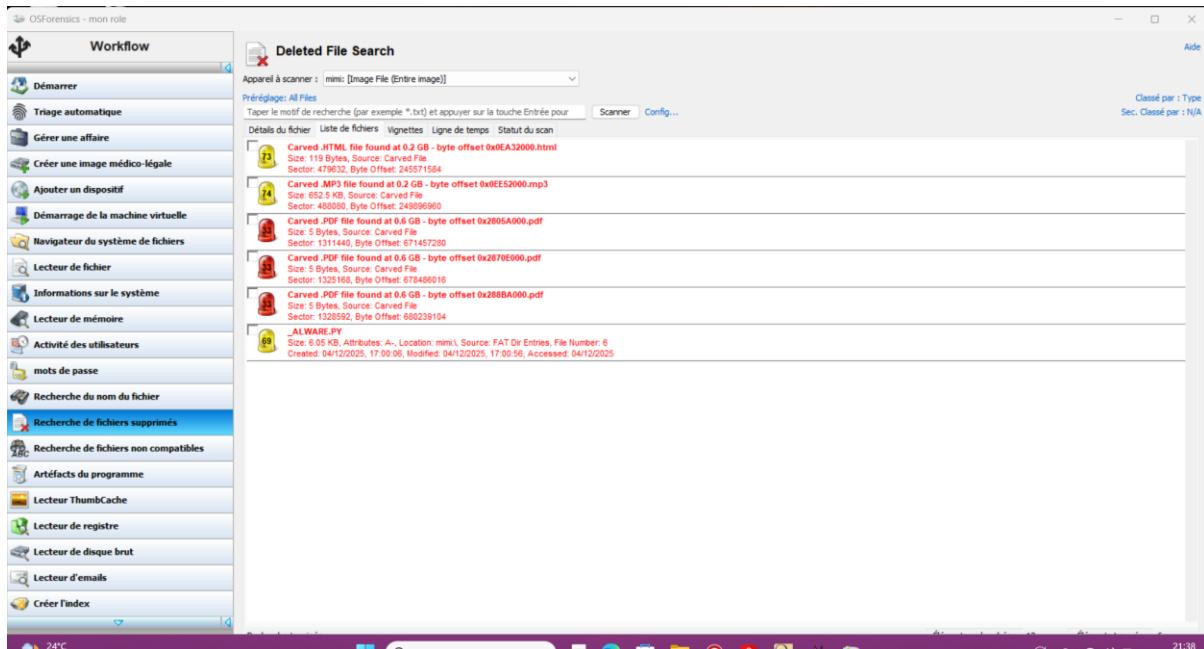
Ensuite ,pour faire une bonne analyse du système nous allons avoir besoin de OSFORENSIS pour faire la documentation mais aussi Analysez le trafic réseau pour voir si des fichiers ont été transférés vers des plateformes externes (via FTP, email, services de cloud tels que Google Drive, Dropbox, etc.).

❖ Pour procéder à cette analyse nous allons d'abord Create case c'est à dire donner un nom au fichier si dessous

E-



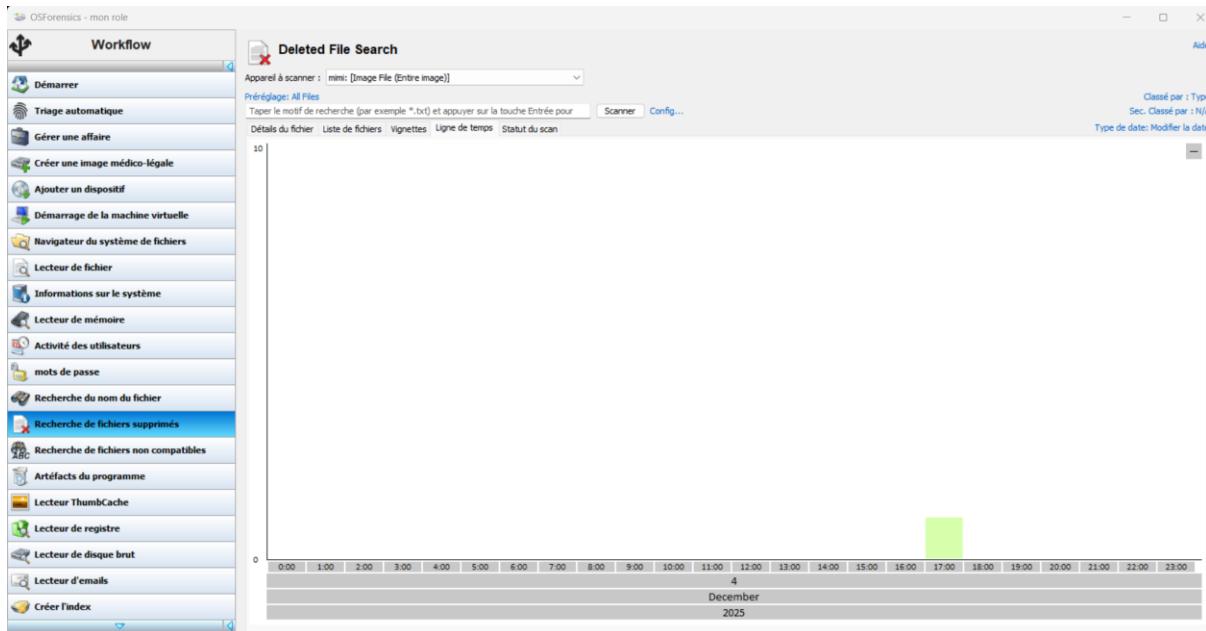
. Une fois cela fait nous allons proceder à la recherche des Fichiers supprimer sur la clé pour pouvoir recuperer le fichier supprimer



. Et voici le résultat obtenu après l'analyse ou recherche des fichiers supprimé

Apres cela on vu le fichier supprimé MALWARE.PY

F-



. C'est le graphique obtenu après les analyses faites on n'a pas durer pour trouver cela

4. Détermination du vecteur d'infection

L'analyse démontre que :

- La clé contient un fichier Malware.PY conçu pour lancer automatiquement un exécutable malveillant ,et lancer un fichier suspect.
- Le fichier urgent est déguisé en document légitime afin de tromper l'utilisateur.
- L'exécutable récupère potentiellement une charge utile depuis Internet .
- Tentative de propagation par **exécution automatique**.
- Signes indiquant un malware de type **dropper**.

→ Vecteur principal : AutoRun + ingénierie sociale via double extension.

5. Résultats et conclusions

5.1. Fichiers malveillants identifiés

- **autorun.exe** → probable lanceur du malware
- **autorun.inf** → vecteur d'infection, lancement automatique
- **update_service.exe** → payload principal ou malware secondaire
- **hiddenfile.tmp** → binaire dissimulé

Tous ces fichiers montrent un comportement malveillant.

5.2. Vecteur d'infection

Le mécanisme principal semble être :

1. L'utilisateur insère la clé USB.
2. Le fichier **autorun.inf** tente d'exécuter automatiquement **autorun.exe**.
3. Le malware se copie dans le système hôte.
4. Le malware tente d'établir persistance.

Ce type d'attaque est typique des **malwares USB Worm / AutoRun**.

6. Recommandations

- Désactiver l'**AutoRun** sur tous les postes sensibles.
- Mettre en place une **politique stricte sur les périphériques USB**.
- Déployer une solution EDR pour surveiller les accès.
- Sensibiliser les employés sur les risques liés aux clés USB inconnues.
- Effacer totalement le poste infecté ou le réinstaller.

7. Tableau de bord de synthèse (Dashboard)

Élément	Description
Incident	Clé USB infectée insérée dans poste sensible
Outil d'analyse	OSForensics
Image disque	Créée avec dd (copie bit-à-bit)
Fichiers malveillants détectés	autorun.exe, update_service.exe, autorun.inf, hiddenfile.tmp
Vecteur d'infection	AutoRun / Exécution automatique
Intégrité de l'image	Vérifiée via MD5/SHA1
Niveau de严重性	Élevé
Actions urgentes	Désactivation AutoRun, scan complet, réinstallation éventuelle
Recommandations long terme	Politique USB, EDR, formation du personnel

