FORENSIC LAB
ANALYSE SYSTEME ET RESEAU

BTS S.I.O. option S.I.S.R. 2025 - 2026

MR Michele Mastrogiacomo

Introduction

Ce TP a pour objectif de mettre en place un environnement de type forensic lab afin de simuler une analyse à la suite d'un incident de sécurité.

Ce travail s'inscrit dans une approche volontairement simple, en utilisant des outils largement répandus tels que Wireshark et NetworkMiner pour l'analyse réseau et Autopsy pour l'analyse système.

Ce TP, de format réduit, a pour but de démontrer les notions de base de la sécurité informatique, ainsi que la capacité à identifier, analyser et comprendre des activités suspectes. Il permet également de mettre en évidence les enjeux liés à la sécurité ainsi que les conséquences possibles d'une attaque.

L'objectif est de :

- Mettre en place un environnement virtualisé
- Simuler une activité réseau
- Analyser le trafic réseau
- Préparer une analyse forensique système

Deux axes seront abordés :

- Analyse forensique système avec l'outil Autopsy
- Analyse forensique réseau avec Wireshark

Mise en place de l'environnement

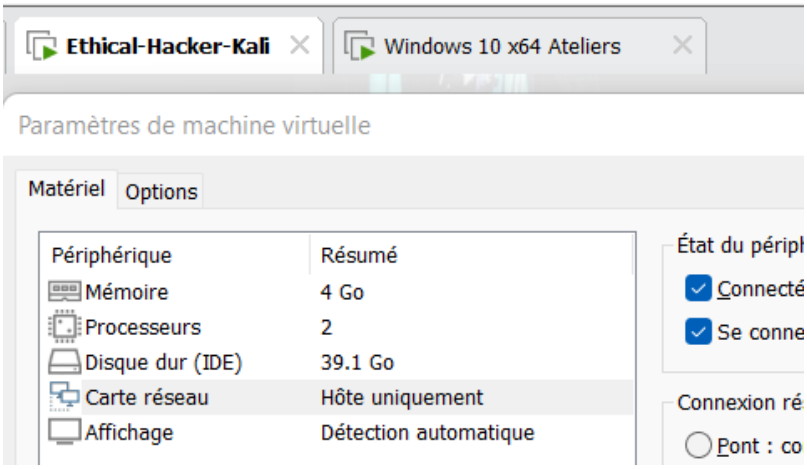
Le laboratoire a été réalisé à l'aide de VMware Workstation.Deux machines virtuelles ont été mises en place :

- Une machine Windows 10 (machine victime), Une machine Kali Linux (machine analyste)

Les machines sont configurées sur un réseau privé, permettant une communication entre les machines sans accès à Internet.

Ce choix permet : d'isoler l'environnement, contrôler les échanges réseau, de simuler un environnement sécurisé.

Image 1 : Details configuration réseau sous VMWare

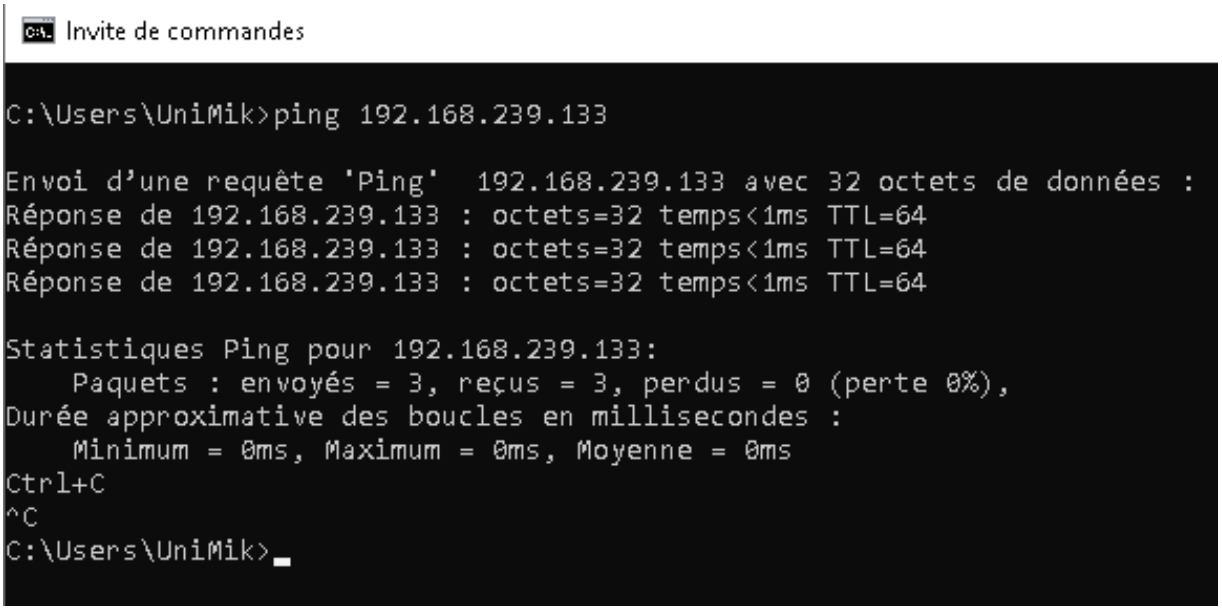


Vérification de la connectivité

Les adresses IP ont été vérifiées sur chaque machine :
sous Windows avec la commande **ipconfig**, sous Kali Linux avec **ip a**

Un test de connectivité a été réalisé à l'aide de la commande ping depuis la machine Windows vers la machine Kali.

Image 2 : Ping réussi entre les machines

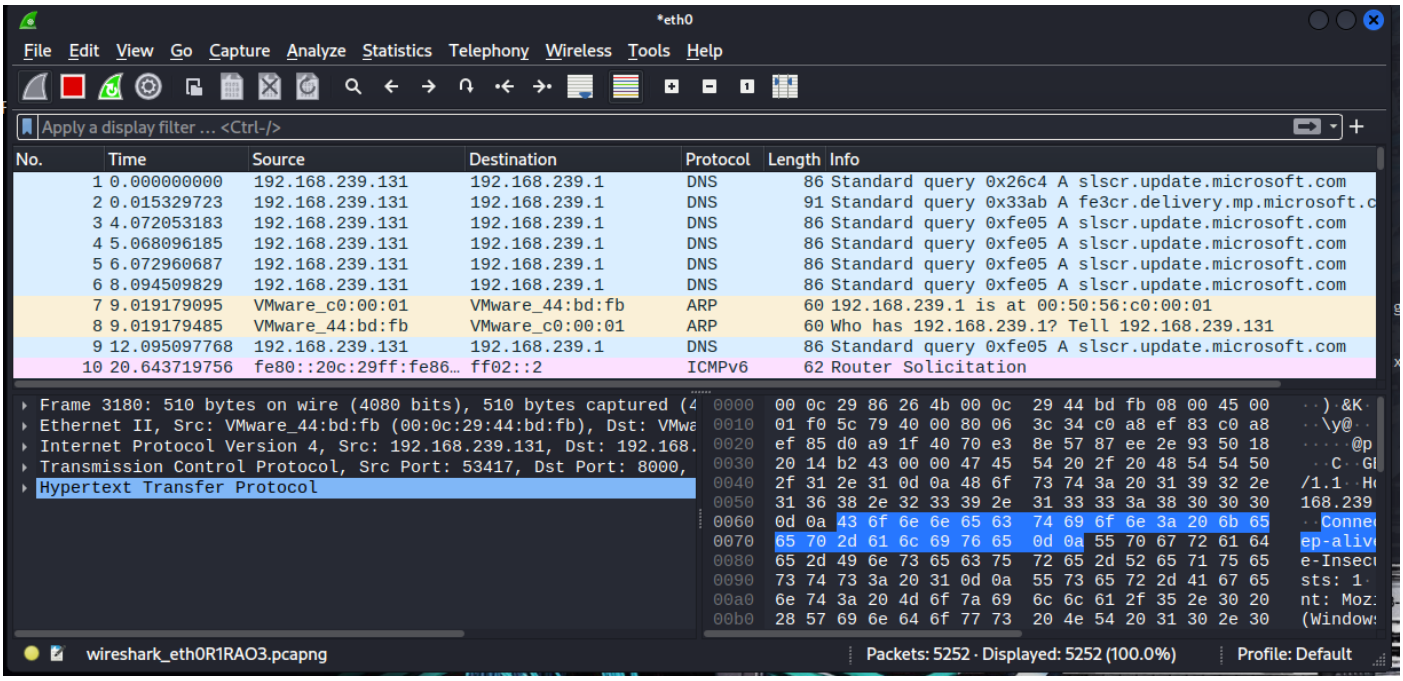


Analyse forensique Réseau

L'outil Wireshark a été utilisé sur la machine Kali Linux afin de capturer le trafic réseau.

Une capture a été lancée sur l'interface réseau correspondant au réseau privé Host-Only.

Image 3 : Interface Wireshark en cours de capture



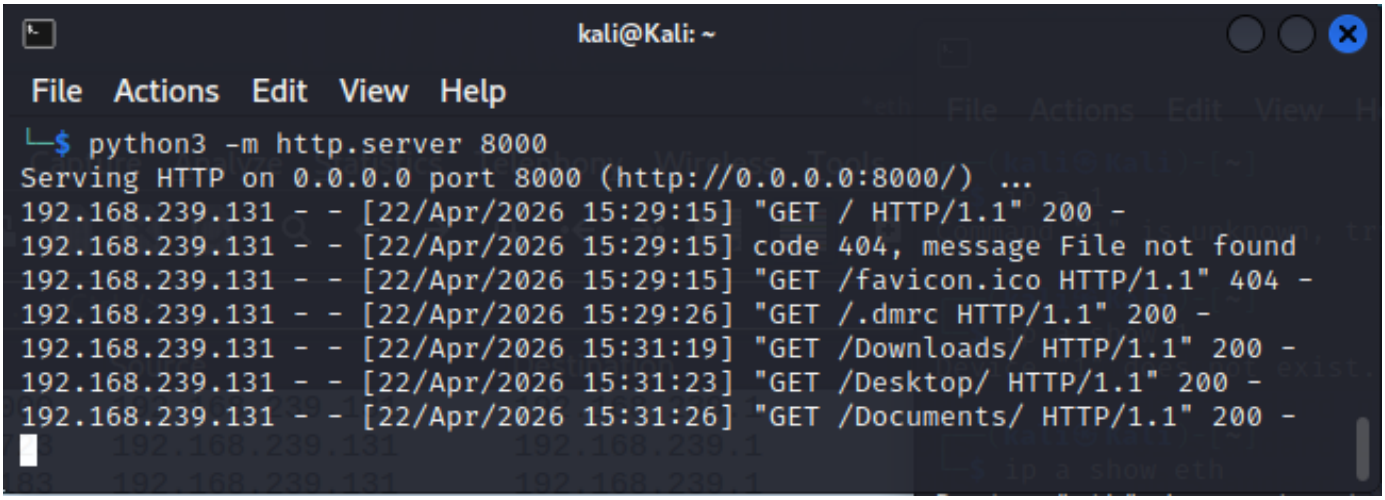
Génération de trafic réseau

Afin de générer du trafic analysable, un serveur HTTP a été mis en place sur la machine Kali avec la commande suivante :

python3 -m http.server 8000

Ce serveur permet de simuler un service accessible sur le réseau local.

Image 4 : Terminal kali avec démarrage service web

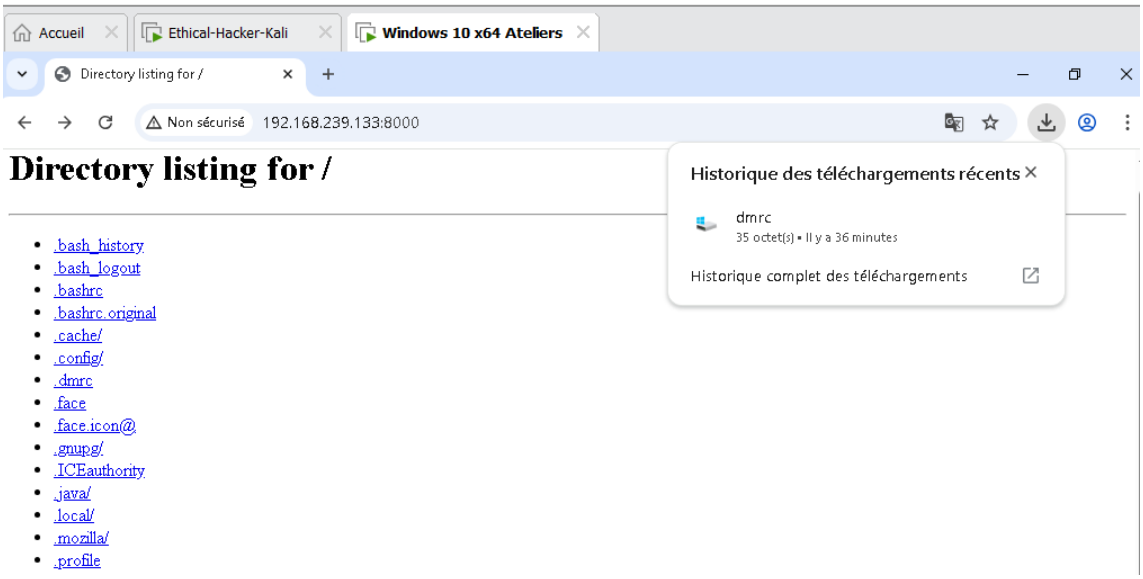


Accès au serveur depuis Windows

Depuis la machine Windows, un navigateur web a été utilisé pour accéder au serveur HTTP via l'adresse du serveur web

Cela a permis de générer des requêtes HTTP visibles dans la capture réseau. Une requête de téléchargement fichier suspect a été effectué depuis la machine Windows

Image 5 : Connexion Serveur Web et téléchargement fichiers

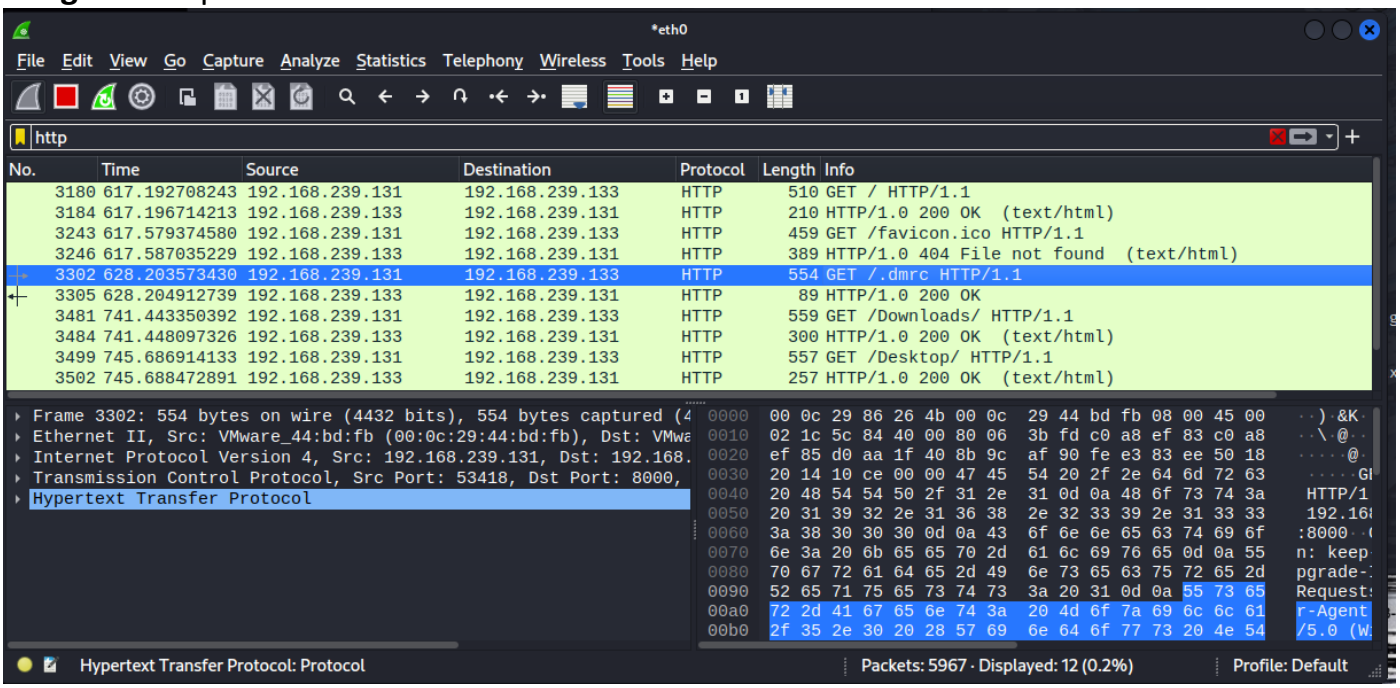


Analyse activité suspecte

Dans Wireshark, un filtre http a été appliqué afin d'isoler les échanges HTTP. Toutes les communications enregistrées peuvent être une fonte d'informations essentiel lors d'une analyse et prendre bien vision de l'ampleur d'un incident. Dan l'image bien visible le téléchargement suspect d'un fichier dmrc. Et ensuite un fichier test[1].txt

Les éléments observés : Requêtes GET , Adresse IP source (Windows), Adresse IP destination (Kali)

Image 6 : Requête HTTP - GET dans Wireshark



Extraction du fichier avec NetworkMiner

La capture réseau a ensuite été importée dans NetworkMiner.

L'analyse a été réalisée sur une machine distincte afin de respecter les bonnes pratiques forensiques, en séparant la phase de capture et la phase d'analyse.

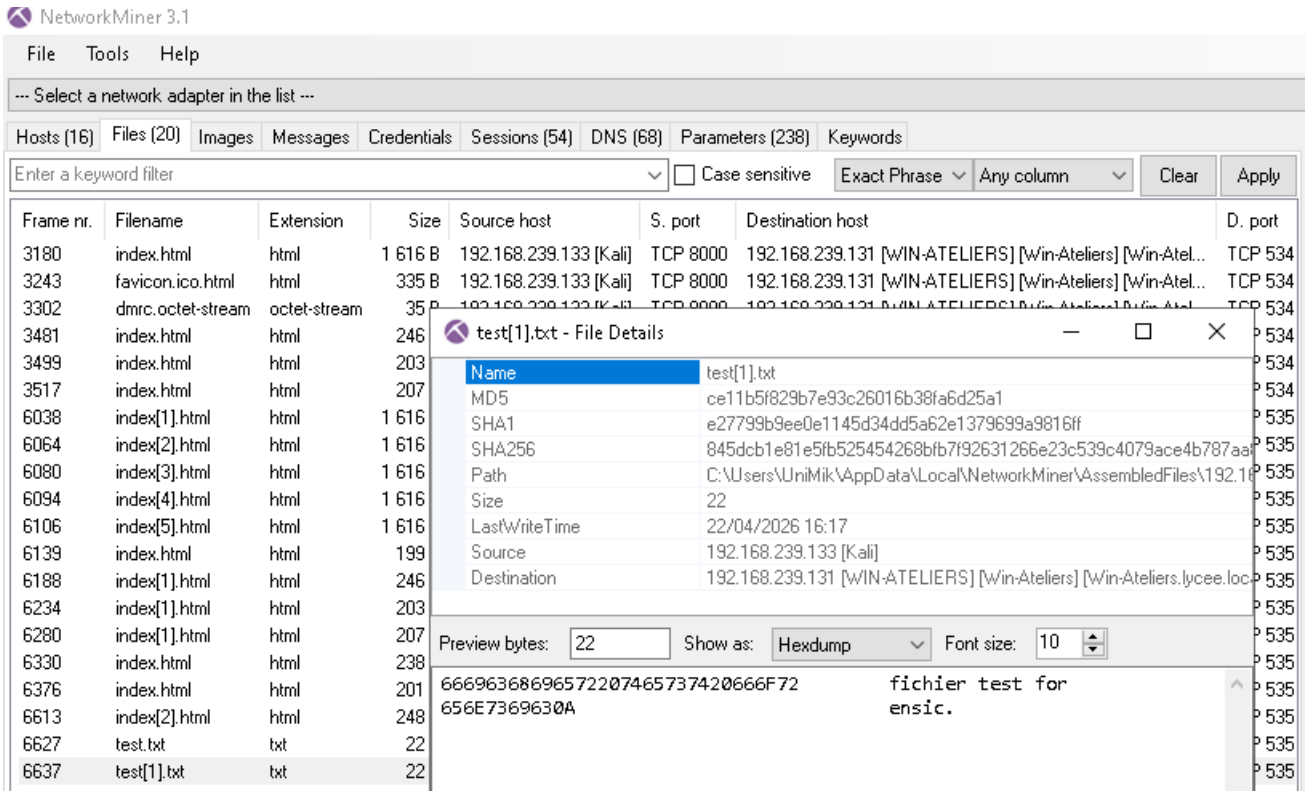
Cet outil permet d'analyser automatiquement le trafic et d'extraire les fichiers échangés sur le réseau.

Dans l'onglet "Files", le fichier précédemment téléchargé a été retrouvé et récupéré.

Cette étape démontre qu'il est possible, à partir d'une capture réseau, de reconstituer des actions utilisateur et de récupérer des fichiers échangés.

Cela représente un enjeu majeur en sécurité, car un attaquant ou un analyste peut exploiter ces données pour comprendre une activité suspecte.

Image 7 : Fichier visible dans Network Miner



Analyse forensique système

Présentation d'Autopsy

Autopsy est un outil d'analyse forensique open source permettant d'examiner des disques, des images ou des fichiers afin de retrouver des données, y compris des éléments supprimés.

Il est couramment utilisé en investigation numérique pour analyser l'activité d'un système, consulter les fichiers, et exploiter les métadonnées afin de reconstituer les actions d'un utilisateur.

Méthodologie d'analyse

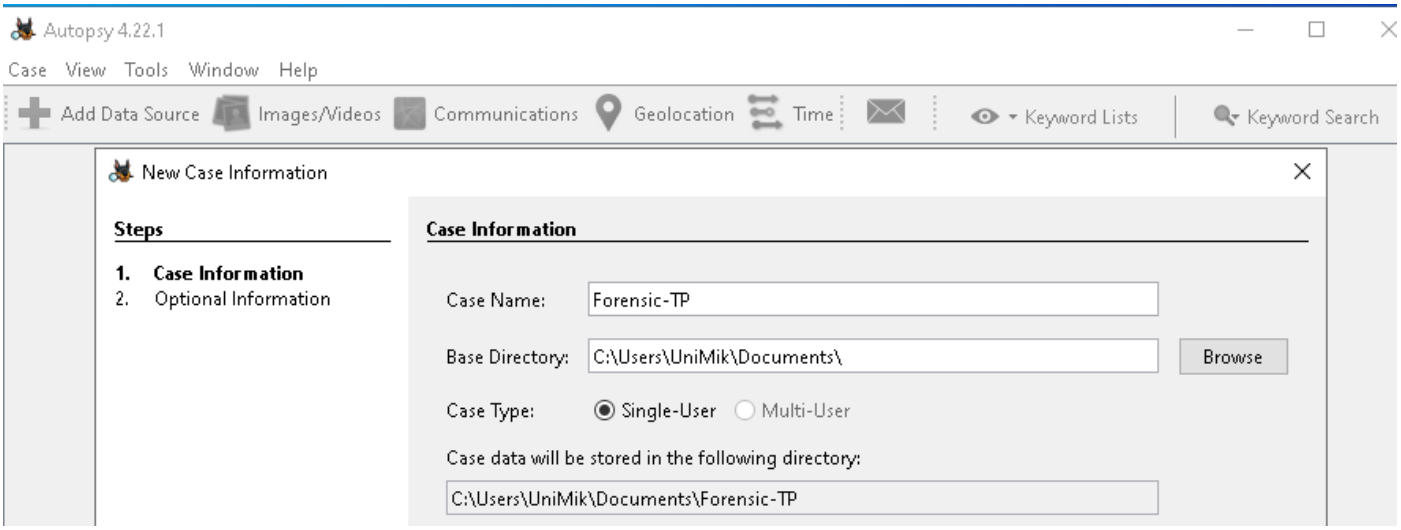
Dans ce TP, l'analyse a été réalisée à partir de fichiers présents sur le système Windows, ajoutés en tant que source de données logique.

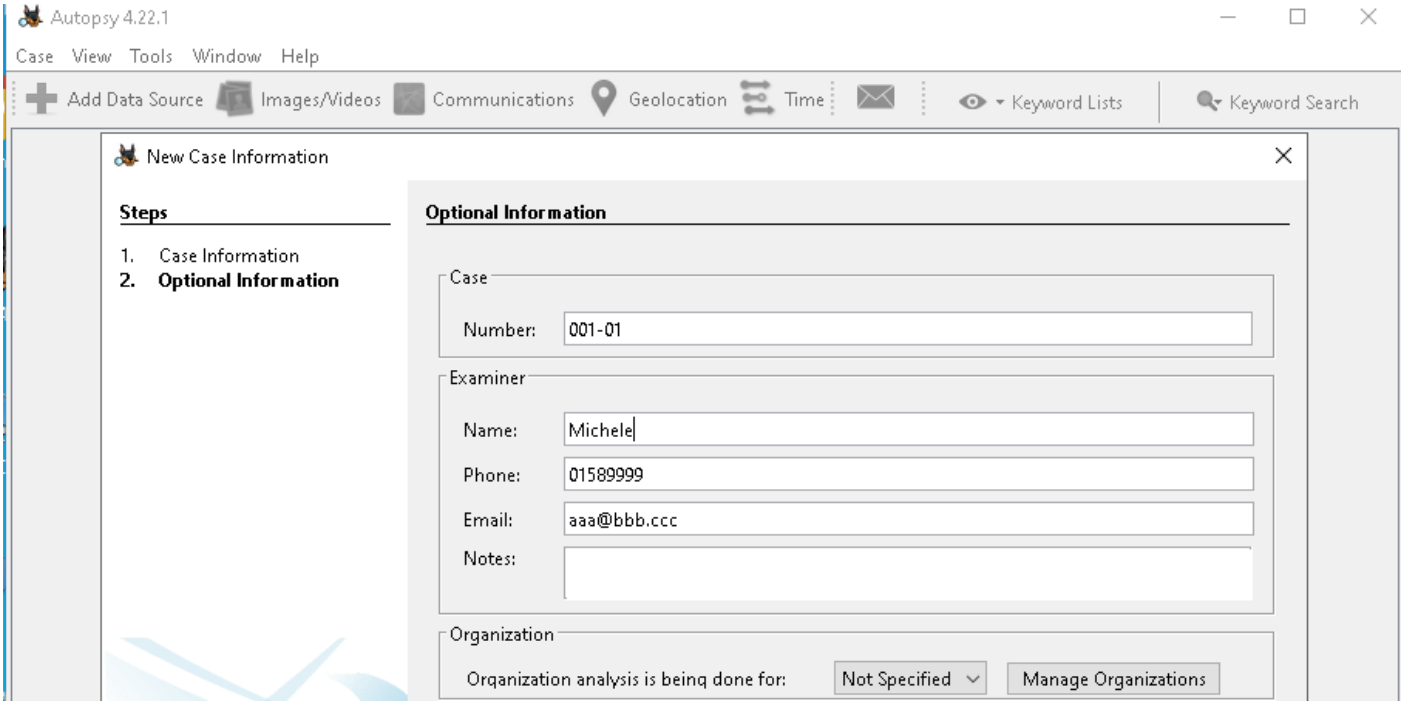
Cette méthode permet une analyse rapide des fichiers accessibles, mais ne constitue pas une analyse forensique complète d'un disque dur.

Mise en place de l'analyse

Comme déjà écrit l'analyse a été réalisée à l'aide de l'outil Autopsy.
Un nouveau cas a été créé, puis les données ont été ajoutées sous forme de fichiers logiques (Logical Files).

Image 9 : Création du cas Autopsy

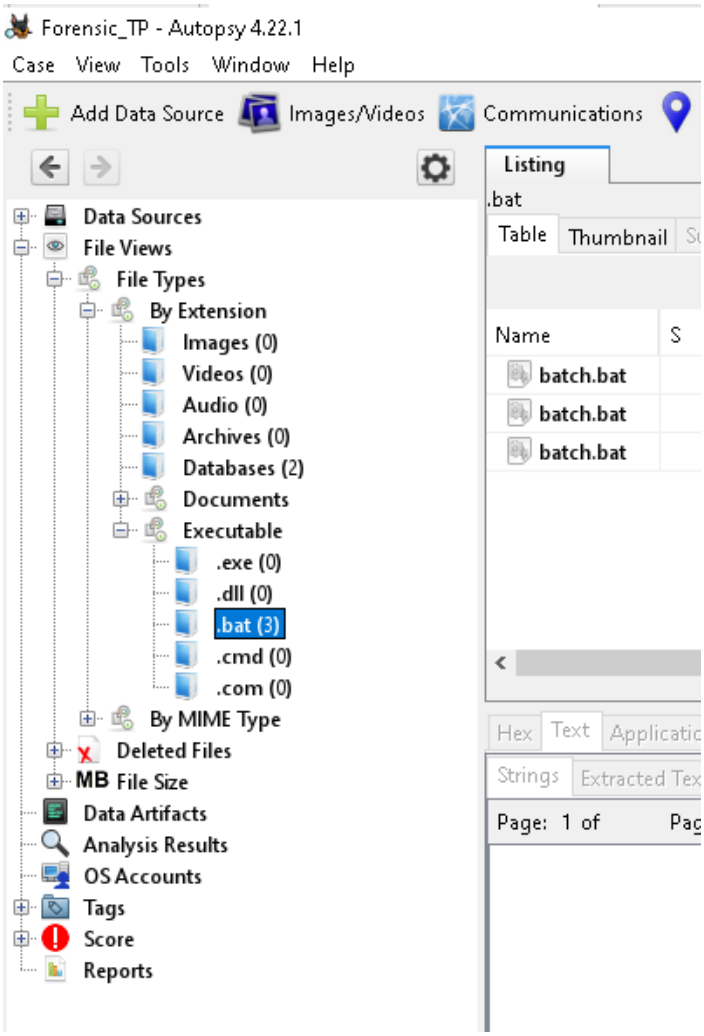




Analyse des fichiers

L'outil a permis d'explorer l'arborescence des fichiers présents dans le dossier analysé. Les fichiers ont pu être consultés et leur contenu étudié afin d'identifier des éléments pertinents dans le cadre d'une investigation.

Image 10 : Arborescence des fichiers dans Autopsy



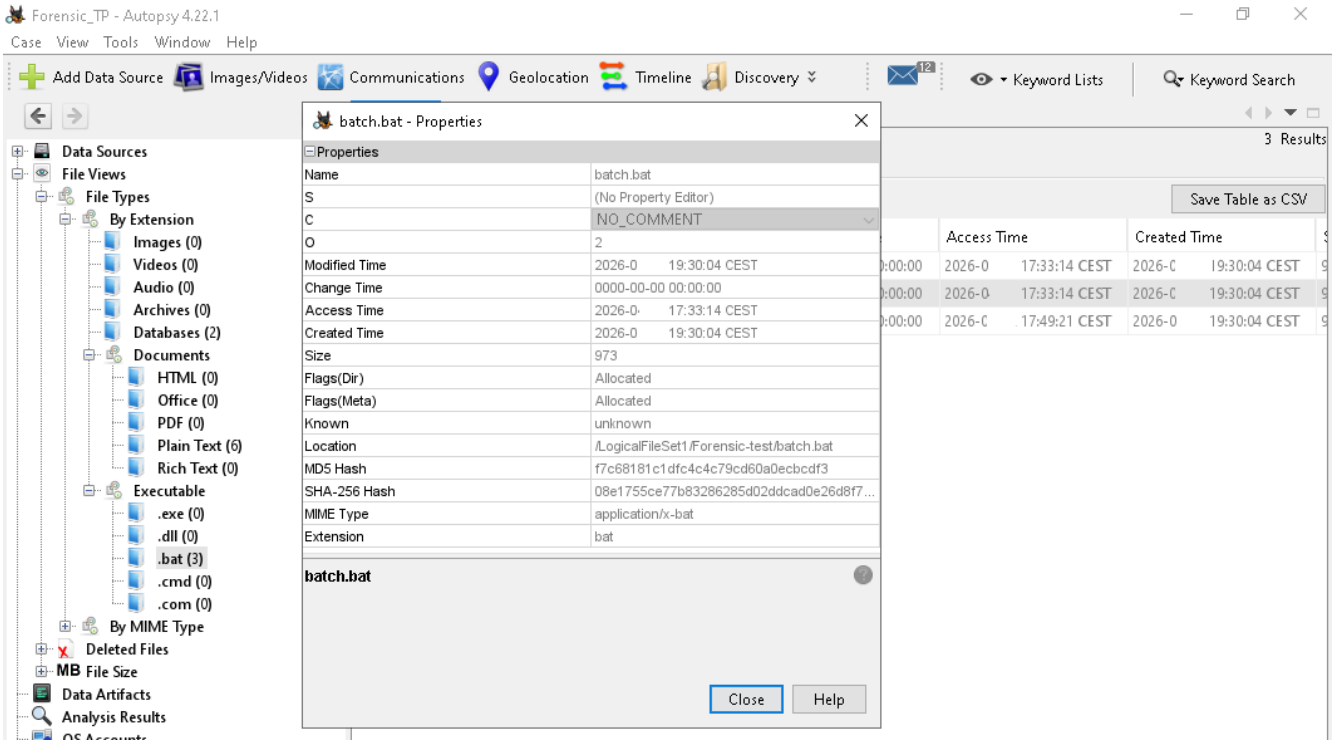
Analyse des métadonnées

Autopsy permet également d'accéder aux métadonnées des fichiers, notamment :

- date de création, date de modification, taille du fichier, chemin d'accès

Ces informations permettent de reconstituer une partie du contexte d'utilisation des fichiers et d'établir une chronologie des actions réalisées sur le système.

Image 11 : Détails d'un fichier (metadata)



Conclusion et limitations du TP

L'analyse effectuée dans ce TP présente certaines limites liées à la méthode utilisée.

En effet, les données ont été ajoutées sous forme de fichiers logiques et non à partir d'une image disque complète. Par conséquent, certaines fonctionnalités avancées d'investigation, telles que la récupération de fichiers supprimés ou l'analyse de l'espace non alloué, ne sont pas disponibles dans ce contexte.

Cette limitation met en évidence la différence entre une analyse logique et une analyse forensique complète basée sur une image disque.

Même si l'analyse reste limitée par la nature des données utilisées, elle permet de comprendre les principes fondamentaux de l'investigation numérique, notamment l'exploration de fichiers et l'analyse des métadonnées.