

FORENSIC LAB

ANALYSE SYSTEME ET RESEAU

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

MR Michele Mastrogiacomo



Introduction

PAG. 2

- Contexte
- Objectifs

Mise en place de l'environnement

PAG. 3

- Machines utilisées
- Vérification de la connectivité

Analyse forensique Réseau

PAG. 4

- Génération de trafic réseau
- Téléchargement fichier
- Analyse activité suspecte
- Analyse avec NetworkMiner

Analyse forensique système

PAG. 7

- Présentation d'Autopsy
- Analyse des fichiers
- Analyse des métadonnées

Conclusion et limitations du TP

PAG. 10

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

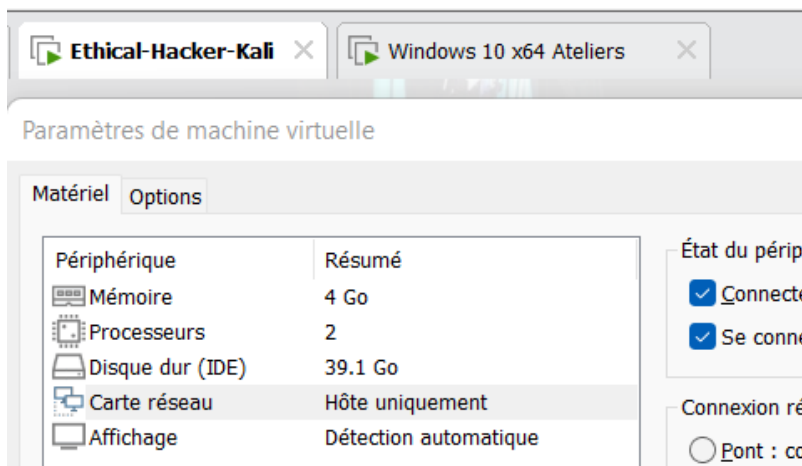
Le laboratoire a été réalisé à l'aide de VMware Workstation. Deux machines virtuelles ont été mises en place :

- 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 : Détails 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

```
C:\Users\UniMik>ping 192.168.239.133

Envoi d'une requête 'Ping' 192.168.239.133 avec 32 octets de données :
Réponse de 192.168.239.133 : octets=32 temps<1ms TTL=64
Réponse de 192.168.239.133 : octets=32 temps<1ms TTL=64
Réponse de 192.168.239.133 : octets=32 temps<1ms TTL=64

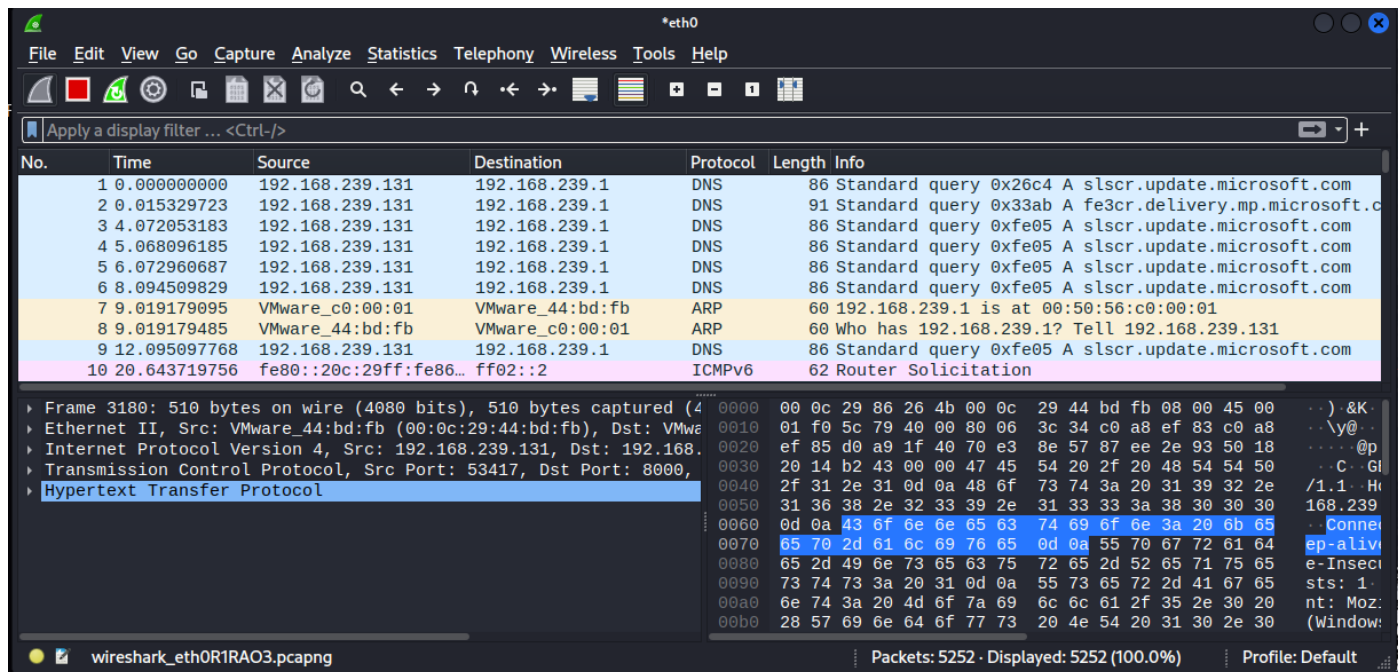
Statistiques Ping pour 192.168.239.133:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
Ctrl+C
^C
C:\Users\UniMik>
```

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



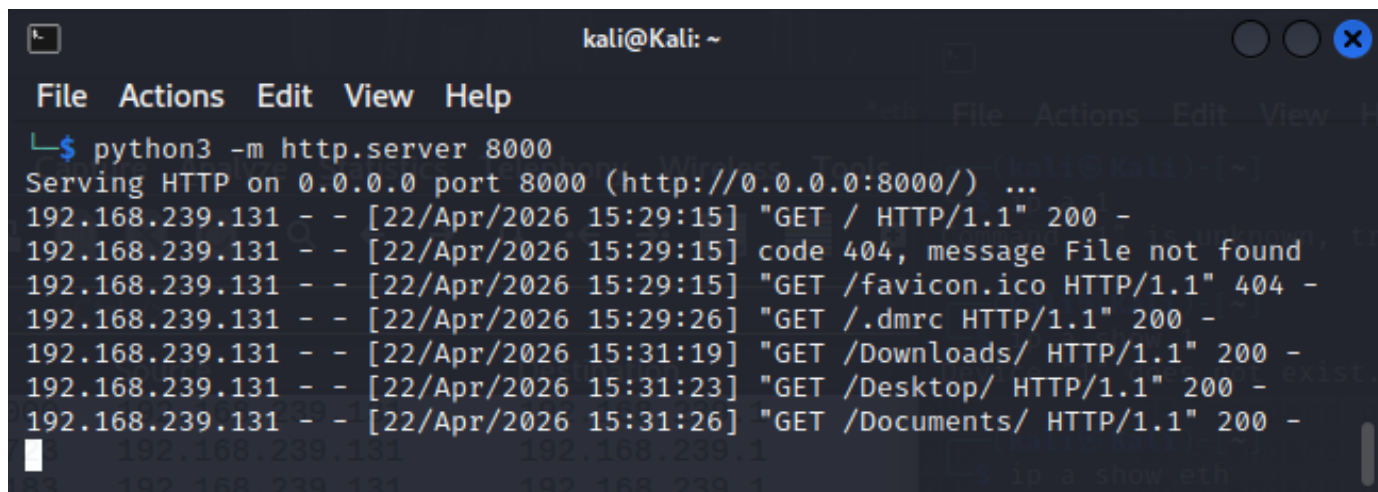
Génération de trafic réseau

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

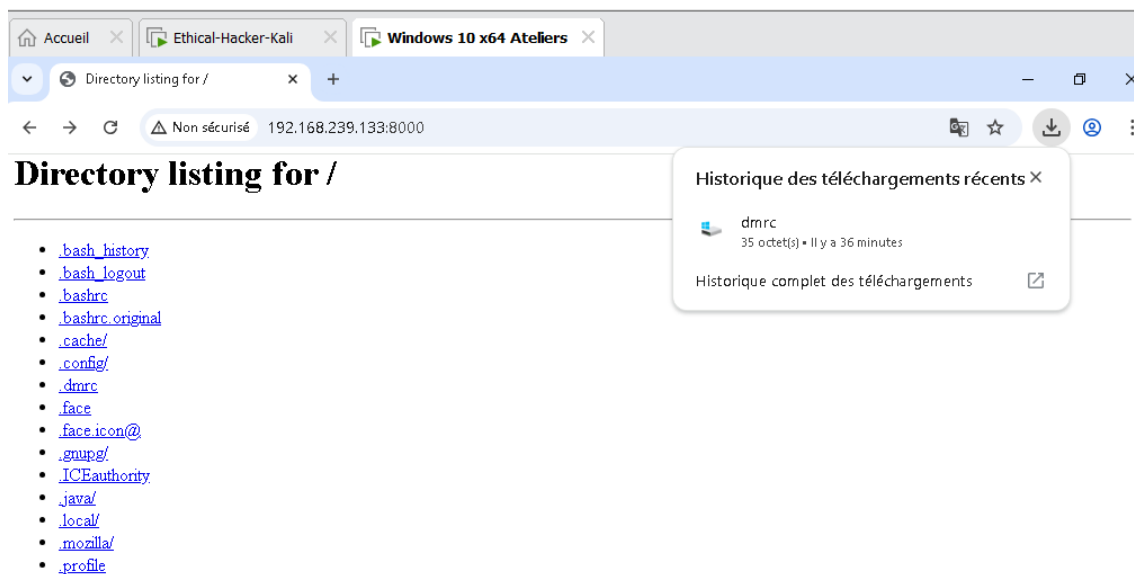


Accès au serveur depuis Windows

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 effectuée depuis la machine Windows

Image 5 : Connexion Serveur Web et téléchargement fichiers

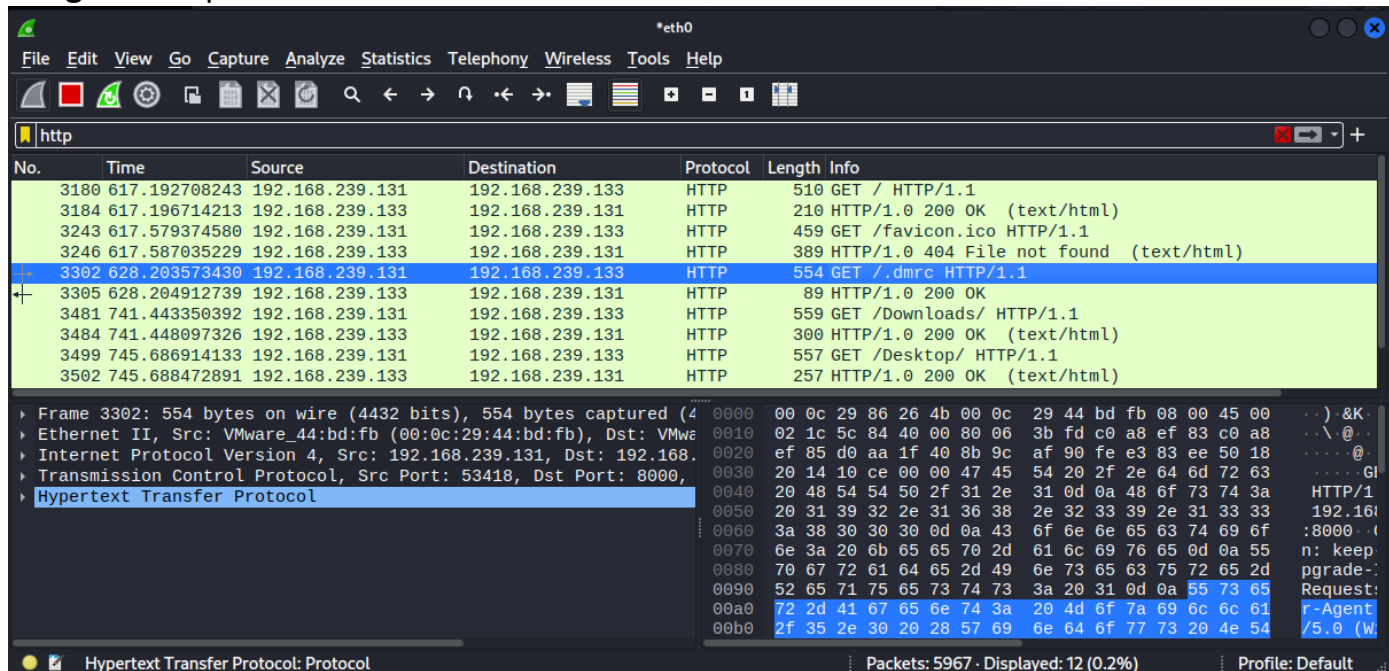


Analyse activité suspecte

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

The screenshot shows the NetworkMiner 3.1 application interface. At the top, there is a menu bar with 'File', 'Tools', and 'Help'. Below it is a dropdown menu for selecting a network adapter. The main area displays a list of files with columns for Frame nr., Filename, Extension, Size, Source host, S. port, Destination host, and D. port. A modal window titled 'test[1].txt - File Details' is open, showing the file's metadata and a hex dump of its content.

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port
3180	index.html	html	1 616 B	192.168.239.133 [Kali]	TCP 8000	192.168.239.131 [WIN-ATELIERS] [Win-Ateliers] [Win-Atel...	TCP 534
3243	favicon.ico.html	html	335 B	192.168.239.133 [Kali]	TCP 8000	192.168.239.131 [WIN-ATELIERS] [Win-Ateliers] [Win-Atel...	TCP 534
3302	dmrc.octet-stream	octet-stream	35 B	192.168.239.133 [Kali]	TCP 8000	192.168.239.131 [WIN-ATELIERS] [Win-Ateliers] [Win-Atel...	TCP 534
3481	index.html	html	246				534
3499	index.html	html	203				534
3517	index.html	html	207				534
6038	index[1].html	html	1 616				535
6064	index[2].html	html	1 616				535
6080	index[3].html	html	1 616				535
6094	index[4].html	html	1 616				535
6106	index[5].html	html	1 616				535
6139	index.html	html	199				535
6188	index[1].html	html	246				535
6234	index[1].html	html	203				535
6280	index[1].html	html	207				535
6330	index.html	html	238				535
6376	index.html	html	201				535
6613	index[2].html	html	248				535
6627	test.txt	txt	22				535
6637	test[1].txt	txt	22				535

Name	Value
MD5	ce11b5f829b7e93c26016b38fa6d25a1
SHA1	e27799b9ee0e1145d34dd5a62e1379699a9816ff
SHA256	845dcb1e81e5fb525454268bf7f92631266e23c539c4079ace4b787aa
Path	C:\Users\UniMik\AppData\Local\NetworkMiner\AssembledFiles\192.168.239.133\3481\index.html
Size	22
LastWriteTime	22/04/2026 16:17
Source	192.168.239.133 [Kali]
Destination	192.168.239.131 [WIN-ATELIERS] [Win-Ateliers] [Win-Ateliers.lycee.occid...

Preview bytes: 22 Show as: Hexdump Font size: 10

```
66696368696572207465737420666F72          fichier test for
656E7369630A                                ensic.
```

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.

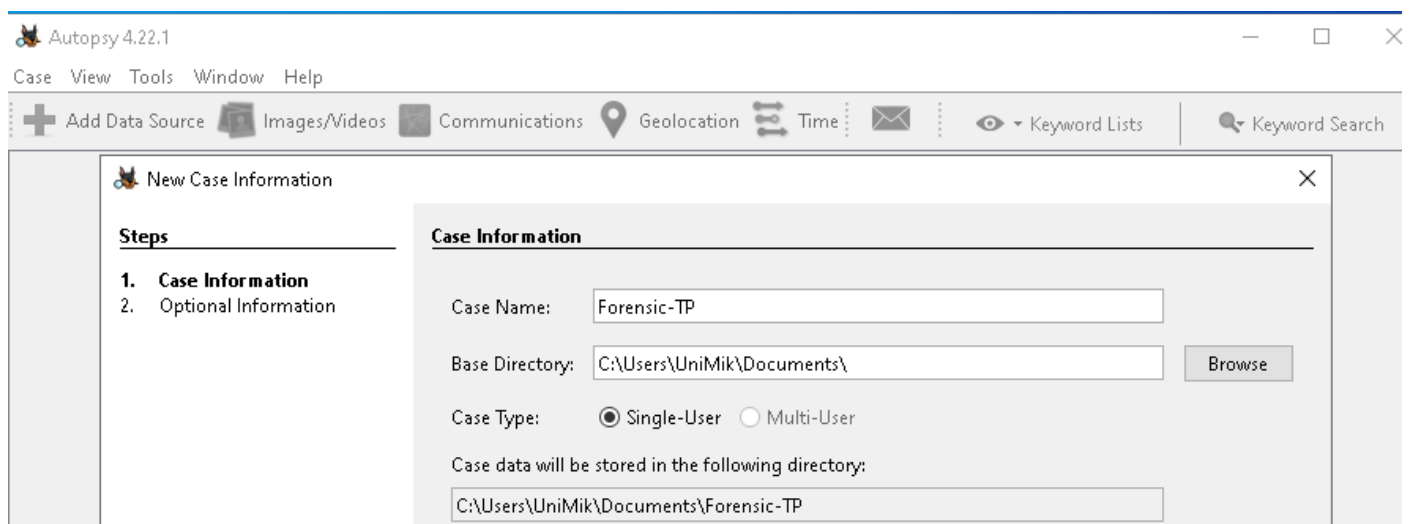
Cette méthode permet une analyse rapide des fichiers accessibles, mais ne constitue pas une analyse forensique complète d'un disque dur.

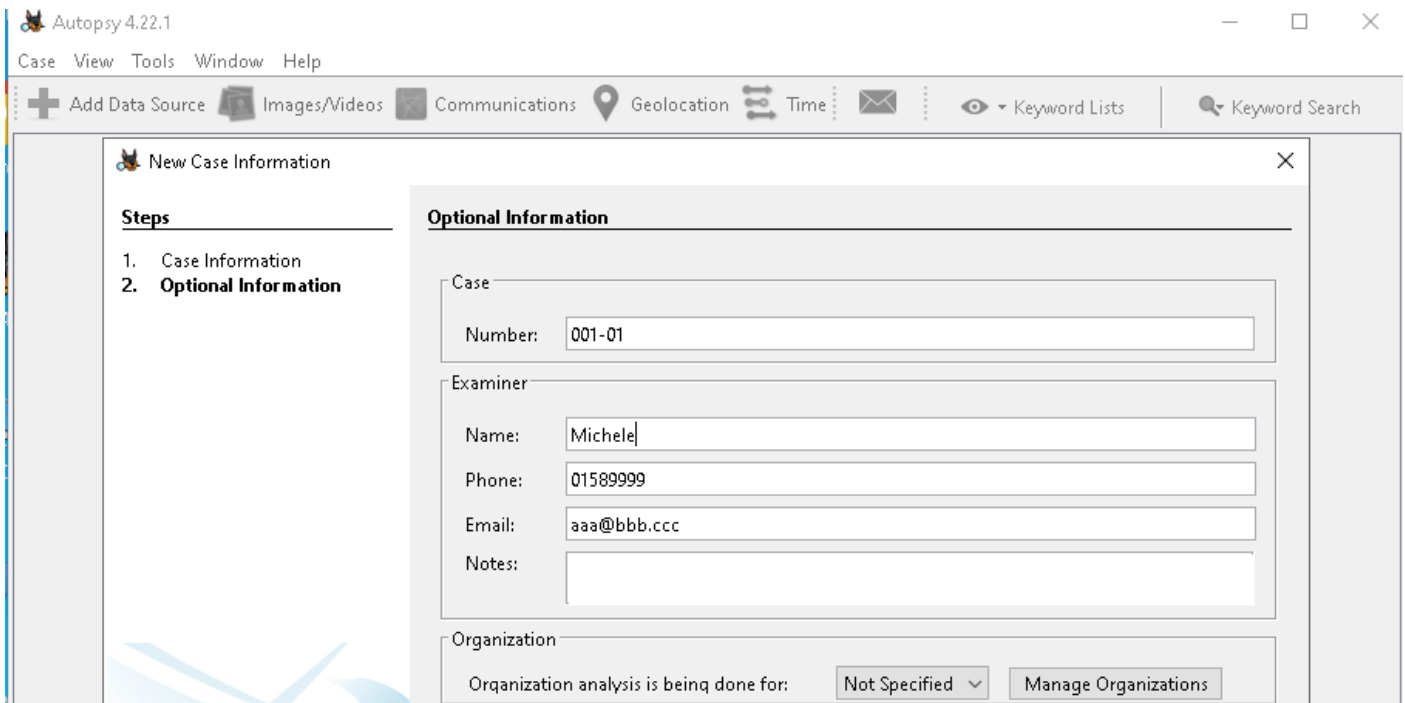
Mise en place de l'analyse

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

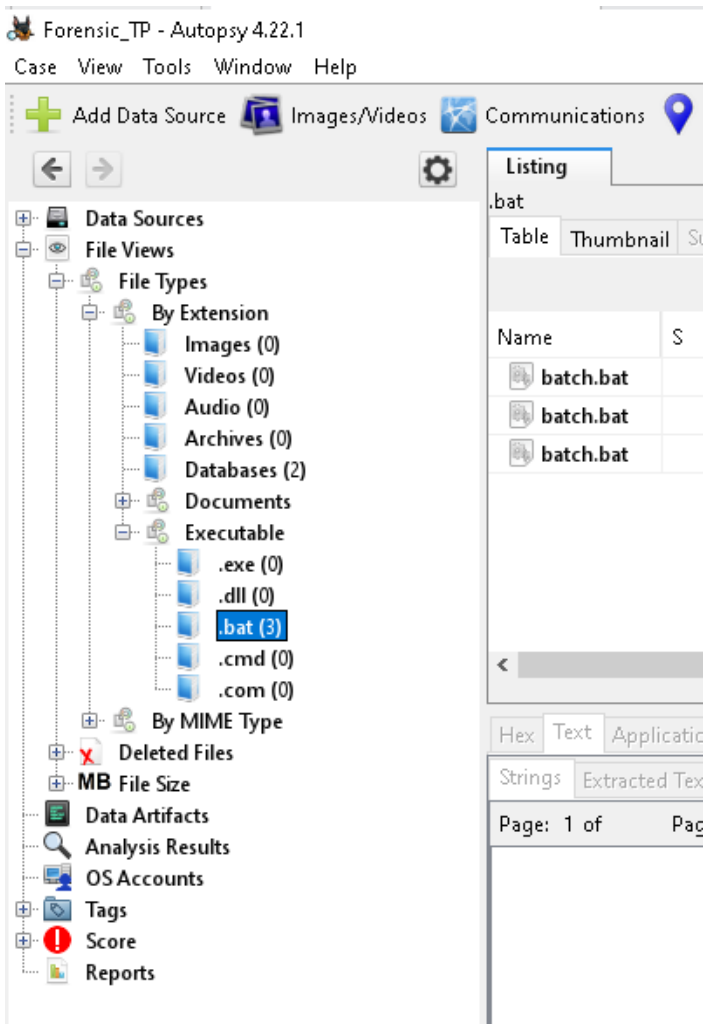




Analyse des fichiers

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)

The screenshot displays the Autopsy 4.22.1 interface. On the left, a tree view shows 'Data Sources' and 'File Views'. Under 'File Views', 'By Extension' is expanded, showing categories like 'Images (0)', 'Videos (0)', 'Audio (0)', 'Archives (0)', 'Databases (2)', 'Documents', and 'Executable'. The 'Executable' category is further expanded to show file types: '.exe (0)', '.dll (0)', '.bat (3)', '.cmd (0)', and '.com (0)'. The main window shows the 'batch.bat - Properties' dialog box. The 'Properties' tab is active, displaying the following metadata:

Property	Value
Name	batch.bat
S	(No Property Editor)
C	NO_COMMENT
O	2
Modified Time	2026-0 19:30:04 CEST
Change Time	0000-00-00 00:00:00
Access Time	2026-0 17:33:14 CEST
Created Time	2026-0 19:30:04 CEST
Size	973
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Known	unknown
Location	I:LogicalFileSet1\Forensic-test\batch.bat
MD5 Hash	f7c68181c1dfc4c4c79cd60a0ecbcd3
SHA-256 Hash	08e1755ce77b83286285d02ddcad0e26d8f7...
MIME Type	application/x-bat
Extension	bat

Below the properties, the file content is displayed as 'batch.bat'. In the background, a search results table is visible with columns for 'Access Time' and 'Created Time', showing three results for the file.

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.