COMPUTER FORENSICS

Analyse approfondie d’images de clé USB et disque dur avec : FTK Imager, Autopsy, Registry Explorer et OSForensics

Travail réalisé par :

EL HANAFI Maha

Objectif : L'objectif de ce rapport c'est de faire une analyse approfondie d'une image créer en utilisant des outils de l'analyse forensique.

TP1 : l'analyse forensique d'une clé USB

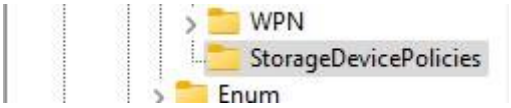
Acquisition d'une image USB

1. FTK imager
2. Image USB
3. dc3dd

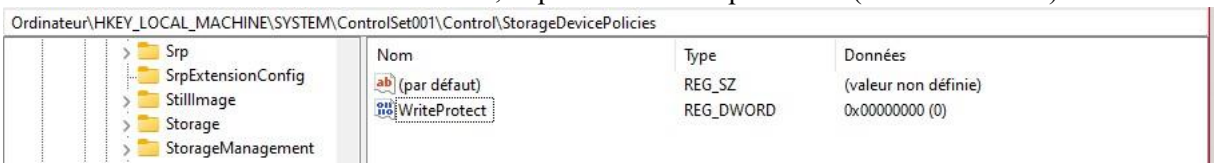
Etape 0 : Installation des outils : FTK imager, Autopsy
Etape 1 : création d'un WriteBlocker software Objectifs :

- Éviter d'une personne ne soit écrite sur la clé USB préserve toutes les données de la clé • Éviter la corruption de la clé.

Les étapes pour créer un WriteBlocker : réaliser un WriteBlocker logiciel pour bloquer l'accès à clé USB c'est-à-dire on aura seulement le droit de la lecture.
Sur Windows, Allons à la base de registre (tapant dans la barre de recherche éditeur de Registre) , cherchons SYSTEM, ❾CurrentControlSet, ❾control, au niveau de ce chemin on va créer une nouvelle clé :

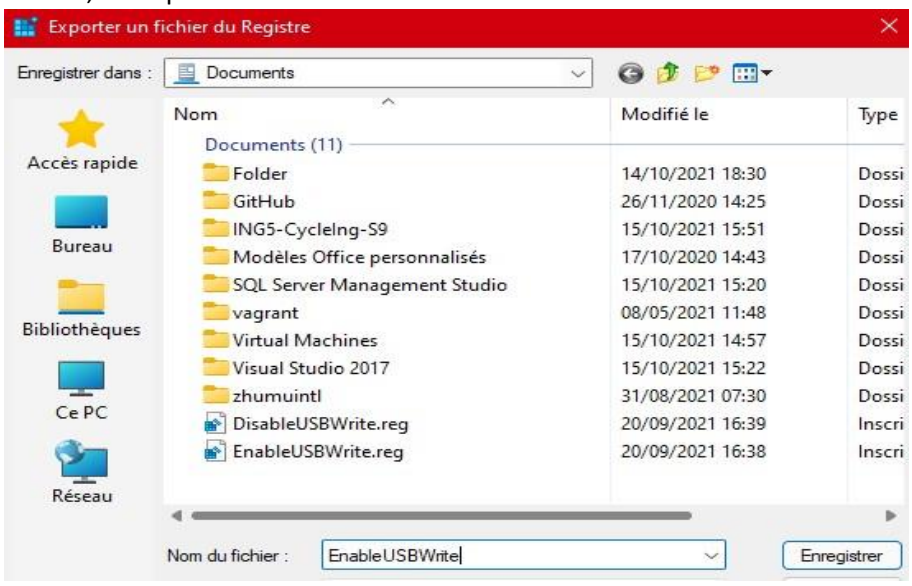


Au niveau de chemin on va créer une nouvelle clé de type DWORD (32 bits) : « WriteProtect », comme la Screenshot ci-dessous le montre, la protection n'est pas active (la valeur c'est 0)

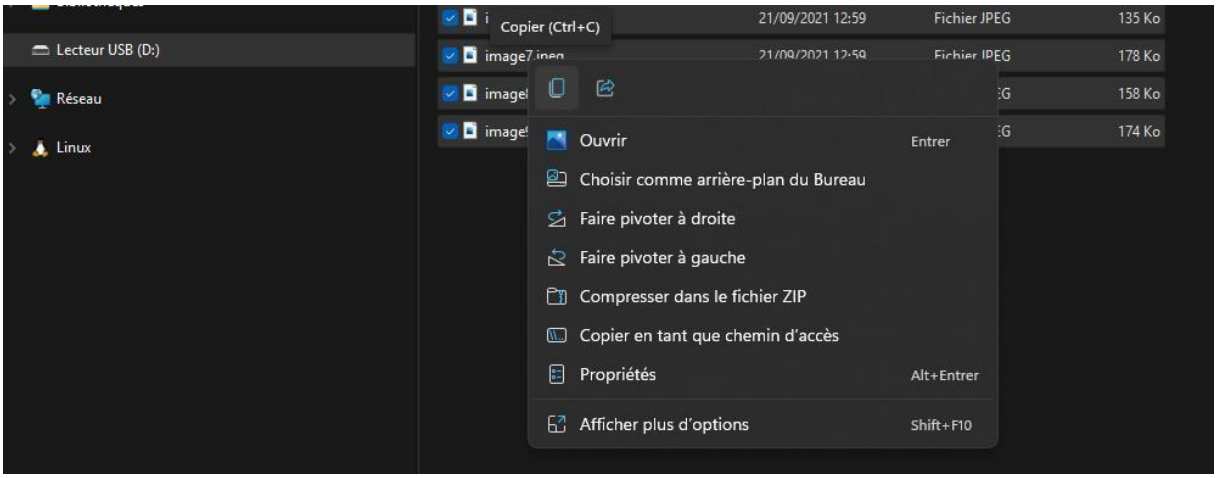


Dans ce cas, je vais l'activer en la donnant la valeur 1 automatiquement la protection sera active.

Ensuite, on exporte la clé

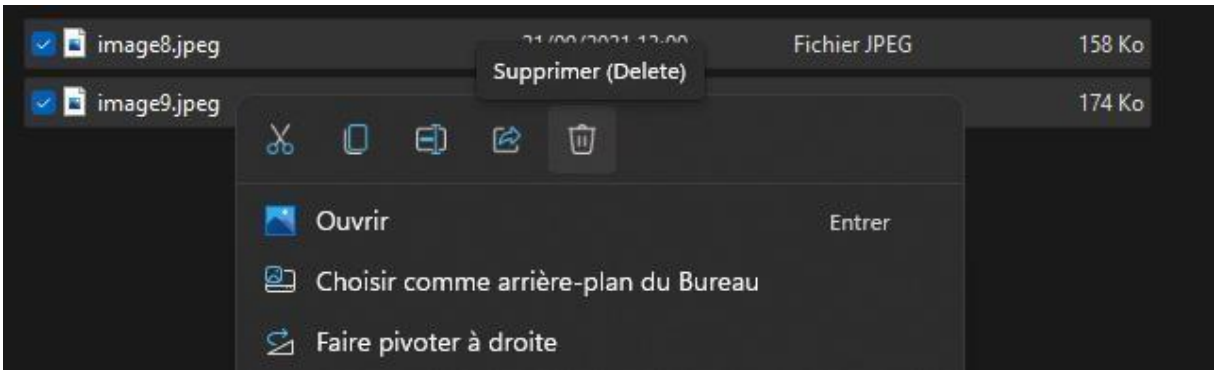


-On branche une clé USB et on vérifie les droits d'accès :
comme la Screenshot ci-dessous le montre, je ne peux ni supprimer les fichiers sélectionnés ni créer un nouveau.



-Ensuite si je clique sur « DisableUsbWrite » sa valeur est 0, c'est-à-dire je désactive la protection et j'aurai l'accès à la clé USB du coup je peux modifier ou supprimer le contenu de cette clé.

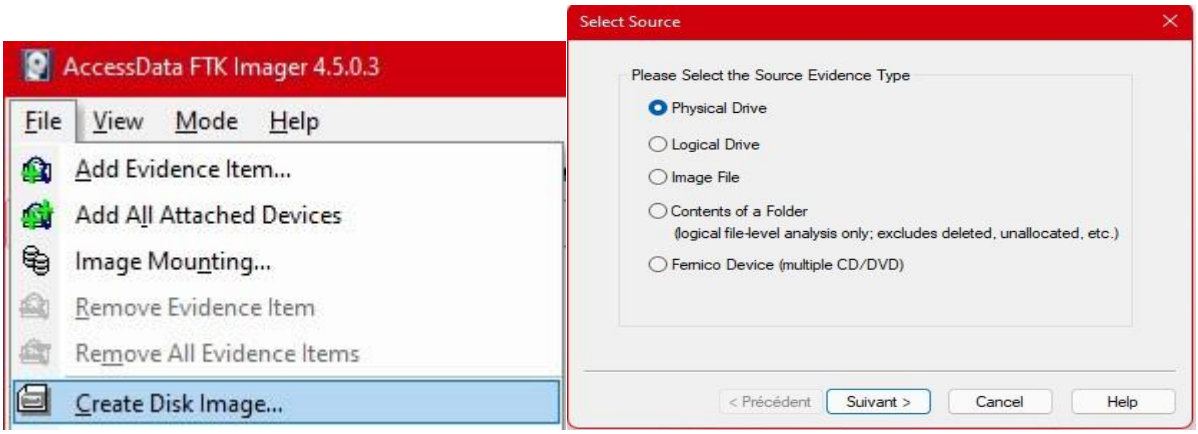
-Apres que je branche la clé USB, comme le Screenshot ci-dessous le montre, je peux supprimer les fichiers.



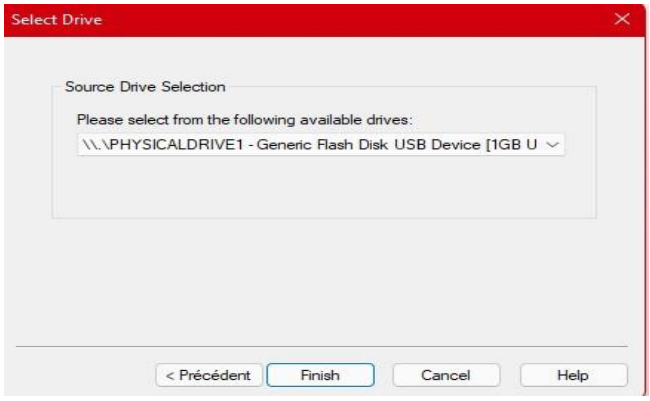
La création d'une image de la clé USB en utilisant FTK imager

FTK Imager est un outil d'aperçu et d'imagerie de données utilisé pour acquérir des données (preuves) d'une manière solide sur le plan médico-légal en créant des copies de données sans apporter de modifications aux preuves originales. Après avoir créé une image des données, utilisez Forensics Toolkit pour effectuer un examen médico-légal approfondi et créer un rapport de vos conclusions.

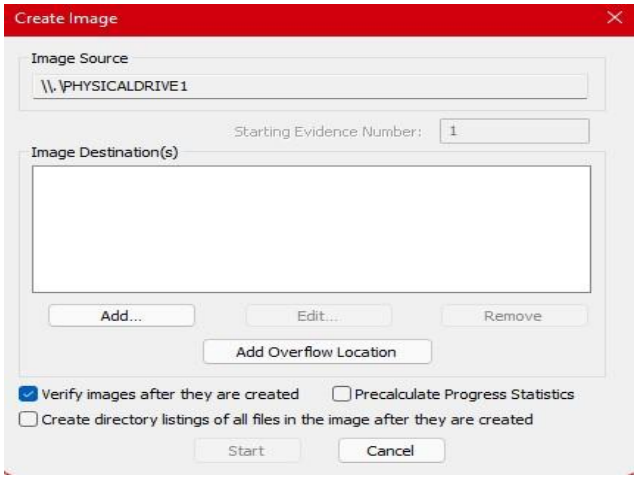
Dans cette étape, nous allons utiliser **FTK imager**. Ce dernier est un outil d'acquisition d'images. Il est possible de faire une image d'un disque dur, d'une clé USB etc. avant d'en récupérer les données.
❾Voici les étapes qui montrent la création d'une image de clé USB :



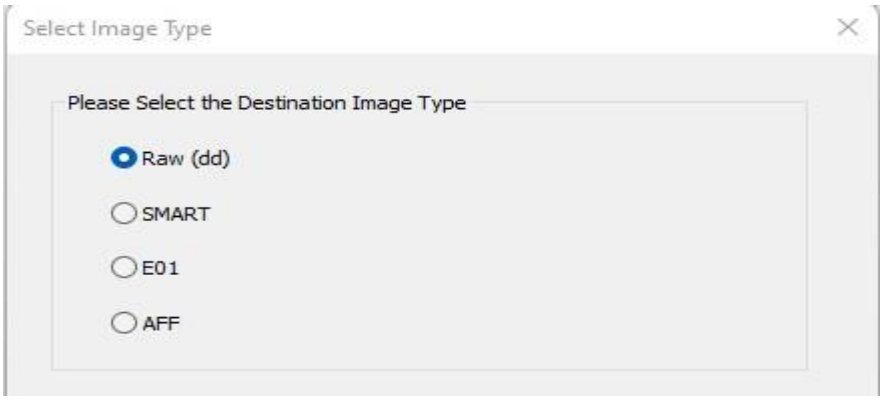
-Après on sélectionne la clé USB :



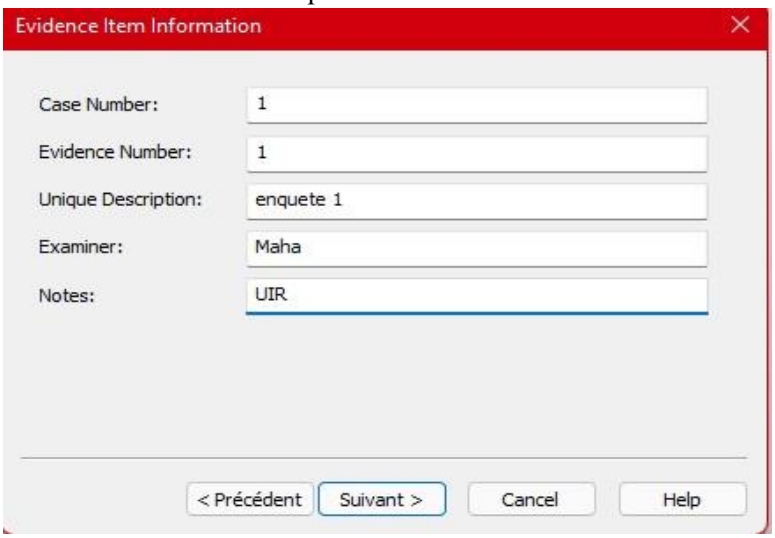
-Ensuite, on choisit la destination (l'image de clé USB sera enregistrer où exactement ?)



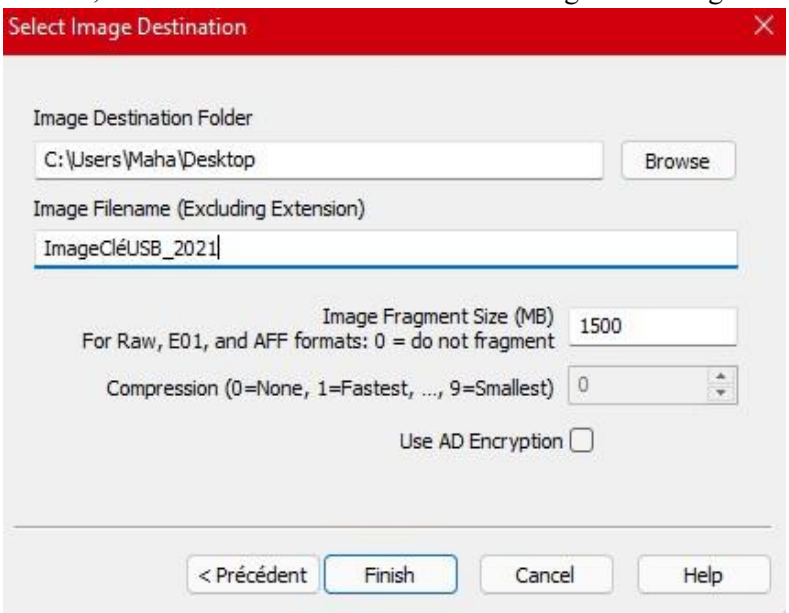
-On choisit le type d'image qu'on veut : nous allons choisir le type Raw (dd) :



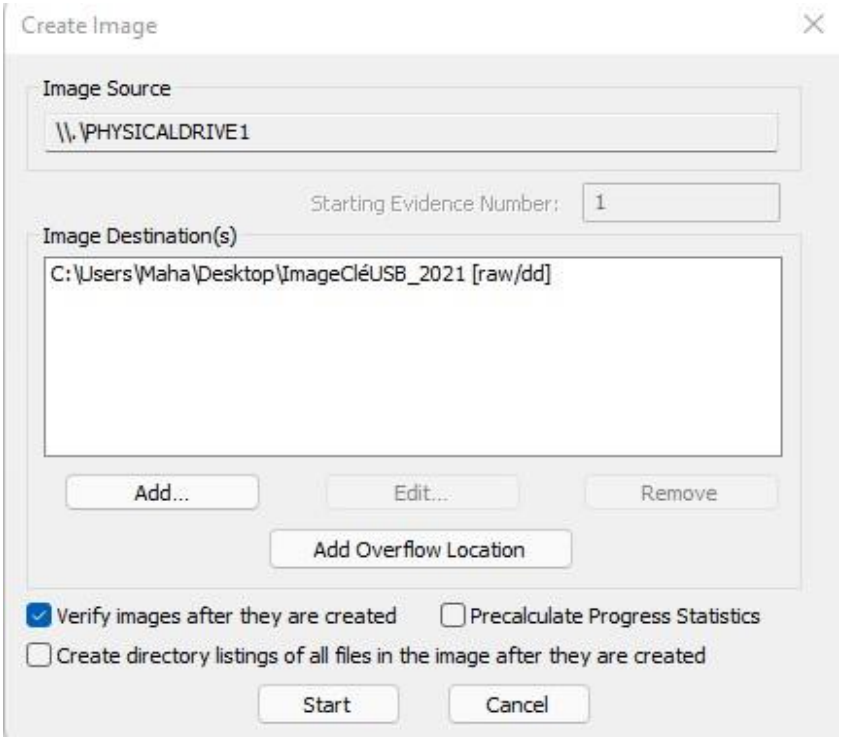
-Les informations sur l'enquête en cours :



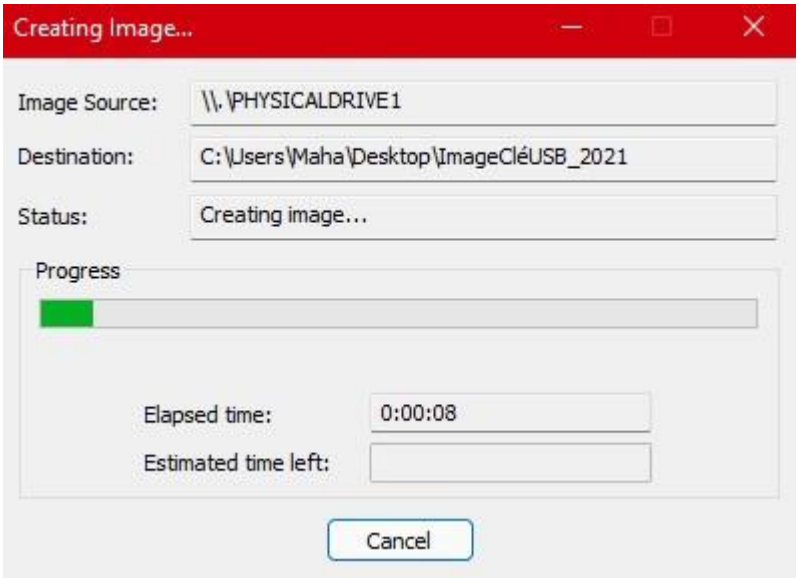
-Ensuite, on sélectionne le chemin où on va enregistrer l'image :



-Enfin on démarre :

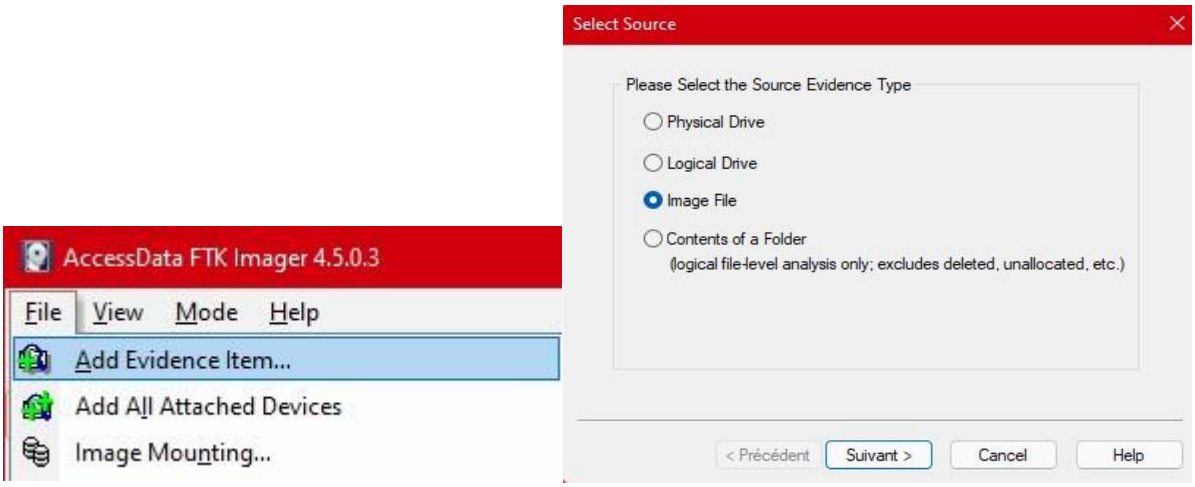


-Comme le Screenshot ci-dessous le montre, il est entrain de copier le contenu (clonage bit à bit) de la clé USB et de le mettre dans un fichier appelé ImageCléUSB_2021 et il va l'enregistrer dans le bureau

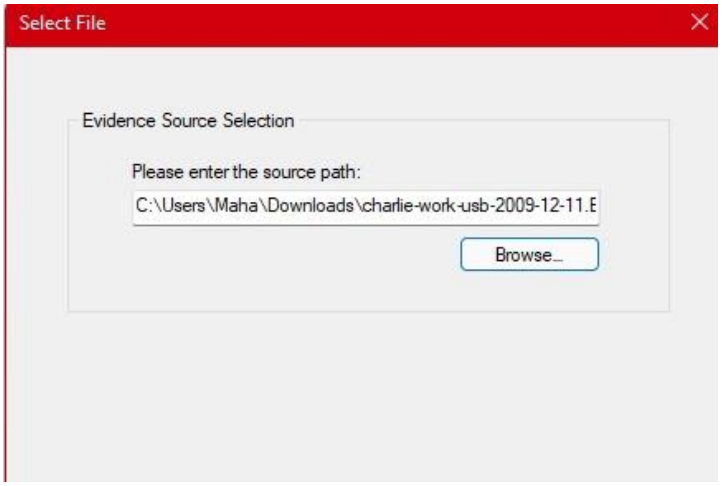


-Et voilà l'image a été créé dans le bureau :

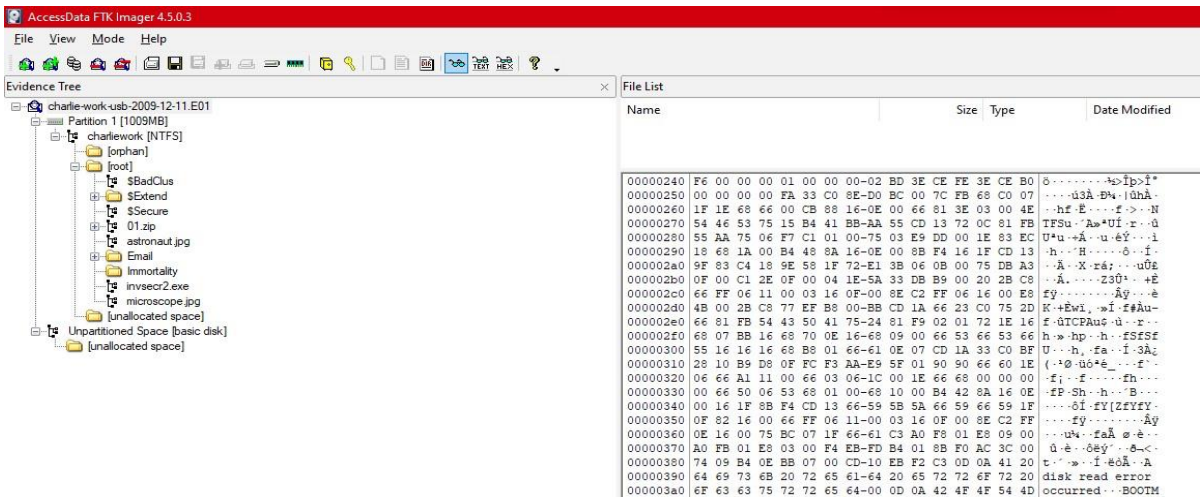
❾Une fois la création de l'image est terminée, nous maintenant l'analyser :



-Ensuite, On va sélectionner une image :

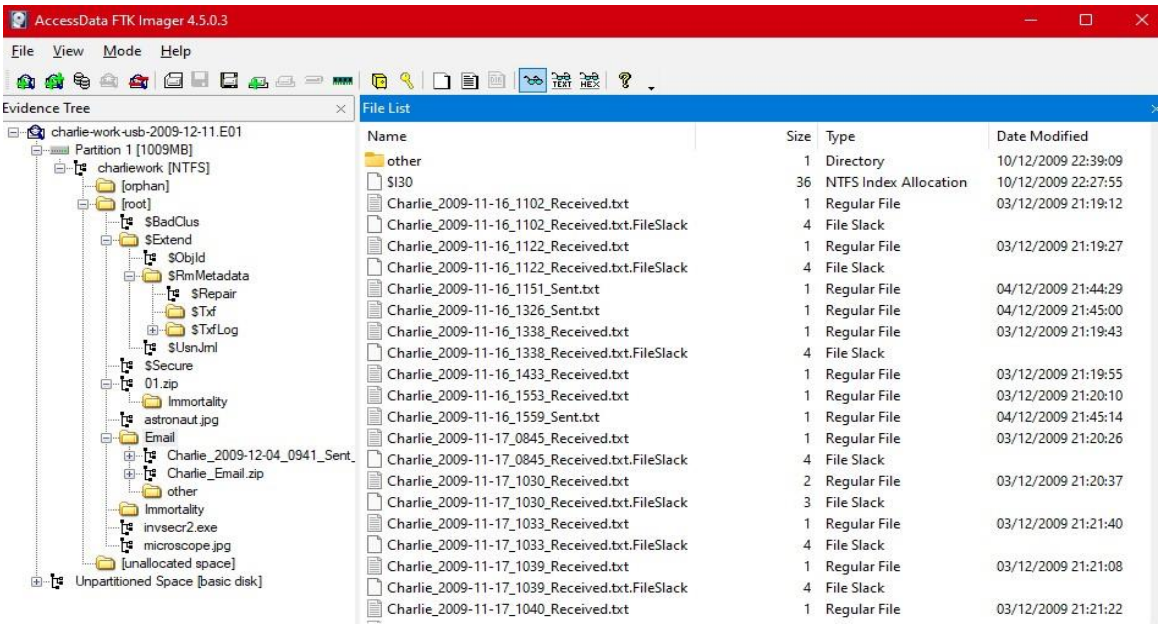


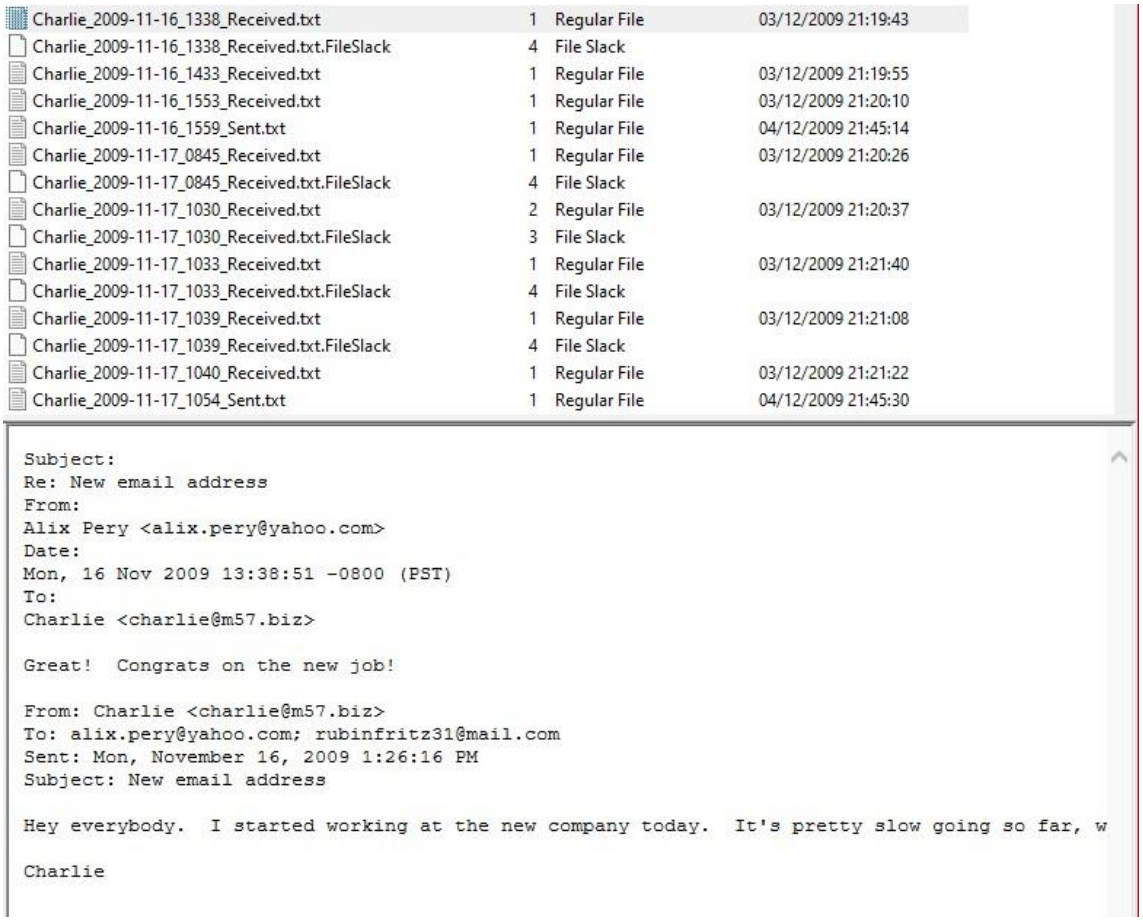
-On va maintenant l'arborescence de la partition de la clé USB, ce qui nous intéresse c'est la Partition 1 :



-

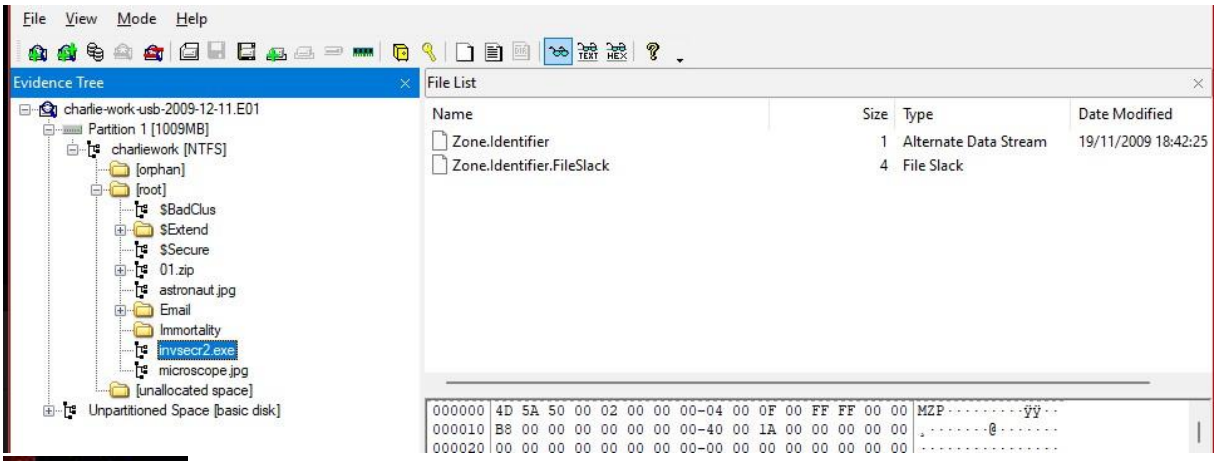
Ceci c'est juste un exemple théorique : le Screenshot on voit les courriels envoyés et reçus :





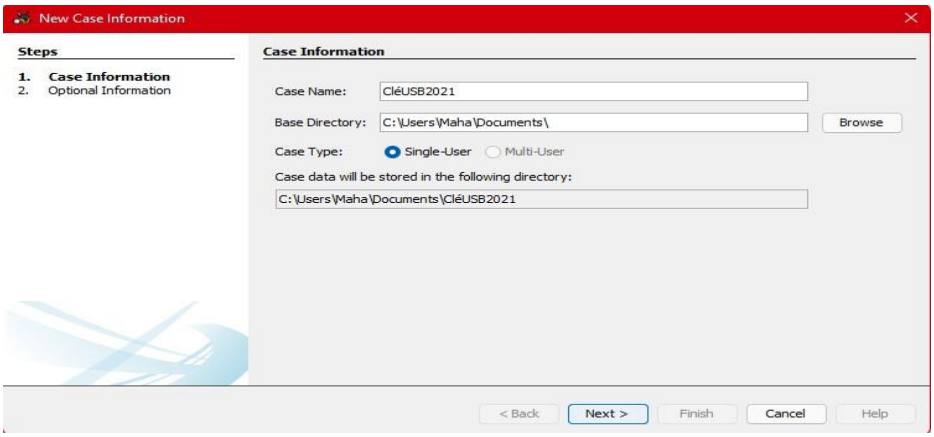
-

Aussi, je peux exporter ce fichier (un fichier exécutable) pour l'analyser



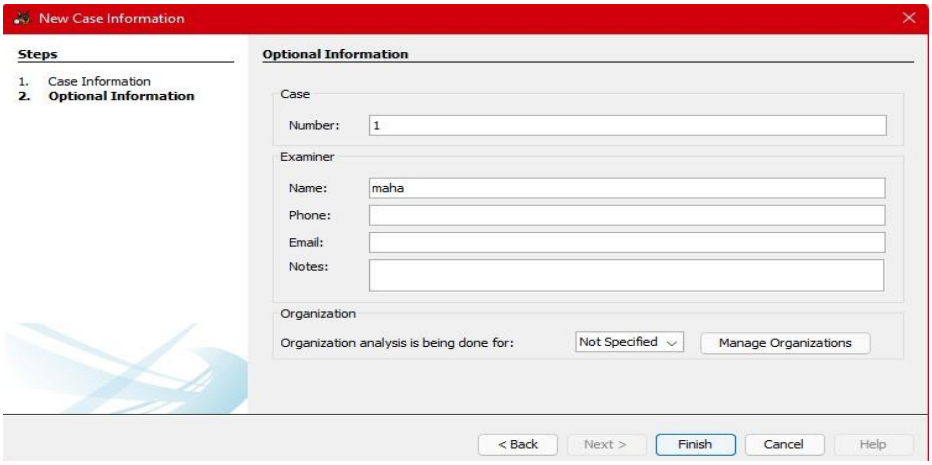
L'analyse de la Clé USB avec l'outil Autopsy

Autopsy est un outil de criminalistique numérique open source développée par Basis Technology, publié pour la première fois en 2000. C'est un outil gratuit à utiliser et assez efficace pour l'enquête sur le disque dur avec des fonctionnalités telles que les cas multi-utilisateurs, l'analyse chronologique, l'analyse du registre, la recherche par mot-clé, l'analyse des courriels, la lecture multimédia, l'analyse EXIF, la détection de fichiers malveillants et bien plus encore. Source -Créer une case :

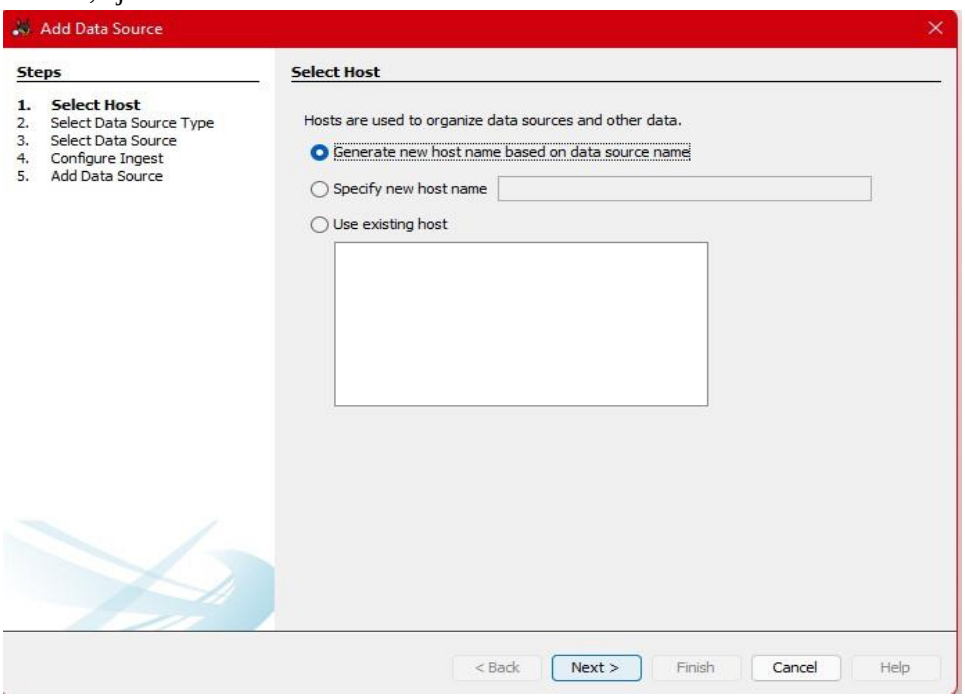


Les informations sur l'enquêteur :

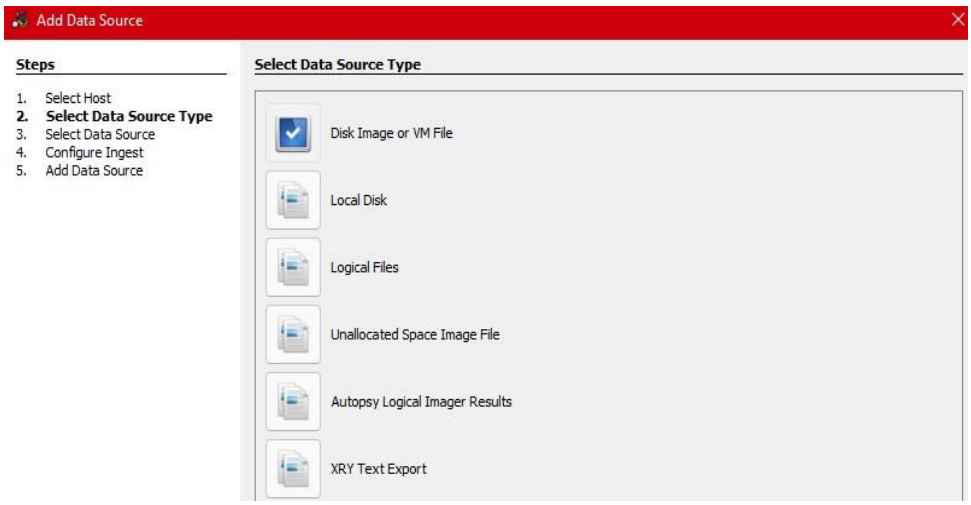
-



-Ensuite, ajouter la source des données :

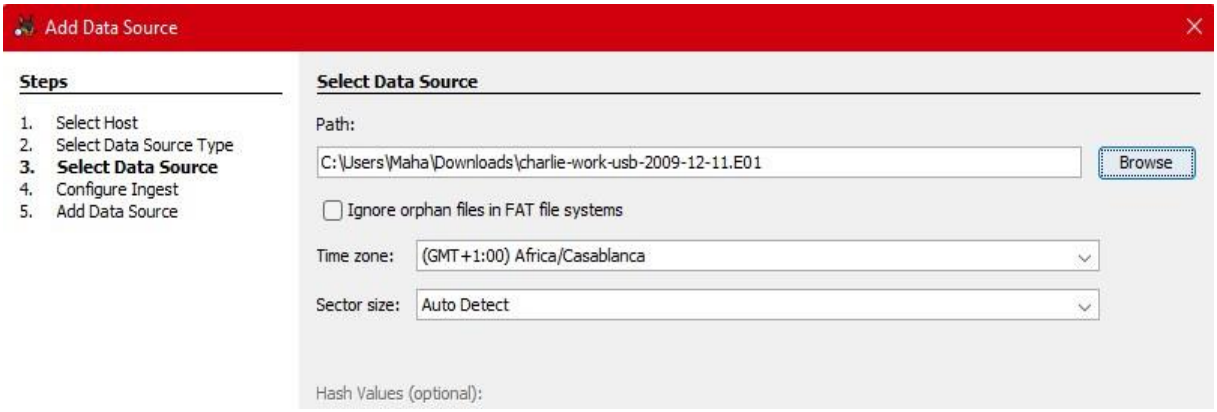


-Choisir le type de la source de données : ici on va choisir image de disque :

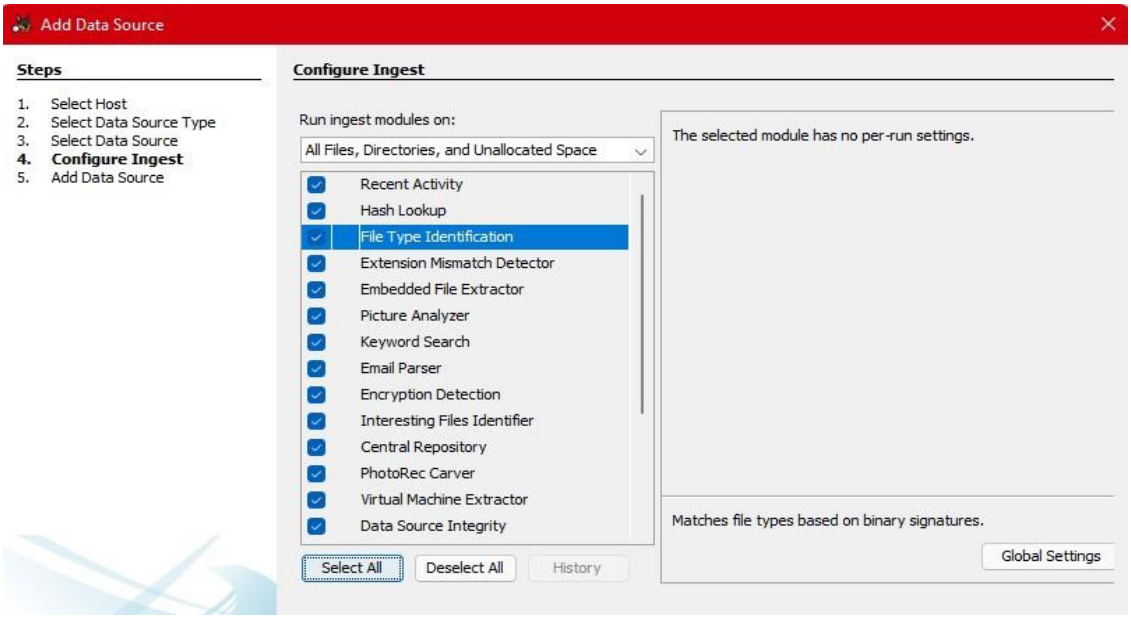


On sélectionne maintenant la source de données :

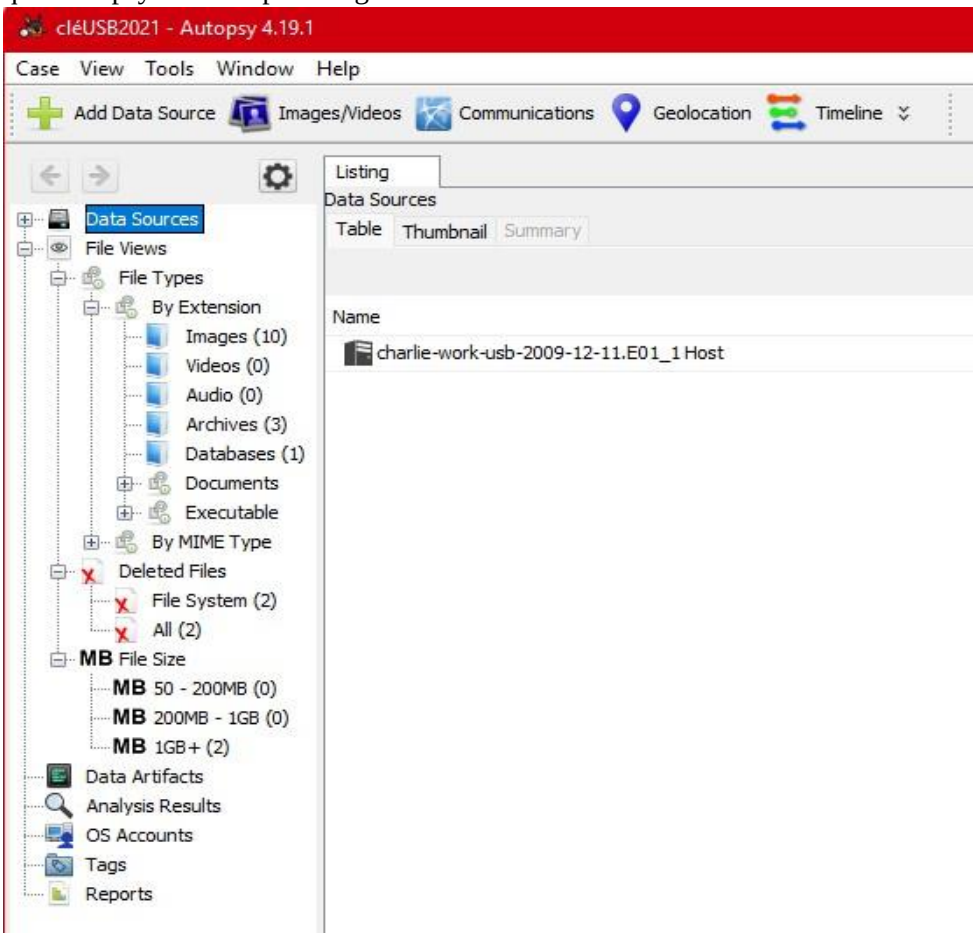
-



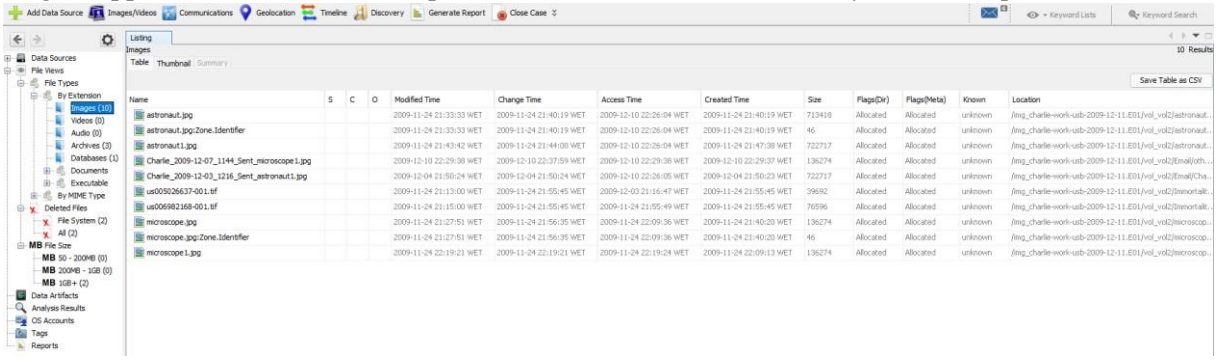
-Autopsy affiche la configuration et les modules qui va activer pour rechercher des informations spécifiques : Par exemple, il va chercher l'activité récente, à identifier le type des fichiers selon le besoin etc..



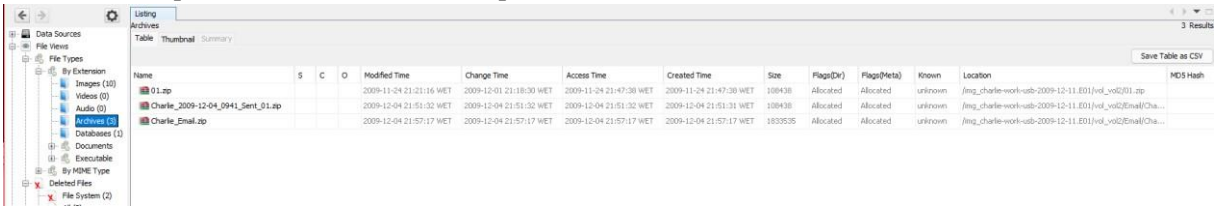
Résultat : comme la figure ci-dessous le montre, File views nous donne un aperçu de tous les fichiers que Autopsy a trouvé par catégories.



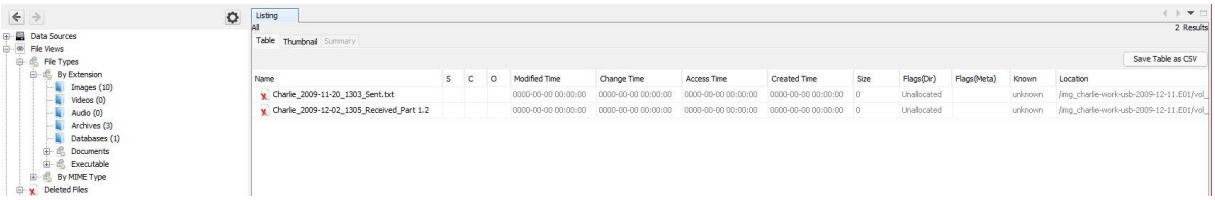
-Il a trouvé par exemple 10 images, il a regroupé toutes les images en extensions par rapport au FTK imager Autopsy donne plus d'information par catégories. Il nous donne aussi plus de détails sous forme d'un tableau, ces informations concernant la date de création, de modification et même les images supprimées. Tous ces détails peuvent nous aider et faciliter l'analyse d'un disque.



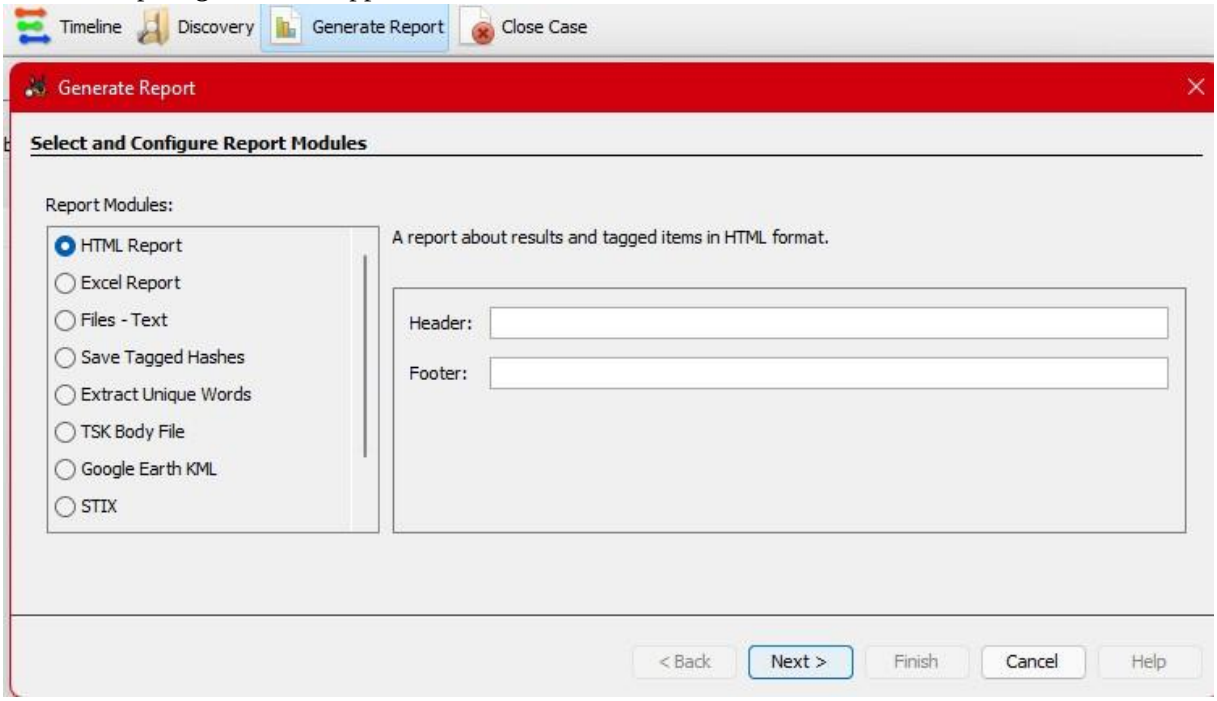
-On voit aussi qu'il a trouvé 4 fichiers compressés :



-Ici les fichiers supprimés :



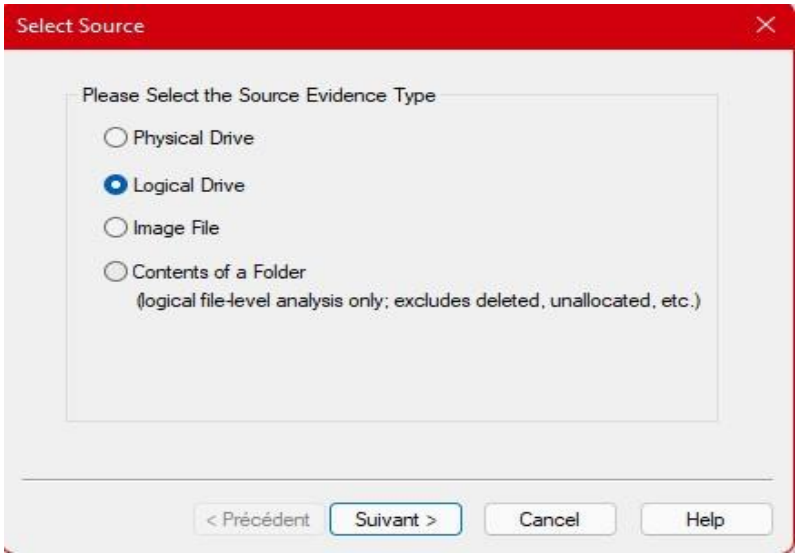
-Ensuite on peut générer un rapport soit en HTML ou Excel etc..



TP 2 : Analyse de bases de registre

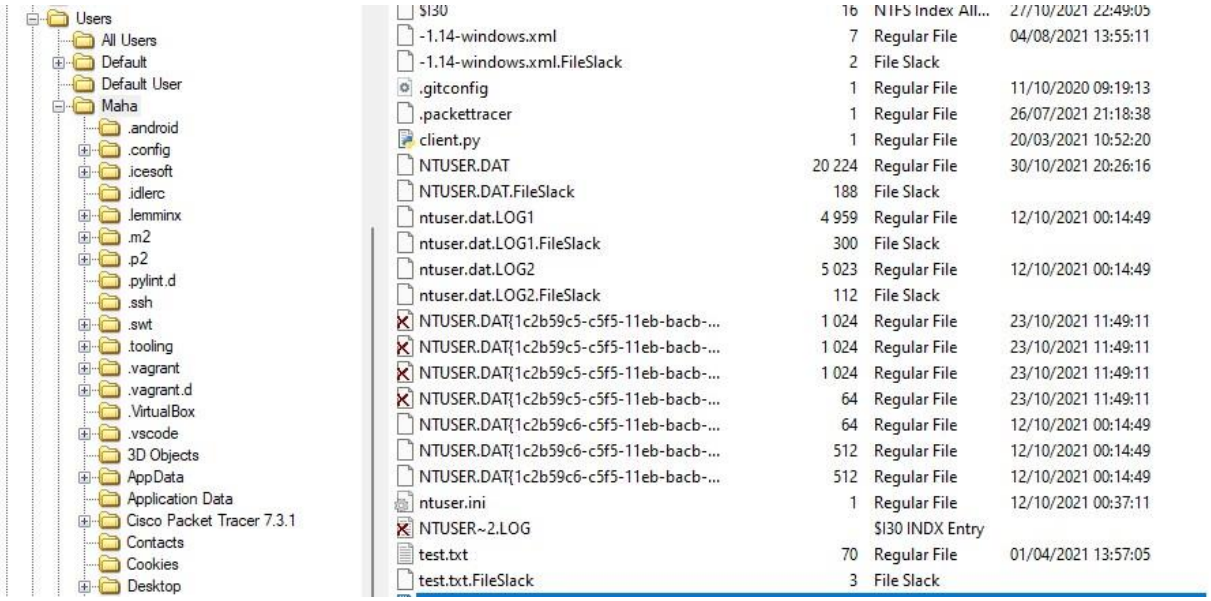
Etape 1 : C'est l'étape de l'exportation des ruches en utilisant FTK Imager

-On crée une preuve en suivant les étapes : File ❾Add and Evidence ❾ on sélectionne le type de la source de la preuve

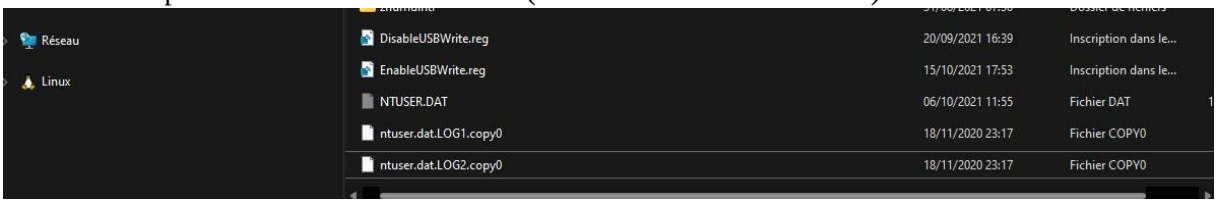


-Ici la preuve représente une partition C:\ :

-Maintenant on cherche les fichiers *NTUSER.DAT, ntuser.dat.LOG1, ntuser.dat.LOG2 : en suivant le chemin suivant : C:/ ❾root ❾Users ❾ 'utilisateur normal'*



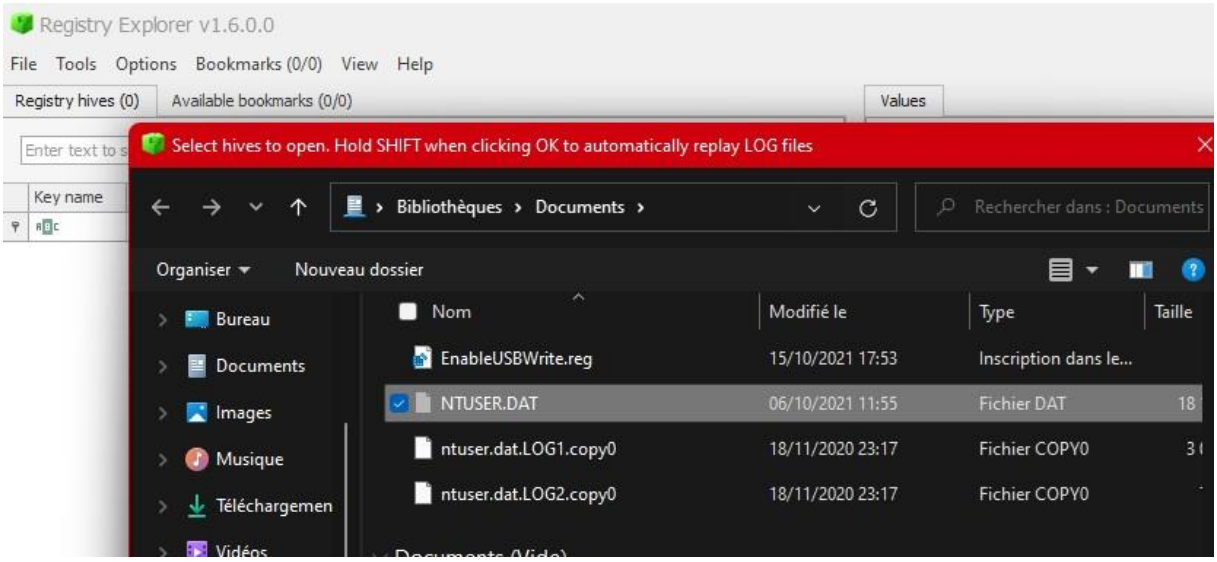
-Ensuite on export les fichiers vers le bureau (ou un chemin de votre choix) :



Etape 2 : Importation des ruches en utilisant Registry Explorer

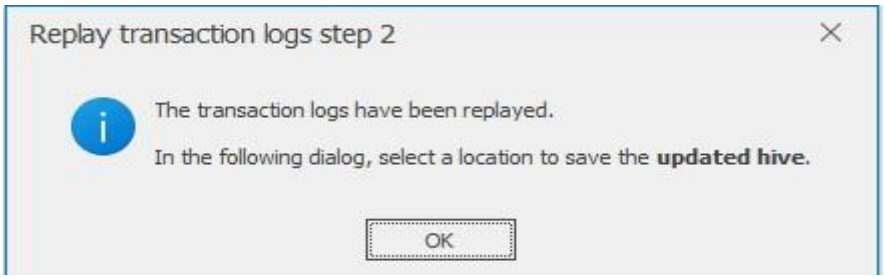
Registry Explorer est un outil dont l'objectif est de remplacer l'éditeur du registre proposé par Windows. On appréciera notamment le gestionnaire de signets, l'import/export de données, l'historique complet, la sauvegarde automatique des manipulations effectuées ou encore la recherche performante intégrée.

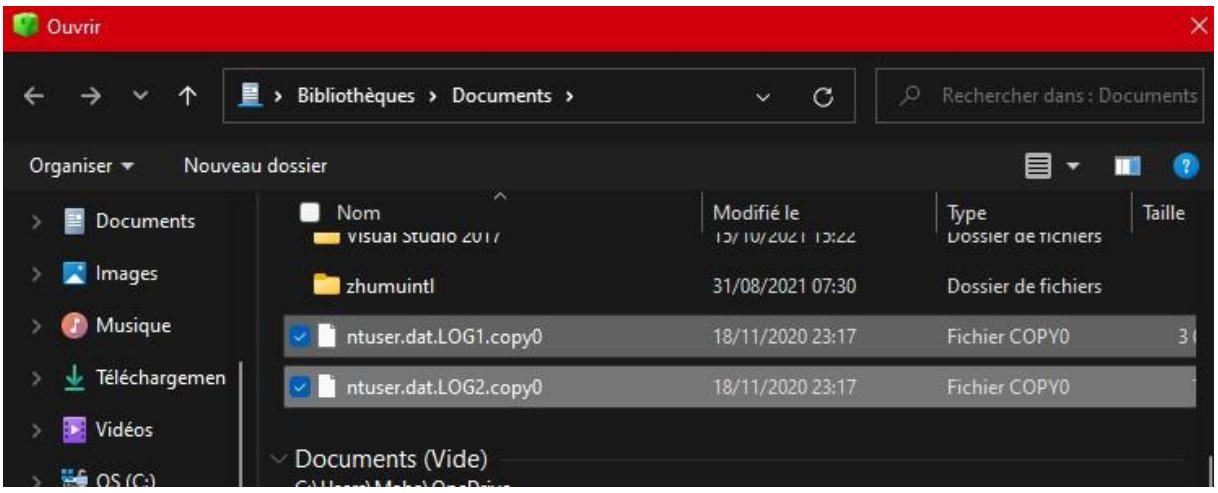
Dans cette étape, on importe les ruches qu'on a exporté dans la première étape. On clique sur File❾Load hive et on sélectionne le fichier NTUSER.DAT



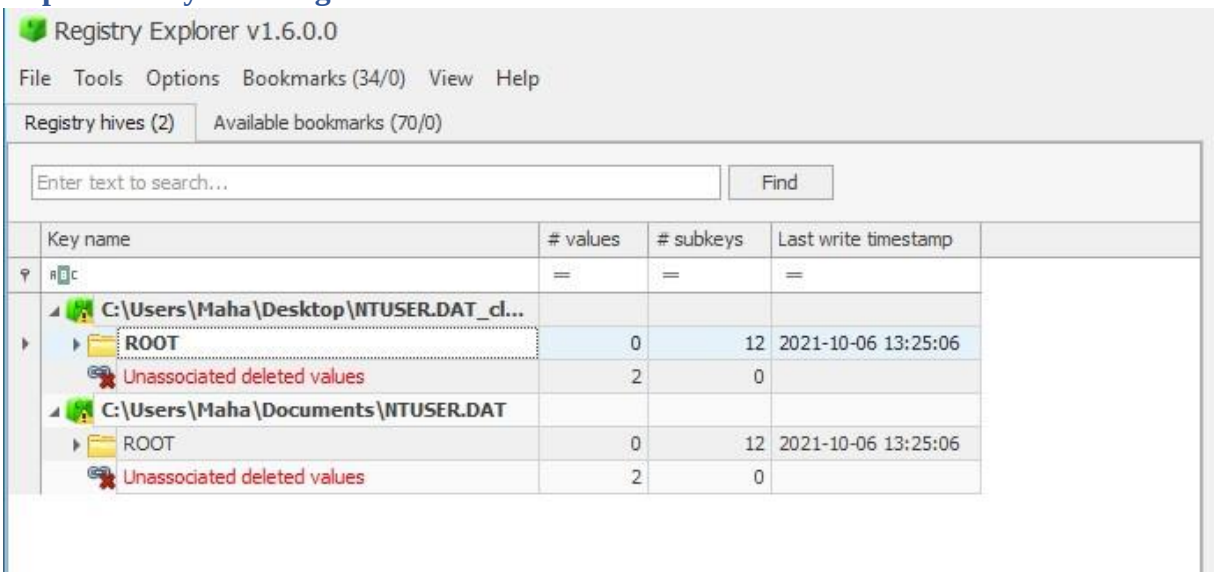
-On clique sur Yes :

-On clique sur ok puis on importe les fichiers ntuser.dat.LOG1 et ntuser.dat.LOG2 :





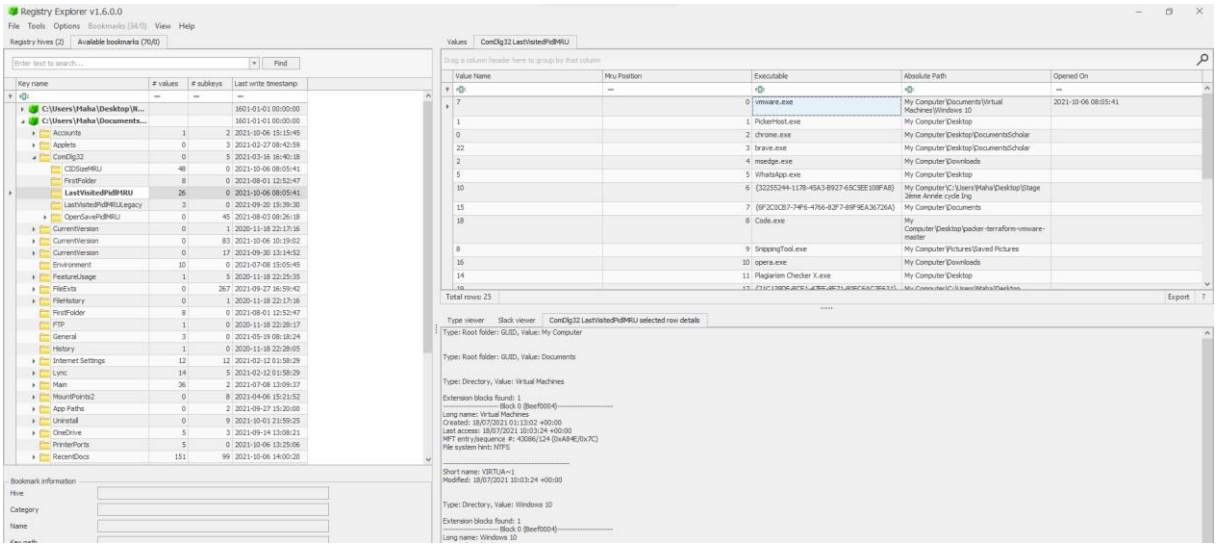
Etape 3 : analyse des registres



-On analyse les derniers PID les plus utilisés récemment :

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

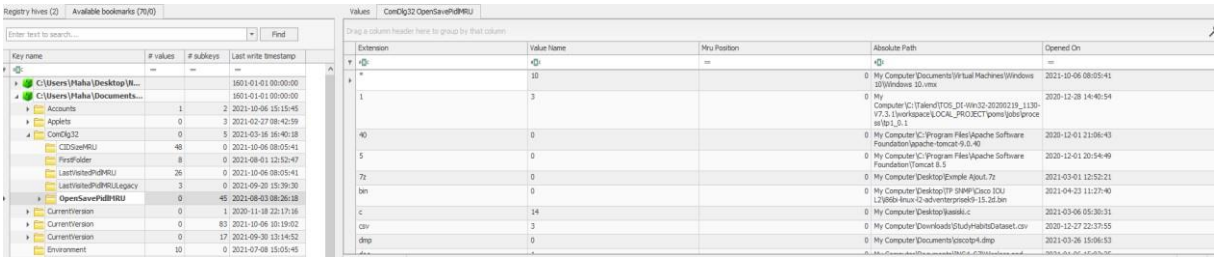
- \ComDlg32
  - \LastVistedPidlMRU



-On analyse les fichiers ouverts ou enregistrés récemment par une application via la boite dialogue du Shell Windows :

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

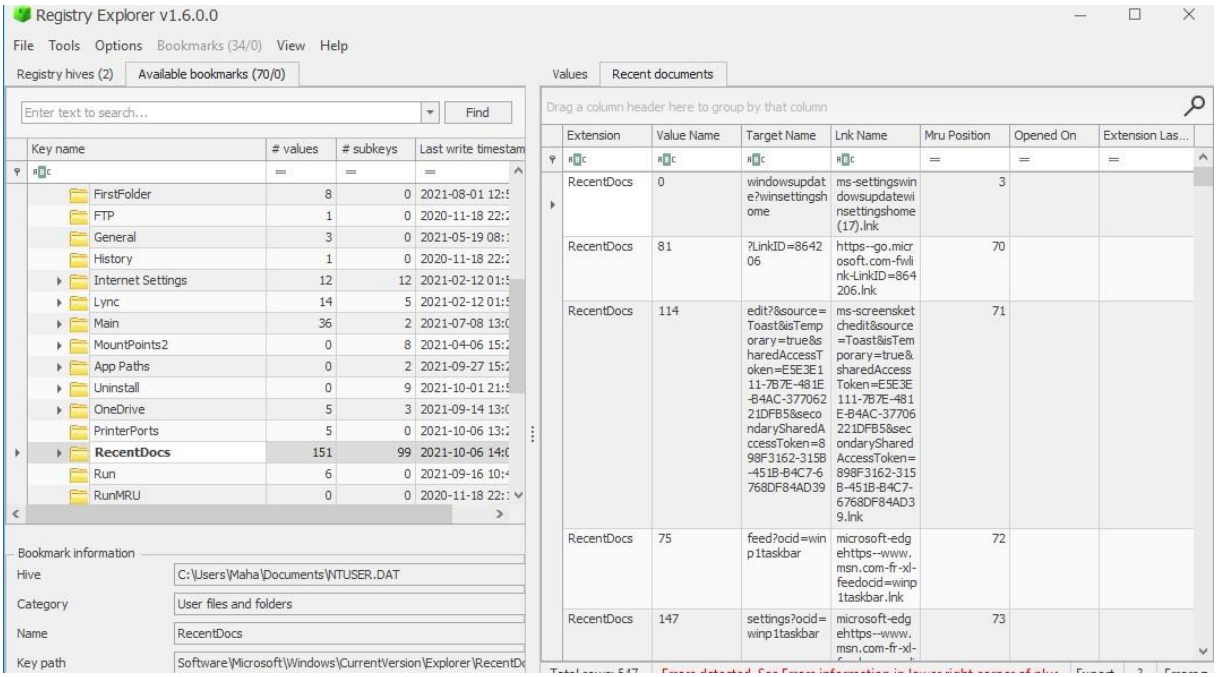
- \ComDlg32
  - \LastVistedPidlMRU
  - \OpenSavePidlMRU



-On analyse la liste des fichiers récemment consultés :

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

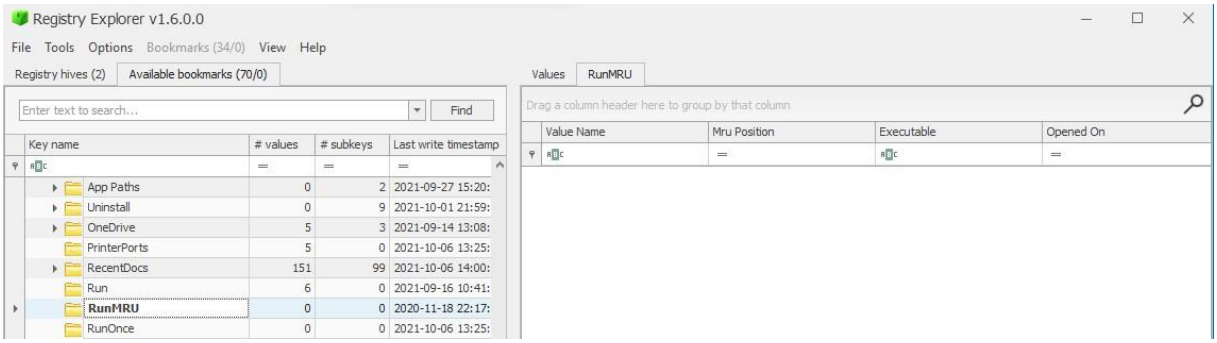
- \ComDlg32
  - \LastVistedPidlMRU
  - \OpenSavePidlMRU
- \RecentDocs



-On analyse la liste des programmes exécutes récemment **:**

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

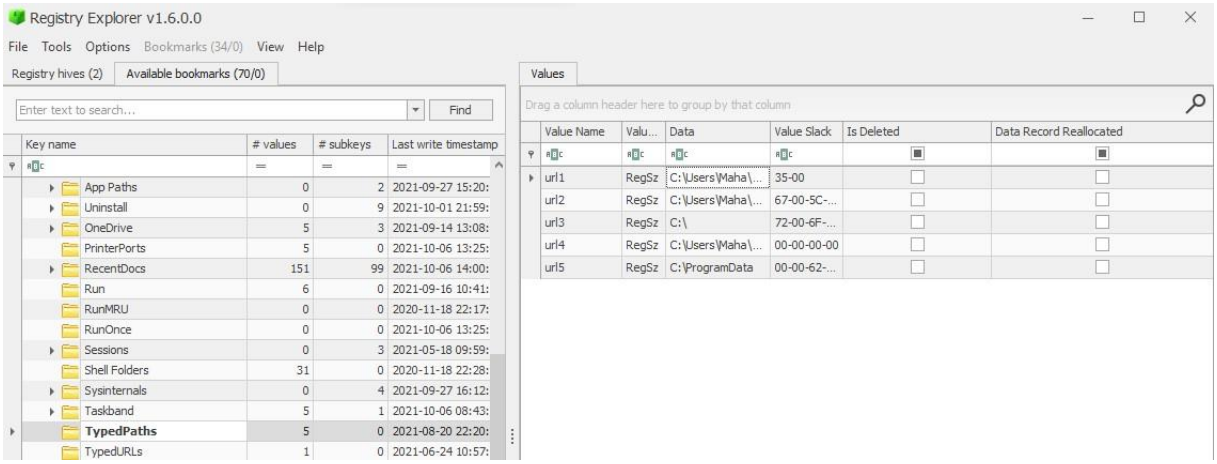
- \ComDlg32
  - \LastVistedPidlMRU
  - \OpenSavePidlMRU
- \RecentDocs
- \RunMRU



-On analyse les derniers chemins tapés ou insérés dans la barre de chemin de l'Explorateur de fichiers :

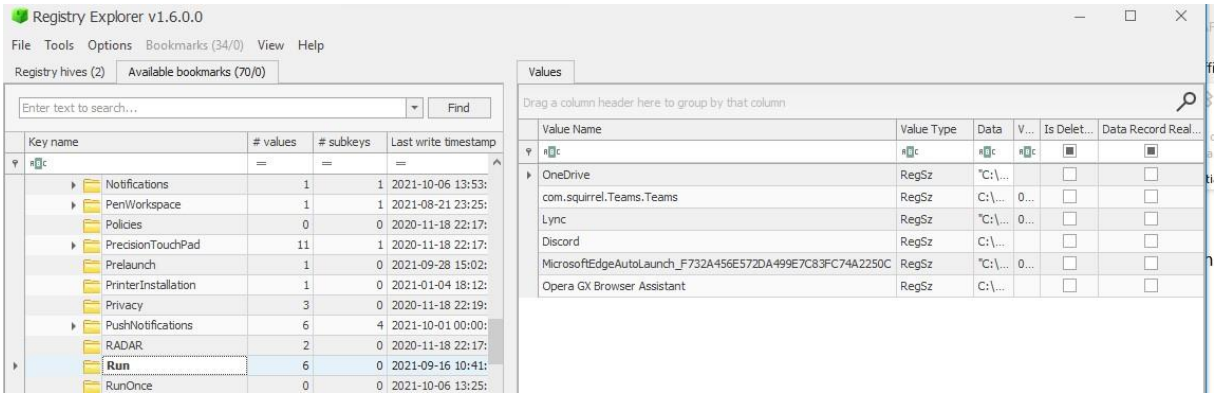
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

- \ComDlg32
  - \LastVistedPidlMRU
  - \OpenSavePidlMRU
- \RecentDocs
- \RunMRU
- \TypedPaths



-On analyse les programmes exécutes :

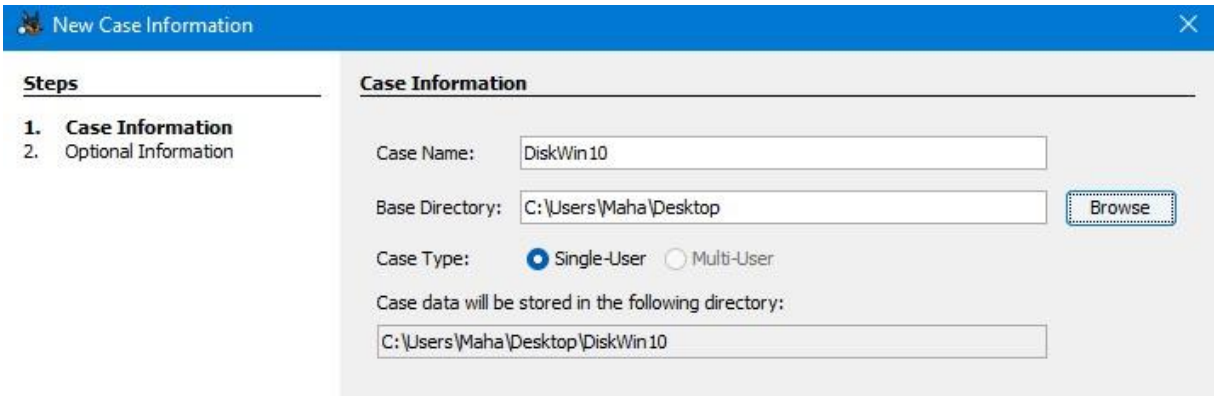
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

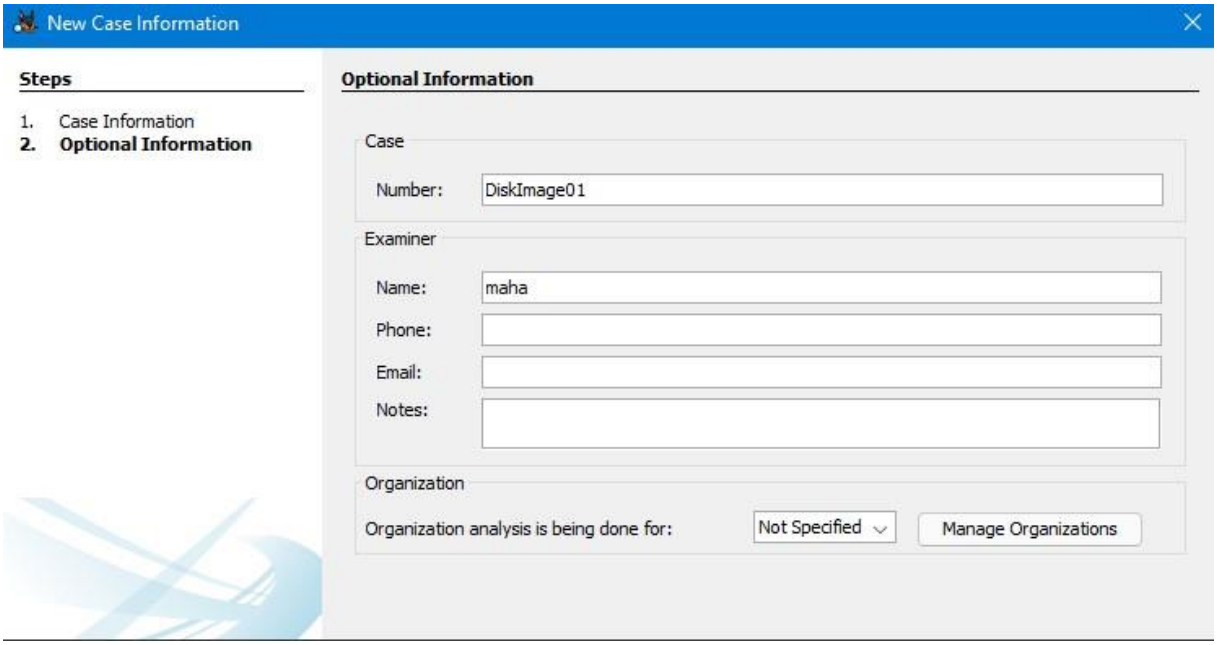


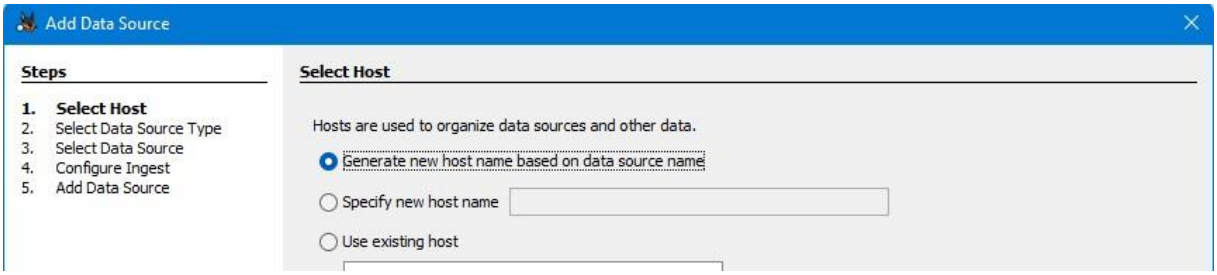
Cas 1 : Analyse approfondie d'une image de disque (cas réel : win10 UIR) Avec Autopsy

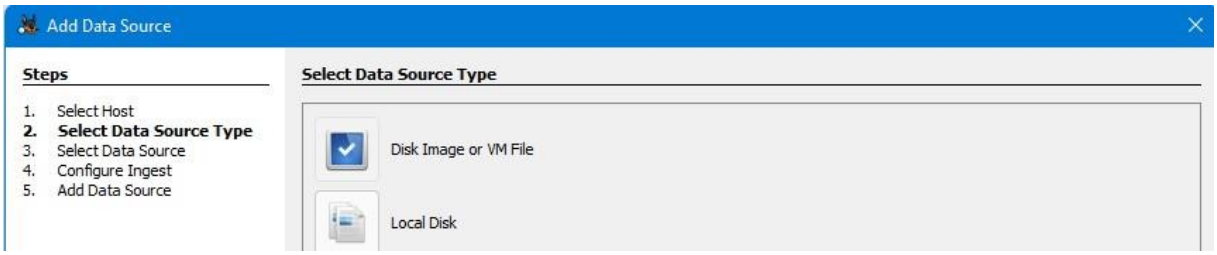
Dans cette étape nous allons faire une analyse forensique d'un cas réel en utilisant l'outil Autopsy : une image de disque dur externe.

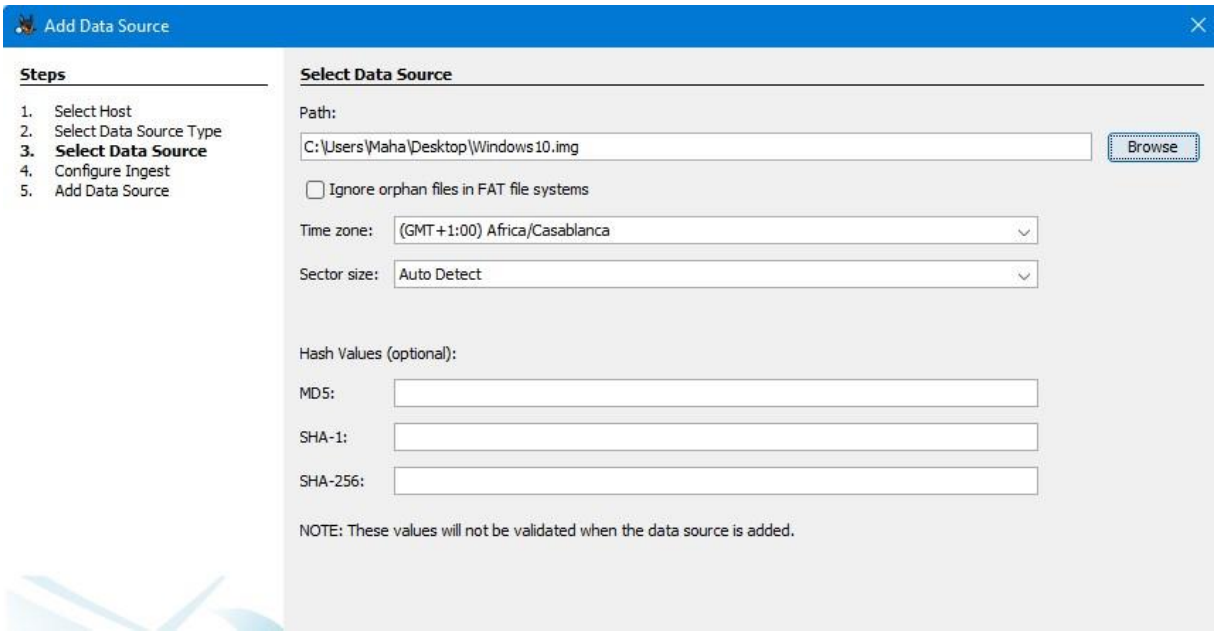
Création d'une case :

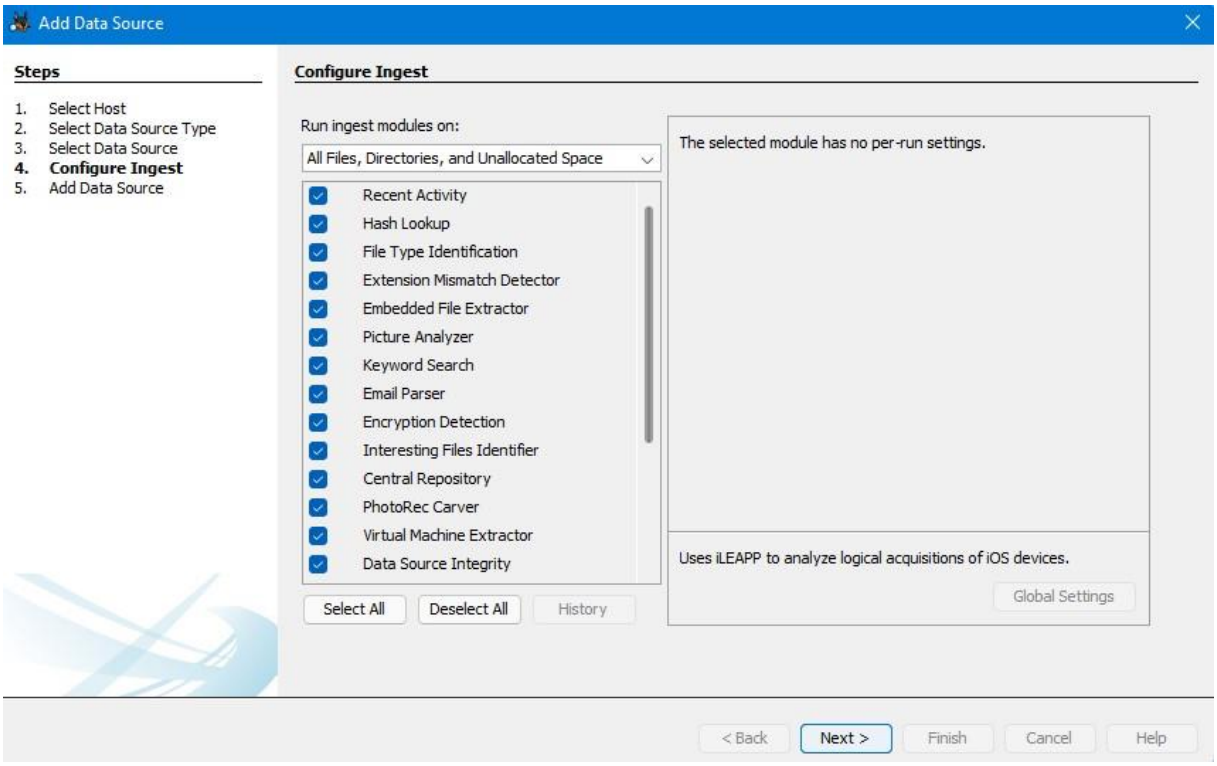

New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name: DiskWin10
Base Directory: C:\Users\Maha\Desktop
Browse
Case Type: Single-User Multi-User
Case data will be stored in the following directory:
C:\Users\Maha\Desktop\DiskWin10


New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number: DiskImage01
Examiner
Name: maha
Phone:
Email:
Notes:
Organization
Organization analysis is being done for: Not Specified
Manage Organizations

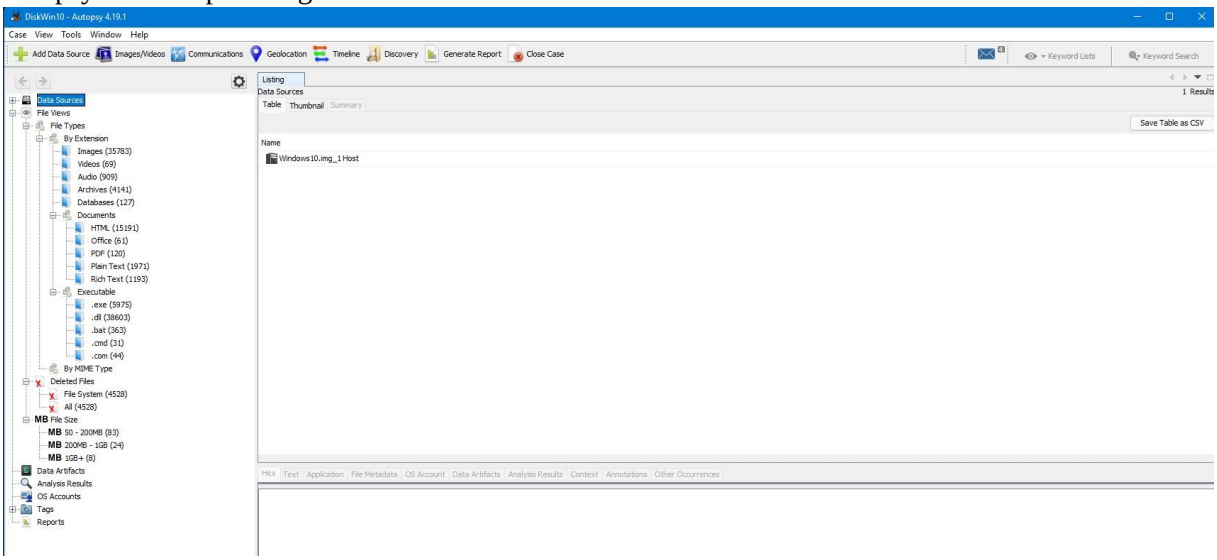

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host

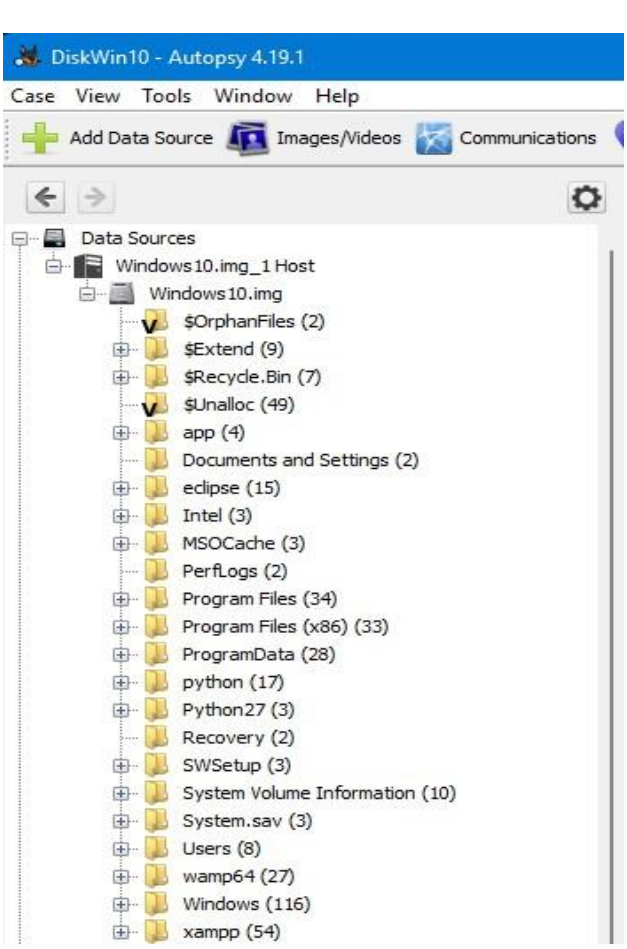

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk

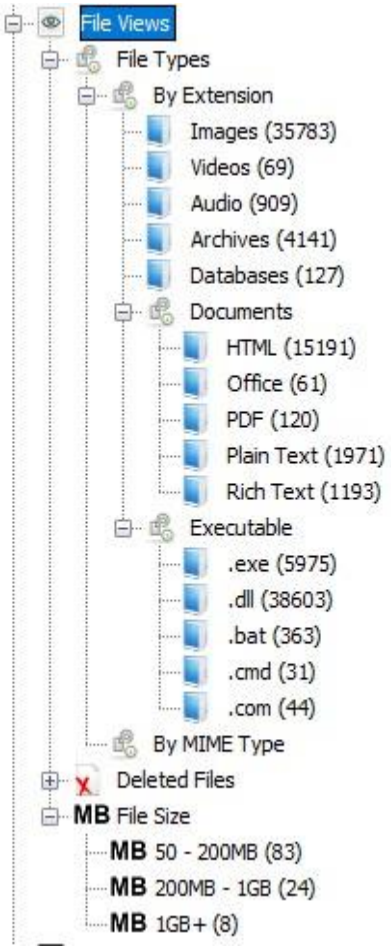

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Path:
C:\Users\Maha\Desktop\Windows10.img
Browse
Ignore orphan files in FAT file systems
Time zone:
(GMT+1:00) Africa/Casablanca
Sector size:
Auto Detect
Hash Values (optional):
MD5:
SHA-1:
SHA-256:
NOTE: These values will not be validated when the data source is added.


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Configure Ingest
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Data Source Integrity
Select All
Deselect All
History
The selected module has no per-run settings.
Uses iLEAPP to analyze logical acquisitions of iOS devices.
Global Settings
< Back
Next >
Finish
Cancel
Help

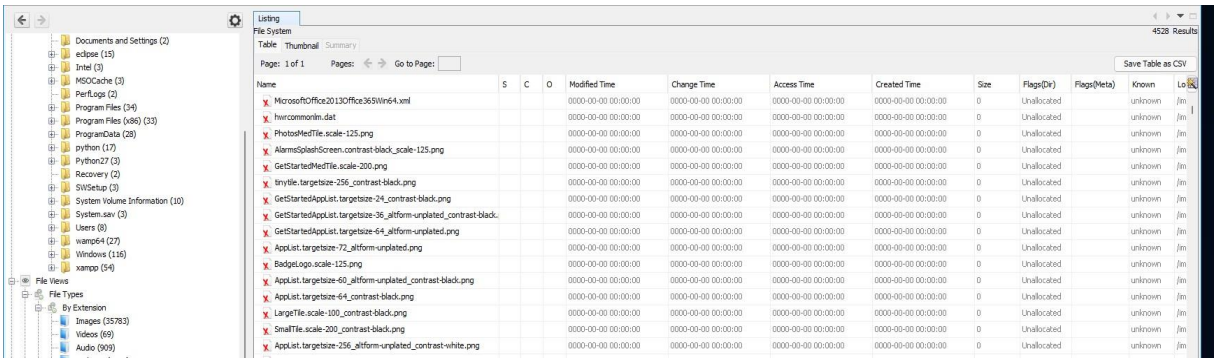
Comme les figures ci-dessous le montre, File views nous donne un aperçu de tous les fichiers que Autopsy a trouvé par catégories.



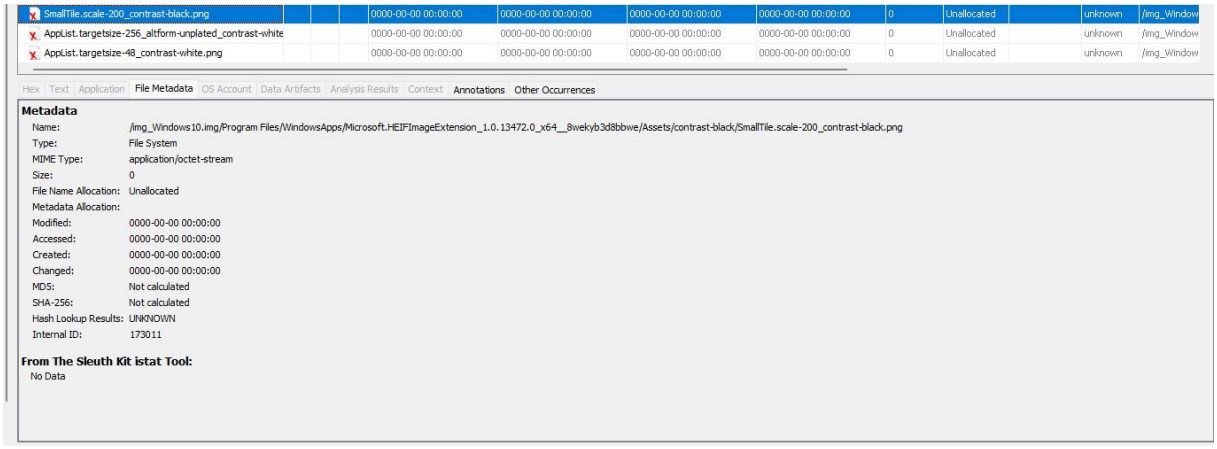




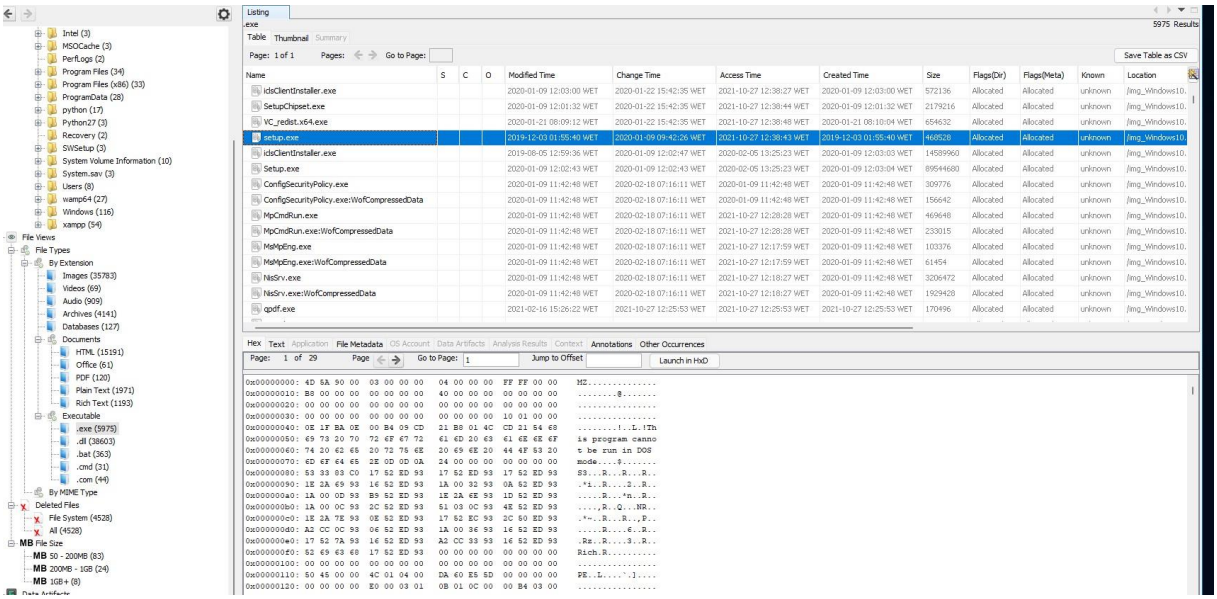
La liste des fichiers supprimés :



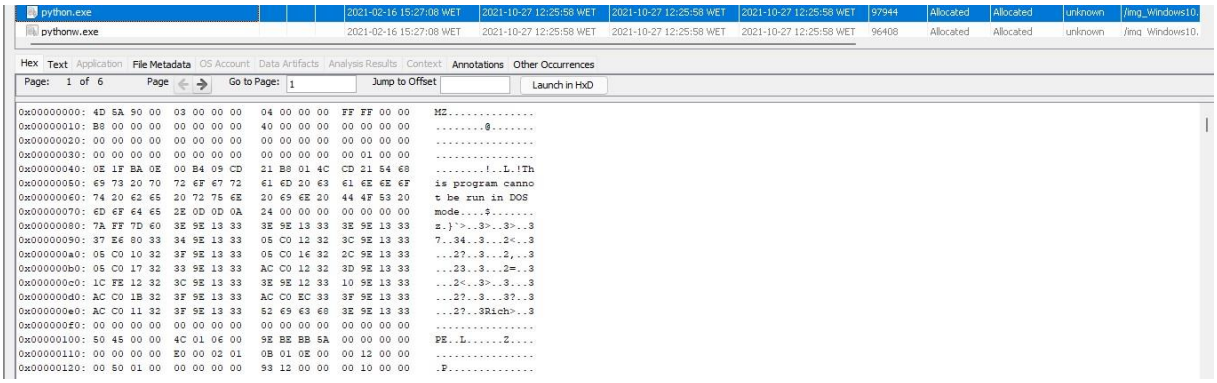
Exemple d'un fichier supprimé avec plus d'information :



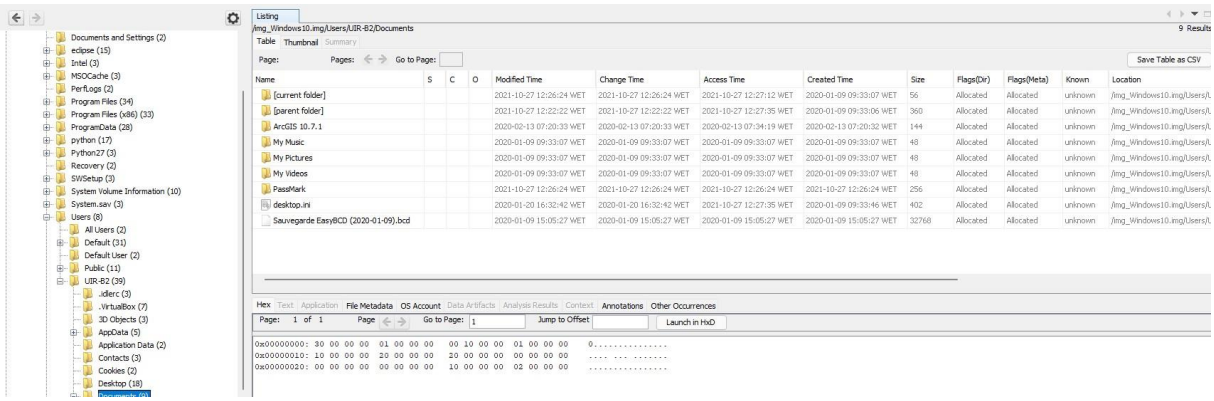
La liste des exécutables :



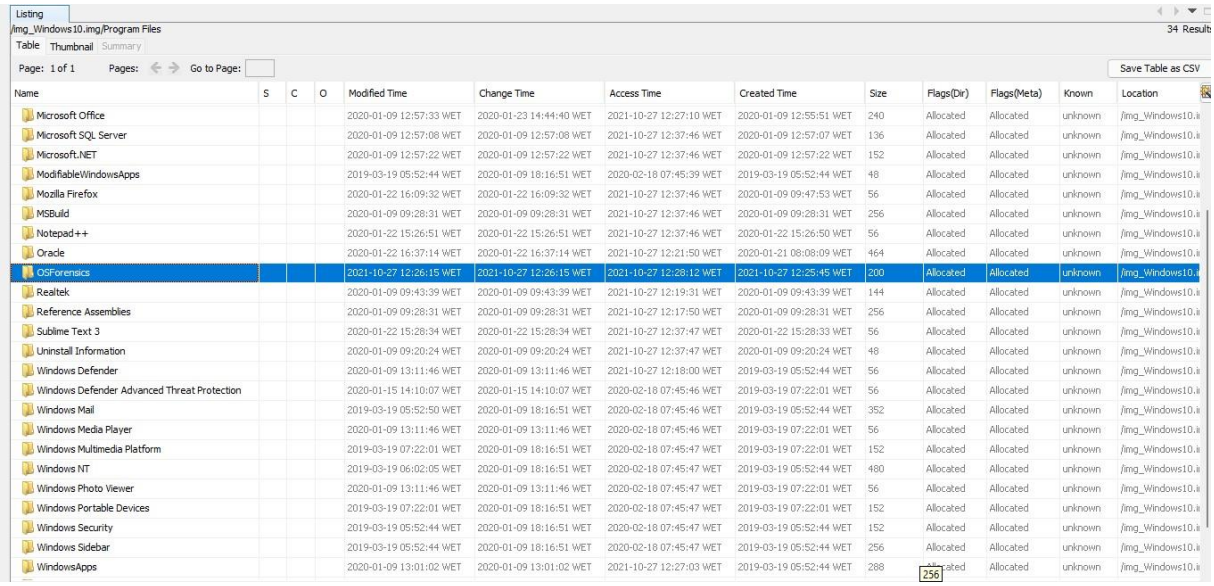
Exemple d'un programme python qui est installé dans ce disque : cette analyse des ce types de fichiers nous permet de détecter s'il y a un processus malveillant installé



Aussi, on peut analyser les fichiers enregistrés au niveau du fichier d'un utilisateur normal :



La listes des logiciels installées :

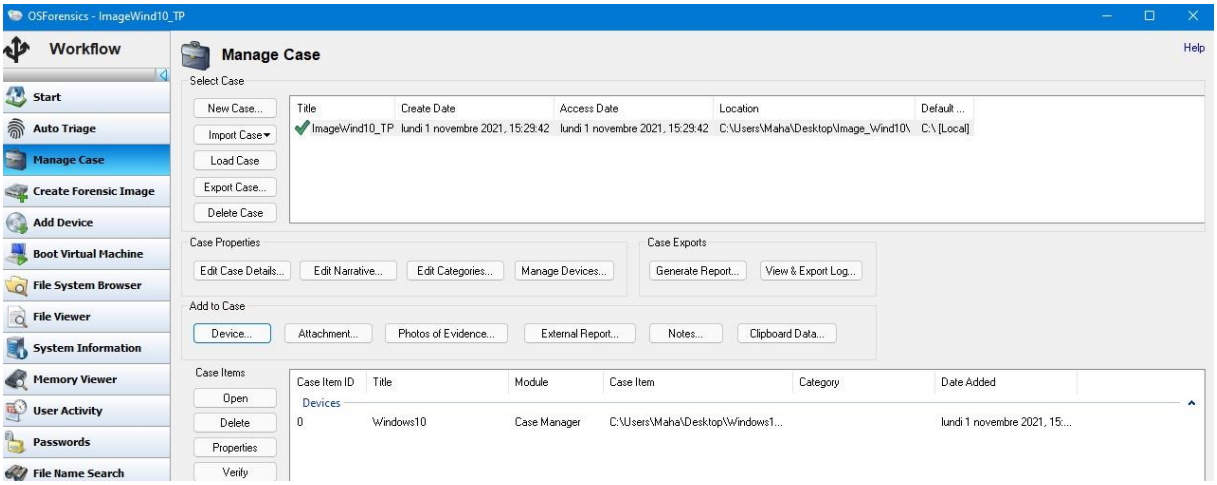


Cas 2 : Analyse approfondie d'une image de disque (cas réel : win10 UIR) Avec OSForensics

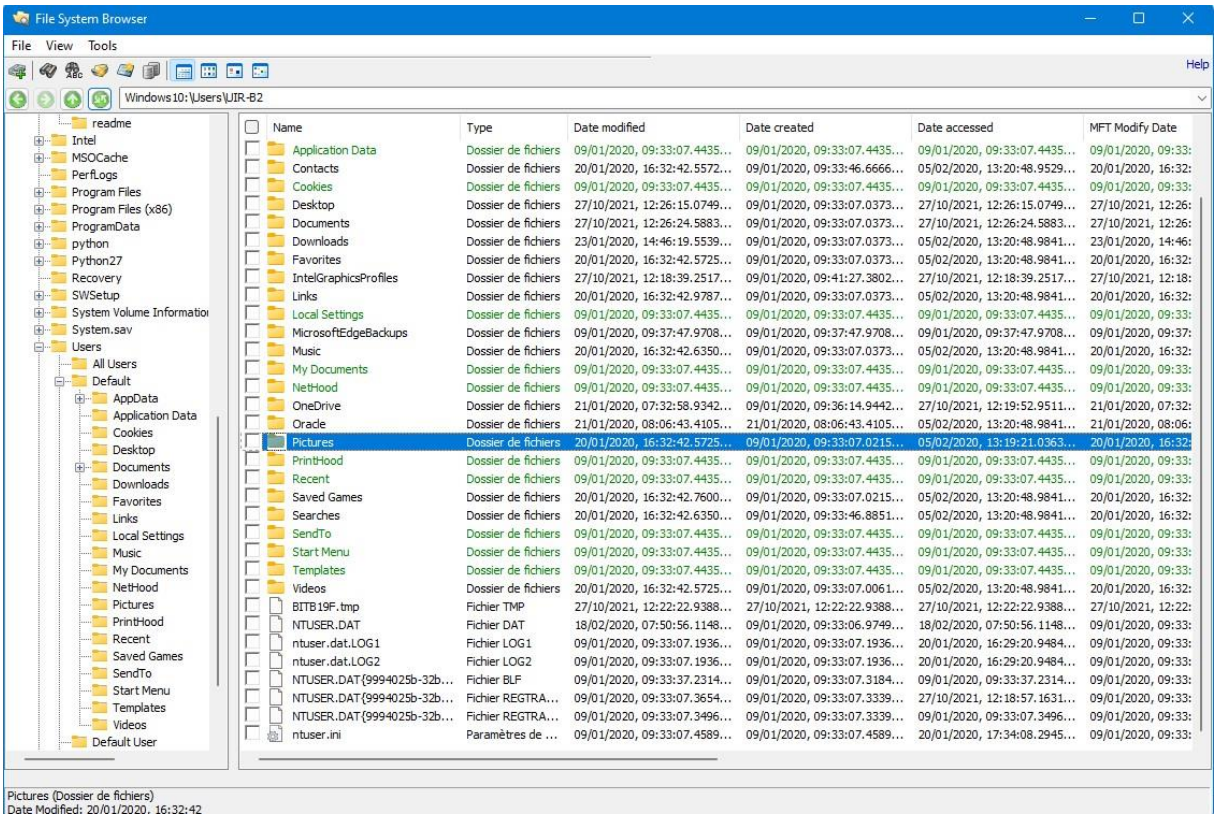
Dans cette étape nous allons analyser la même image de disque avec OSforensics.

OSForensics fournit l'un des moyens les plus rapides et les plus puissants de localiser des fichiers sur un ordinateur Windows. OSForensics Extrayez les données médico-légales des ordinateurs, plus rapidement et plus facilement que jamais. Découvrez tout ce qui se cache à l'intérieur d'un PC.

Création d'une case et on ajoute l'image de disque dur externe :

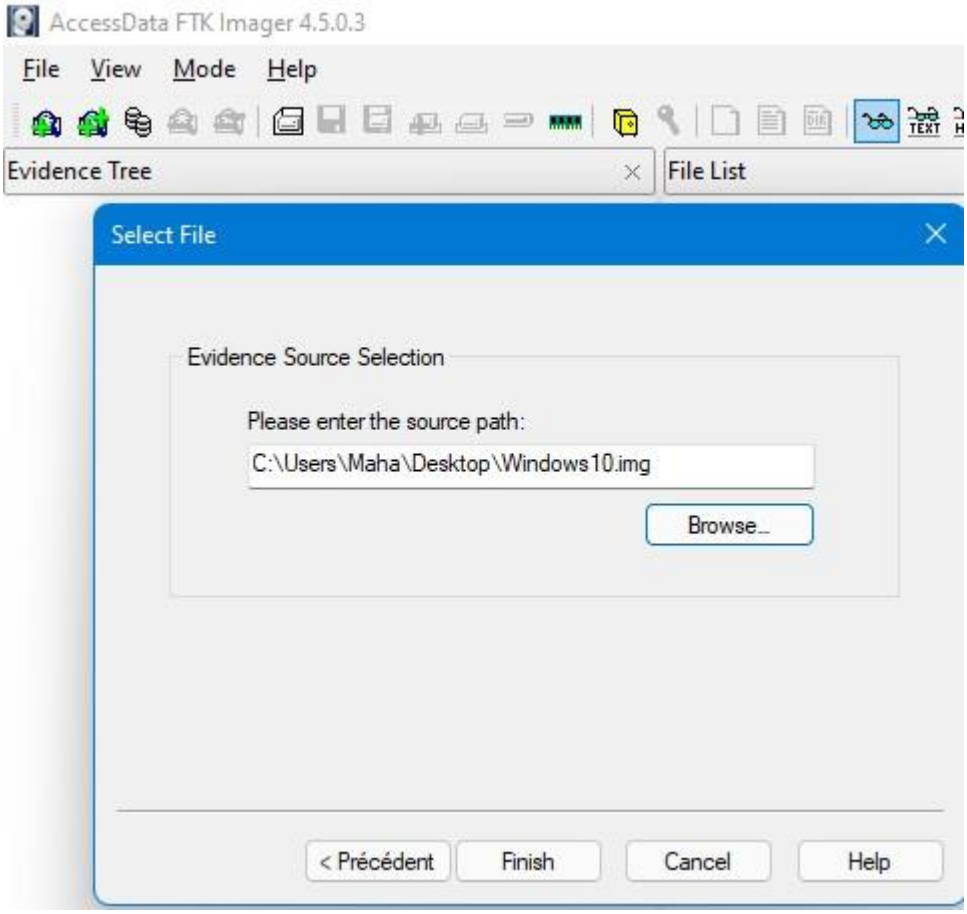


Après on scanne les fichiers systèmes :

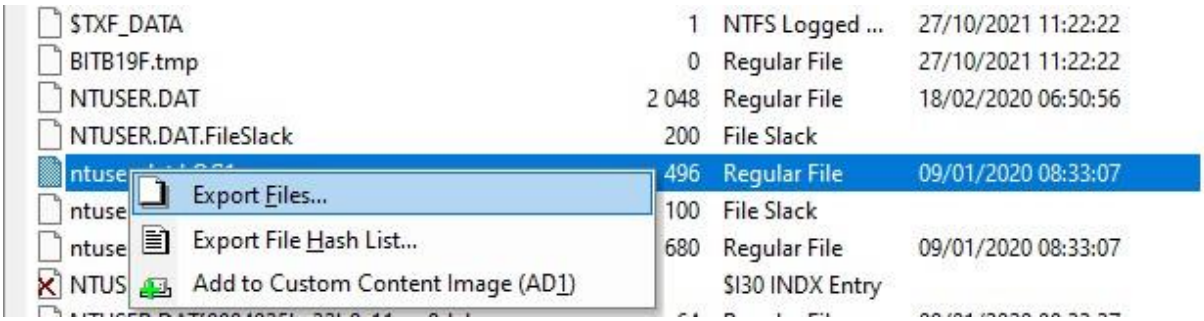


On remarque les trois fichiers NTUSER.DAT, ntuser.dat.LOG1, ntuser.dat.LOG2 , on peut utiliser Registry Explorer pour analyser la base de registre de ce système comme on a déjà fait dans les parties précédentes.

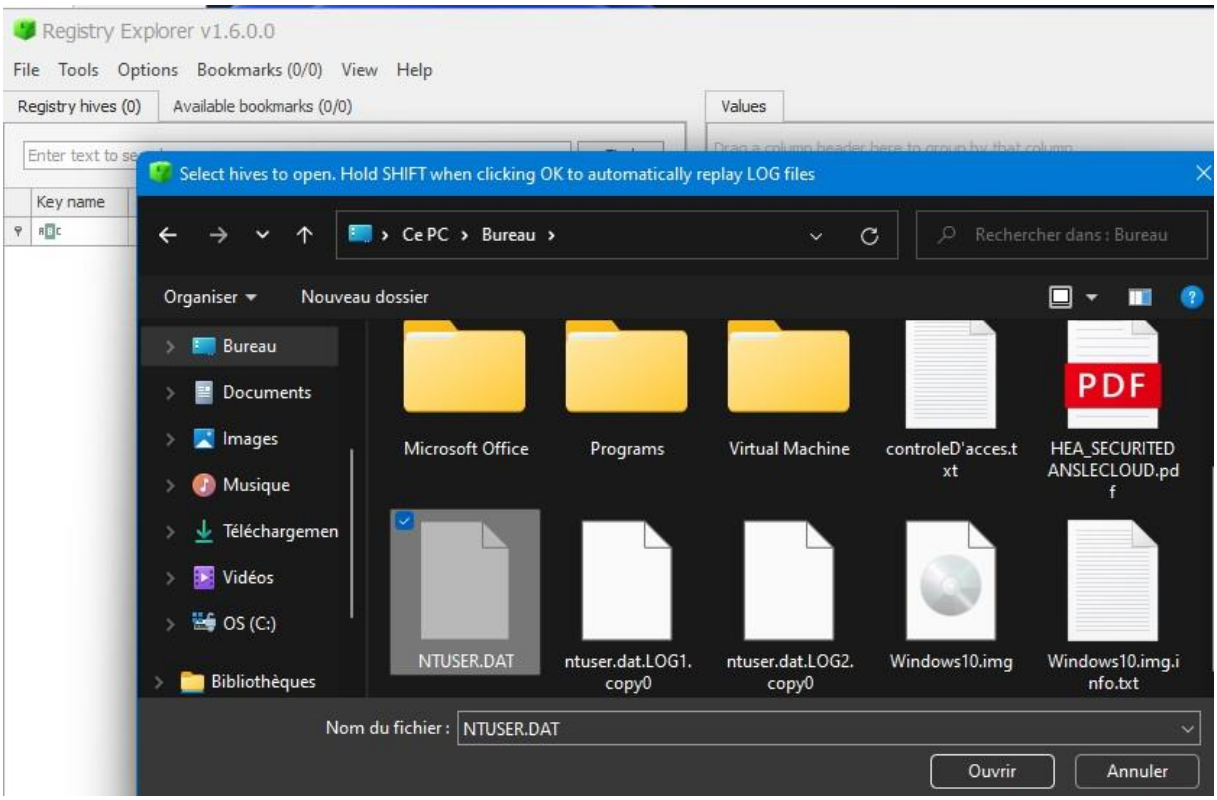
On utilise FTK Imager pour l'exportation des ruches



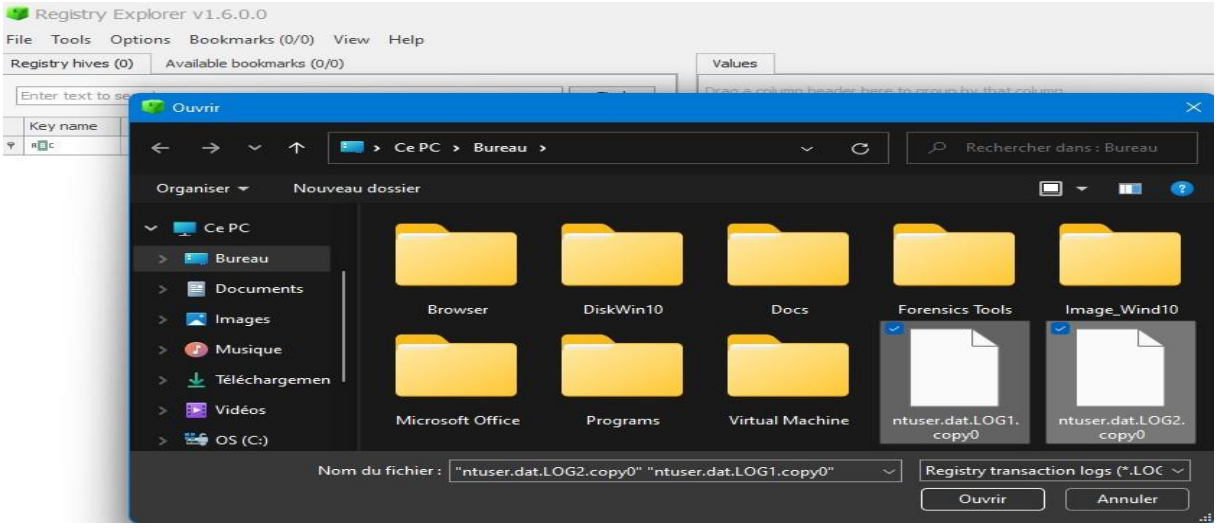
On exporte :

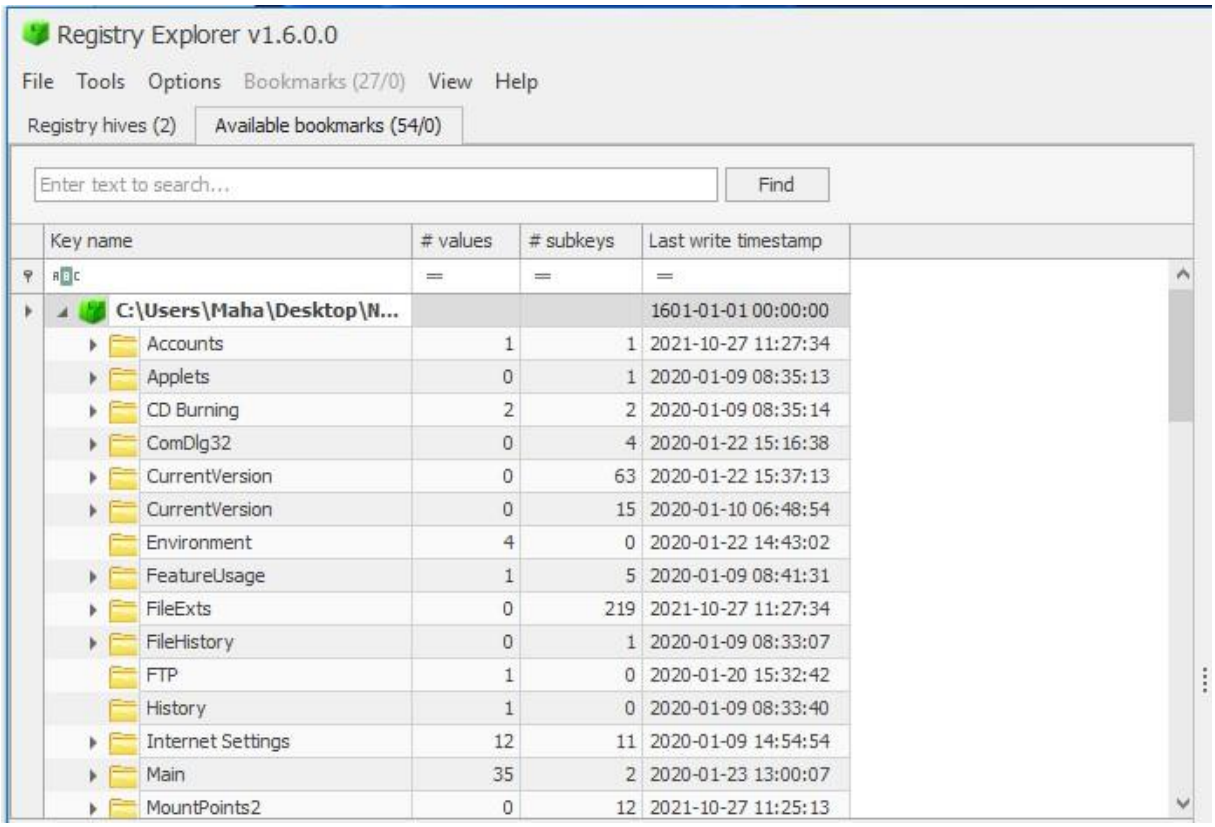


Dans Regitry Explorer : importation des ruches

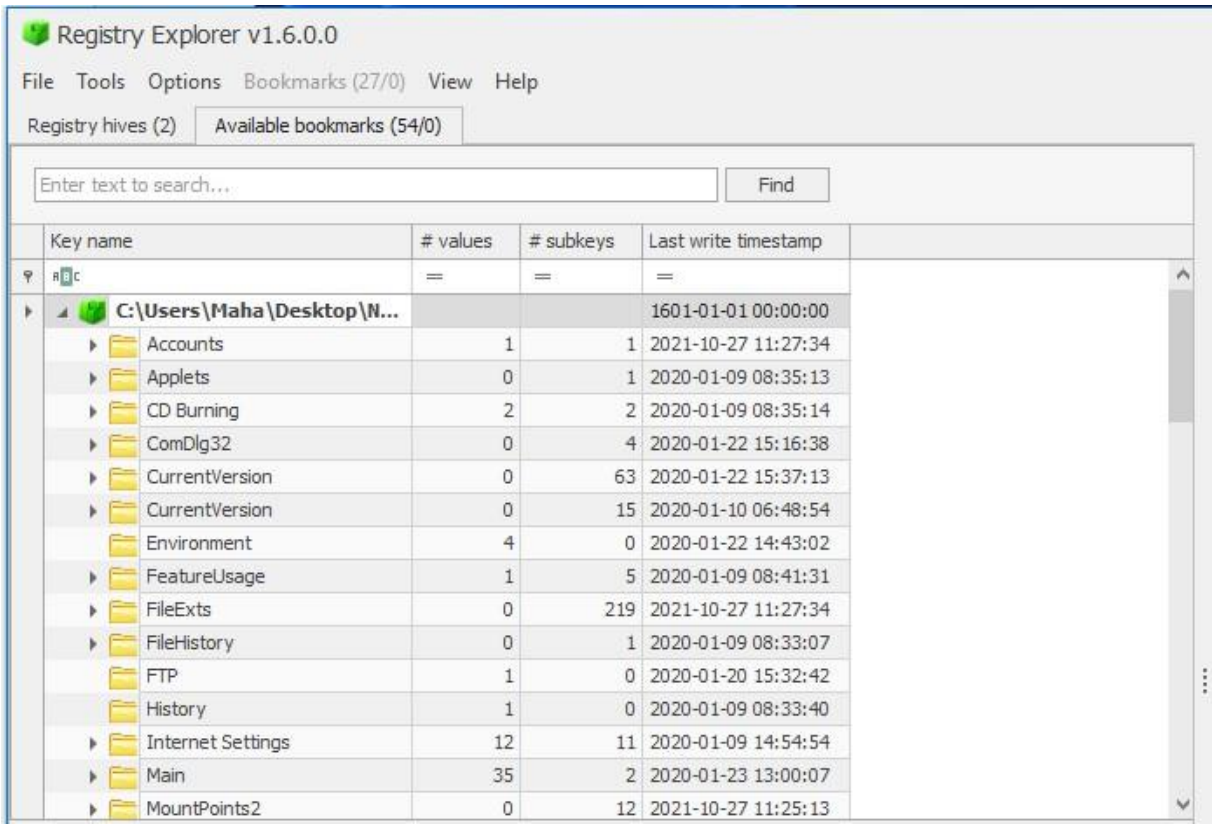


Importe ntuser.dat.LOG1 et ntuser.dat.LOG2 :



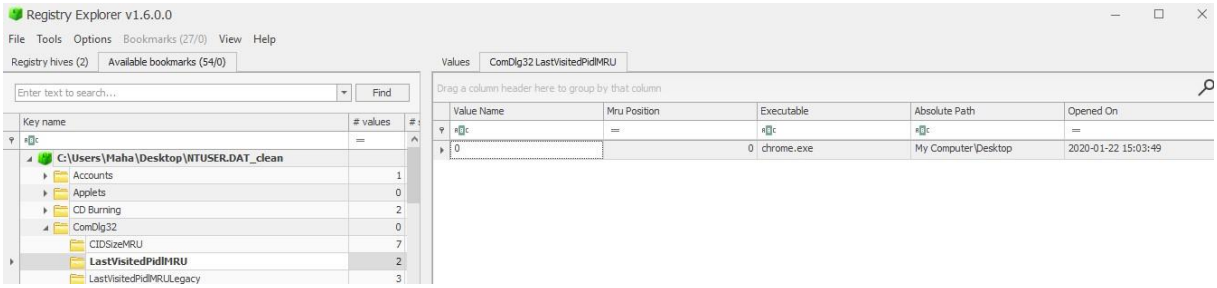


Analyse des registres d'image de disque win10 :



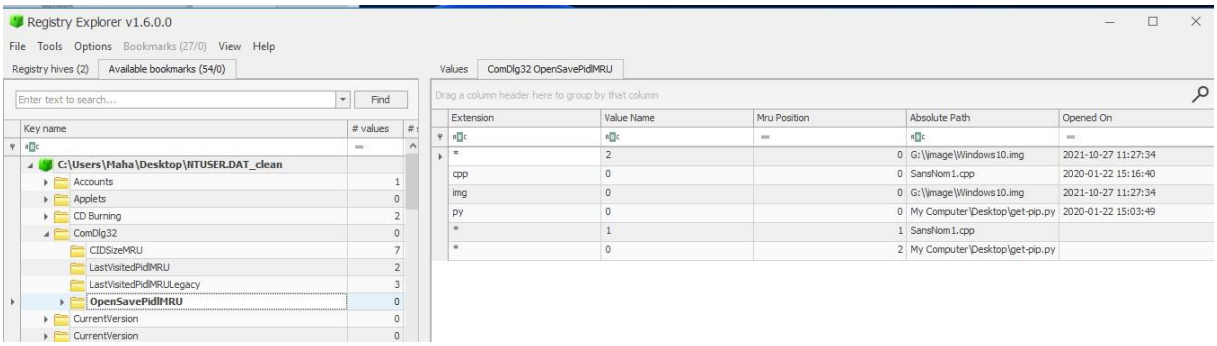
-Analysons les derniers PID les plus utilisés récemment :

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVistedPidlMRU

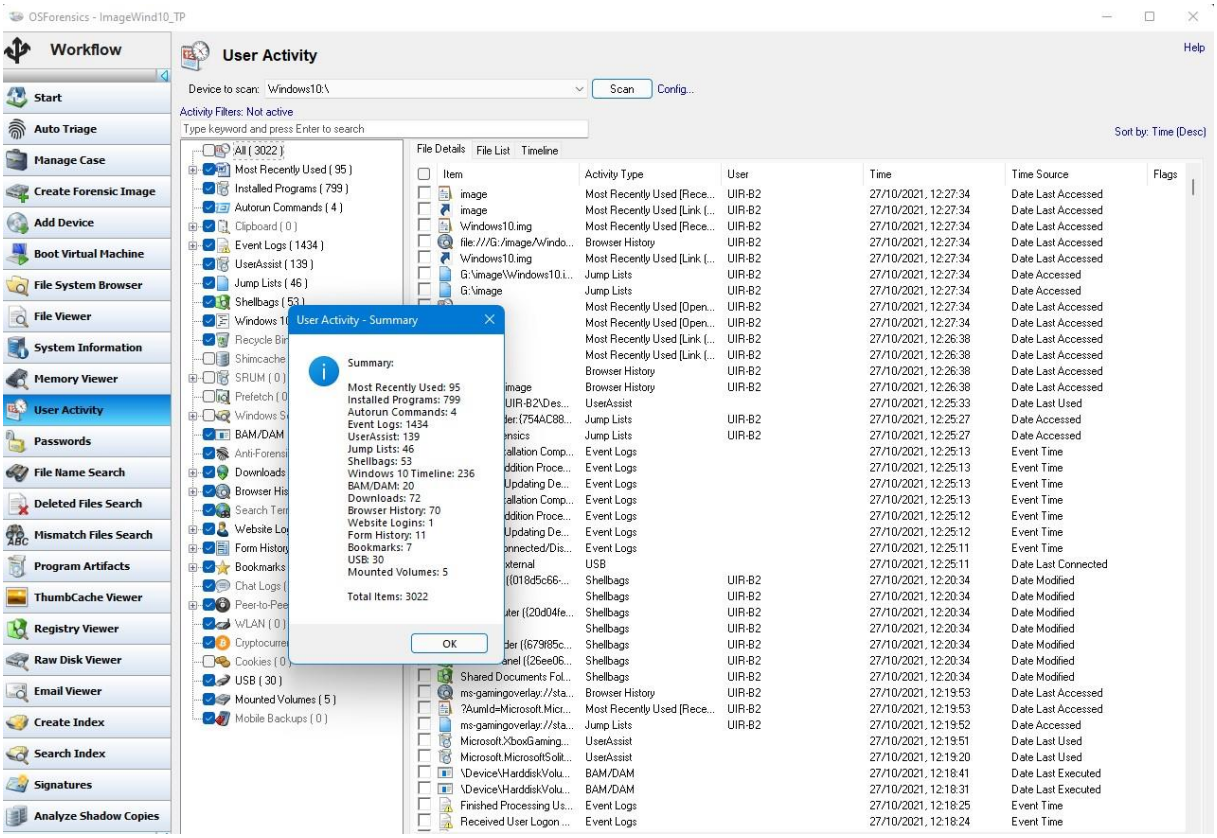


-Analysons les fichiers ouverts ou enregistrés récemment par une application via la boîte de dialogue du shell Windows :

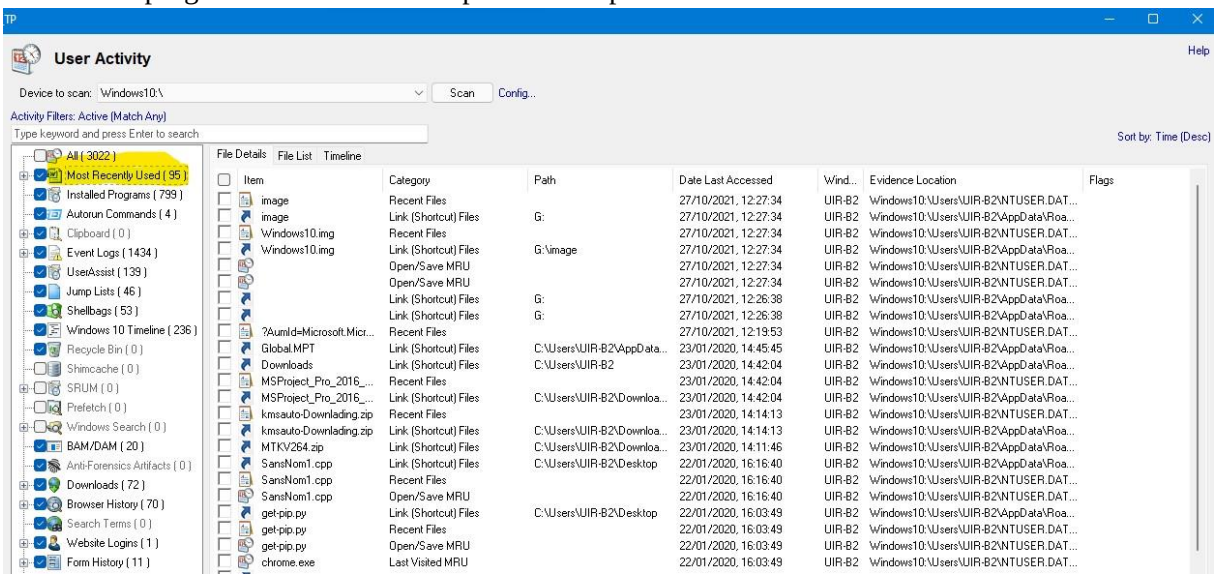
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU



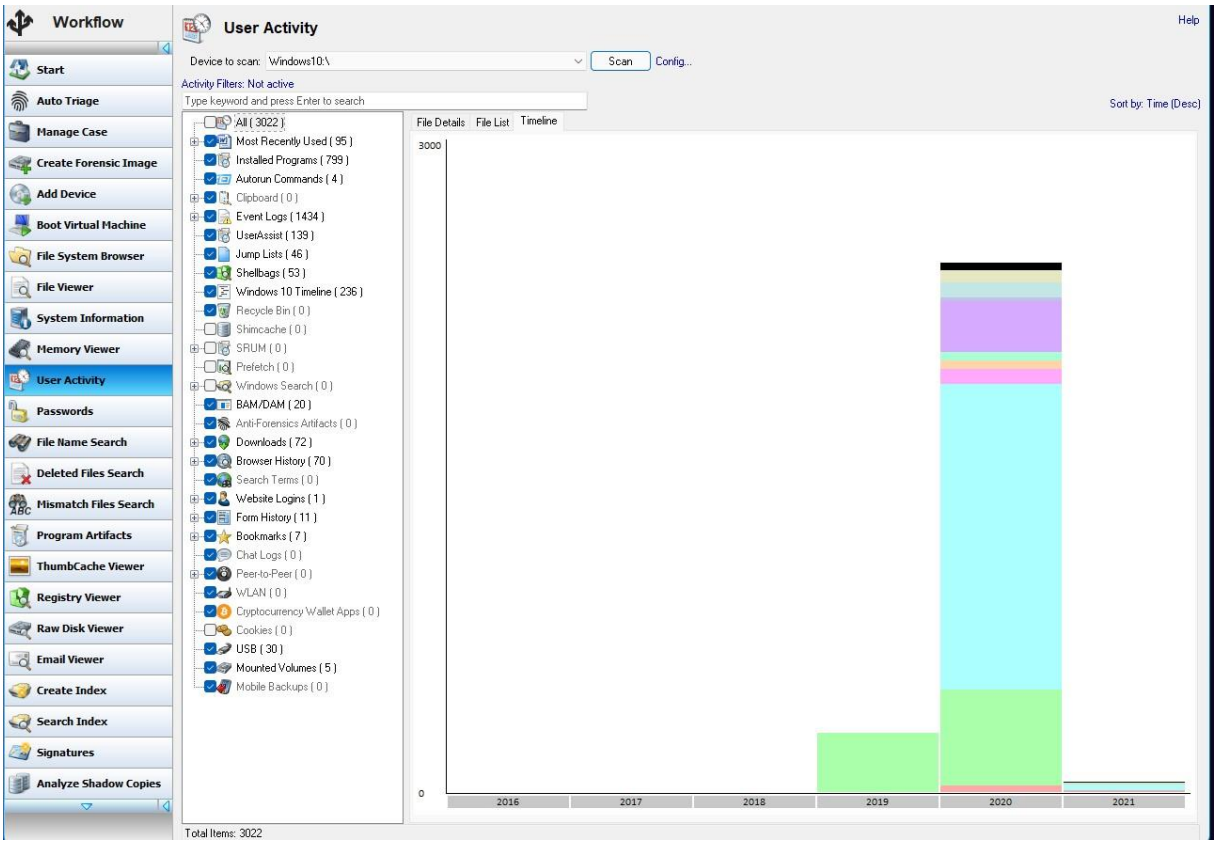
Dans OSForensics:
-Scan User activity



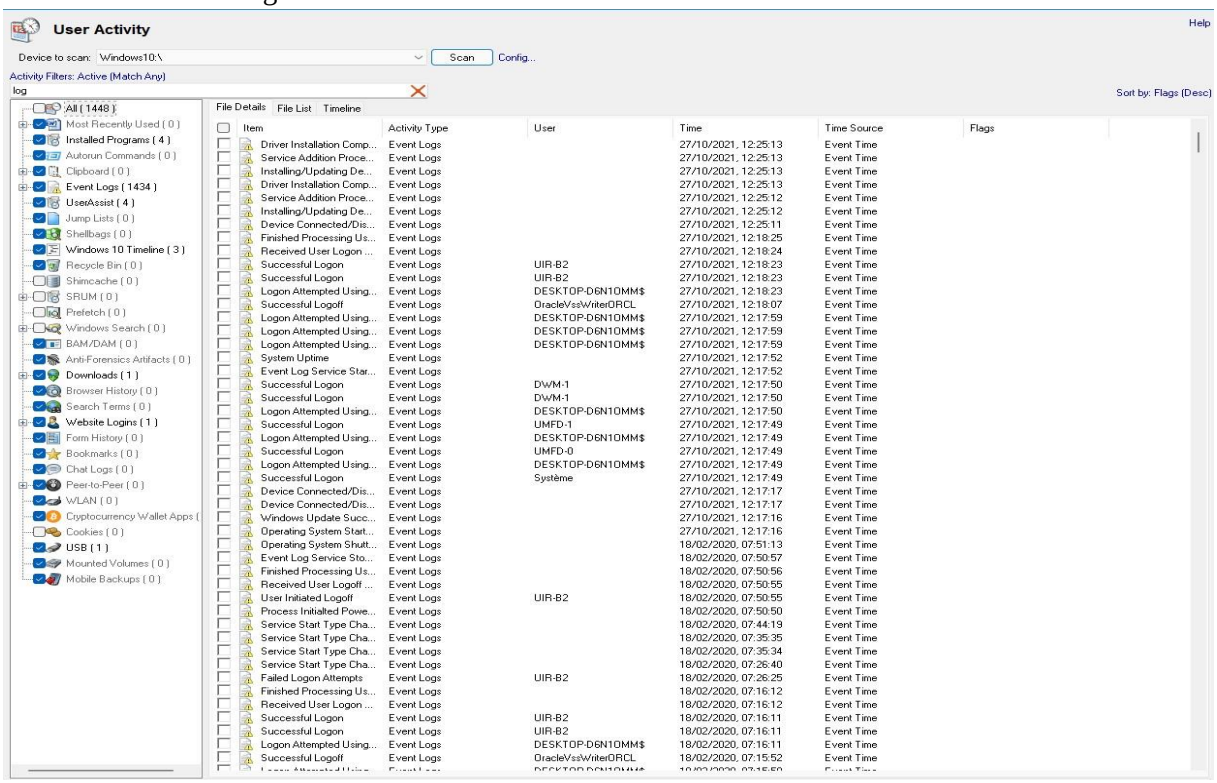
-La liste des programmes et fichiers les plus utilisés par utilisateur UIRB2 :



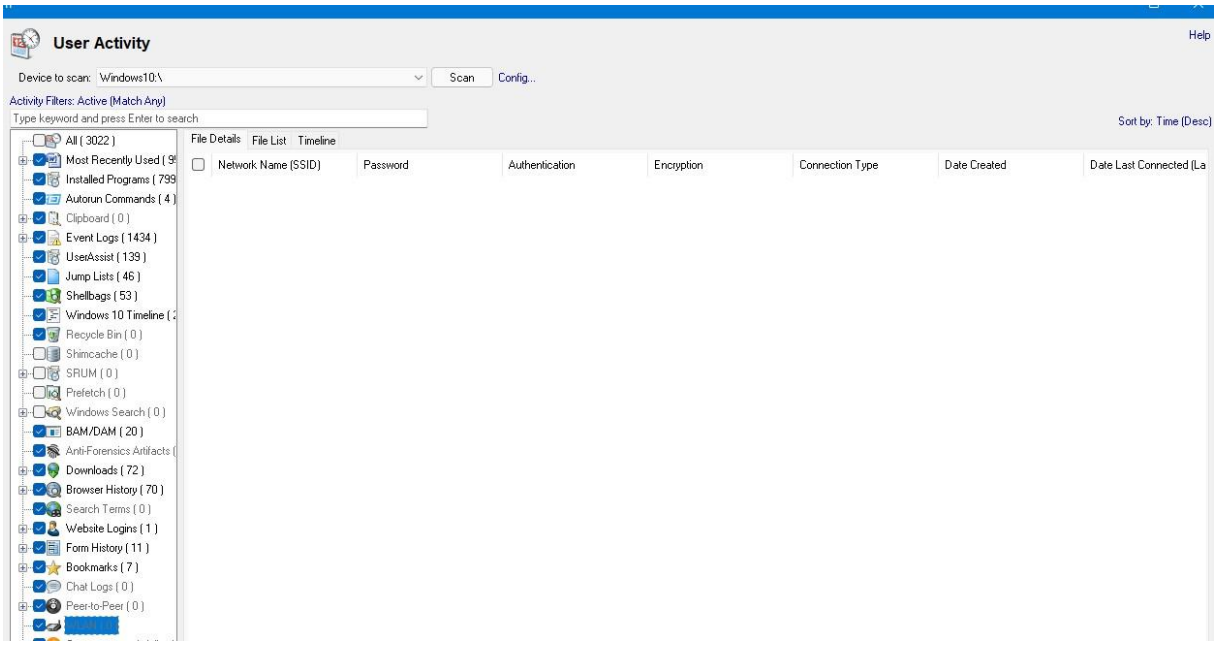
-Le temps d'utilisation :



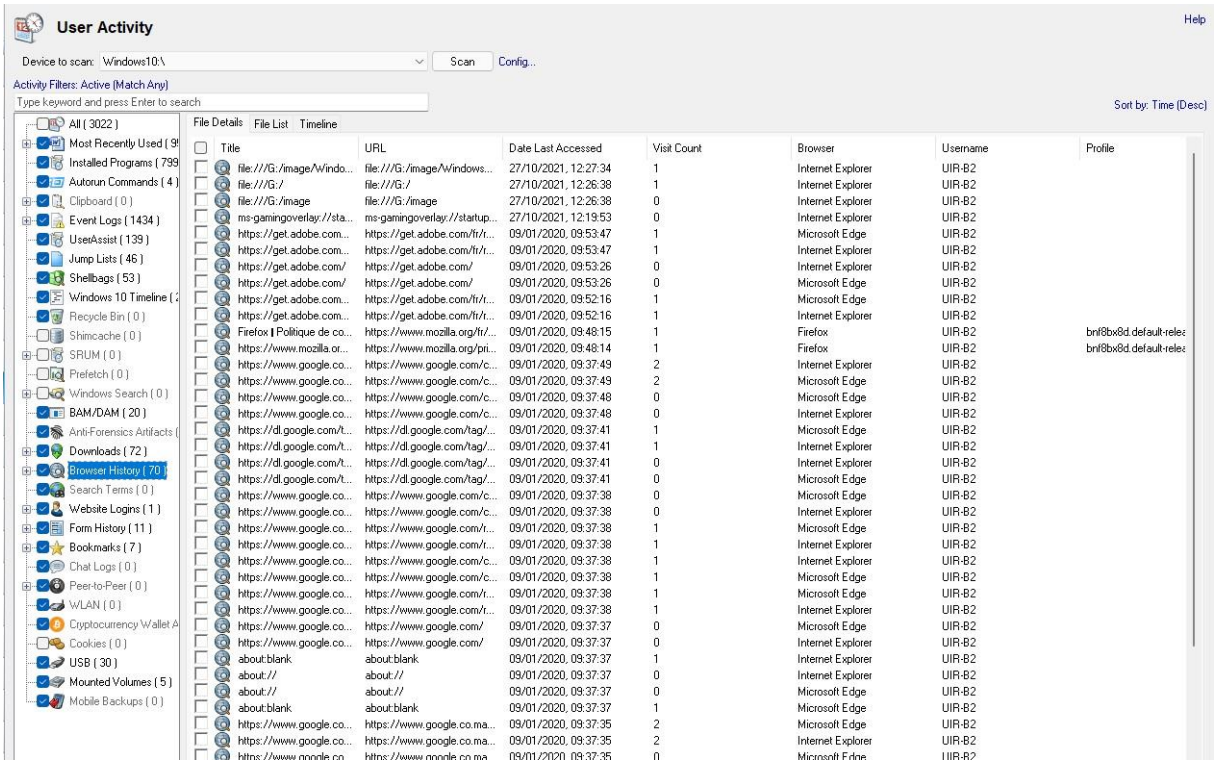
-La liste des fichiers log :



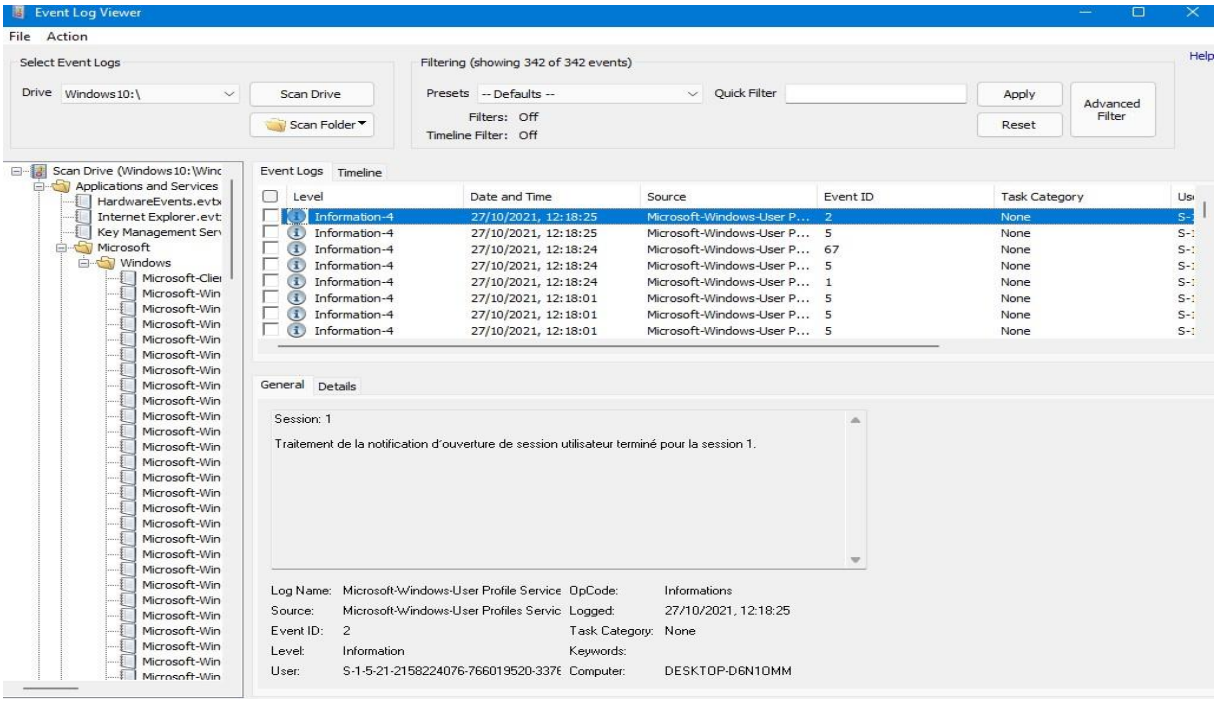
Aucun réseau Wifi enregistré trouvé, cela indique que cette machine ne se connecte pas à un réseau Wifi



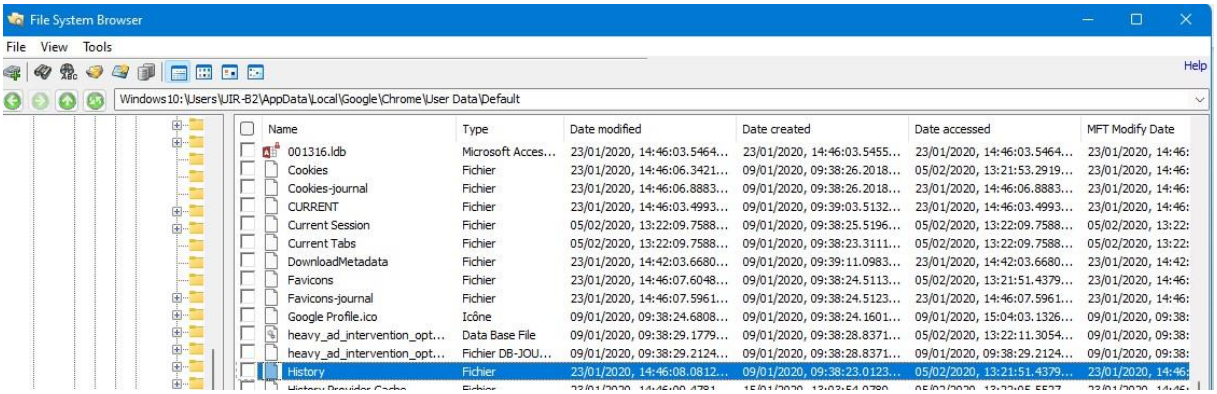
La liste d'historique Web :

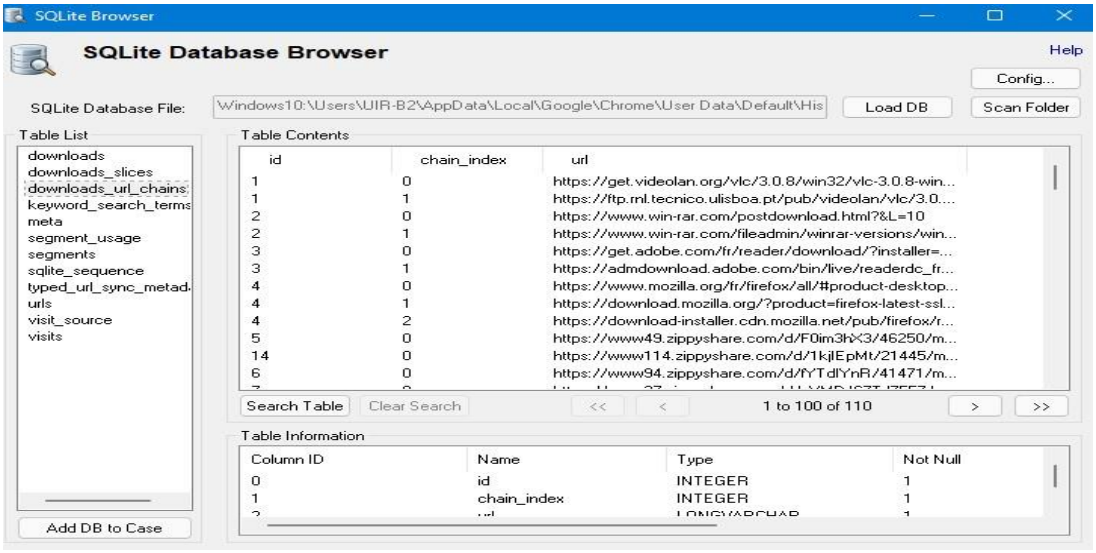


-Exemple d'un fichiers log que j'ai consulté pour avoir lus d'information :

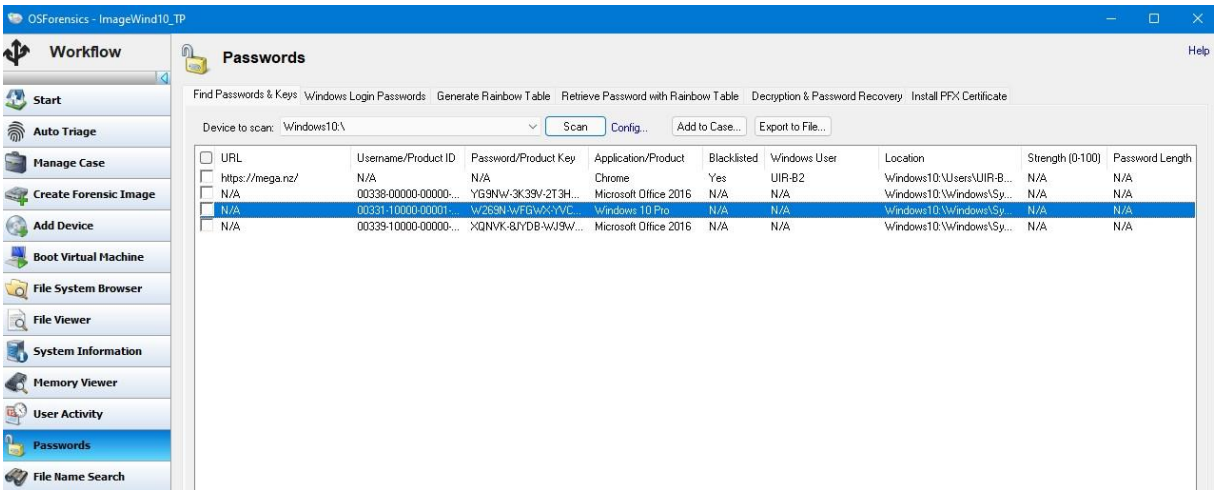


-Consulter un fichier **History** de Google chrome

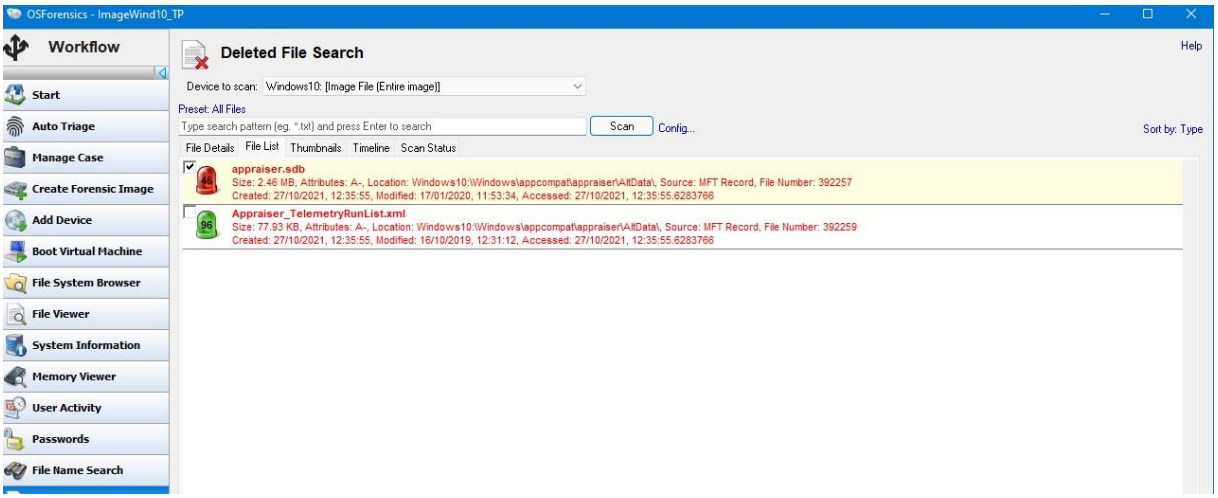




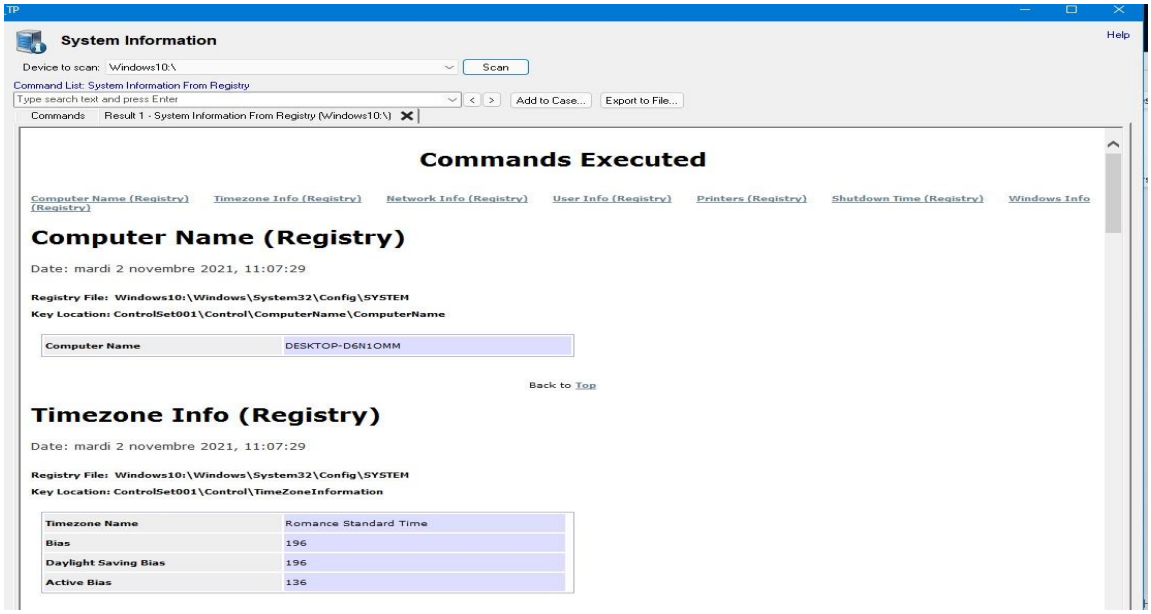
-Passwords: les mots de passe qui sont enregistrés dans la machine



-Les fichiers supprimés :



-Les informations sur le system :



-Sur la carte réseau :

Network Info (Registry)

Date: mardi 2 novembre 2021, 11:07:29

Registry File: Windows10:\Windows\System32\Config\SYSTEM
Key Location: ControlSet001\services\Tcpip\Parameters\Interfaces
Timezone: +1:00

Network GUID	{b419bc18-32b8-11ea-8dea-806e6f6e6963}
Network Name	
IP (using DHCP)	(No)
Network GUID	{b86fbc20-32f6-4ab4-a779-b58fbca656c5}
Network Name	Ethernet
IP (using DHCP)	(No)
Network GUID	{d655a026-f976-435c-b04d-24a7434bf345}
Network Name	VirtualBox Host-Only Network
IP (using DHCP)	(No)
Network GUID	{fc33b7c6-e146-40d4-bf4b-e115b0eea9e4}
Network Name	Ethernet (Kernel Debugger)
IP (using DHCP)	(Yes)
DHCP Server	
DHCP Name Server	
Lease Obtained	mercredi 22 janvier 2020, 15:17:34
Lease Expires	mercredi 22 janvier 2020, 15:17:34

-Sur les comptes utilisateurs :

User Info (Registry)

Date: mardi 2 novembre 2021, 11:07:29

Registry File: Windows10:\Windows\System32\Config\SAM
Key Location: SAM\Domains\Account\Users
Using Timezone: +1:00

Username [ID]	Administrator [500]
Full Name	
Description	Built-in account for administering the computer/domain
Password Hint	
Account Created	N/A
Last Login	Never
Password Reset	Never
Password Fail Date	N/A
Password Fail Count	0 (reset after correct login)
Login Count	0
Notes	*Password never expires*
Username [ID]	Guest [501]
Full Name	
Description	Built-in account for guest access to the computer/domain
Password Hint	
Account Created	jeudi 9 janvier 2020, 09:26:32 (can be inaccurate if registry permissions have been updated)
Last Login	Never
Password Reset	Never
Password Fail Date	N/A
Password Fail Count	0 (reset after correct login)
Login Count	0
Notes	*Password never expires*

Username [ID]	UIR-B2 [1001]
Full Name	UIR-B2-DEV
Description	
Password Hint	
Account Created	jeudi 9 janvier 2020, 09:26:32 (can be inaccurate if registry permissions have been updated)
Last Login	mercredi 27 octobre 2021, 12:18:23
Password Reset	lundi 13 janvier 2020, 11:12:54
Password Fail Date	lundi 13 janvier 2020, 10:23:44
Password Fail Count	0 (reset after correct login)
Login Count	50
Notes	*Password never expires*

-Sur le temps d'arrêt de la machine :

Shutdown Time (Registry)

Date: mardi 2 novembre 2021, 11:07:29

Registry File: Windows10:\Windows\System32\Config\SYSTEM

Key Location: ControlSet001\Control\Windows

Last shutdown time:	mardi 18 février 2020, 07:51:12

Sur le système d'exploitation installé :

Windows Info (Registry)

Date: mardi 2 novembre 2021, 11:07:29

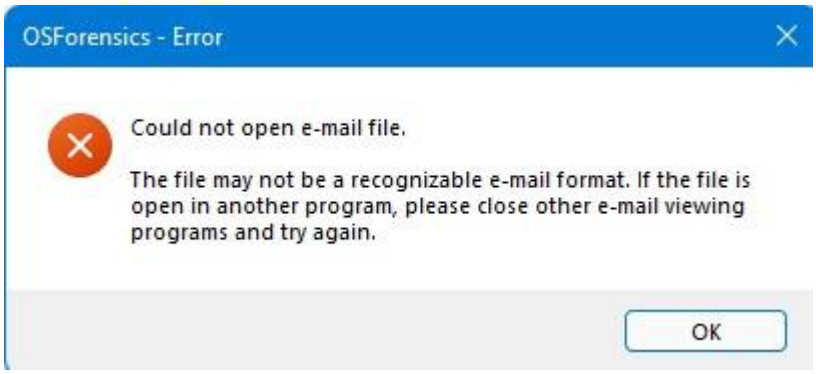
Registry File: Windows10:\Windows\System32\Config\SOFTWARE

Key Location: Microsoft\Windows NT\CurrentVersion

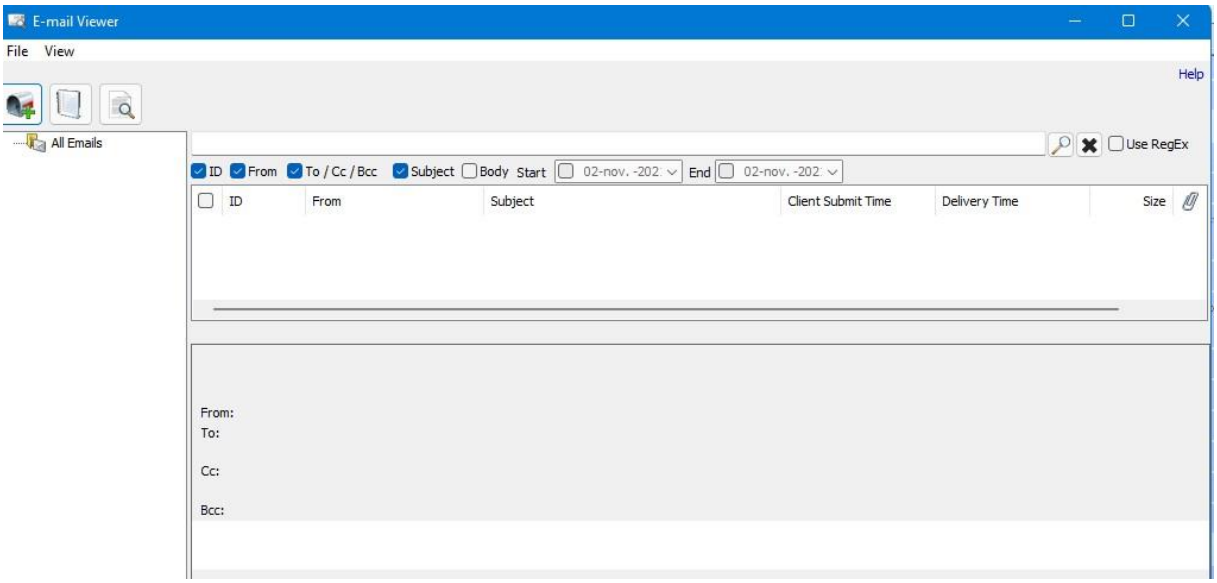
Timezone: +1:00

Install path	C:\Windows
Build string	18362.19h1_release.190318-1202
Extended build string	18362.1.amd64fre.19h1_release.190318-1202
Build number	18362
Install date	jeudi 9 janvier 2020, 09:29:10
ProductName	Windows 10 Pro
Version	1903
ProductId	00331-10000-00001-AA734
DigitalProductId	W269N-WFGWX-YVC9B-4J6C9-T83GX
RegisteredOwner	UIR-B2
RegisteredOrganization	

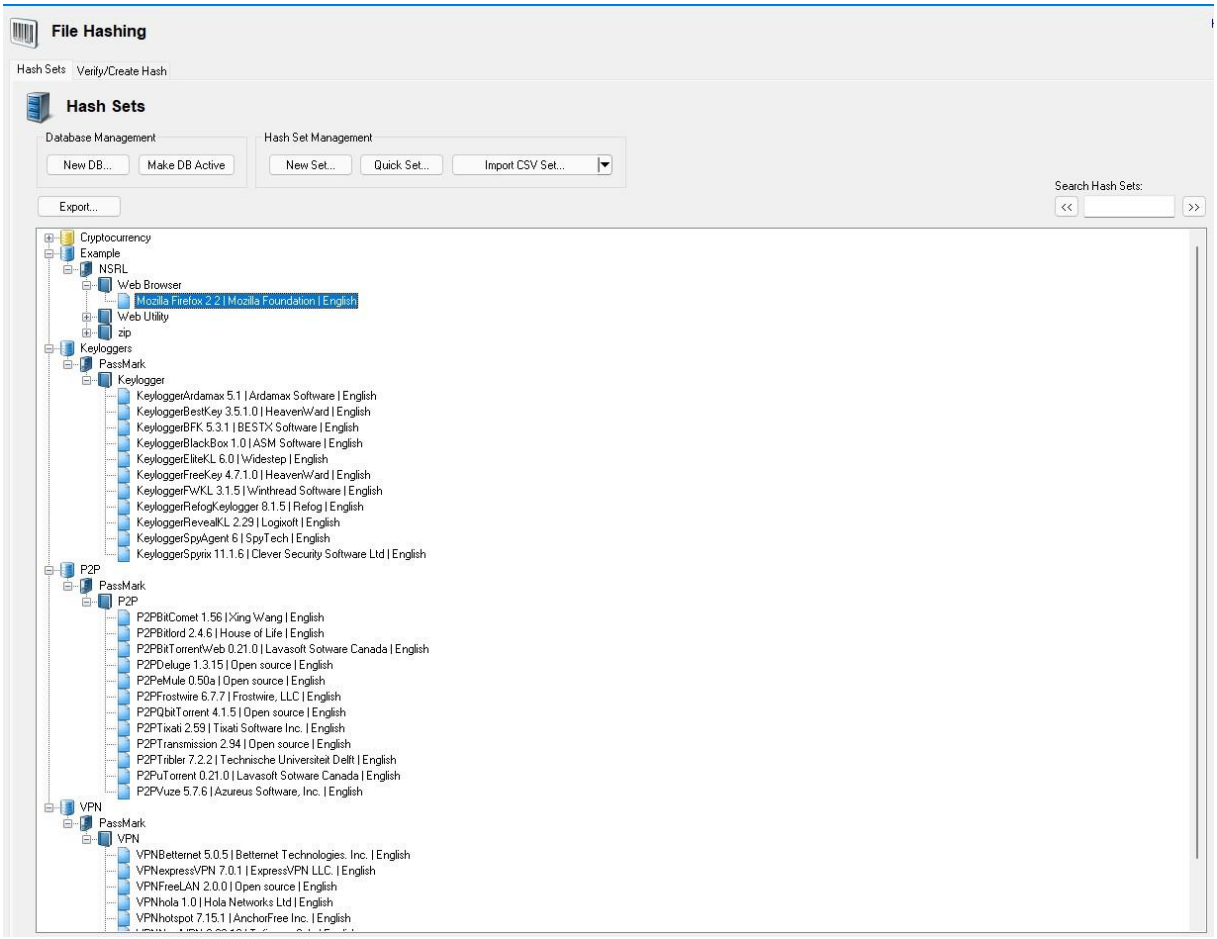
Pour les emails : je ne peux pas avoir un aperçu sur les emails, une erreur s'affiche lors de consulter email viewer :



Aucun courriel trouvé :



Les fichiers hachés :



Conclusion :

Une analyse forensique fait suite à un incident, on utilise le forensique pour analyser les malwares c'est-à-dire surveiller un PC pour détecter des actions malveillantes, ou bien récupérer des preuves numériques. Il existe plusieurs domaines de forensique : forensique réseau qui se limitent à analyse la connexion réseau, etc.

Les différentes approches pour faire une analyse forensique :

Dans ce rapport on a fait de types d'approches, la première c'est analyse à chaud (live Forensics) on a utilisé Registry Explorer pour analyser la base de registre et étudier l'état du système qui allumé

La deuxième c'est l'analyse à froid (Dead Forensics) on a analysé à l'aide des outils OSforensics, Autopsy un système éteint, on a copié un ensemble de données d'une machine réel.