REPUBLIQUE DU SENEGAL

Un Peuple-Un But-Une Foi

****

Ministère de l'Enseignement Supérieur de la Recherche et de l'innovation Direction Générale de l'Enseignement Supérieur Privé

BEM TECH

BEM School of Technology

Rapport

Investigation numérique sur clé USB suspect

Présenté par :

Moustapha SY

Sommaire

Table des figures

Résumé

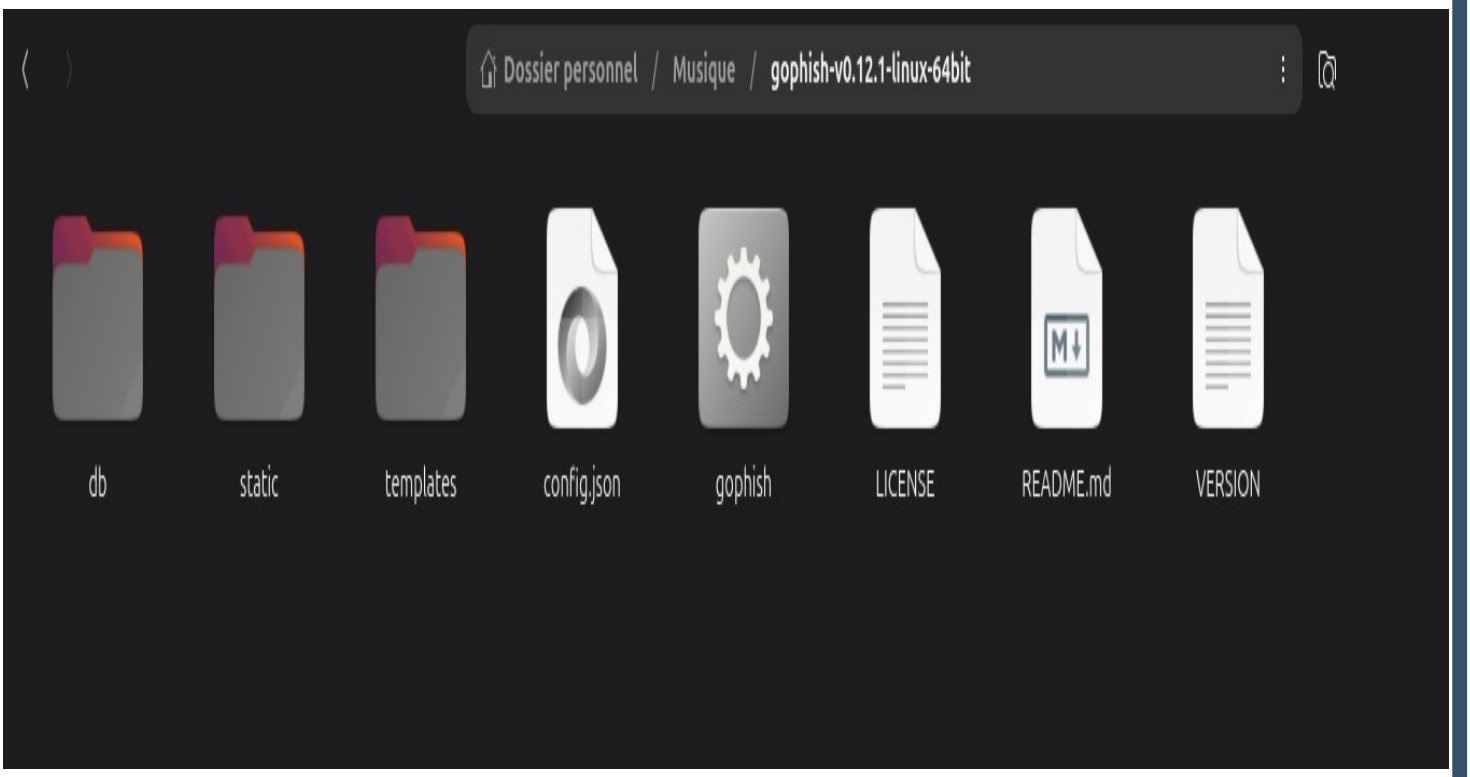
Une copie forensique complete de la clé usb a etait créée à l’aide de FTK Imager afin de preserver l’intégrité des données et d’éviter toute modification du support original. Ensuite l’image est importer et analyser dans Autopsy.
L’examen détaillé a permis d’identifier un élément suspect, notamment un fichier .exe exécutable non légitime. Maintenant pour vérifier que si c’est un fichier malveillant , nous avons utilisé un service en ligne ‘MetaDefender cloud’ , et ensuite de cela , effectivement le fichier est reconnu comme malveillant.

Glossaires

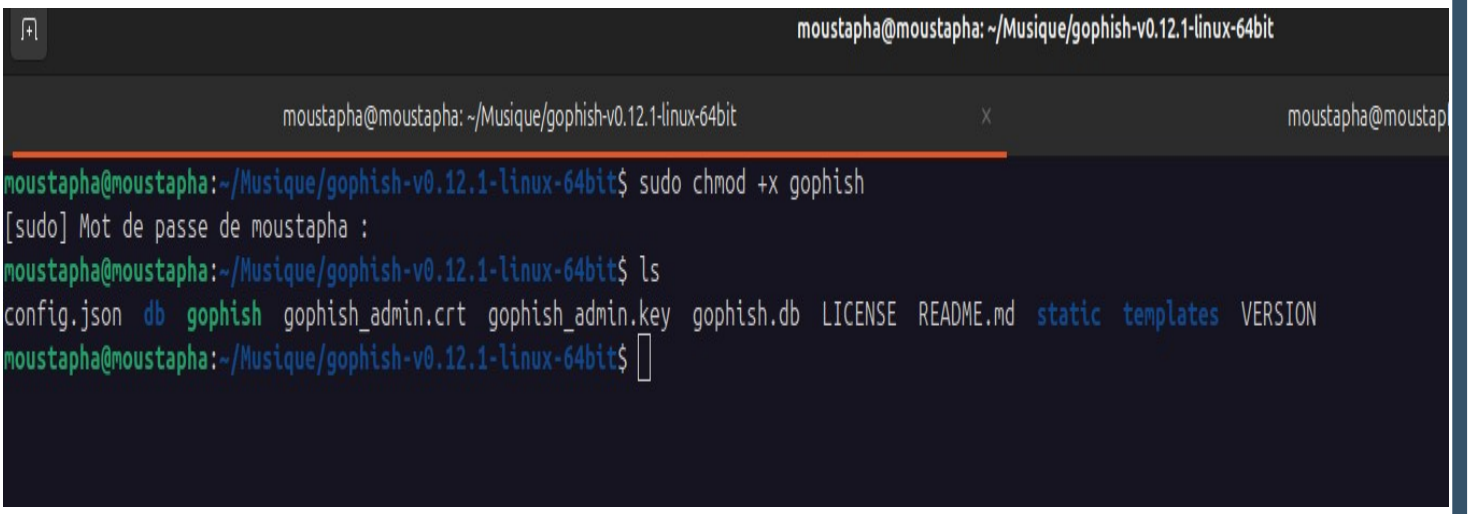
Introduction

Dans le cadre de la sécurité du système d’information, une clé usb suspecte a été introduite dans un poste de travail . L’objectif de cette investigation est de déterminer si la clé contient des éléments malveillant , de l’identifier et de déterminer le vecteur d’infection. Et nous allons utilisé un les outils FTK imager et Autopsy pour procéder à cela.

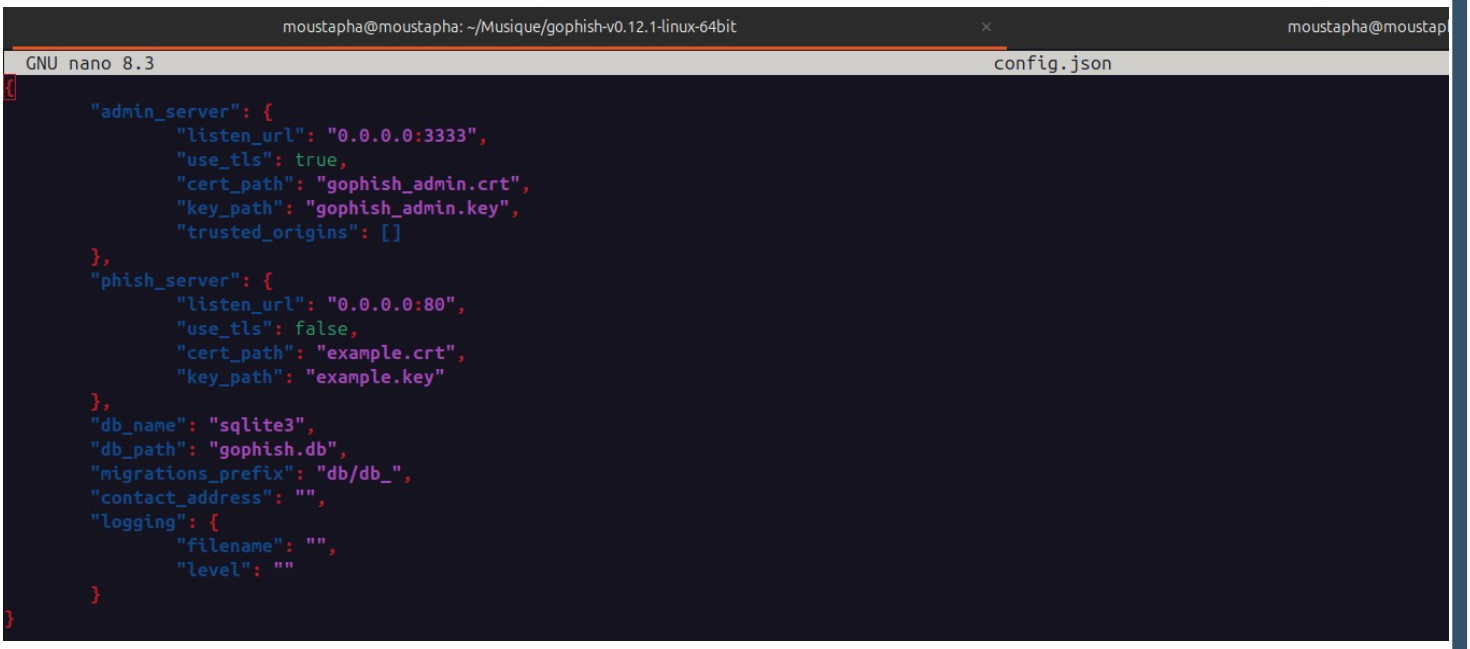
Préparation de clé



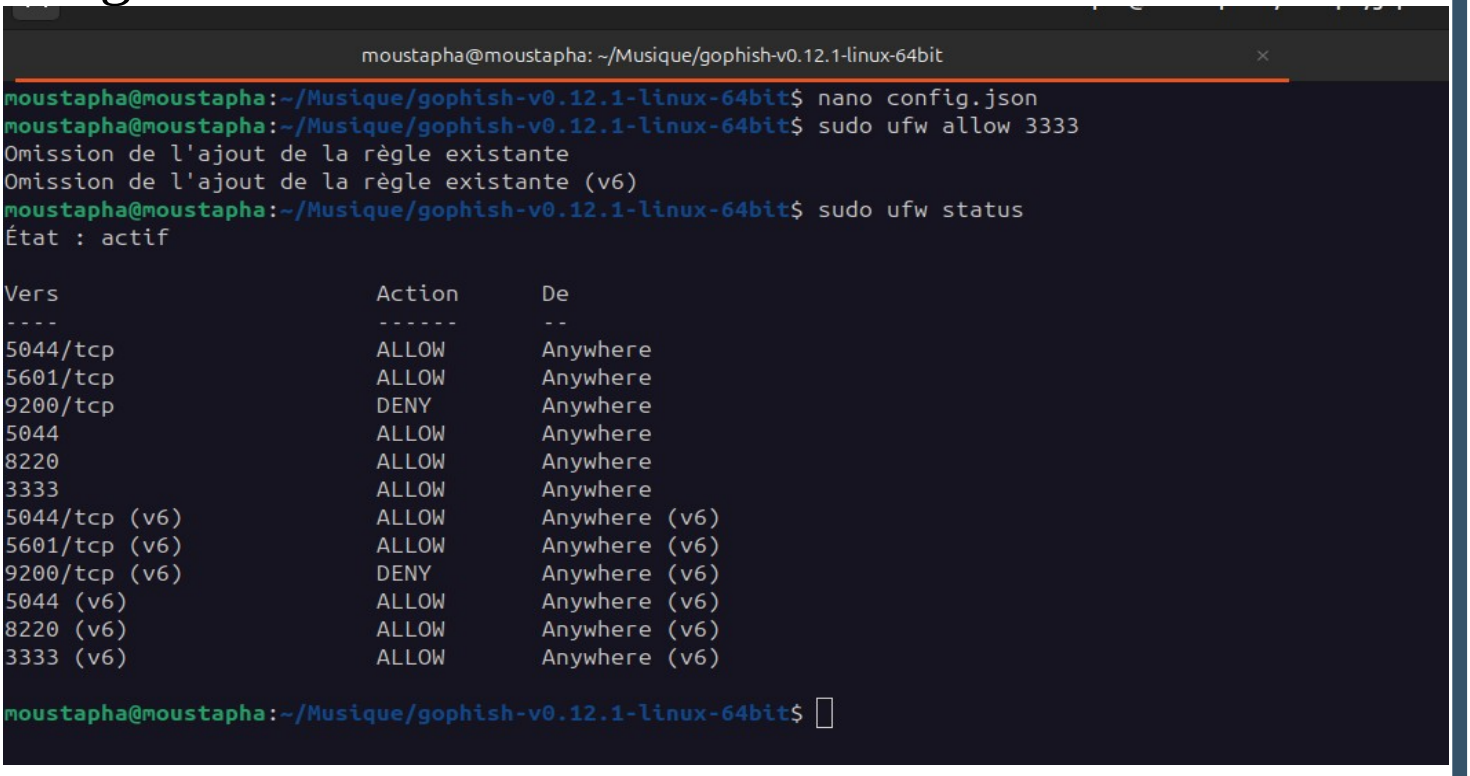
Ici on a mis un fichier malveillant Facture.exe avec d’autres fichiers



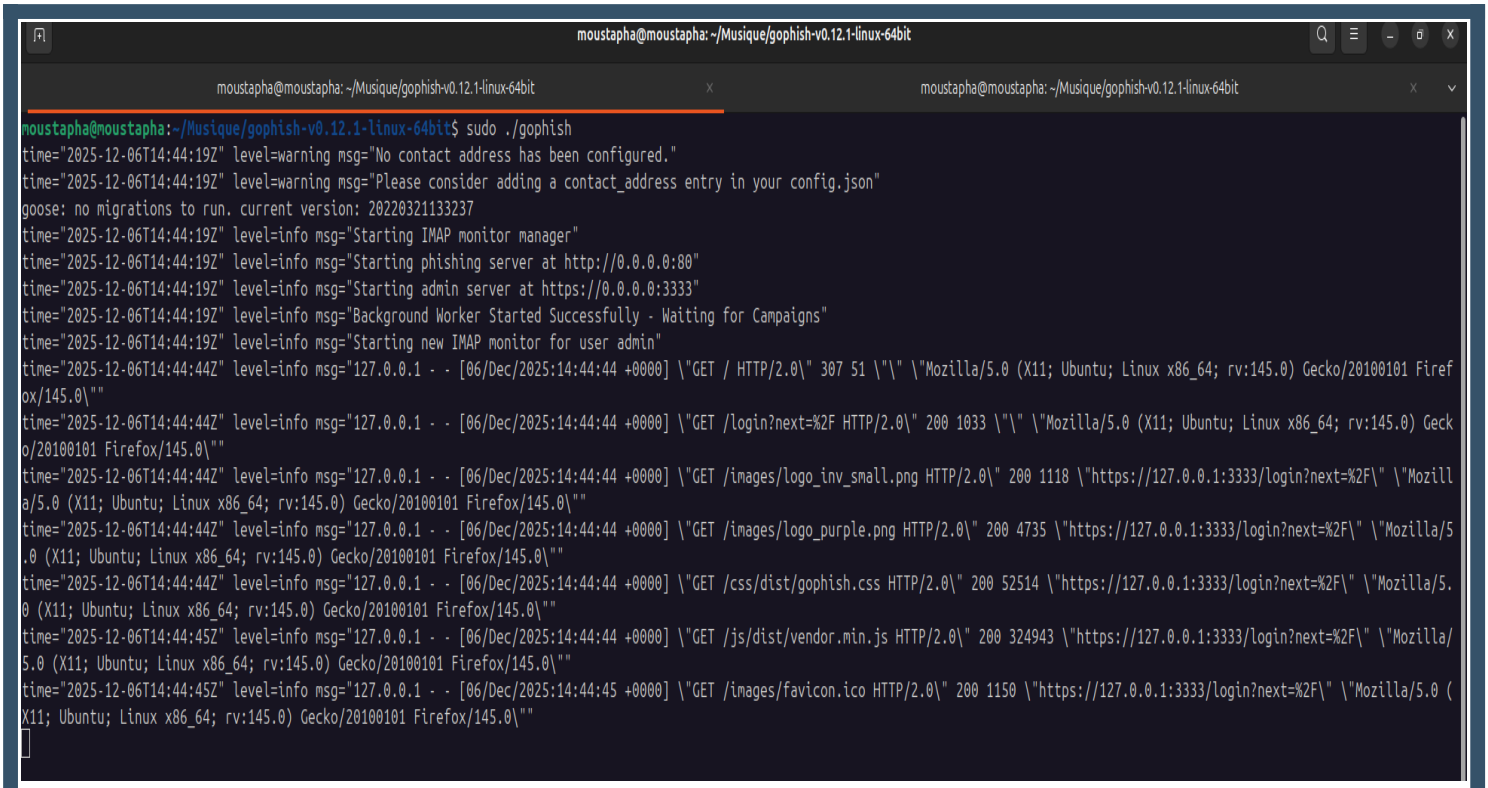
Ici , on vient de formater la clé



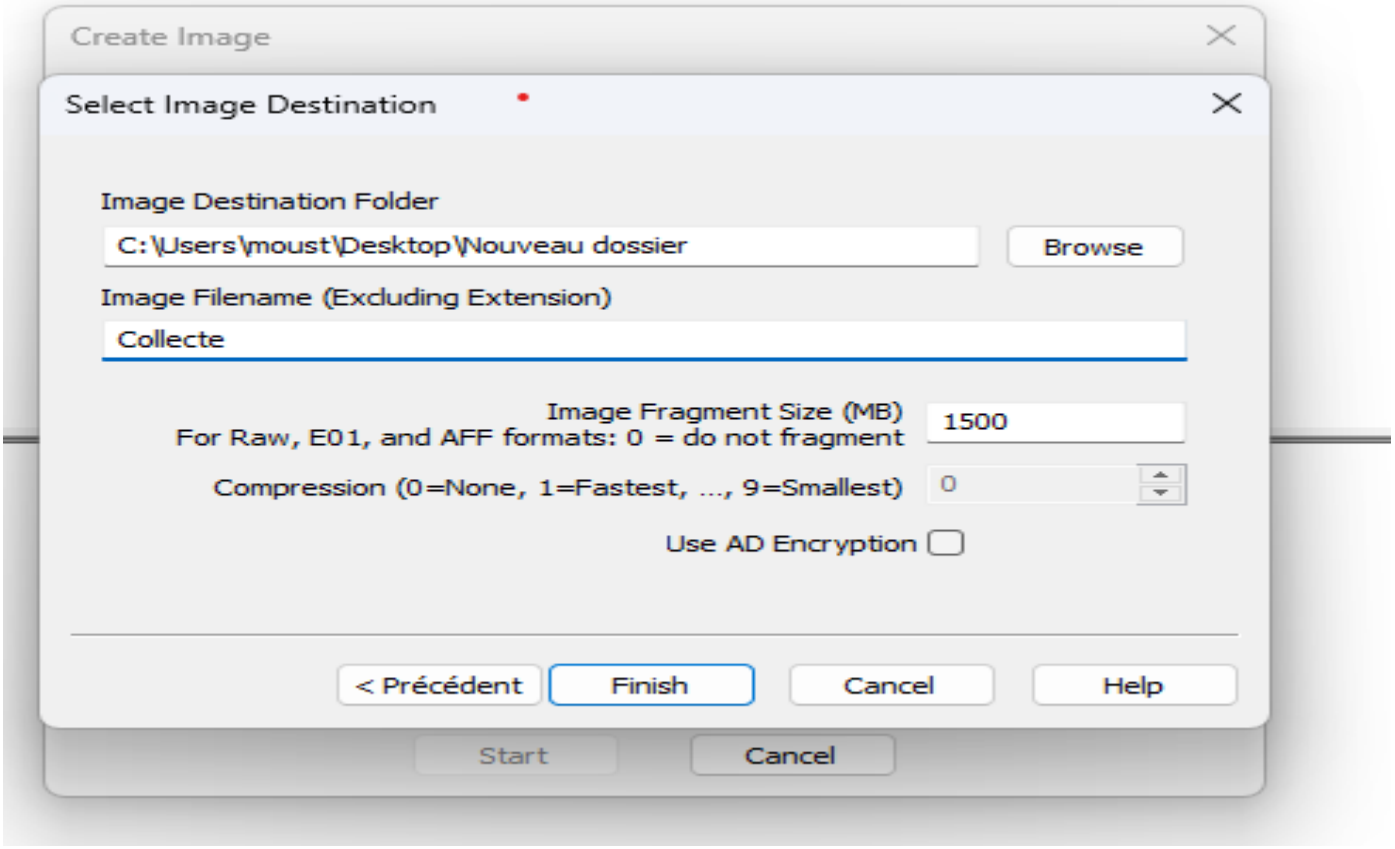
Maintenant , on ouvre FTK et on click sur ‘Create disk image’



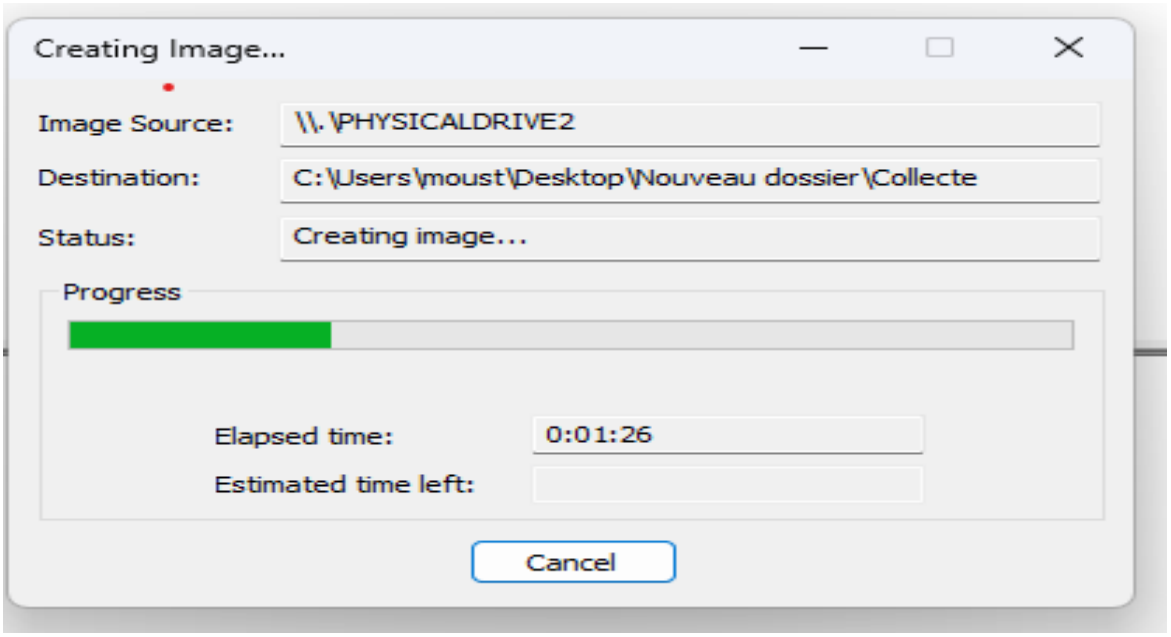
On choisi , ‘Physical drive’ puis ‘Raw dd’ pour faire une copie bit à bit’

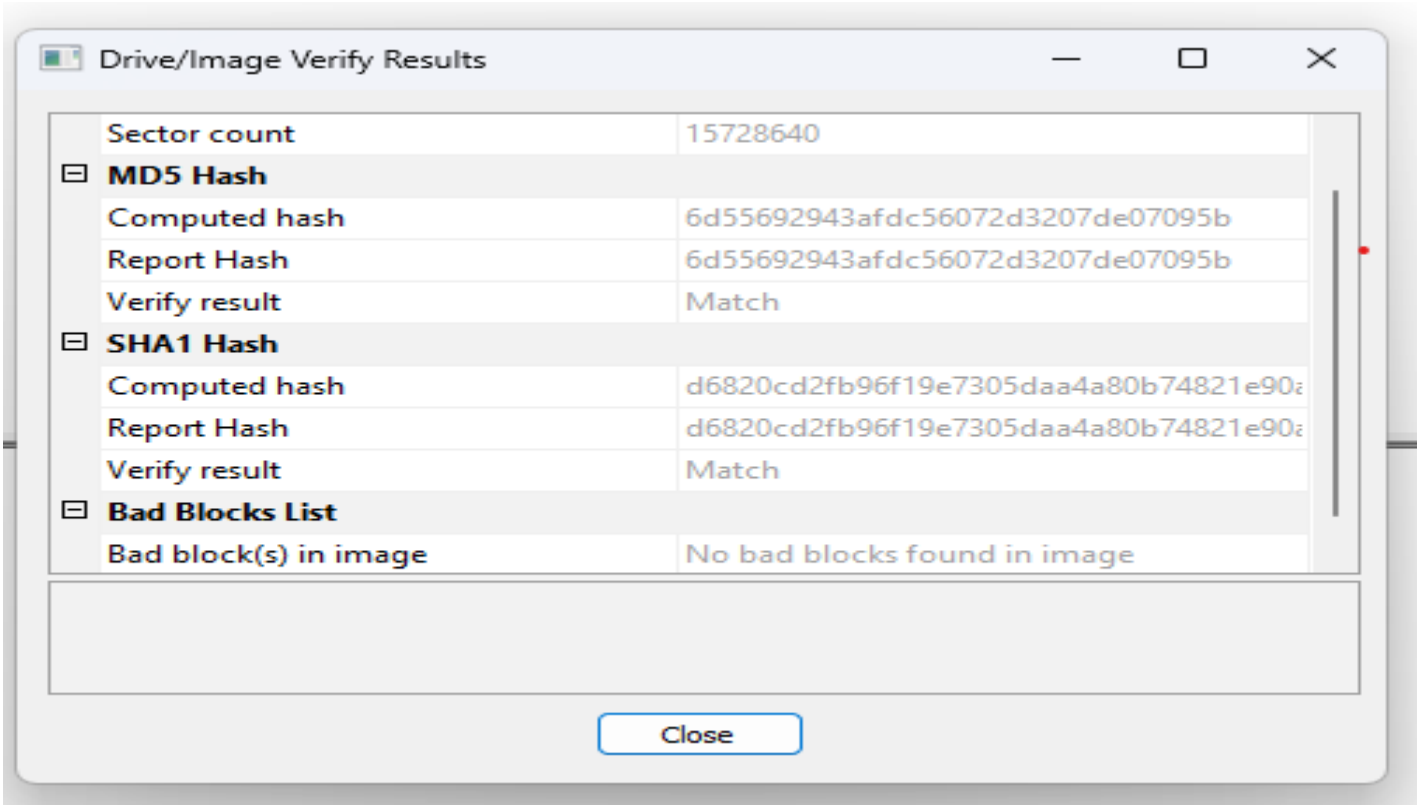


Ici on défini un case number



On met le chemin ou on doit mettre l’image, et apres ça on click sur finish > start

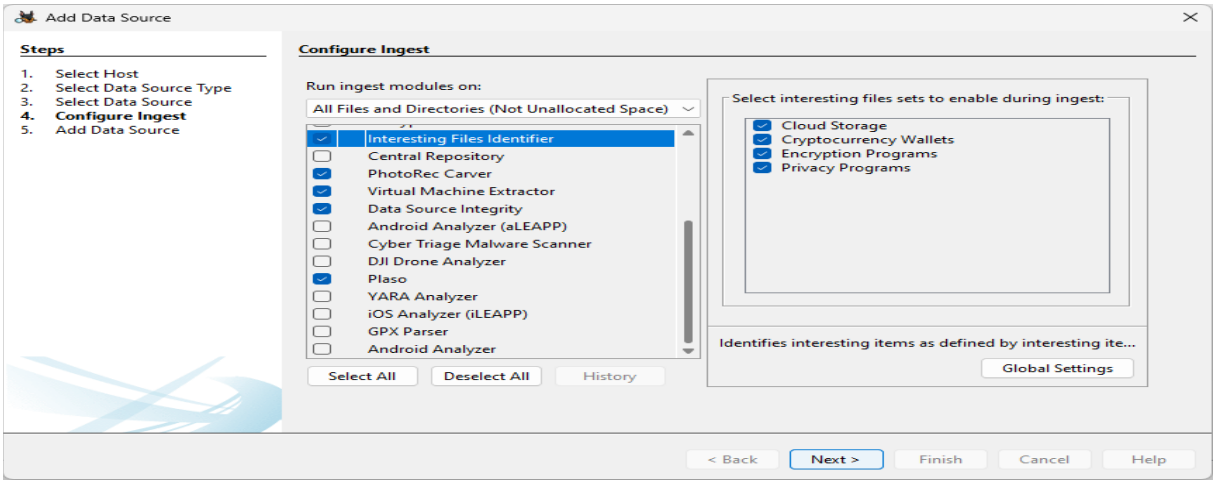




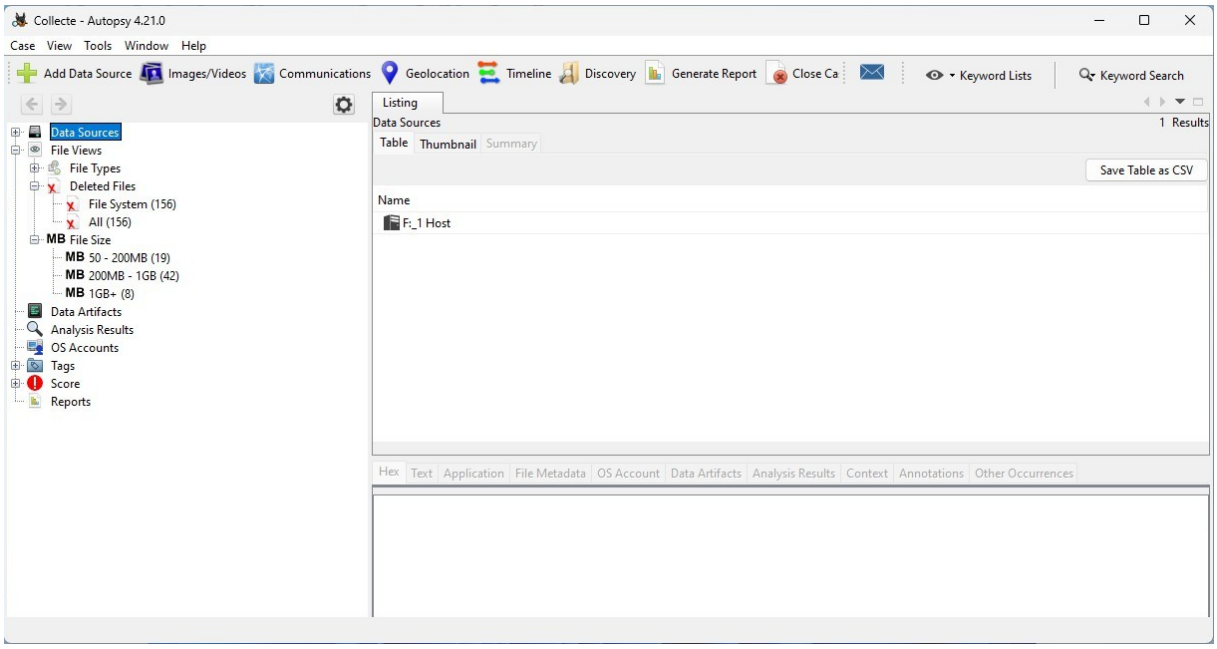
Maintenant l’image est entrain d’etre copier et apres la copie terminer , on peut voir en md5 et à SHA1

Analyse de l’image

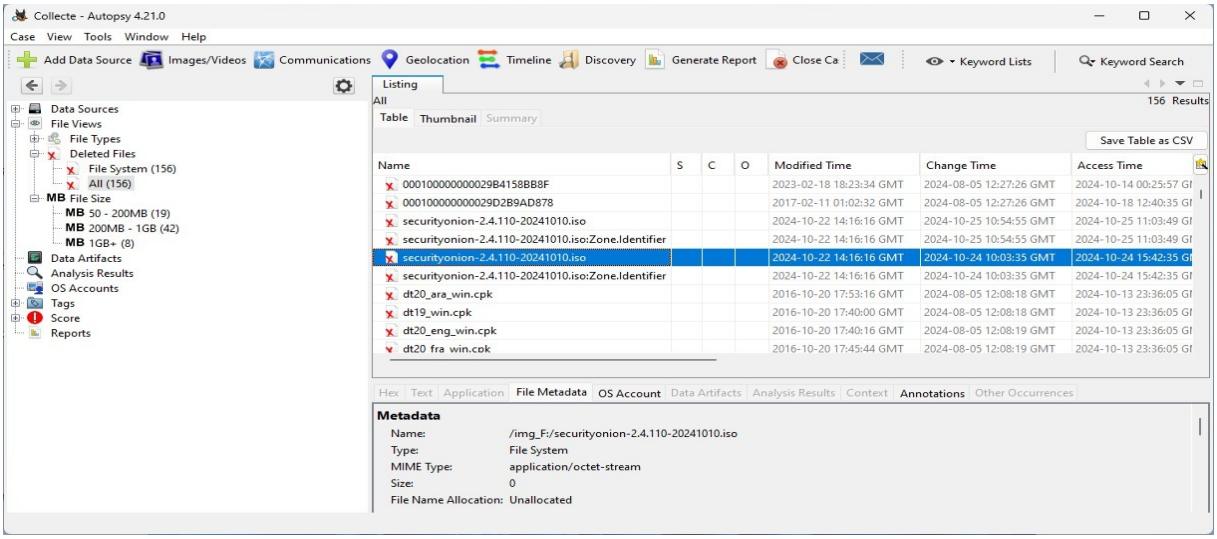
Ici, on ouvre autopsy



On configure le ingest pour filtrer les elements a recuperer

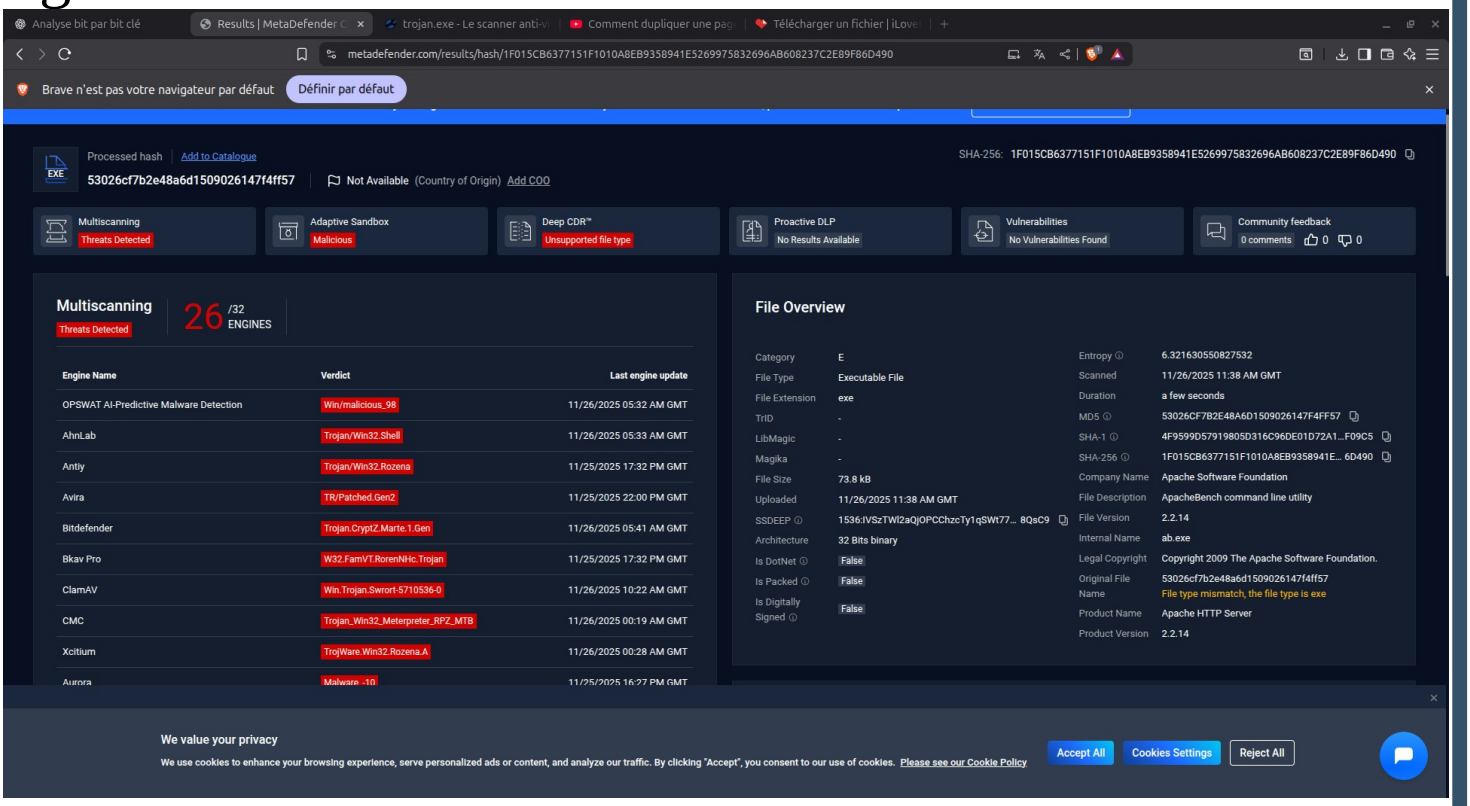


Ici , on a resultat de la recuperation



Ici , on a identifié un fichier nommé Facture.exe

Pour le moment on peut pas affirmer que cest un fichier malveillant , donc on va verifier avec un service en ligne nommé MetaDefence Cloud



Apres avoir mis le fichier dans site du service , 26 structures on affirmé que ce fichier est malveillant et peut compromettre un systeme , cest a dire ce fichier s’evolue comme un trojan.

Détermination du vecteur d’infection

ce fichier infecte le systeme apres que la victime l’est executer . La stenographie a été utilisais pour tromper l’utilisateur à cliquer sur une facture , et apres click click , l’attaquant peut même acceder au webcame de la victime.