

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



Rapport

Investigation numérique sur clé USB suspect

Présenté par :

Moustapha SY

Sommaire

Table des figures.....	1
Résumé.....	2
Glossaire.....	3
Introduction générale.....	4
Préparation de clé.....	5
Copie l'image de la clé.....	6
Analyse de l'image.....	7
Identifications des fichiers vulnérables.....	8
Détermination du vecteur d'infection	9

Table des figures

Figure 1 : Consultation de clé

Figure 2 : Formatage de la clé

Figure 3 : Premier etape avec ftk

Figure 4 : Deuxieme etape avec FTK

Figure 5 : Troixieme etape avec FTK

Figure 6 : Quatrieme etape FTK

Figure 7 : Cinquieme etape FTK

Figure 9 : Lancement de Autopsy

Figure 10 : Selection des filtres et recuperation des hash

Figure 11 : Affichage du resultat

Figure 12 : Identification du fichier malveillante

Figure 13 : Verification du fichier malveillant

Résumé

Une copie forensique complete de la clé usb a etait créée à l'aide de FTK Imager afin de préserver 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

```
moustapha@moustapha: ~/Musique/gophish-v0.12.1-linux-64bit

moustapha@moustapha: ~/Musique/gophish-v0.12.1-linux-64bit x moustapha@moustapha:

moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ sudo chmod +x gophish
[sudo] Mot de passe de moustapha :
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ ls
config.json db gophish gophish_admin.crt gophish_admin.key gophish.db LICENSE README.md static templates VERSION
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$
```

Ici , on vient de formater la clé

```
moustapha@moustapha: ~/Musique/gophish-v0.12.1-linux-64bit
GNU nano 8.3 config.json

{
  "admin_server": {
    "listen_url": "0.0.0.0:3333",
    "use_tls": true,
    "cert_path": "gophish_admin.crt",
    "key_path": "gophish_admin.key",
    "trusted_origins": []
  },
  "phish_server": {
    "listen_url": "0.0.0.0:80",
    "use_tls": false,
    "cert_path": "example.crt",
    "key_path": "example.key"
  },
  "db_name": "sqlite3",
  "db_path": "gophish.db",
  "migrations_prefix": "db/db_",
  "contact_address": "",
  "logging": {
    "filename": "",
    "level": ""
  }
}
```

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

```
moustapha@moustapha: ~/Musique/gophish-v0.12.1-linux-64bit
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ nano config.json
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ sudo ufw allow 3333
Omission de l'ajout de la règle existante
Omission de l'ajout de la règle existante (v6)
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ sudo ufw status
État : actif

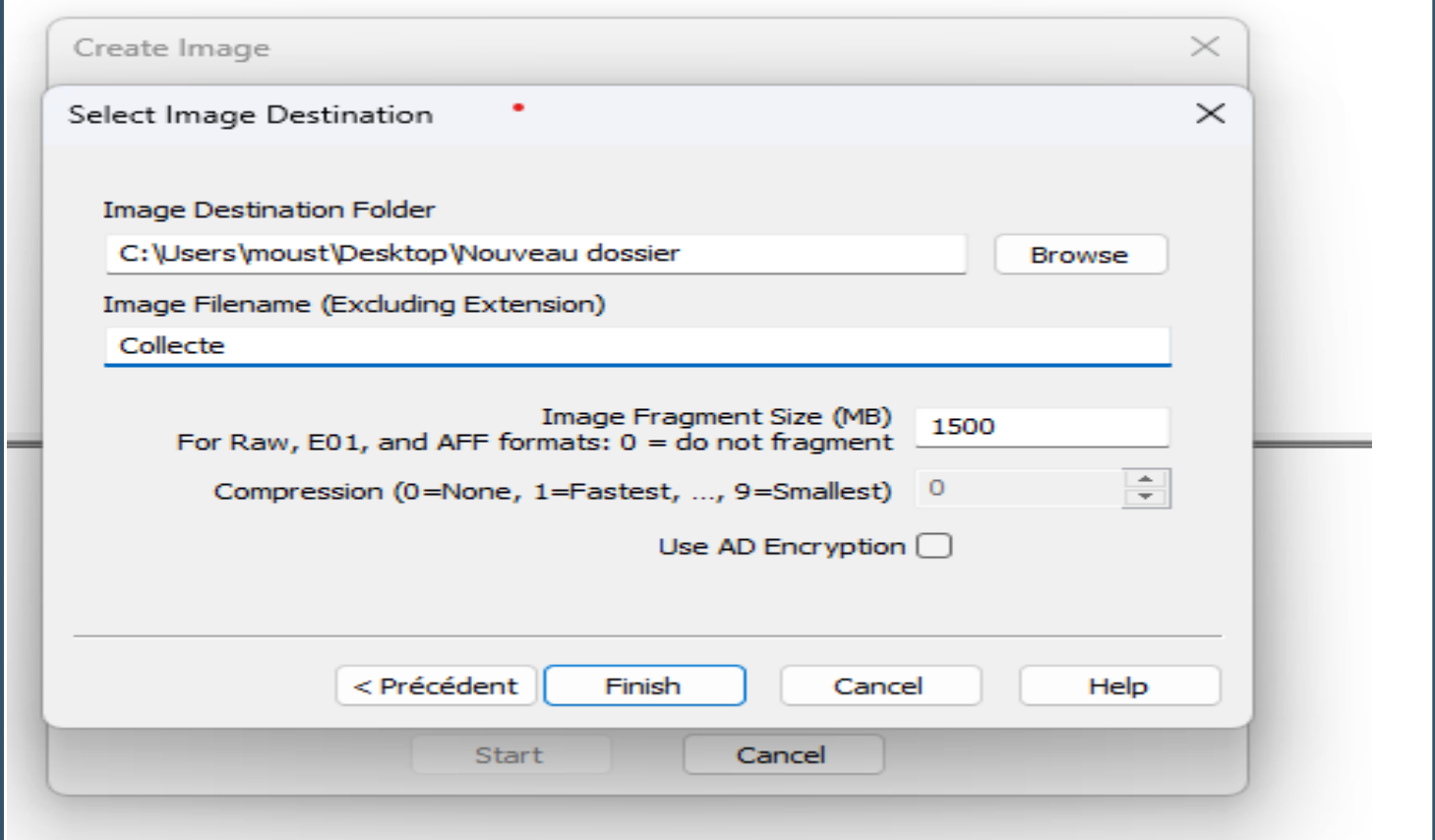
Vers                Action              De
-----
5044/tcp             ALLOW               Anywhere
5601/tcp             ALLOW               Anywhere
9200/tcp             DENY                Anywhere
5044                 ALLOW               Anywhere
8220                 ALLOW               Anywhere
3333                 ALLOW               Anywhere
5044/tcp (v6)        ALLOW               Anywhere (v6)
5601/tcp (v6)        ALLOW               Anywhere (v6)
9200/tcp (v6)        DENY                Anywhere (v6)
5044 (v6)            ALLOW               Anywhere (v6)
8220 (v6)            ALLOW               Anywhere (v6)
3333 (v6)            ALLOW               Anywhere (v6)

moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$
```

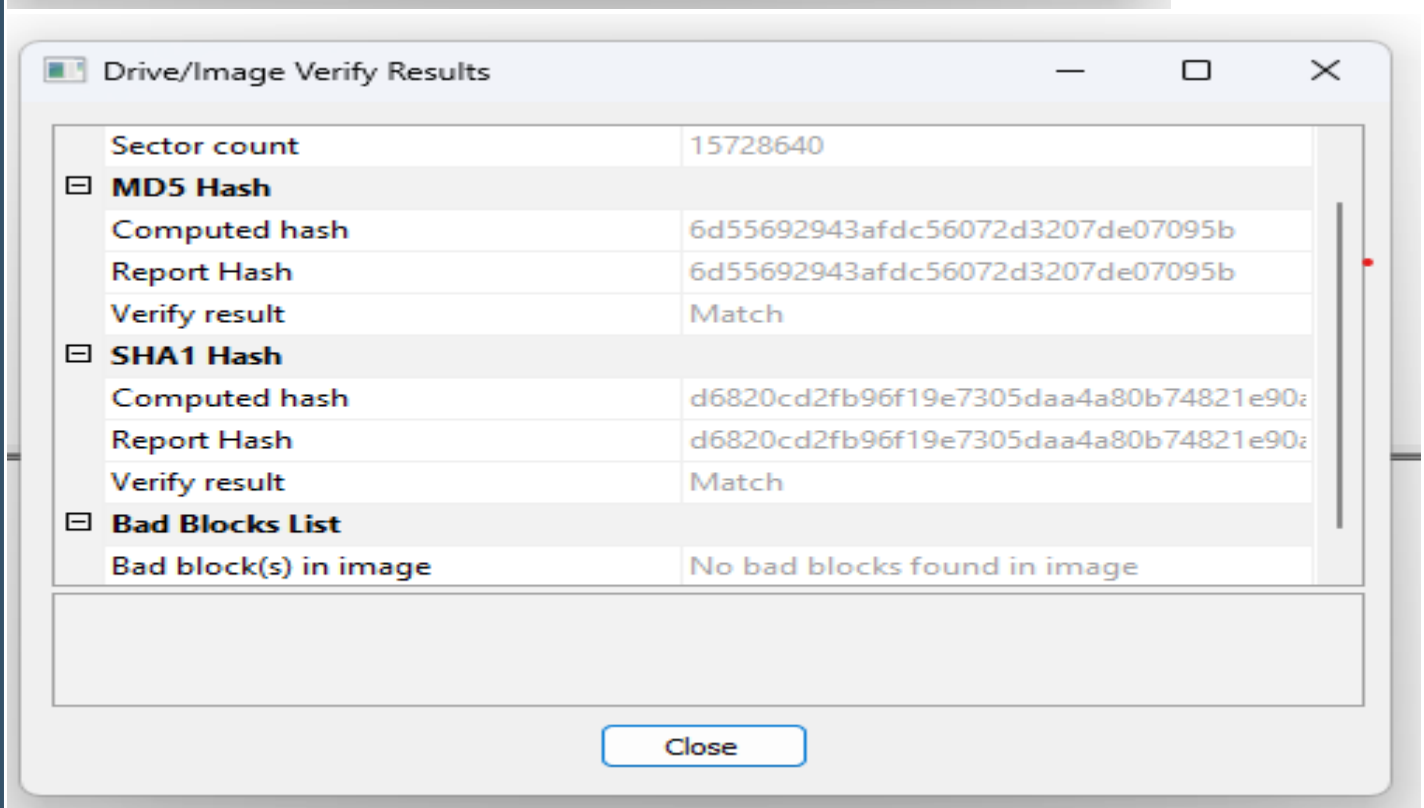
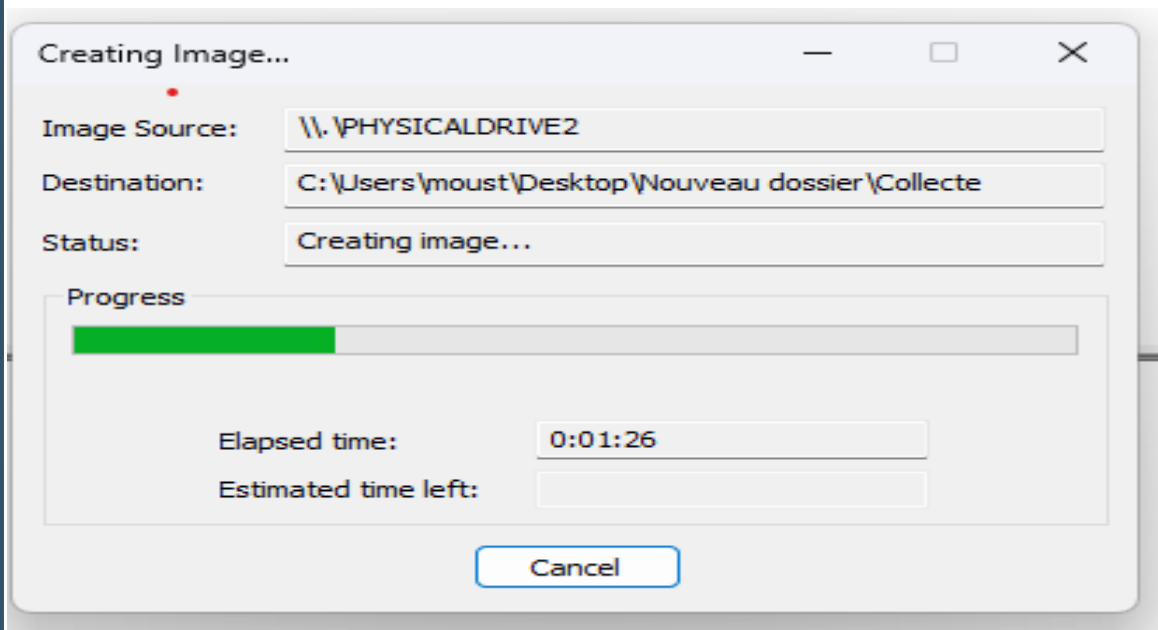
On choisi , ‘Physical drive’ puis ‘Raw dd’ pour faire une copie bit à bit’


```
moustapha@moustapha: ~/Musique/gophish-v0.12.1-linux-64bit
moustapha@moustapha: ~/Musique/gophish-v0.12.1-linux-64bit
moustapha@moustapha: ~/Musique/gophish-v0.12.1-linux-64bit$ sudo ./gophish
time="2025-12-06T14:44:19Z" level=warning msg="No contact address has been configured."
time="2025-12-06T14:44:19Z" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: no migrations to run. current version: 20220321133237
time="2025-12-06T14:44:19Z" level=info msg="Starting IMAP monitor manager"
time="2025-12-06T14:44:19Z" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2025-12-06T14:44:19Z" level=info msg="Starting admin server at https://0.0.0.0:3333"
time="2025-12-06T14:44:19Z" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2025-12-06T14:44:19Z" level=info msg="Starting new IMAP monitor for user admin"
time="2025-12-06T14:44:44Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET / HTTP/2.0\" 307 51 \"\" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:44Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET /login?next=%2F HTTP/2.0\" 200 1033 \"\" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:44Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET /images/logo_inv_small.png HTTP/2.0\" 200 1118 \"https://127.0.0.1:3333/login?next=%2F\" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:44Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET /images/logo_purple.png HTTP/2.0\" 200 4735 \"https://127.0.0.1:3333/login?next=%2F\" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:44Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET /css/dist/gophish.css HTTP/2.0\" 200 52514 \"https://127.0.0.1:3333/login?next=%2F\" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:45Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET /js/dist/vendor.min.js HTTP/2.0\" 200 324943 \"https://127.0.0.1:3333/login?next=%2F\" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:45Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:45 +0000] \"GET /images/favicon.ico HTTP/2.0\" 200 1150 \"https://127.0.0.1:3333/login?next=%2F\" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
```

Ici on défini un case number



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

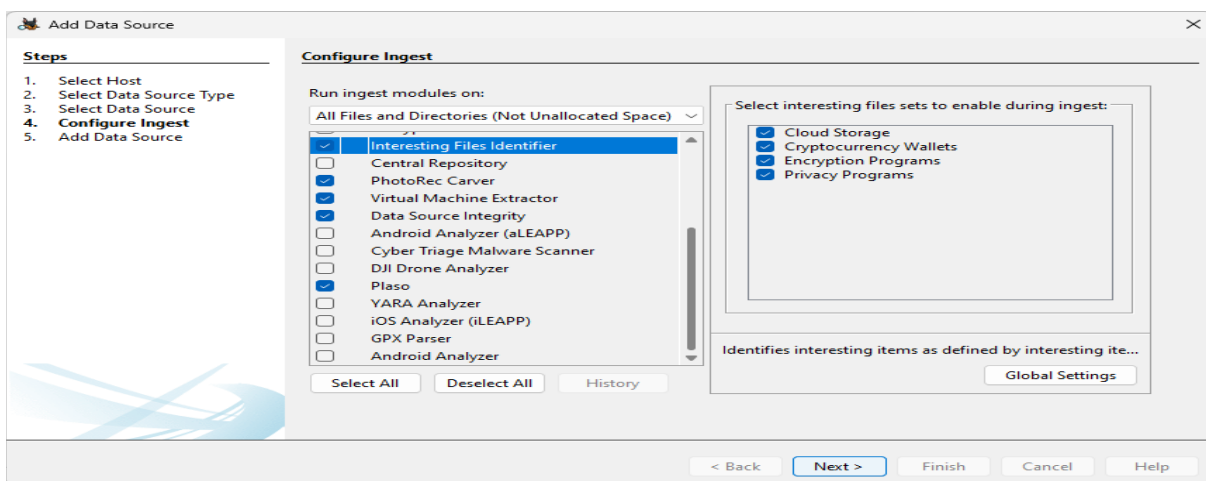


Maintenant l'image est entrain d'etre copier et apres la copie terminer , on peut voir en md5 et à SHA1

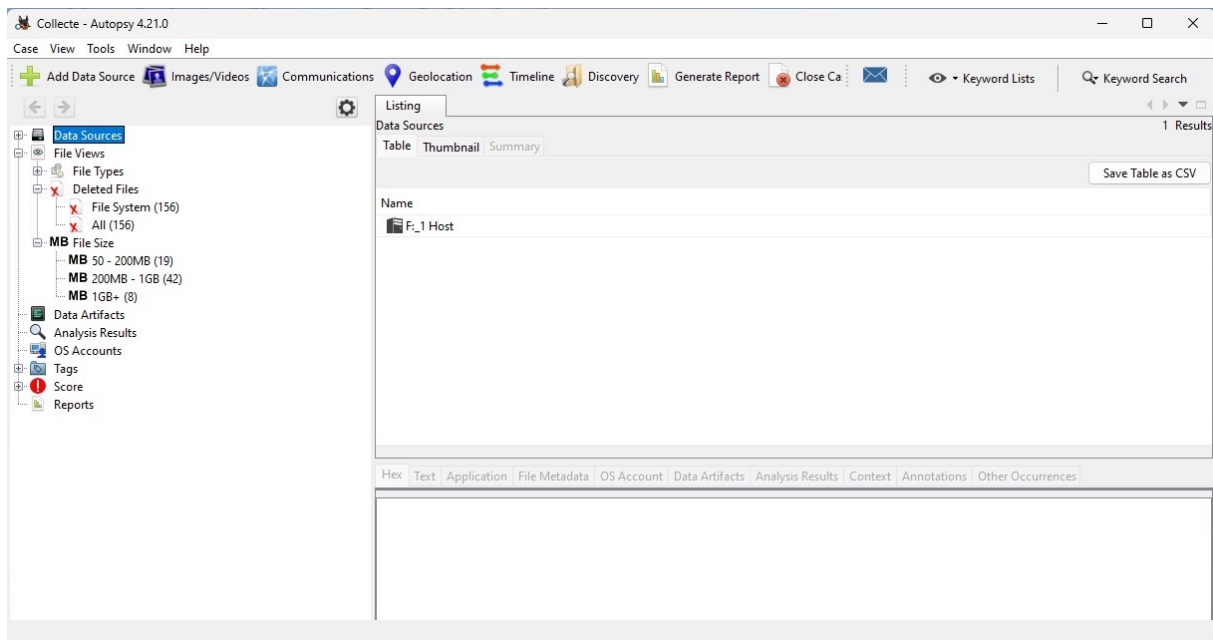
Analyse de l'image



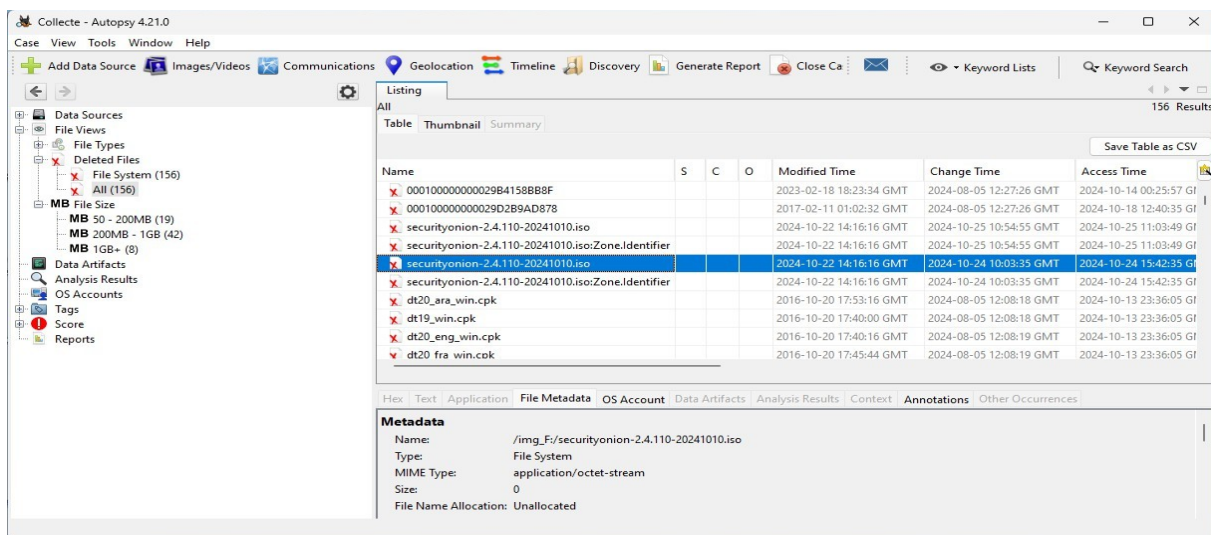
Ici, on ouvre autopsy



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

trojan.exe - Le scanner anti-virus

Comment dupliquer une page | Télécharger un fichier | iLovePDF

metadefender.com/results/hash/1f015cB6377151F1010A8EB9358941E5269975832696AB608237C2E89F86D490

Brave n'est pas votre navigateur par défaut Définir par défaut

Processed hash Add to Catalogue

SHA-256: 1F015CB6377151F1010A8EB9358941E5269975832696AB608237C2E89F86D490

53026cf7b2e48a6d1509026147f4ff57 Not Available (Country of Origin) Add CQO

MultiscanningThreats DetectedAdaptive SandboxMaliciousDeep CRRUnreported file typeProactive DLPNo Results AvailableVulnerabilitiesNo Vulnerabilities FoundCommunity feedback0 comments

MultiscanningThreats Detected26/32 ENGINES

Engine Name	Verdict	Last engine update
OPSWAT AI-Predictive Malware Detection	Win/malicious_98	11/26/2025 05:32 AM GMT
AhnLab	Trojan/Win32.Shell	11/26/2025 05:33 AM GMT
Antiy	Trojan/Win32.Rozema	11/25/2025 17:32 PM GMT
Avira	TR/Patched.Gen2	11/25/2025 22:00 PM GMT
Bitdefender	Trojan.Crypt2.Marte.1.Gen	11/26/2025 05:41 AM GMT
Bkav Pro	W32.FamIT.RorenNsis.Trojan	11/25/2025 17:32 PM GMT
ClamAV	Win.Trojan.Sword-5710S38-0	11/26/2025 10:22 AM GMT
CMC	Trojan_Win32_Meterpreter_RPZ_MTB	11/26/2025 00:19 AM GMT
Xcitium	TrojWare Win32.Rozema.A	11/26/2025 00:28 AM GMT
Autora	Malware -10	11/25/2025 16:27 PM GMT

File Overview

Category	E	Entropy	6.321630550827532
File Type	Executable File	Scanned	11/26/2025 11:38 AM GMT
File Extension	.exe	Duration	a few seconds
TrID	-	MDS	53026CF7B2E48A6D1509026147F4FF57
LibMagic	-	SHA-1	4F95990579198050316C96DE0D72A1...F09C5
Magika	-	SHA-256	1F015CB6377151F1010A8EB9358941E...6D490
File Size	73.8 kB	Company Name	Apache Software Foundation
Uploaded	11/26/2025 11:38 AM GMT	File Description	ApacheBench command line utility
SSDEEP	1536:IVSzTWI2aQJOPCchzcYt1qSWt77...@Qsc9	File Version	2.2.14
Architecture	32 Bits binary	Internal Name	ab.exe
Ia DotNet	False	Legal Copyright	Copyright 2009 The Apache Software Foundation.
Is Packed	False	Original File Name	53026cf7b2e48a6d1509026147f4ff57 File type mismatch, the file type is exe
Is Digitally Signed	False	Product Name	Apache HTTP Server
		Product Version	2.2.14

We value your privacy We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept", you consent to our use of cookies. Please see our Cookie Policy Accept All Cookies Settings Reject All

Après 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.