Rapport travail en autonomie

Système de fichier : NTFS

Roumache Grégoire
Sénéchal Julien
Wallemme Maxime

IR317 - Forensics and cyberattack evidence 2021-2022
Sécurité des systèmes, Hénallux
Troisième année, Classe A Groupe 1

09 Novembre 2021

1 Introduction

Le système de fichiers NTFS (New Technology File System) est le système de fichier de Microsoft, il succède au système de fichier FAT. Il est plus performant en termes de vitesse et d'utilisation du disque. Il est aussi plus fiable grâce à l'utilisation d'un système de journalisation. Son support des métadonnées est aussi très intéressant et nous allons nous y intéresser dans ce rapport.

2 Principes de fonctionnement

2.1 Fichiers système

Avec NTFS tout est un fichier, y compris les données utilisées par le système de fichier lui-même. On les appelle les fichiers systèmes, ils se situent à la racine et sont cachés parce que leurs noms commencent par un dollar $.

Il y a deux types d'index dans NTFS, la MFT (**M**aster **F**ile **T**able) qui contient la liste de tous les fichiers sur le système, dont elle-même. Il y a aussi les index I30 qui se trouvent dans chaque dossier et contiennent la liste des fichiers du dossier dans lequel ils se trouvent.

2.2 Métadonnées

La MFT contient les métadonnées du système. Voici les attributs qu'un fichier peut avoir :

Attribut	**Description**
Nom	Nom du fichier
Taille	Taille du fichier sur le disque
Horodatage	Date et heure de dernier accès, dernière modification et création
ACL	Liste de permissions pour contrôler l'accès au fichier
Adresse du fichier	Précise l'endroit sur le disque qui contient les données du fichier

NTFS note quelle opération va être lancée avant de l'exécuter. Par exemple, il va écrire dans les logs qu'il va supprimer un fichier avant de le supprimer. Ça permet d'achever correctement la transaction si la machine redémarre en plein pendant la suppression.

2.3 Flux alternatifs

Les fichiers NTFS peuvent avoir plusieurs flux (*streams* en anglais). Chaque fichier a un flux de données : `$DATA` qui contient les données du fichier. Cependant, il peut aussi avoir d'autres flux, appelé flux de données alternatif contenant des données pas directement visible à l'utilisateur. Exemple avec des commandes CMD :

```
echo test > test.txt
echo hello > test.txt:hello
dir
more < test.txt
more < test.txt:hello
del test.txt
dir
```

Ici, nous a créé le fichier *test.txt* et on a mis :

- "test" dans le flux : `$DATA`
- "hello" dans le flux `hello`

Ensuite, nous avons bien vérifié qu'il n'y avait qu'un seul fichier présent. Nous avons lu les données des deux flux. Et nous avons supprimé le fichier. Une fois supprimé, aucun des deux flux n'est plus accessible.

3 Outils d'analyses

3.1 FTK Imager

Cet outil permet d'analyser l'entièreté d'un système de fichiers NTFS. Celui-ci peut vous permettre de retrouver, par exemple, le *$MFT* qui contient tous les enregistrements des fichiers stockés et leurs informations (nom, horodatage, type de fichier, etc.) comme on peut le voir à la figure 1. Il s'agit d'un élément crucial de l'investigation numérique, car elle permet de retracer les évènements.

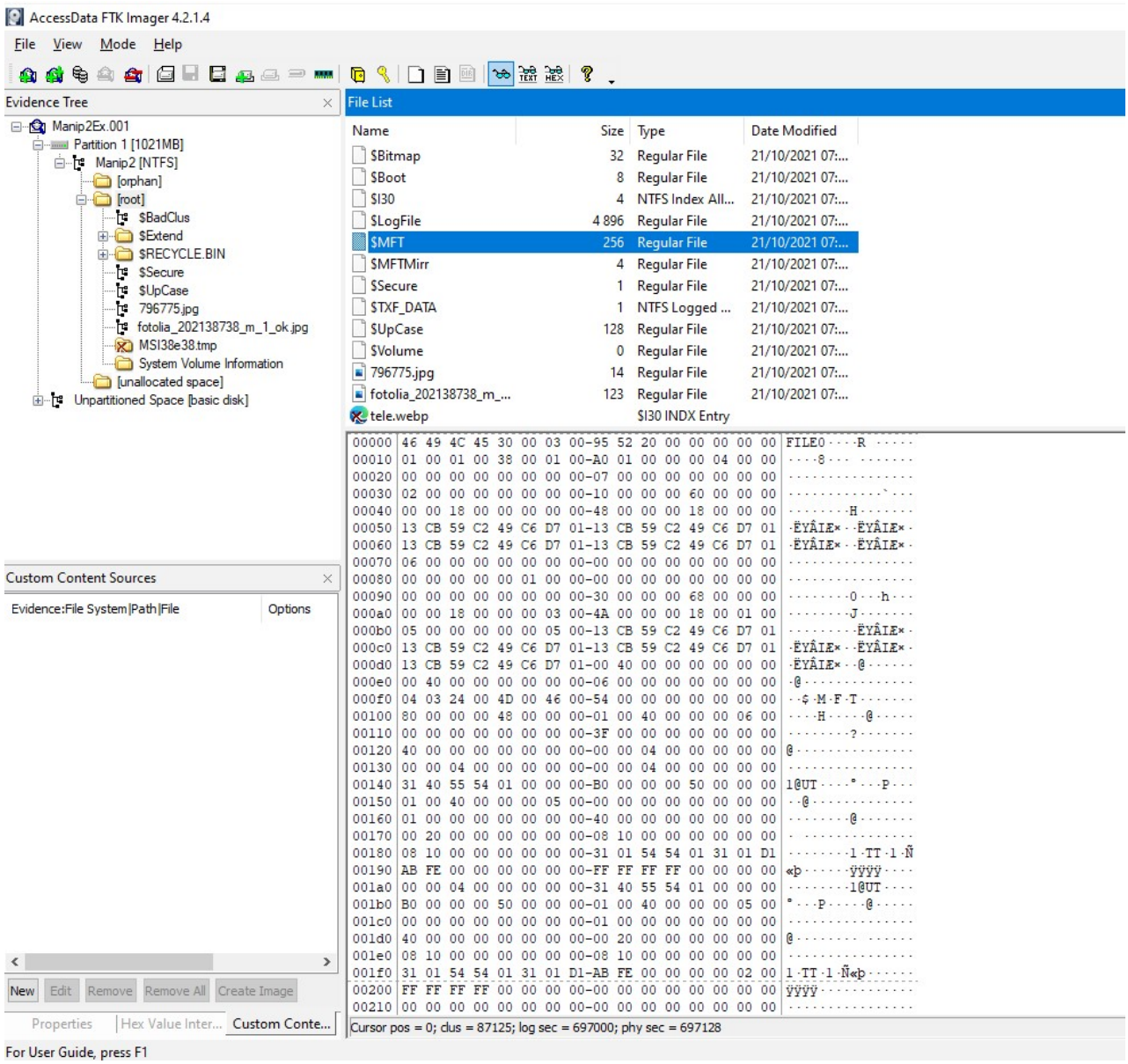

Figure 1 – Découverte du $MFT avec FTK Imager

3.2 Mft2Csv

Il s'agit d'un outil permettant de décoder les données et de traiter les données contenues dans le $MFT (Voir Figure 2). Une fois le traitement terminé, nous obtenons un fichier en format CSV. Le CSV va nous permettre la facilité de lecture (une fois la mise en page adaptée) et ainsi pouvoir inspecter la chronologie des évènements (Voir Figure 3).

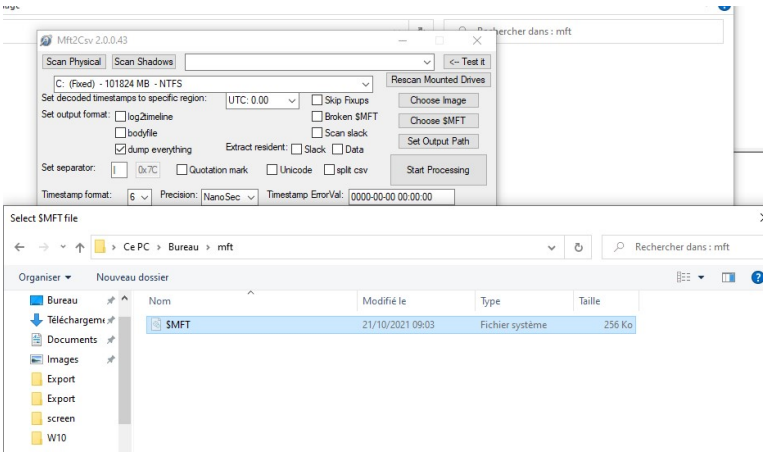

FIGURE 2 – Analyse de la Master File Table

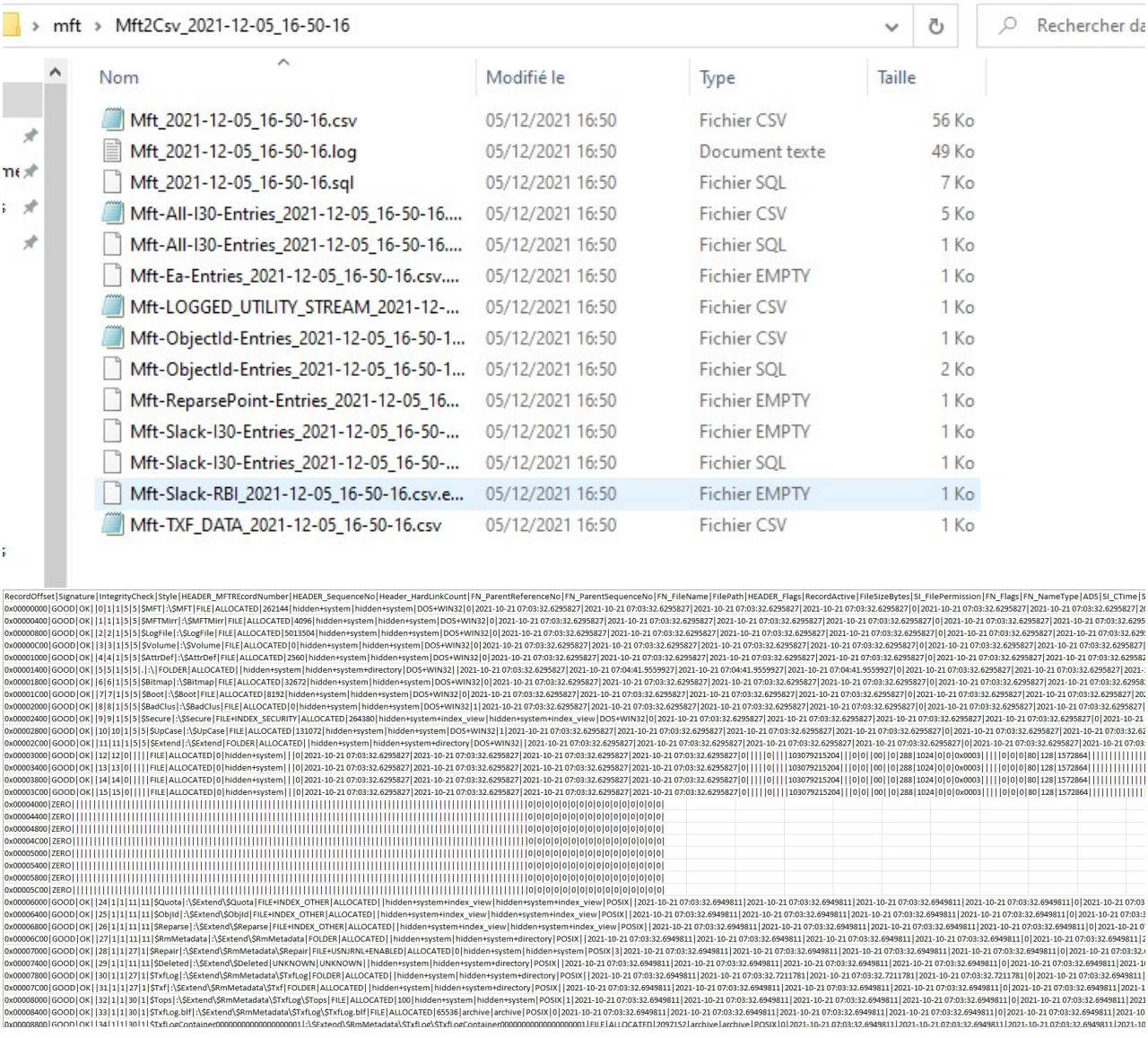

FIGURE 3 – Exportation en CSV de la MFT

3.3 Autopsy

Avec Autopsy, on peut également analyser les fichiers du système de fichiers NTFS. Pour illustrer cette analyse, nous avons surligner, sur la figure 4, une image supprimée. On peut voir le flux principal *$RORROW3.jfif*, le flux alternatif *Zone.Identifier* et *$IORROW3.jfif* qui contient le chemin du fichier comme vous pouvez le voir à la figure 5.

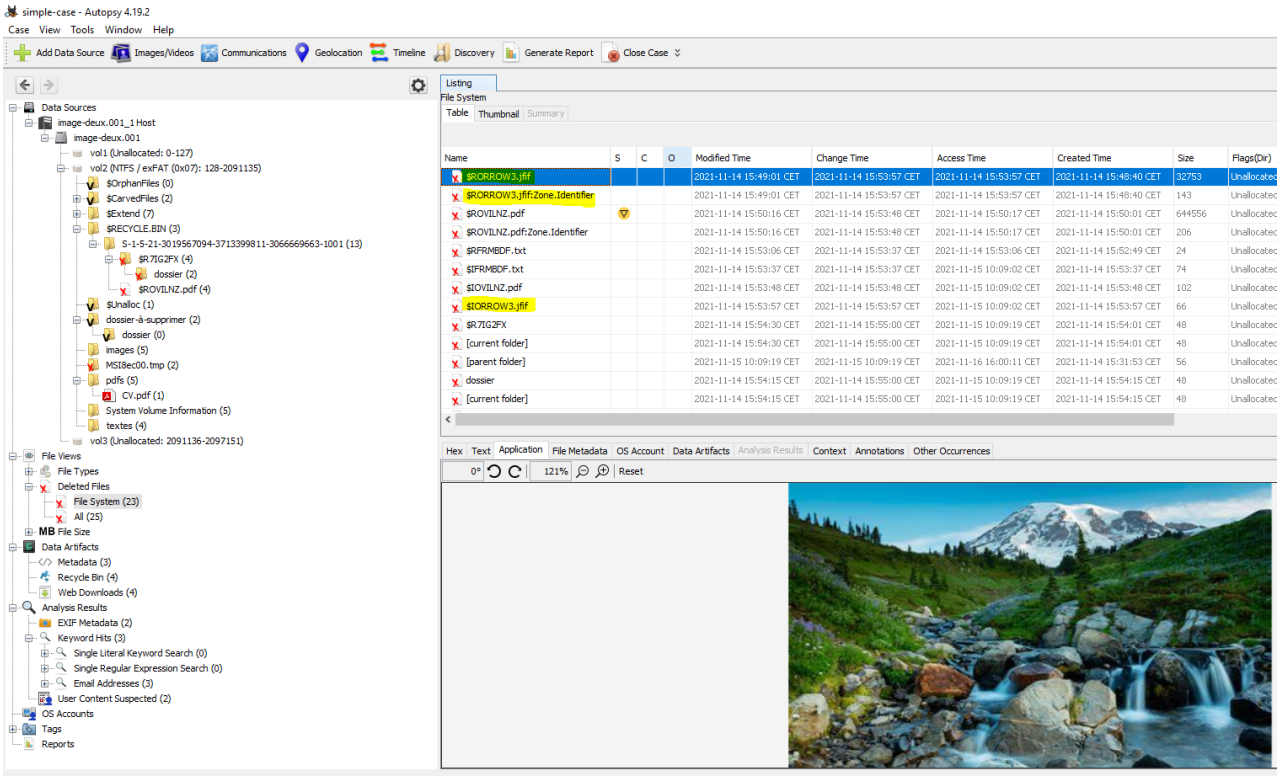

Figure 4 – Analyse d'un fichier supprimé avec Autopsy

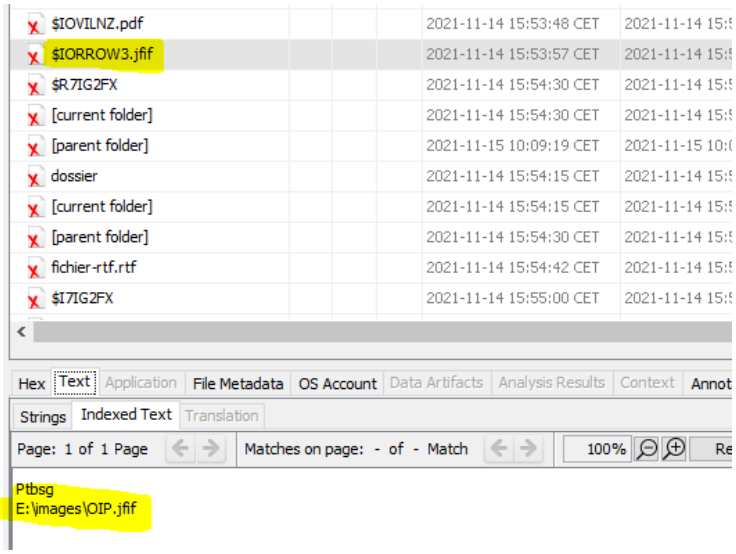

Figure 5 – Métadonnées contenant le chemin du fichier supprimé

4 Exemple de métadonnées que l'on peut trouver pour un fichier

Sur le système de fichier NTFS, on peut retrouver différentes métadonnées pour un fichier comme :
- Nom
- Type de fichier
- Le chemin du dossier dans lequel il se situe
- La taille du fichier
- La date de création et de modification
- Les attributs du fichier : Ceux-ci permettent de donner une fonction à un fichier (exemple : l'attribut H permet de caché le fichier même lorsque la commande dir est utilisée.).
  Dans mon cas, l'attribut A permet de marquer le fichier comme créé ou modifié après la dernière sauvegarde.
- Le propriétaire du fichier
- L'ordinateur sur lequel le fichier à été créé

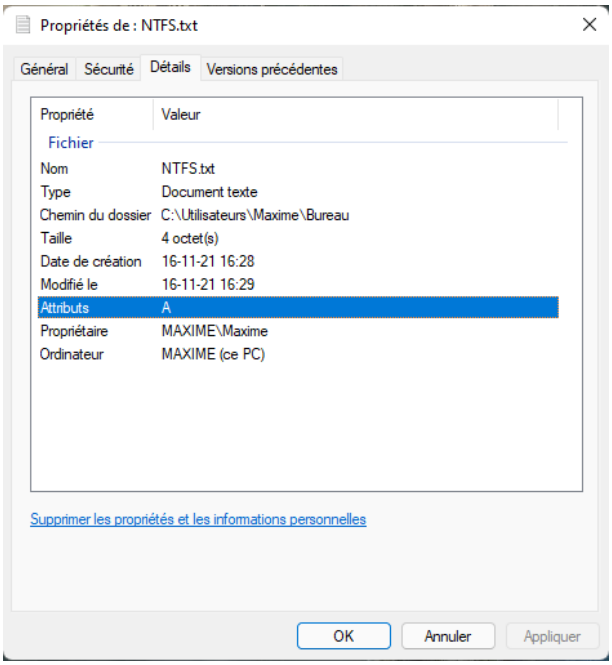

FIGURE 6 – Exemples de métadonnées d'un fichier sur NTFS

5 Conclusion

Nous avons eu l'occasion de faire un rapide tour du système de conclusion. En effet, nous avons tout d'abord pu voir le principe de fonctionnement de NTFS tel que l'utilité de sa master file table, de ses métadonnées ou encore en découvrant les flux alternatifs. Ensuite, nous avons pu découvrir 3 outils intéressant dans le processus d'analyse de ce système de fichiers. Et enfin, nous avons pu avoir un avant-goût d'une analyse du système de fichiers en utilisant Autopsy.