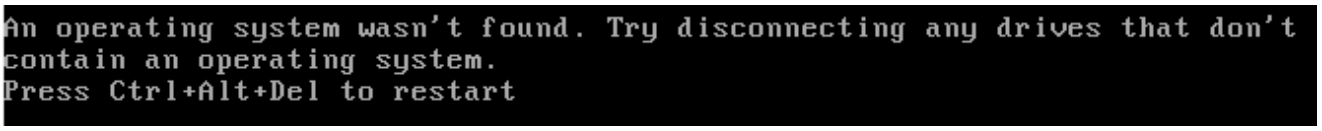
Correction Atelier S02 Mme Michou

Nous somme sur une structure bios et non pas UEFI.
Erreur dès le lancement



Pasted image 20251024093333.png

Le Bios va initialiser tout les périphérique puis il va chercher s'il y a un OS.
Il ya 3 étapes au démarrage de Windows :

- BootMGT
- WINload
- Chargé le WINload

Restaurer le BootMGR

#Bootmgr
Le processus de démarrage de Windows en MBR

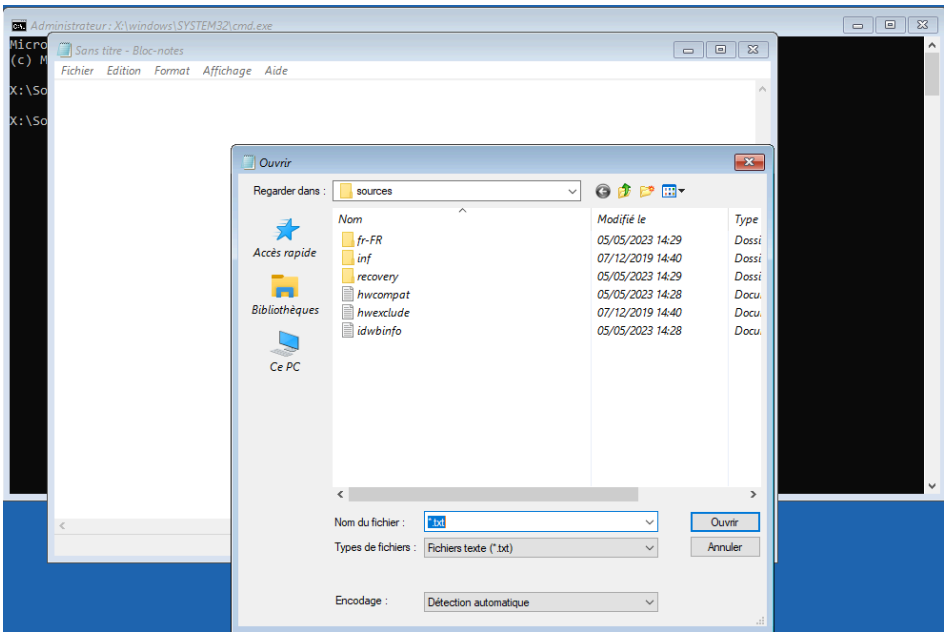
On va rester le démarrage de BootMGT.
On insérer un ISO de Windows 10 pour tenter une réparation.

Pasted image 20251024094555.png

Restauration du système => Restaure l'ordinateur à un état en antérieur
Récupération de l'image système => On ne connaît pas l'ordinateur de Mme Michou on n'y touche pas
Désinstaller des mises à jours => on ne sais pas si celà provient de mise à jour

Invite de commande

Lancer le **notepad** pour ouvrir le bloc note et avoir une interface graphique. Et l'avantage on peut parcourir plus facile les fichiers sur le Windows.

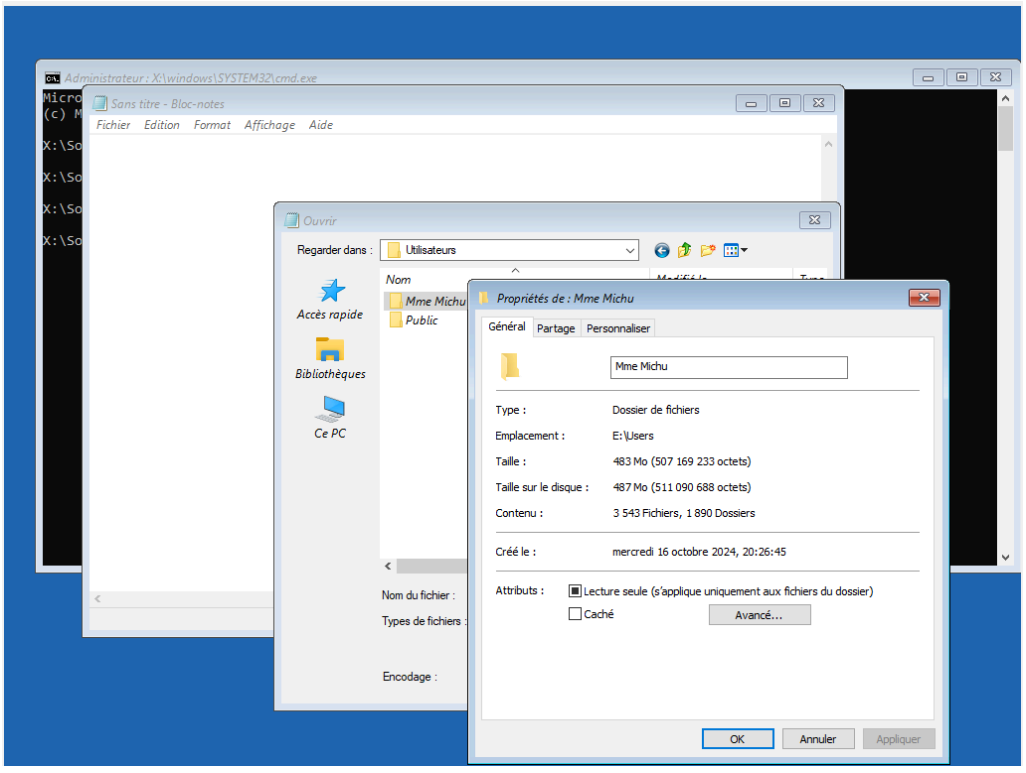


Pasted image 20251024095043.png

Le lecteur x : environnement Windows détecté.
Actuellement, nous sommes dans l'environnement de récupération Windows (WinRE), lancé depuis le support d'installation (CD ou image ISO). Il s'agit d'une session d'exploration du système via le **Windows Recovery Environment**.

Lecteur E:\

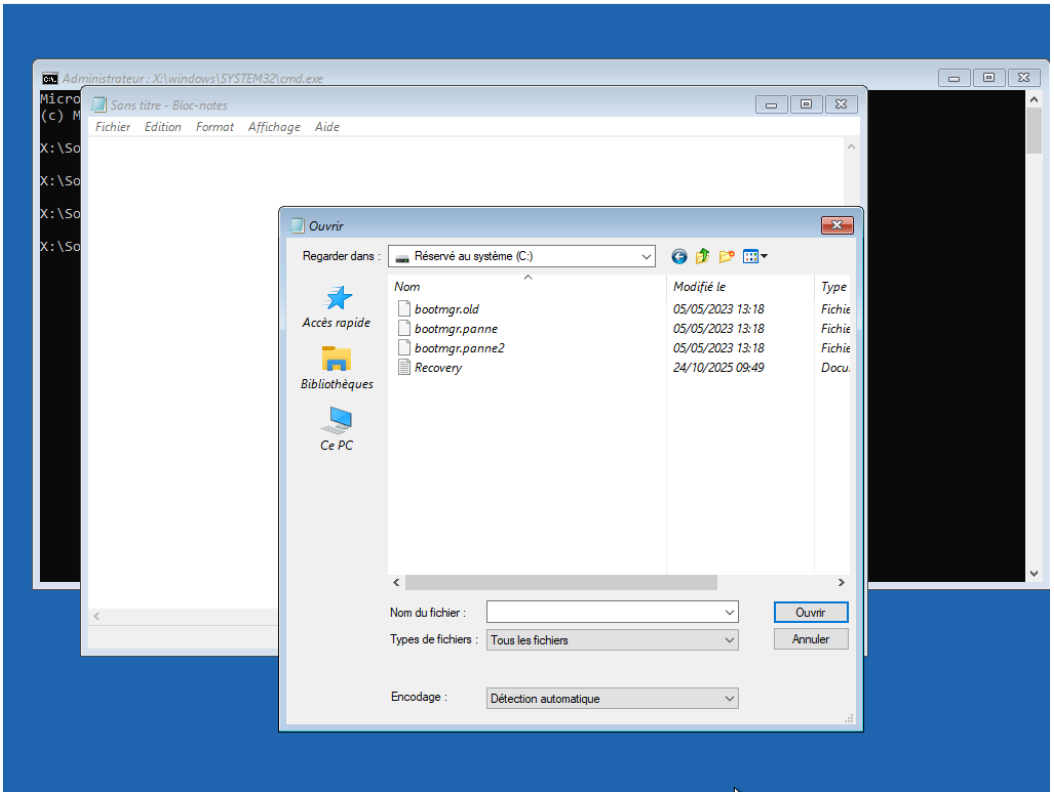
En fouillant, on constat que le système de Mme Michu se trouve dans E:\Users.
Nous avons accès à toutes les données



Pasted image 20251024095830.png

Lecteur C:\

On trouve des fichiers pannes.
Pour rectifier, il suffit de modifier les fichier en **bootmgr**
`Bootmgr.old => Bootmgr`
Cependant, avec notepad on ne voit pas les fichiers systèmes et généralement le fichier de bootmgr ce trouve dans ces fichiers systèmes.

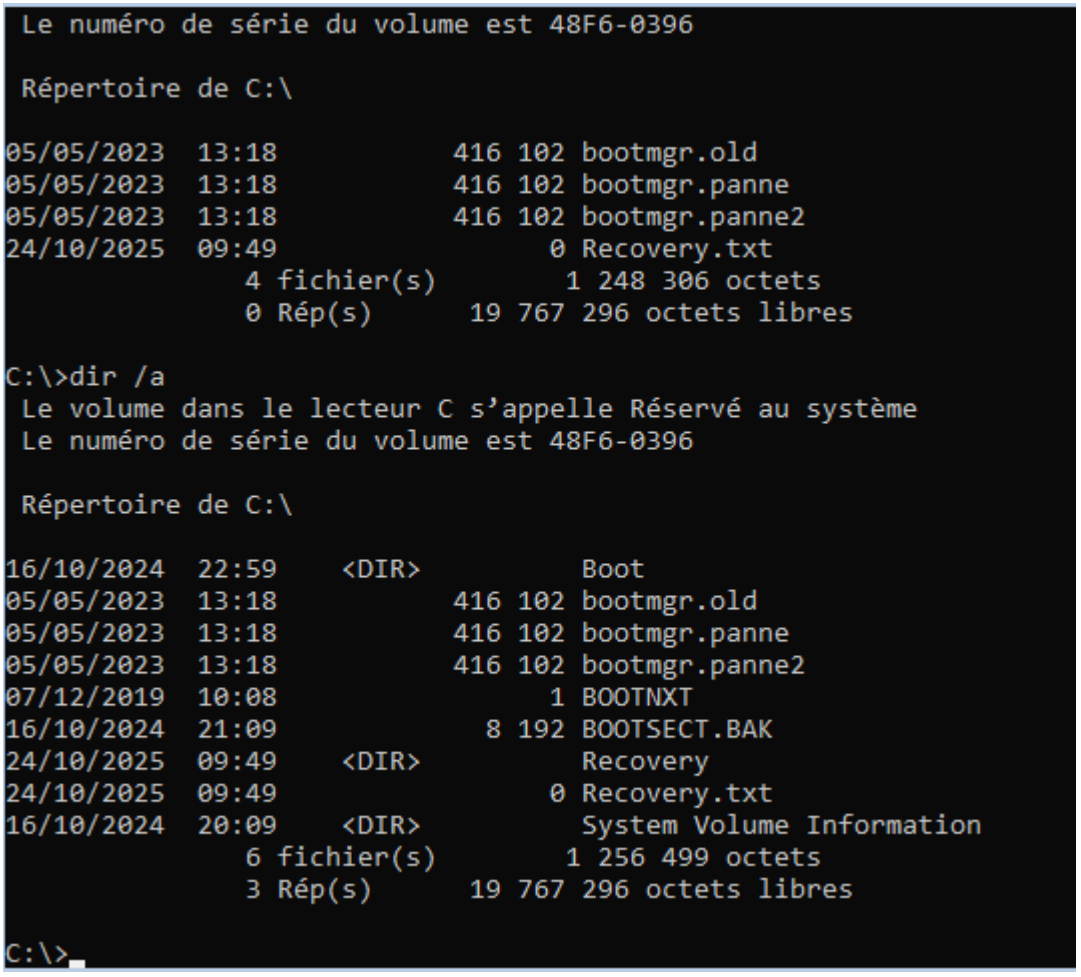


Pasted image 20251024100133.png

FixBoot && Diskpart

Commande de réparation

Dans **L'invite de commande** on va dans le volume c:/ pour récupérer les fichier



Pasted image 20251024100656.png

#fixboot #bootrec

Pour changer de répertoire : entre seulement le nom du lecteur (c: ou e:)

Pour lister toutes les fichiers dans le répertoire :

- `dir` : liste tout les fichier
- `dir /a` liste tout les fichier + les dossiers cachés

`bootrec` => Répare les structures de disques critiques. Les commandes suivantes sont prises en charge

- `/FixMbr` - Réécrit le secteur de démarrage principal (MBR) de la partition système en utilisant une version fonctionnelle compatible avec Windows. Cette commande **ne modifie pas la table de partition existante**
- `/FixBoot` Installe un nouveau secteur de démarrage sur la partition système, basé sur un modèle compatible avec Windows.
- `/ScanOs` Analyse tous les disques à la recherche d'installations Windows valides et affiche celles qui ne sont pas encore enregistrées dans le magasin de configuration de démarrage (BCD).
- `/RebuiIdBcd` Explore tous les disques pour détecter les installations Windows, puis permet à l'utilisateur de sélectionner celles à ajouter au magasin de configuration de

démarrage.

Dans notre cas ces solutions ne fonctionne pas **mais à tester en 1er**

Botsect

Outil de restauration de secteur d'amorçage
Met à jour le code démarrage principal pour les partitions du disque dur afin de basculer entre BOOTMGR et NTLDR.
Restaure le secteur d'amorçage pour l'ordinateur

`\nt80` plus récent que NTLDR mais permet d'applique le code de démarrage principale pour bootMGR

```
C:\>bootsect /nt52 E:
Les volumes cibles seront mis à jour avec un code de démarrage compatible NTLDR.

E: (\\?\Volume{19c52418-0000-0000-0000-300300000000})

    Mise à jour du code de démarrage du système de fichiers NTFS réussie.

Le code de démarrage a été mis à jour sur tous les volumes ciblés.
```

Pasted image 20251024102839.png

Puis tenter un Fixboot

```
C:\>bootrec /Fixboot
Accès refusé.
```

Pasted image 20251024102918.png

BcdBooT

Options de ligne de commande BCDBoot | Microsoft Learn

#Bcdboot permet de :

- **Copier les fichiers de démarrage essentiels** vers la partition système.
- **Créer un nouveau magasin BCD** (Boot Configuration Data), qui contient les paramètres nécessaires au démarrage de Windows.

< > => option obligatoire
[/] => crochet "donnée optionnel"
/f => uniquement pour les environnements UEFI et pas BIOS
/l => chnotepaange la langue du bootmgr

```
C:\>bcdboot E:\Windows /l fr-fr
Les fichiers de démarrage ont bien été créés.
```

image-2.png

Copie le fichier du bootmgt vers c:

```
C:\>dir /a
 Le volume dans le lecteur C s'appelle Réservé au système
 Le numéro de série du volume est 48F6-0396

 Répertoire de C:\

24/10/2025  11:10    <DIR>          Boot
05/05/2023  13:18           416 102 bootmgr
05/05/2023  13:18           416 102 bootmgr.old
05/05/2023  13:18           416 102 bootmgr.panne
05/05/2023  13:18           416 102 bootmgr.panne2
07/12/2019  10:08                 1 BOOTNXT
16/10/2024  21:09             8 192 BOOTSECT.BAK
24/10/2025  09:49    <DIR>          Recovery
24/10/2025  11:06                 0 Recovery.txt
16/10/2024  20:09    <DIR>          System Volume Information
               7 fichier(s)        1 672 601 octets
               3 Rép(s)      19 341 312 octets libres
```

image-3.png

Pour vérifier si tout est bon, il faut faire un **bcdedit**

```
C:\>bcdedit

Gestionnaire de démarrage Windows
---------------------------------
identificateur          {bootmgr}
device                  partition=C:
description             Windows Boot Manager
locale                  fr-fr
inherit                 {globalsettings}
default                 {default}
resumeobject            {47168df8-b0c1-11f0-a514-d22b8919d2be}
displayorder            {default}
toolsdisplayorder       {memdiag}
timeout                 30

Chargeur de démarrage Windows
-----------------------------
identificateur          {default}
device                  partition=E:
path                    \Windows\system32\winload.exe
description             Windows 10
locale                  fr-fr
inherit                 {bootloadersettings}
allowedinmemorysettings 0x15000075
osdevice                partition=E:
systemroot              \Windows
resumeobject            {47168df8-b0c1-11f0-a514-d22b8919d2be}
nx                      OptIn
bootmenupolicy          Standard
```

image-4.png

Diskpartb

DiskPart permet d'effectuer des opérations avancées sur les supports de stockage physiques ou virtuels #diskpart

- **Lister les disques, partitions et volumes** : `list disk`, `list partition`, `list volume`
- **Sélectionner un disque ou une partition** : `select disk 0`, `select partition 1`
- **Créer une partition** : `create partition primary`
- **Supprimer une partition** : `delete partition`
- **Formater une partition** : `format fs=ntfs quick`
- **Attribuer une lettre de lecteur** : `assign letter=X`
- **Nettoyer complètement un disque** : `clean` (⚠️ supprime toutes les données)

- **Convertir un disque** : `convert gpt` ou `convert mbr`
- **Gérer les disques virtuels (VHD)** : `create vdisk`, `attach vdisk`, etc.

Restaurer Winload.exe

A ce moment là on est du côté de windows qui est complètement bloqué.
On ne peux que redémarrer l'ordinateur.

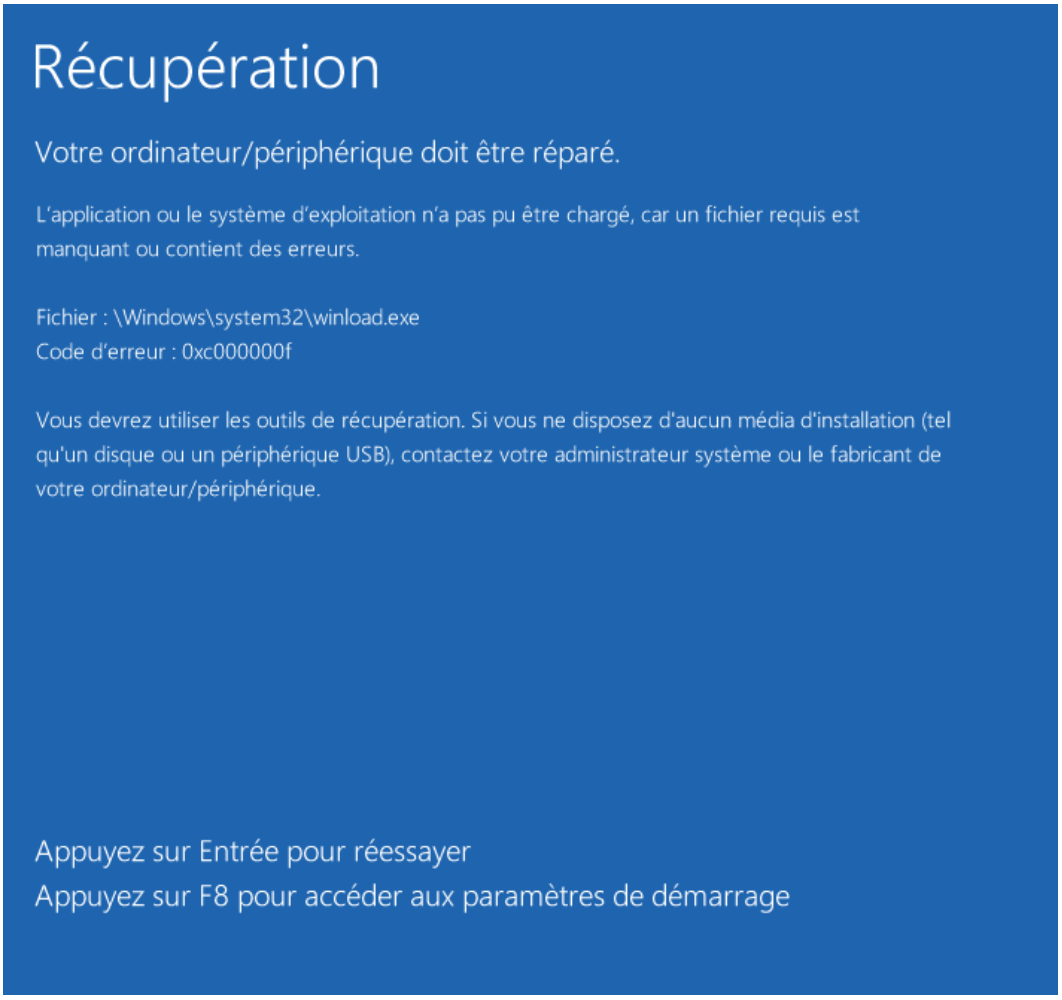


image-5.png

Il est nécessaire de relancer l'environnement de **dépannage** à partir du CD ou de **l'image ISO** de Windows.

Environnement de dépannage

Méthode Simple

Pour savoir ce qui se passe on va voir dans l'invite de commande.
À l'aide du Bloc-notes, on explore le dossier `System32` afin de confirmer que le fichier `winload.efi` est bien présent

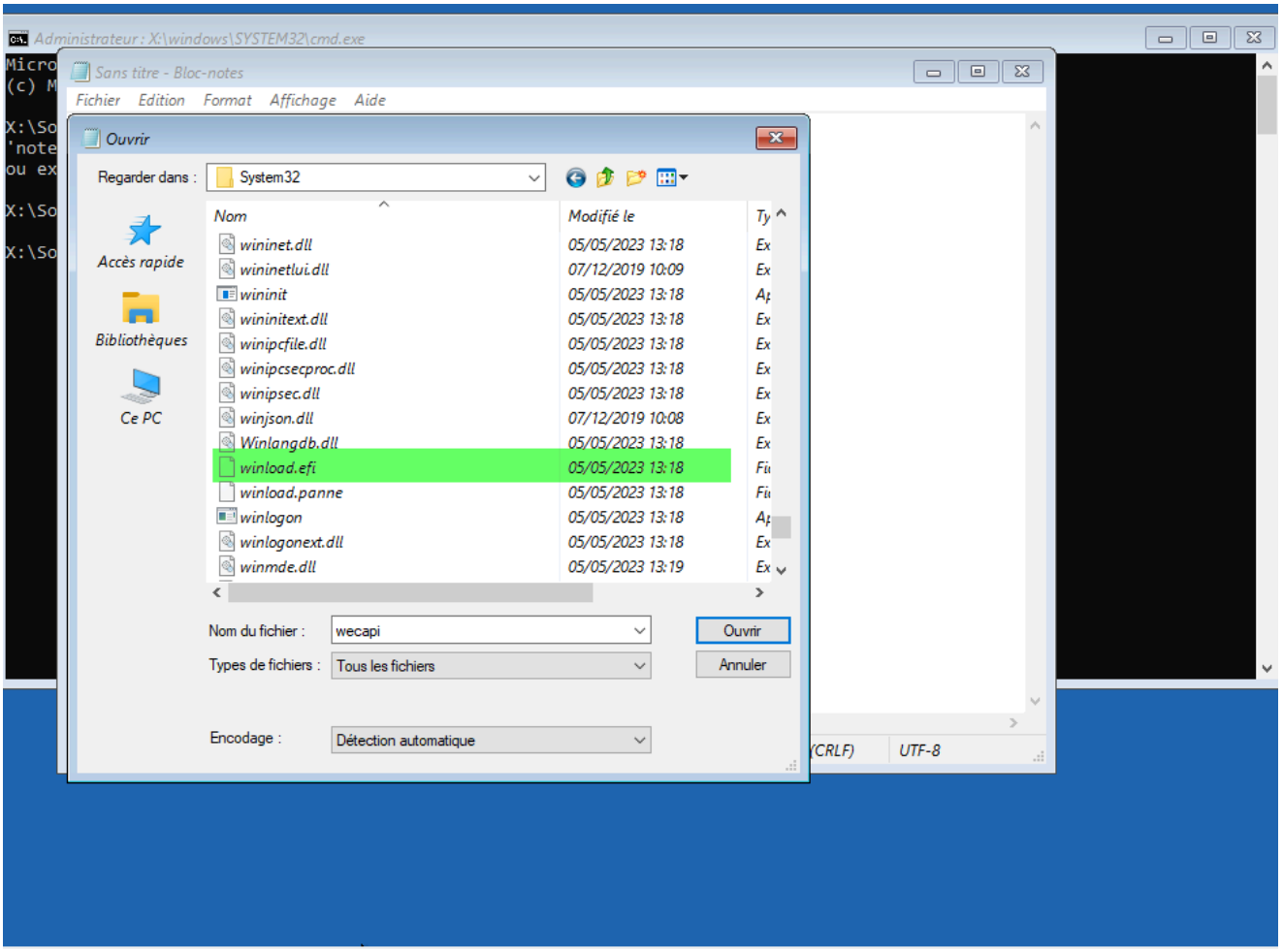


image-6.png

=> on constate que le winload.efi ne correspond pas à winload.exe. Il suffit de renommé

Invite de commande

DISM

#DISM permet d'**énumérer, installer, désinstaller, configurer et mettre à jour** des fonctionnalités et des packages dans des images Windows.
Les commandes disponibles dépendent :

- du type d'image traitée,
- et du fait que l'image soit **hors ligne** ou **en cours d'exécution**

SFC

analyse l intégrité de tous les fichiers système protégés et remplace les versions incorrectes par des versions Microsoft correctes

Exemple :

- `sfc /SCANNOW`
- `sfc /VERIFYFILE=c:\windows\system32\kernel32.dll`

- `sfc /SCANFILE=c:\windows\system32\kernel32.dll /OFFBOOTDIR=c:\ /OFFWINDIR=c:\windows`
- `sfc /SCANFILE=c:\windows\system32\kernel32.dll /OFFBOOTDIR=c:\ /OFFWINDIR=c:\windows /OFFLOGFILE=c:\Log.txt`
- `sfc /VERIFYONLY`

Les commandes

	Description
SCANNOW	Analyse l'intégrité de tous les fichiers système protégés et répare ceux qui posent problème lorsque cela est possible.
VERIFYONLY	Analyse l'intégrité de tous les fichiers système protégés, sans effectuer de réparation.
SCANFILE	Analyse l'intégrité d'un fichier spécifique et le répare si des problèmes sont détectés. Il faut indiquer le chemin complet du fichier.
VERIFYFILE	Vérifie l'intégrité d'un fichier spécifique (chemin complet requis), sans effectuer de réparation.
OFFBOOTDIR	Pour une réparation hors connexion, spécifie l'emplacement du répertoire de démarrage hors ligne.
OFFWINDIR	Pour une réparation hors connexion, spécifie l'emplacement du répertoire Windows hors ligne.
OFFLOGFILE	Pour une réparation hors connexion, permet d'activer la journalisation en indiquant le chemin d'un fichier journal.

Réparation

`sfc /scannow /offbootdir=e\ /offwindir=e:\Windows /OFFLOGFILE=e:\log.txt`

Décomposition des paramètres

- `sfc` : lance l'outil **System File Checker**, qui vérifie l'intégrité des fichiers système Windows protégés.
- `/scannow` : effectue une **analyse complète** de tous les fichiers système protégés et tente de **réparer automatiquement** ceux qui sont corrompus ou manquants.
- `/offbootdir=e:\` : indique le **lecteur de démarrage** (ici `E:`) à utiliser pour une réparation **hors connexion** (offline).
  → Utile quand Windows ne démarre pas et que tu travailles depuis un environnement de récupération (WinRE/ISO).
- `/offwindir=e:\Windows` : précise le **répertoire Windows** de l'installation à réparer (ici `E:\Windows`).
  → Cela permet à SFC de savoir **quelle installation Windows analyser et réparer**.

- `/offlogfile=e:\log.txt` : enregistre les résultats de l'analyse et des réparations dans un **fichier journal** (`log.txt`) situé à la racine du lecteur `E:` .
  → Pratique pour relire les détails après coup ou documenter un dépannage.

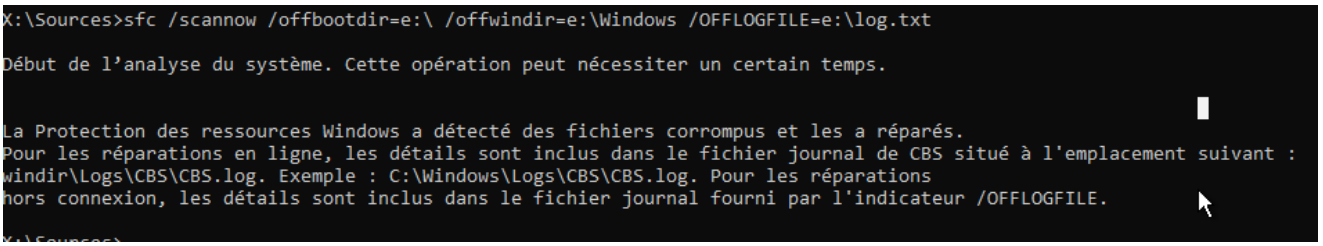


image-9.png

On peut consulter notre log dans E:/

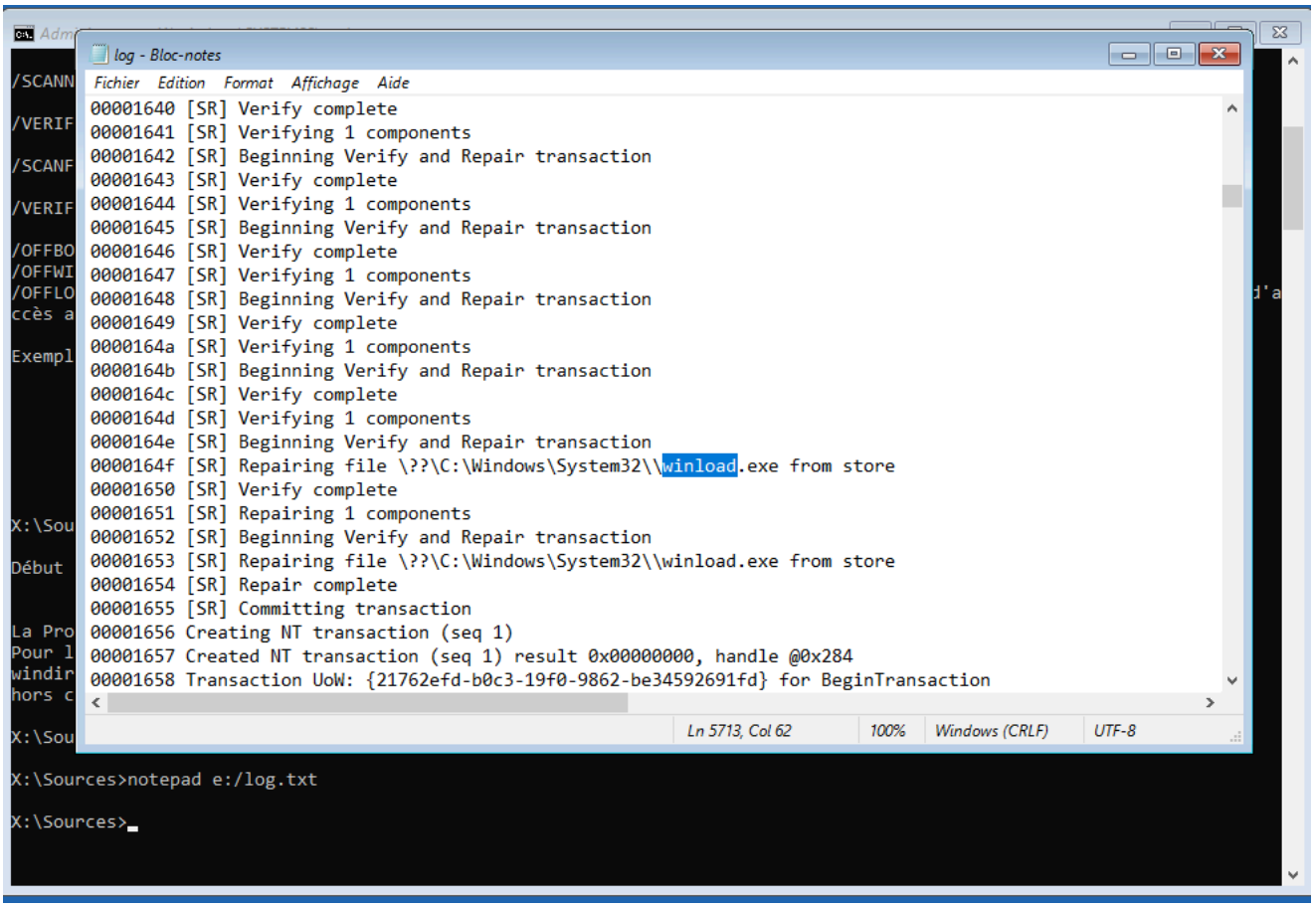


image-10.png

Le fichier **winload.exe** à été réparer.
Il faut redémarrer notre système

Gérer les Performance de Windows

On vérifie dans le gestionnaires des tâches les différences processus.

- Et on regarde ce qui prend de la ressources
- On regarde les programmes au démarrage

Kill un processus

Pour forcer la fermeture d'un processus rapidement, on peux le faire depuis l'invite de commande :
`taskkill /IM ping.exe /F

Tâche planifier

Le **planificateur de tâche** permet de voir ce qui est planifier automatiquement dans windows

il est nécessaire de vérifier de temps en temps le planificateur de tâche

Services

On peut y accèder dans le gestionnaire des tâches de windows
Svc host est un service important qui permet de lancer tout les services sur windows

Dans les processus du gestionnaires du tâches on peut affiche le service qui est utilisée pour chaque processus.

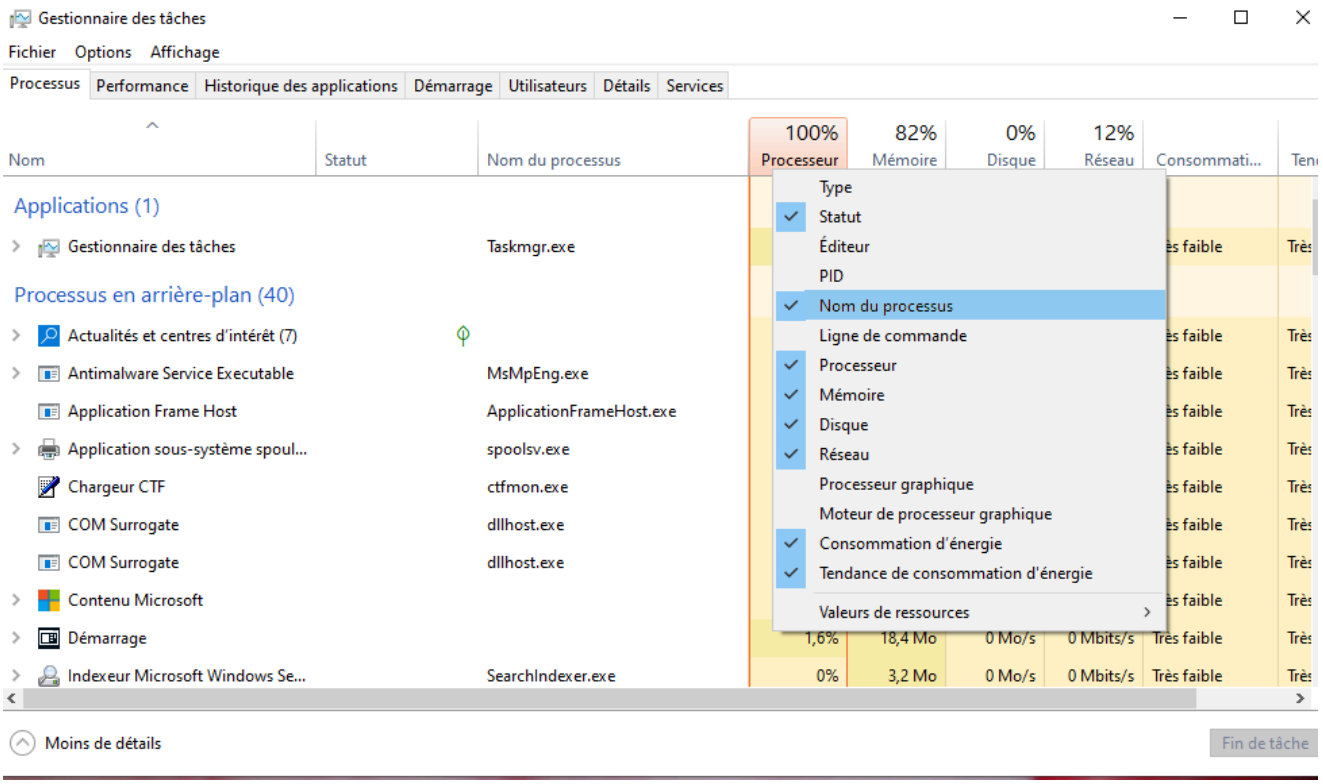


image-12.png

Programme de démarrage

Dans **démarrage** on voit tout les éléments de démarrage dont les scripts d'exécution. Mais on n'a pas tout les détails du problème.

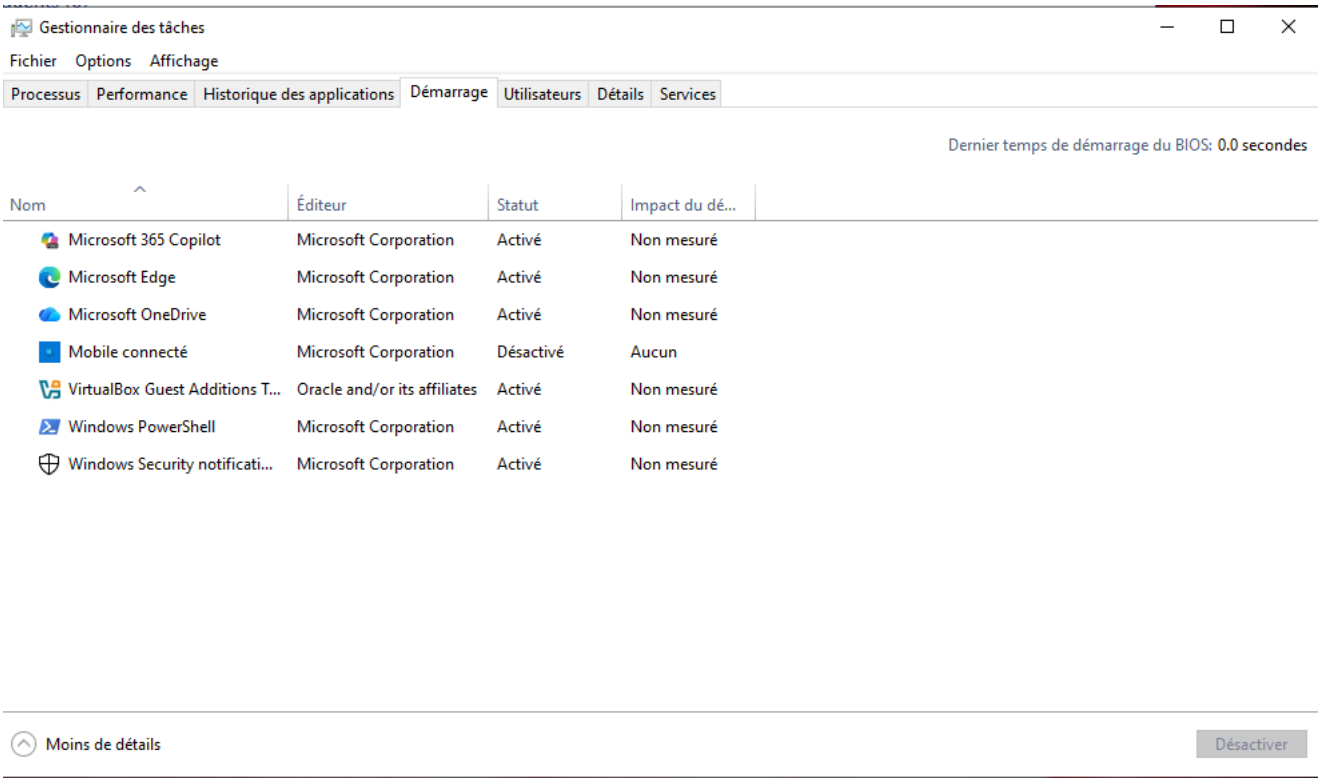


image-13.png

les éléments de démarrage peut être présent dans :

- Les éléments de démarrage de registre
- Dossier de démarrage

Actuellement PowerShell est notre élèvement perturbateur mais l'emplacement du fichier nous amène au programme PowerShell et non pas vers le programme malveillant. Mais ce programme utilise PowerShell dont les commandes sont néfaste

L'emplacement du dossier de menu démarrage :
`C:\Users\Franck\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`
ou dans exécuté :
`shell:startup`

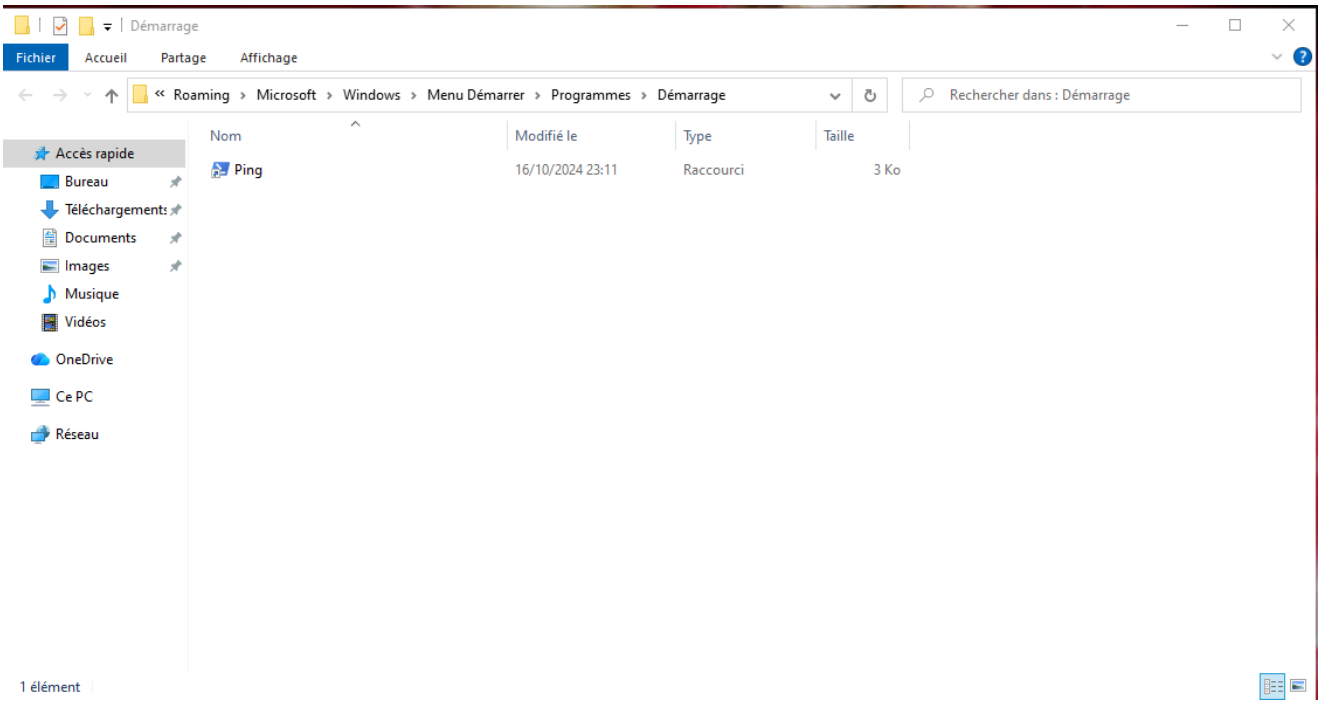


image-14.png

Dans les proprité du racourcis "ping" (fichier malveillant), on peut trouver l'emplacement du fichier ping :
`C:\\Windows\Ping.ps1`

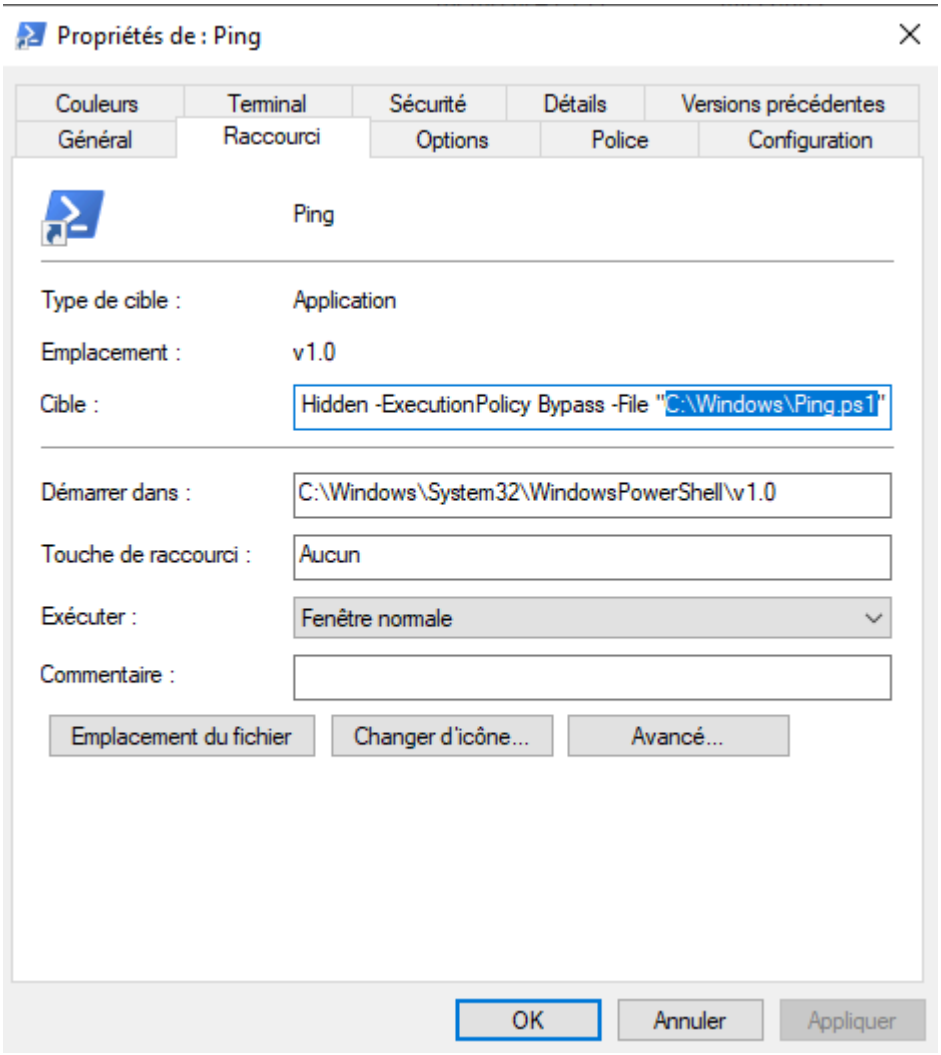


image-15.png

En examinant le code du fichier, on constate qu'il crée une boucle exécutant 500 fois la commande `ping` vers google.com en mode continu (`-t`), chaque instance étant lancée dans une fenêtre masquée via `Start-Process` .

```
for ($i = 0; $i -lt 500; $i++) {
Start-Process "ping" -ArgumentList "google.com -t" -WindowStyle Hidden
}
```

Pour nettoyer correctement il faut :

- Supprimer le fichier ping.ps1 dans c://windows
- Supprimer le raccourcis dans le menu démarrage
- Vidé la corbeille
- ou `SHIFT + SUPPR` pour supprimer défectivement

Vérifier l'état des disques dur

Constaté toujours l'erreur avec l'utilisateur(trice) pour savoir si c'est un disque dur / clé usb etc...
Comprendre si c'est un disque dur interne ou externe.

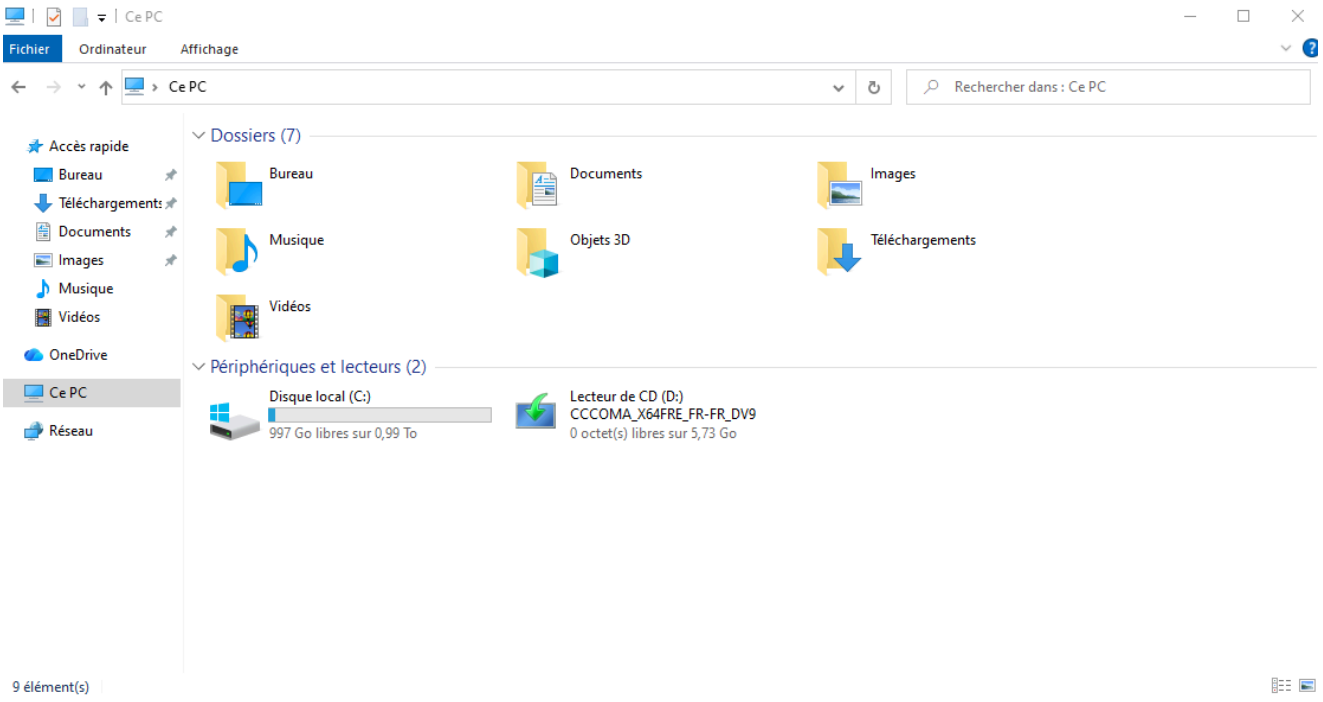


image-16.png

Le disque local C: est un volume.

Pour comprendre ce qui se passe avec les disques :

- Faire un diskpart
- Aller dans gestionnaires des disques

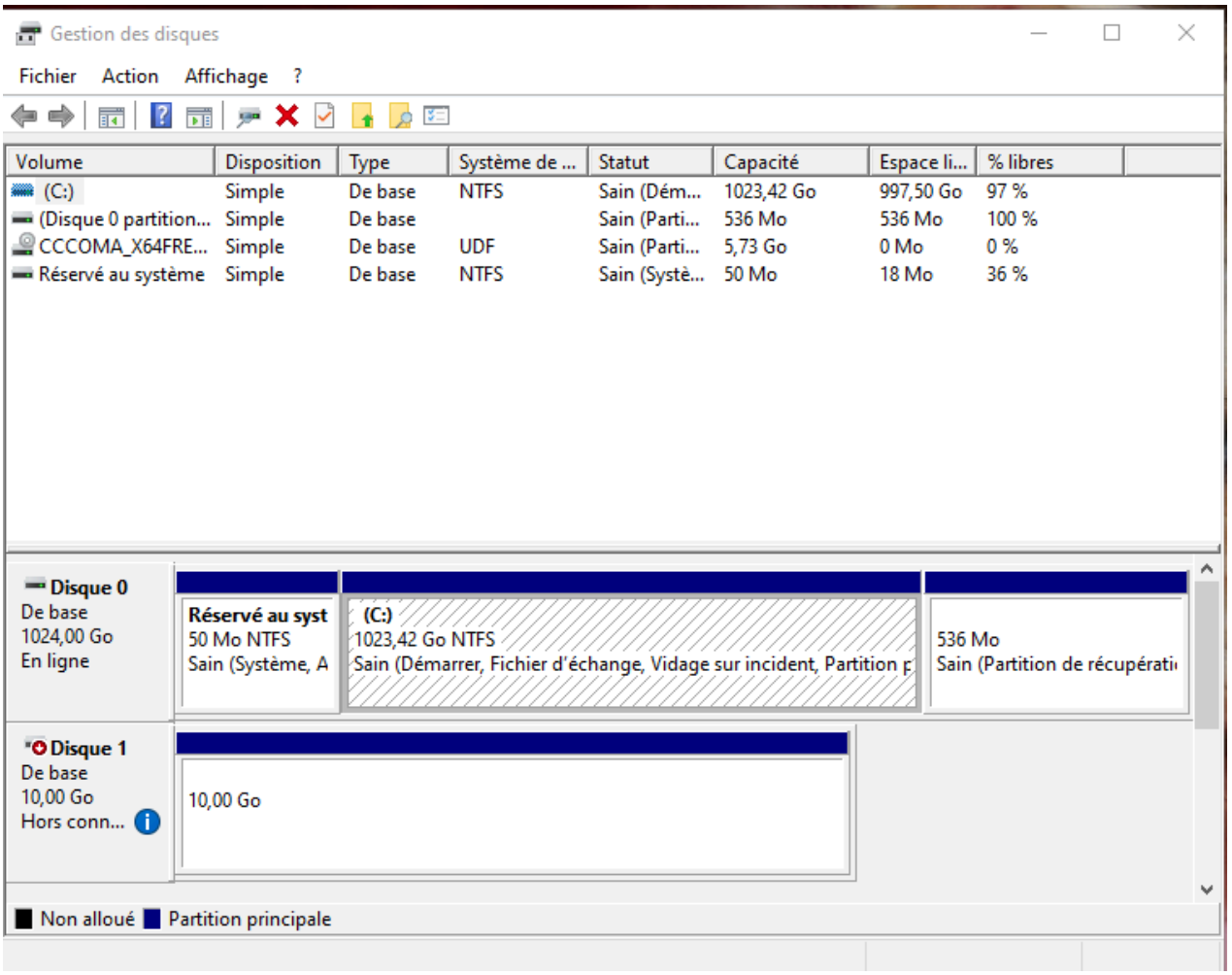


image-17.png

On voit bien deux disques et ces différents volumes.
Le Disque 1 est actuellement hors connexion. Nous somme pas brancher sur ce disque.

- Cliquer droit
- mettre en ligne

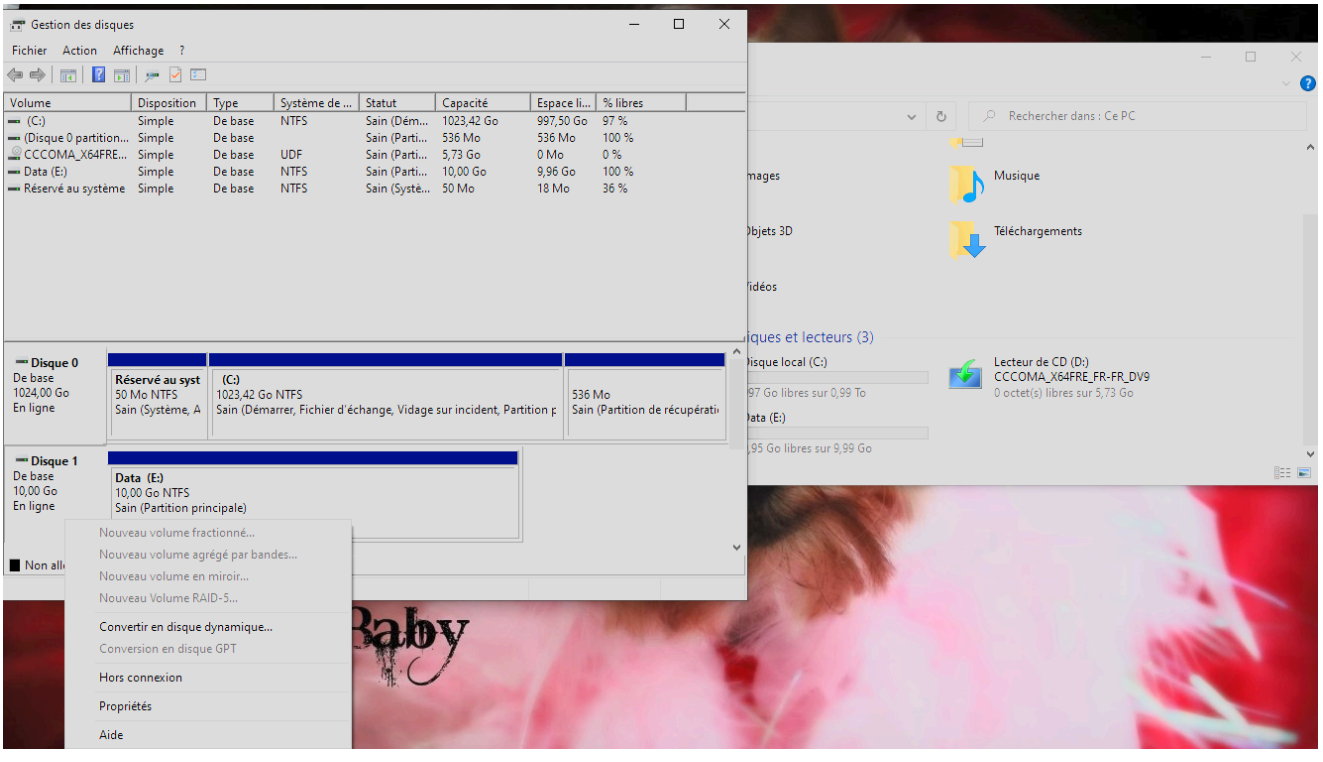


image-18.png

Dans le pire des cas :

- Faire une réparation de disques
- Connaître les raisons de la désactivation de disques

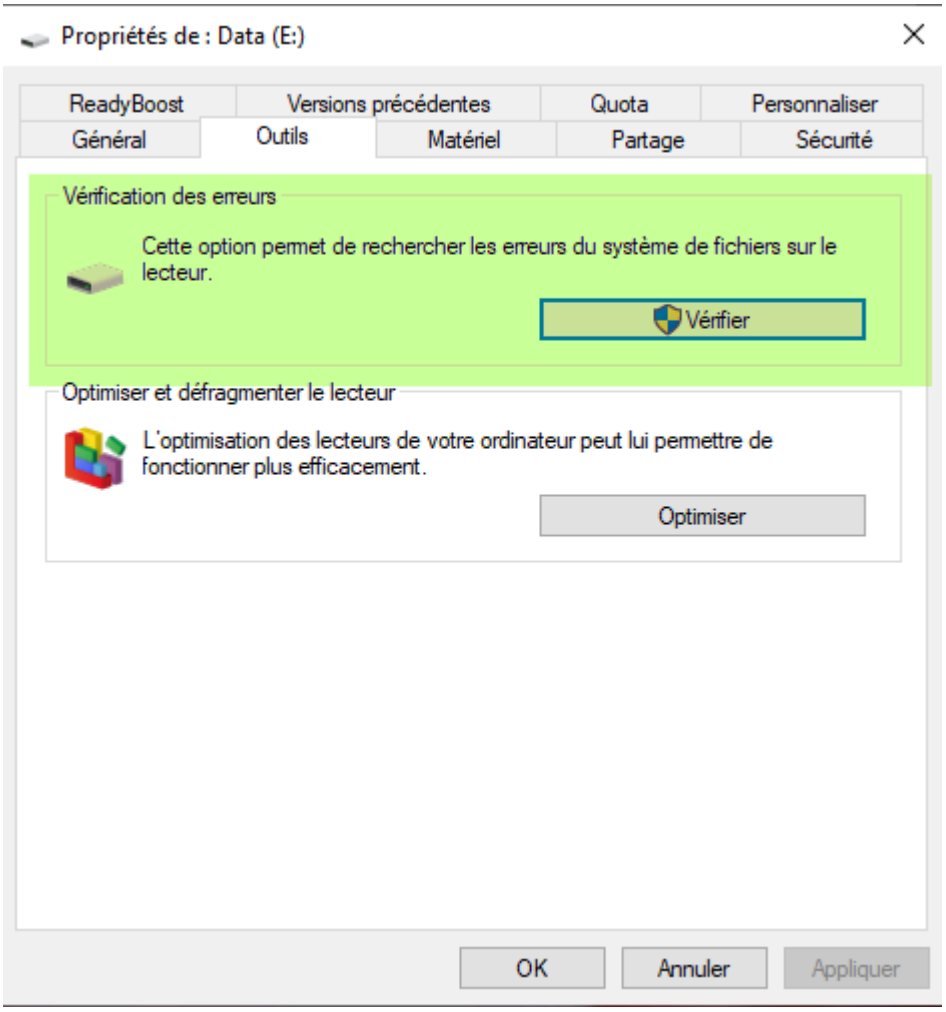


image-20.png

Vérification des erreurs est similaire que le CHKDSK mais en interface graphiques

Récupération d'image

Nous avons deux possibilité

- Outils de récupération de donnée
- Historique des fichiers

Historique de fichier

Via le stockage on peux voir un historique des fichiers.
Dans le volume E on peut voir qu'il y a un dossier FileHistory dans lequel on retrouver les fichiers

Ce fichier est présent quand on alloue une partie du stockage pour l'historique de fichier.

Il n'est pas recommandé de faire copier coller depuis ce dossier

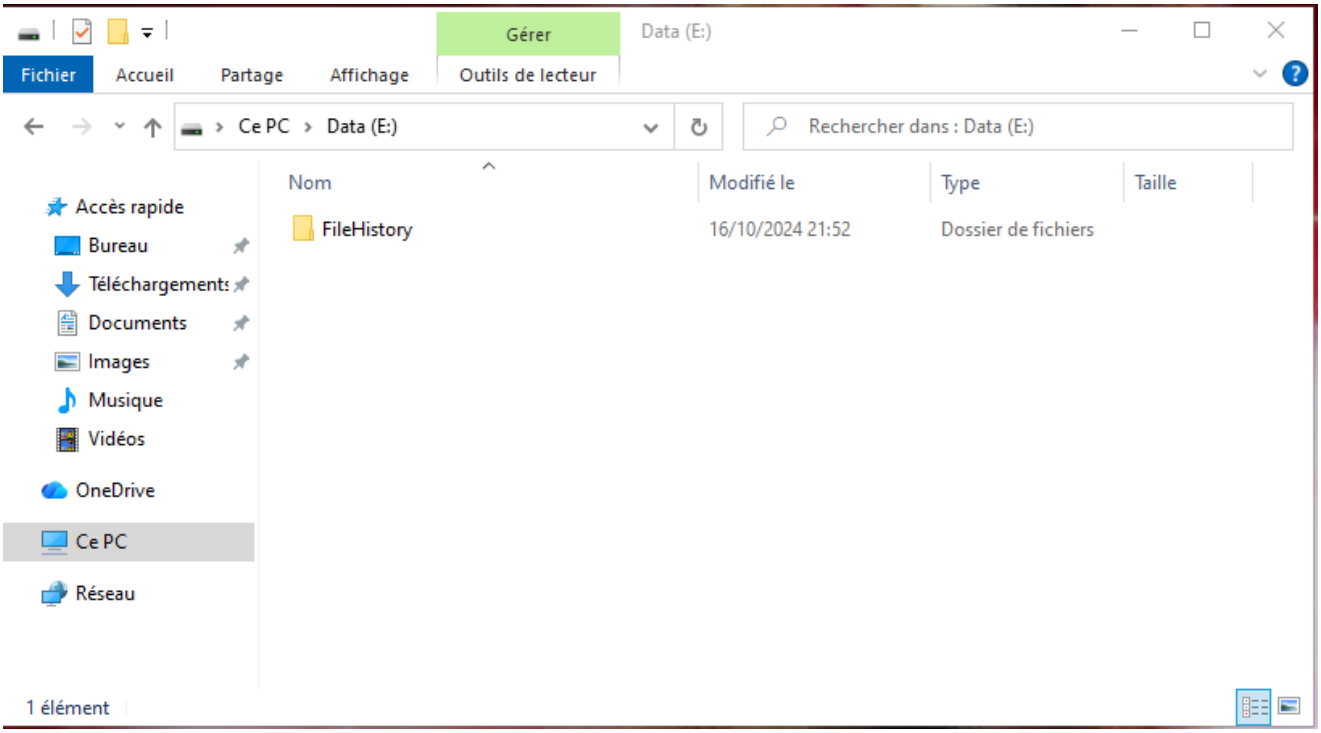


image-21.png

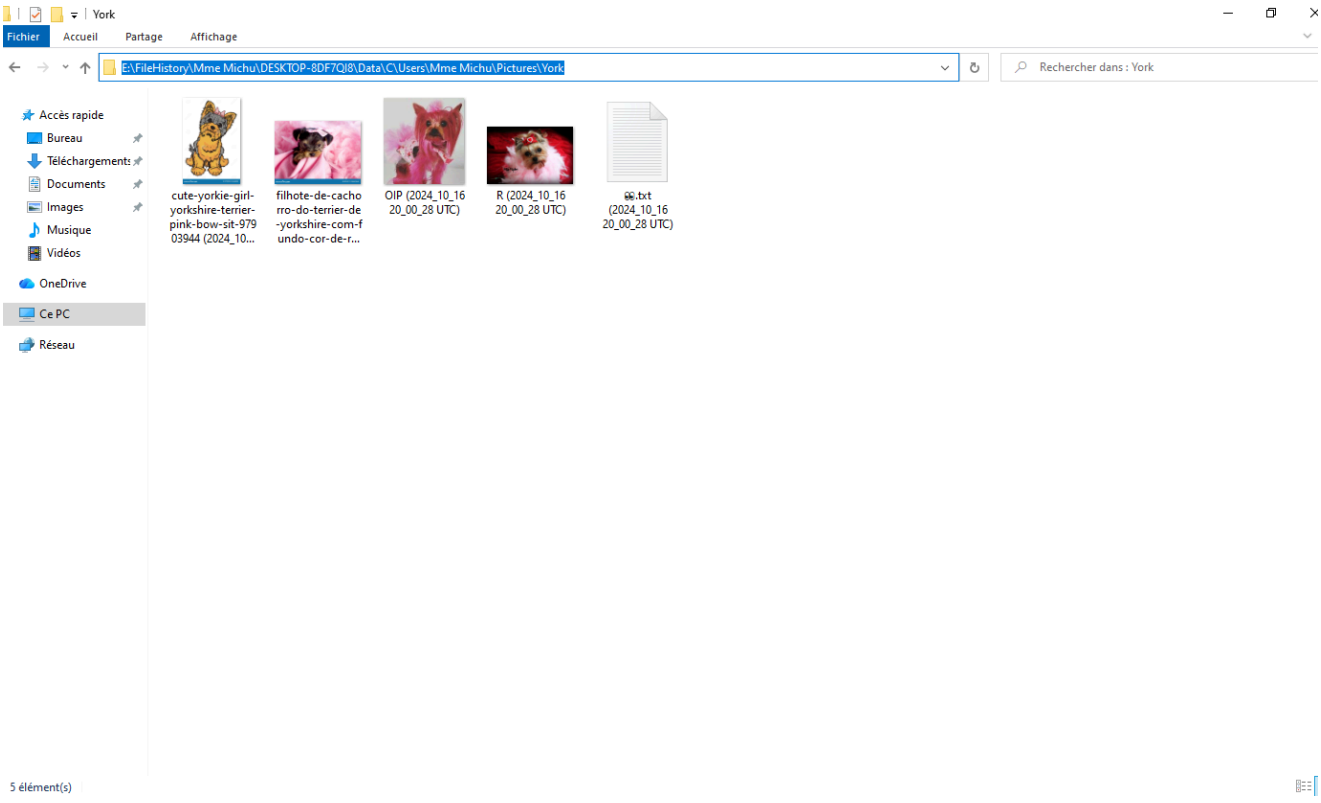


image-22.png

Afin de restaurer à une date précise et avec les même droit d'utilisation on utilise :

- Historique de fichier

Solution 1
Dans le dossier images, aller dans le dossier historique de fichiers

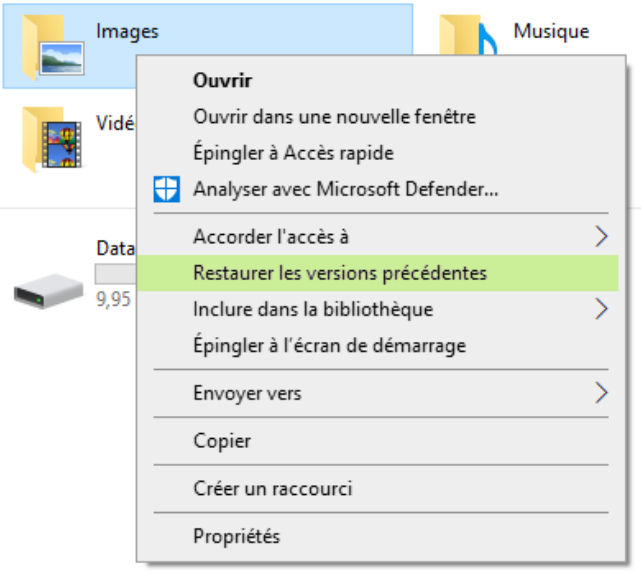


image-23.png

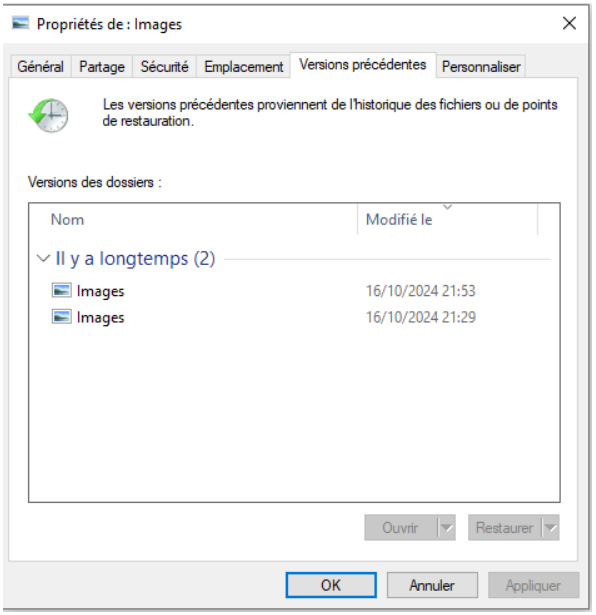


image-24.png

Solution 2
Pour voir l'ensemble de l'historique

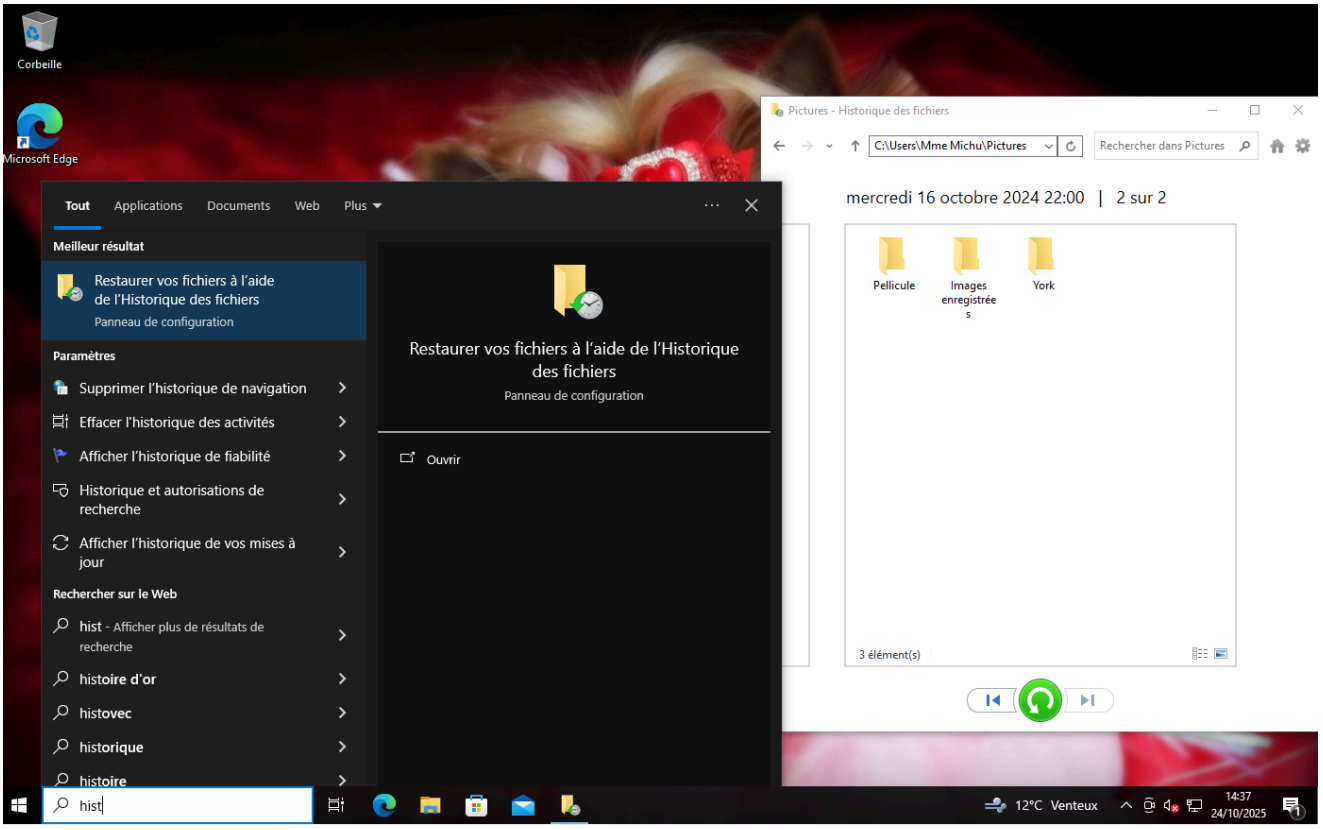


image-25.png