

BEAUX

Baptiste

1TSSIO

TP 05 : Sécuriser un poste de travail Windows

1. Gestion de l'antivirus

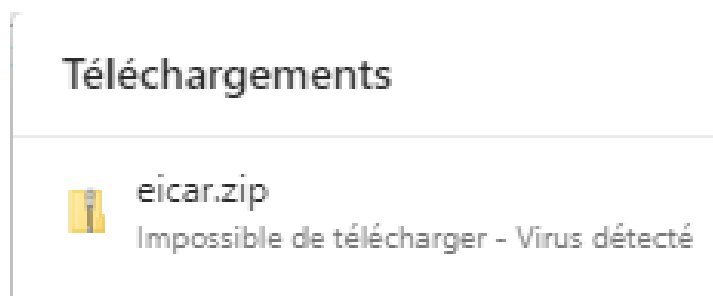
1.1. Nous pouvons voir que le contrôle des navigateurs est bien désactivé :

SmartScreen pour Microsoft Edge

Microsoft Defender SmartScreen aide à protéger votre appareil contre les sites et téléchargements malveillants.

 Désactivé

1.2. Le fichier n'a pas été téléchargé car le virus a été détecté :



1.3. J'ai décidé d'activer l'option "Envoi automatique d'un échantillon car cela permet d'envoyer un ou plusieurs échantillon(s) de fichier qu'on souhaite télécharger à Microsoft, et par la suite Microsoft nous informera s'ils détectent les virus ou non dans nos fichiers.


Envoi automatique d'un échantillon

Envoyez des échantillons de fichier à Microsoft pour vous protéger et protéger les autres utilisateurs contre d'éventuelles menaces. Nous vous informerons si le fichier dont nous avons besoin est susceptible de contenir des informations personnelles.



Activé

1.4. Voici la trace de ce faux virus et ses détails :

 **Mise à jour incomplète**
29/11/2023 10:31 Grave ^

Déecté : Virus:DOS/EICAR_Test_File
État : Échec
Cette menace ou cette application n'est peut-être pas entièrement restaurée.

Date : 29/11/2023 10:32
Détails : Ce programme est dangereux et il se réplique en infectant d'autres fichiers.

Éléments affectés :

containerfile: C:\Users\SIO\Downloads\eicar.zip

file: C:\Users\SIO\Downloads\eicar.zip->eicar/eicar.com

webfile: C:\Users\SIO\Downloads\eicar.zip|https://www.virusanalyst.com/eicar.zip|pid:8820,ProcessStart:133457239085769342

[En savoir plus](#)

1.5. Nous pouvons voir sur l'image ci-dessous que l'antivirus est bien à jour :

Mises à jour de la protection contre les virus et menaces

La veille de sécurité est à jour.

Dernière mise à jour : 29/11/2023 10:32

2. Gestion du pare-feu (Comodo Firewall)

2.1 La connexion à Internet a bien été établie :

```
Microsoft Windows [version 10.0.19045.3324]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>ping www.free.fr

Envoi d'une requête 'ping' sur www.free.fr [212.27.48.10] avec 32 octets de données :
Réponse de 212.27.48.10 : octets=32 temps=30 ms TTL=50
Réponse de 212.27.48.10 : octets=32 temps=15 ms TTL=50
Réponse de 212.27.48.10 : octets=32 temps=14 ms TTL=50
Réponse de 212.27.48.10 : octets=32 temps=15 ms TTL=50

Statistiques Ping pour 212.27.48.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 14ms, Maximum = 30ms, Moyenne = 18ms
```

2.2 Le pare-feu Comodo-Firewall a bien été activé :



2.3 Nous pouvons voir ici présent que la connexion à Internet a échoué :

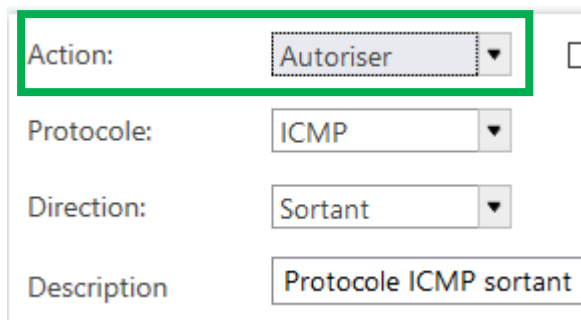
```
Microsoft Windows [version 10.0.19045.3324]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\SIO>ping www.free.fr

Envoi d'une requête 'ping' sur www.free.fr [212.27.48.10] avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 212.27.48.10:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

2.4 Nous pouvons voir qu'à présent, l'option pour autoriser le « ping » est bien activée :



Action:	Autoriser ▼
Protocole:	ICMP ▼
Direction:	Sortant ▼
Description	Protocole ICMP sortant

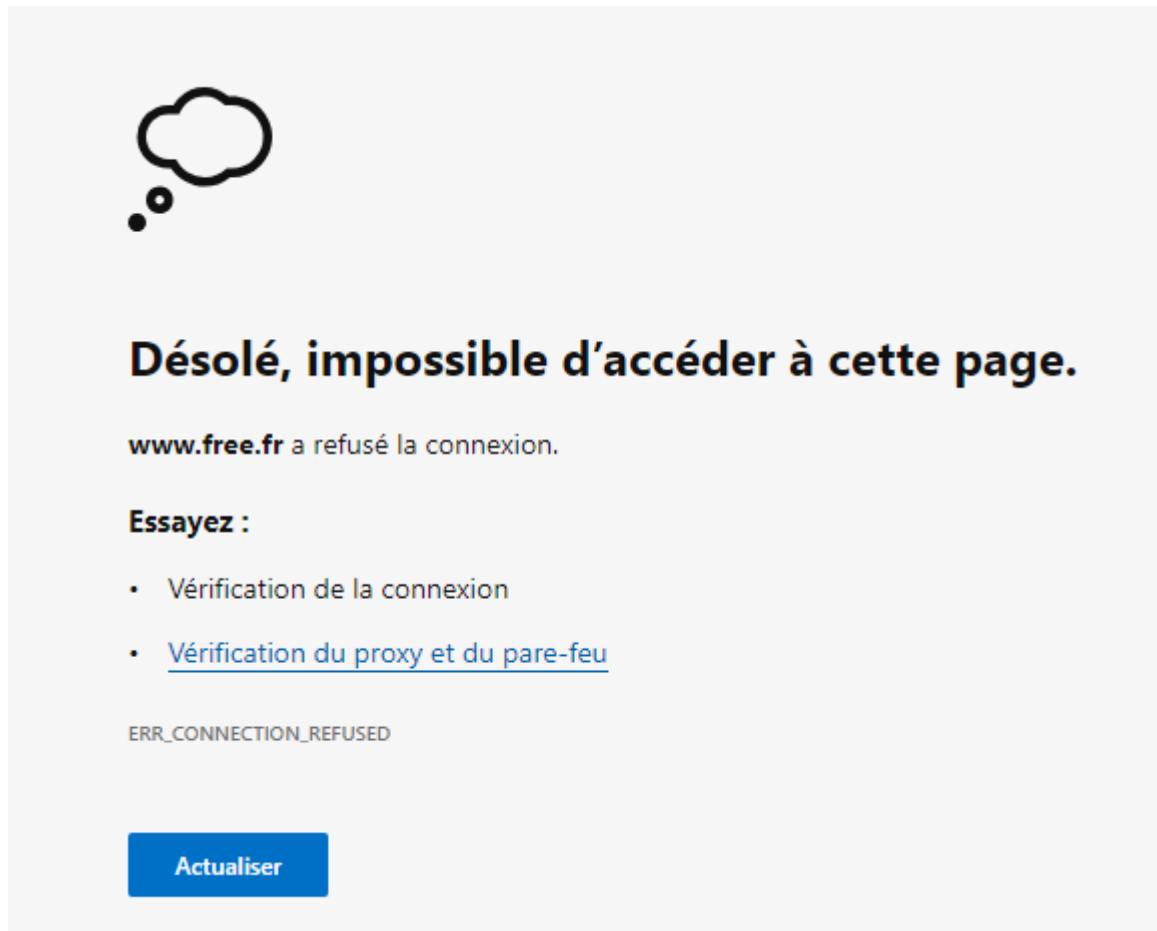
2.5 Le ping à bien fonctionné et la connexion à Internet est bien établie :

```
C:\Users\SIO>ping www.free.fr

Envoi d'une requête 'ping' sur www.free.fr [212.27.48.10] avec 32 octets de données :
Réponse de 212.27.48.10 : octets=32 temps=13 ms TTL=50
Réponse de 212.27.48.10 : octets=32 temps=13 ms TTL=50
Réponse de 212.27.48.10 : octets=32 temps=14 ms TTL=50
Réponse de 212.27.48.10 : octets=32 temps=13 ms TTL=50

Statistiques Ping pour 212.27.48.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 13ms, Maximum = 14ms, Moyenne = 13ms
```

2.6 Non, la connexion à une autre page web (www.free.fr) sur un navigateur est impossible :



2.7 L'option pour autoriser les protocoles http et https en sortie est bien activée :

Action:	Autoriser ▼	<input type="checkbox"/> Con:
Protocole:	TCP ou UDP ▼	
Direction:	Sortant ▼	
Description	Protocole http / https sortant	

2.8 La possibilité d'accéder au web est activée :



2.9

Le protocole http (HyperText Transfer Protocol) est un protocole de communication client-serveur développé pour le Web

Le protocole httpS (HyperText Transfer Protocol Securised) est le même protocole que le http sauf qu'avec le Protocole HTTPS, le navigateur et le serveur établissent une connexion sécurisée et chiffrée avant de transférer des données.

3. Mises à jour Windows

3.1 Nous pouvons voir qu'il y'a bien des mises à jour Windows à faire :

Windows Update



Mises à jour disponibles

Dernière vérification : aujourd'hui, 10:24

Votre appareil ne dispose pas des correctifs de qualité et de sécurité importants.

Outil de suppression de logiciels malveillants Windows x64 - v5.119 (KB890830)

Statut : Installation en attente

2023-11 Mise à jour cumulative de .NET Framework 3.5, 4.8 et 4.8.1 Windows 10 Version 22H2 pour x64 (KB5032339)

Statut : Installation en attente

2023-11 Mise à jour cumulative pour Windows 10 Version 22H2 pour les systèmes x64 (KB5032189)

Statut : Installation en attente

2023-10 Mise à jour pour Windows 10 Version 22H2 sur systèmes x64 (KB4023057)

Statut : Installation en attente

2023-10 Mise à jour pour Windows 10 Version 22H2 sur systèmes x64 (KB5001716)

Statut : Installation en attente

Installer maintenant

3.2 Les téléchargements à partir d'autres PC du même réseau sont bien activés :

Autoriser les téléchargements à partir d'autres PC

Si vous avez une connexion Internet instable ou si vous mettez plusieurs appareils à jour, autoriser les téléchargements à partir d'autres PC peut accélérer le processus.

Si cette fonction est activée, votre PC peut également envoyer des éléments de mises à jour et applications Windows précédemment téléchargées vers des PC sur votre réseau local ou sur Internet. Votre PC ne chargera pas de contenu vers les autres PC sur Internet lorsque votre connexion réseau est limitée.

[En savoir plus](#)

Autoriser les téléchargements à partir d'autres PC

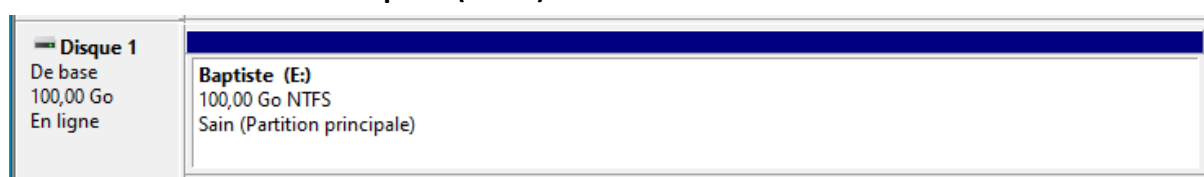
☒ Activé

☒ PC sur mon réseau local

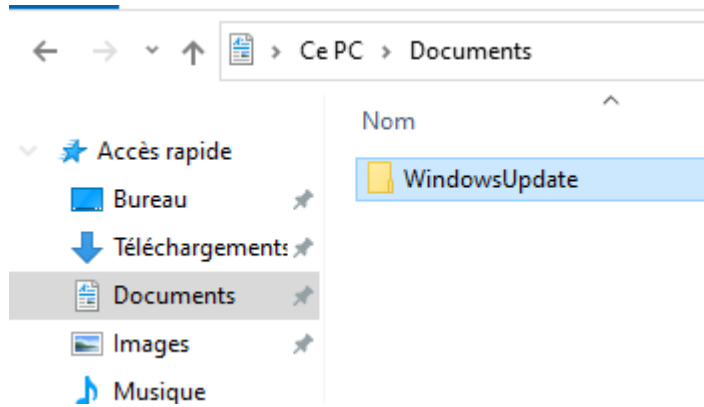
☐ PC sur mon réseau local, et PC sur Internet

4. Sauvegarde et restauration d'un poste Windows

4.4 Le nouveau disque (E :) a bien été initialisé :



4.5 Le répertoire (C:\Windows\Logs\WindowsUpdate) a bien été copié et collé dans les Documents :



4.6 La sauvegarde quotidienne des dossiers Bureau, Documents et Images a bien été initialisé :

Options de sauvegarde

Espace total sur Baptiste (E:) (E:) : 99,9 Go

Sauvegarde de vos données...

Sauvegarder les données maintenant

Sauvegarder mes fichiers

Tous les jours

Conserver mes sauvegardes

Pour toujours (par défaut)

Sauvegarder ces dossiers



Ajouter un dossier



Bureau

C:\Users\SIO



Images

C:\Users\SIO



Documents

C:\Users\SIO

4.7 La sauvegarde a bien été forcée et exécutée :

Vue d'ensemble

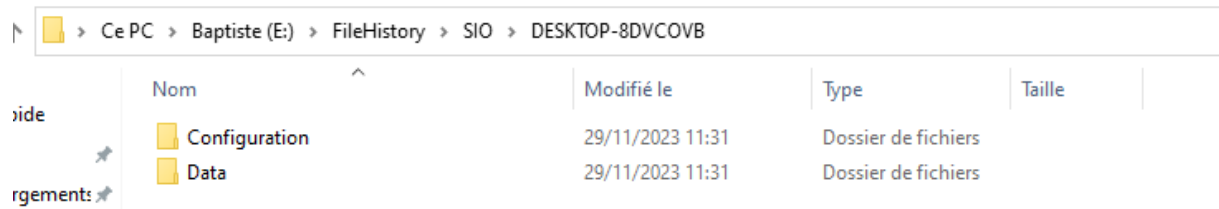
Taille de la sauvegarde : 7,16 Mo

Espace total sur Baptiste (E:) (E:) : 99,9 Go

Dernière sauvegarde : 29/11/2023 11:31

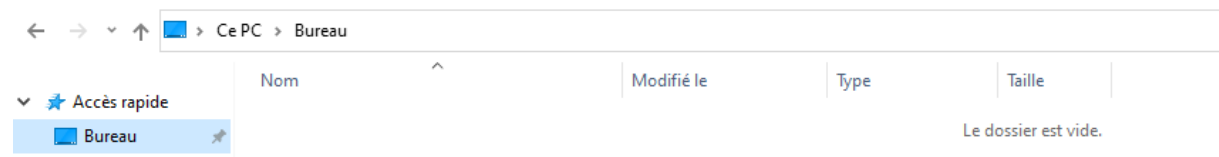
Sauvegarder les données maintenant

4.8 Grâce au chemin affiché, nous pouvons voir qu'il y'a bien un nouveau répertoire (FileHistory) crée et qu'il y'a bien des données à l'intérieur :

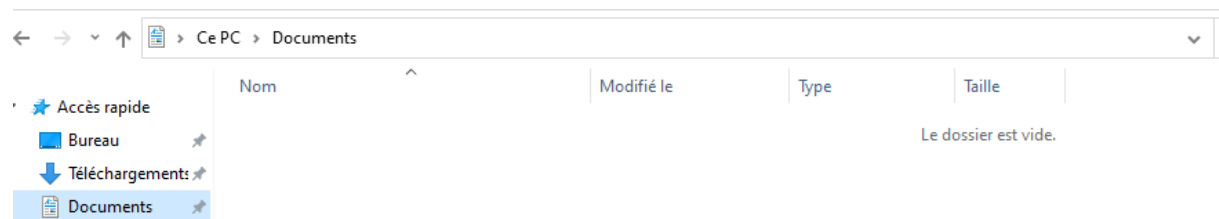


Ce PC > Baptiste (E:) > FileHistory > SIO > DESKTOP-8DVCOVB				
	Nom	Modifié le	Type	Taille
	Configuration	29/11/2023 11:31	Dossier de fichiers	
	Data	29/11/2023 11:31	Dossier de fichiers	

4.9 Le contenu des répertoires bureau et documents sont bien supprimés :

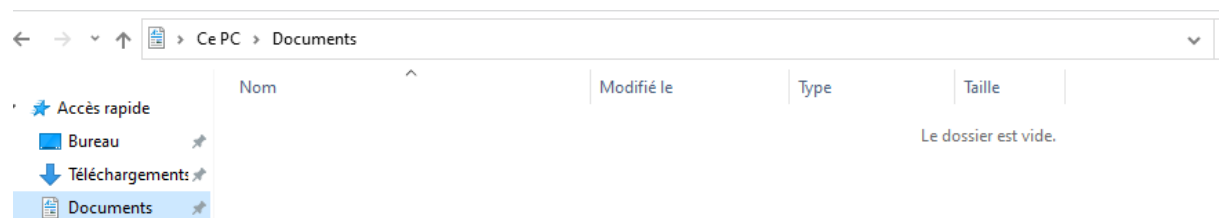


Ce PC > Bureau				
	Nom	Modifié le	Type	Taille
Le dossier est vide.				



Ce PC > Documents				
	Nom	Modifié le	Type	Taille
Le dossier est vide.				

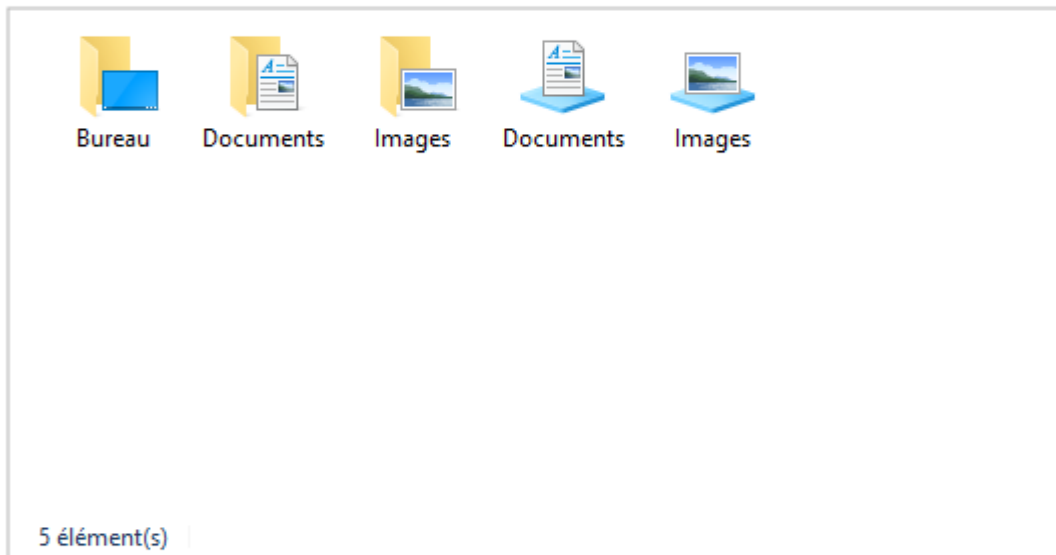
4.10 Les données ne sont plus présentes dans les documents :



Ce PC > Documents				
	Nom	Modifié le	Type	Taille
Le dossier est vide.				

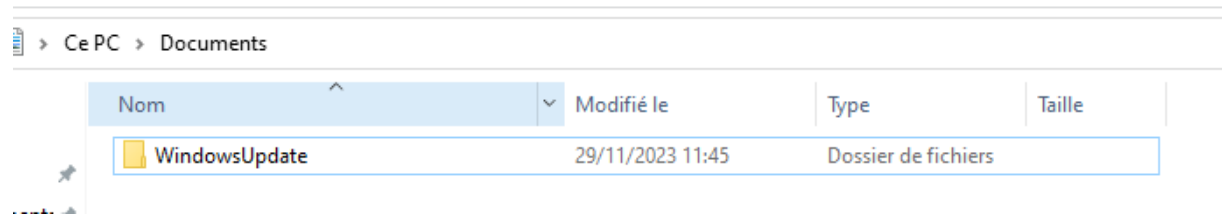
4.11 Nous pouvons voir que la restauration des données à bien marché et qu'on a pu récupérer les données :


mercredi 29 novembre 2023 11:31 | 1 sur 2



Ce PC > Disque local (C:) > Utilisateurs > SIO >				
	Nom	Modifié le	Type	Taille
	Bureau	28/08/2023 16:32	Dossier de fichiers	
	Contacts	23/09/2020 15:31	Dossier de fichiers	
nt:	Documents	29/11/2023 11:45	Dossier de fichiers	
	Favoris	23/09/2020 15:31	Dossier de fichiers	
	Images	23/09/2020 15:34	Dossier de fichiers	
	Liens	23/09/2020 15:31	Dossier de fichiers	
	Musique	23/09/2020 15:31	Dossier de fichiers	
	Objets 3D	23/09/2020 15:31	Dossier de fichiers	
	OneDrive	23/09/2020 15:35	Dossier de fichiers	
	Parties enregistrées	23/09/2020 15:31	Dossier de fichiers	
	Recherches	23/09/2020 15:33	Dossier de fichiers	
	Téléchargements	29/11/2023 10:31	Dossier de fichiers	
	Vidéos	28/08/2023 15:08	Dossier de fichiers	

4.12 Les fichiers dans Documents sont bien accessibles :



Ce PC > Documents			
Nom	Modifié le	Type	Taille
 WindowsUpdate	29/11/2023 11:45	Dossier de fichiers	