**Windows SYSINTERNALS**



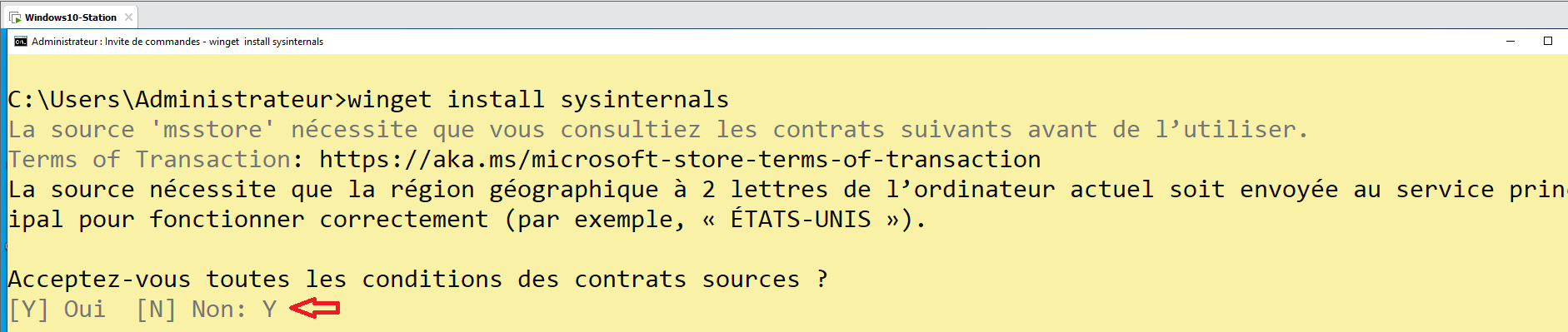
Voyons comment installer Sysinternals Suite, à partir de Microsoft Store. Sysinternals Suite est désormais disponible dans le Microsoft Store et le gestionnaire de packages Windows (winget). Windows Sysinternals Suite offre une grande variété de ressources techniques et d'utilitaires pour effectuer des tâches administratives, gérer, diagnostiquer, dépanner et surveiller un environnement Microsoft Windows de manière avancée.

Les applications Sysinternals peuvent désormais se mettre à jour automatiquement via le Microsoft Store. Au fur et à mesure que de nouvelles versions des utilitaires individuels seront publiées, Microsoft les reconditionnera dans la suite Sysinternals, les applications seront mises à jour automatiquement via le Microsoft Store.

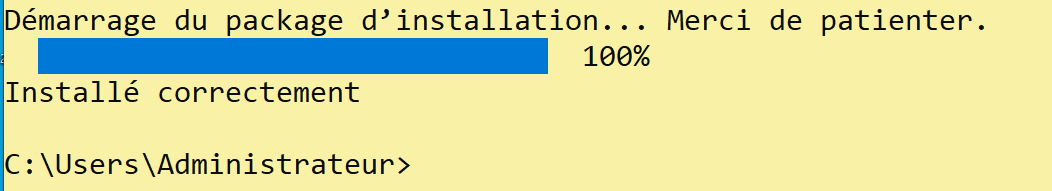
Que vous soyez un professionnel de l'informatique ou un développeur, vous trouverez des utilitaires Sysinternals pour vous aider à gérer, dépanner et diagnostiquer vos systèmes et applications Windows. Les utilitaires Sysinternals peuvent être téléchargés sous la forme d'un package tout-en-un appelé Sysinternals Suite, ou individuellement à partir du site Web Sysinternals.

1. **INSTALLATION**

Vérifier votre internet, et lancer la commande suivante : ACCEPTER LA LICENCE !

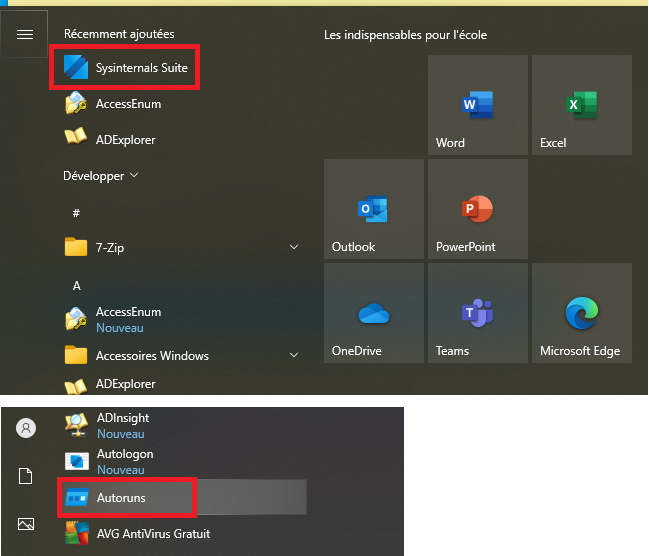


On arrive à la fin au message suivant :

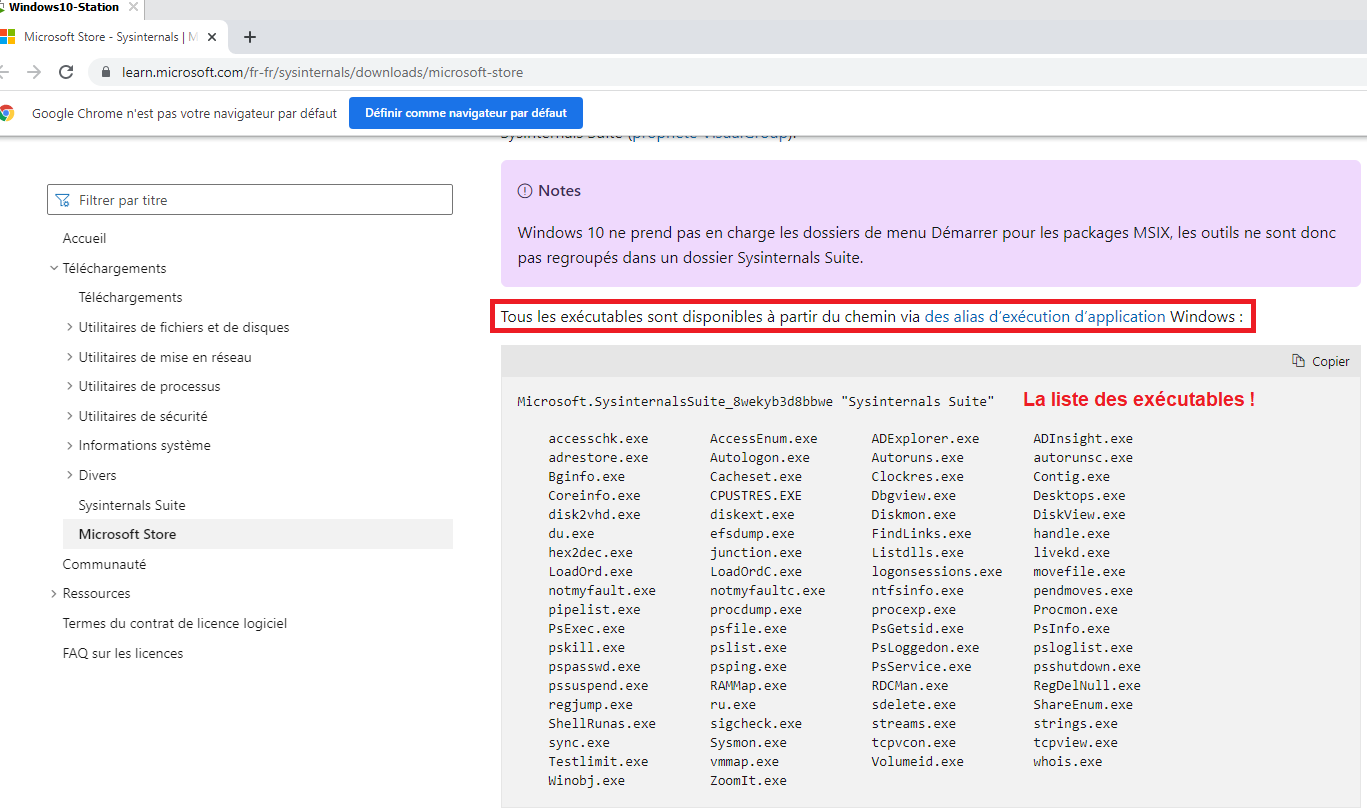


On peut également faire l’installation depuis Microsoft Store !!!!!

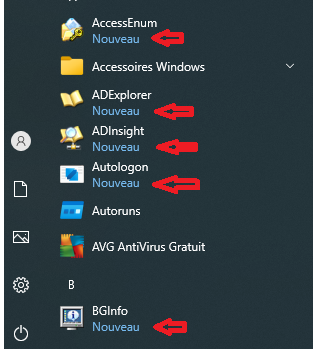
Si la suite est bien installée, vous remarquez l’ajout des deux menus suivants :



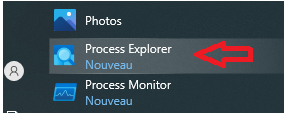
Si vous lancez le Menu Sysinternals Suite, vous tombez dans le site de Microsoft avec toutes les explications de la suite Sysinternals ainsi que les exécutables contenus dans cette suite.

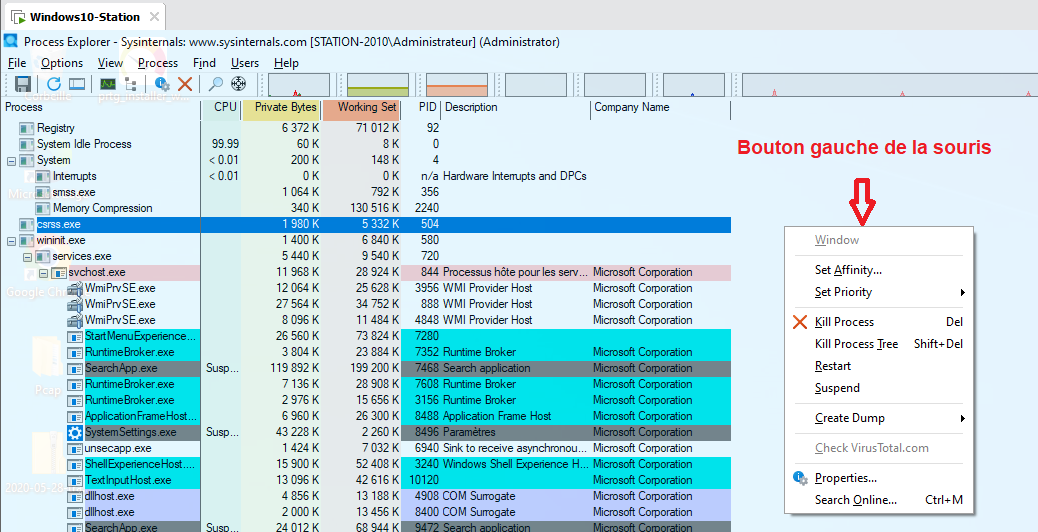


On peut accéder à ces outils avec leurs noms, qui apparaissent dans le Menu démarrer. Vous trouverez le mot nouveau en dessous du nom de l’exécutable :



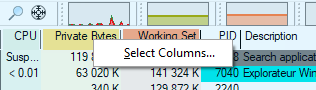
Prenons l’exemple de l’outil **Process Explorer** pour voir les processus et leurs PID, la description, le nom de la compagnie, la charge du CPU : interface graphique élaborée pour afficher les processus en cours et l'activité du système.



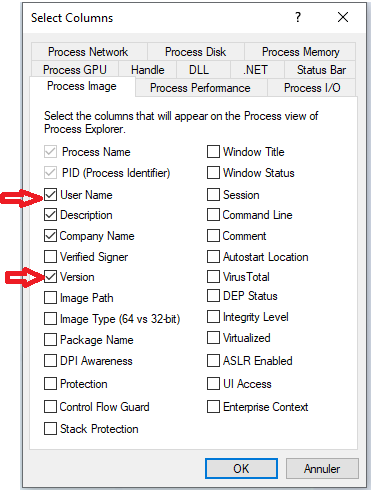


Il est vrai que le gestionnaire de tâches nous permet d’voir ces informations aussi, mais Process Explorer est complémentaire. Pour ajouter d’autres colonnes et ainsi obtenir plus d’informations, procéder comme suit :

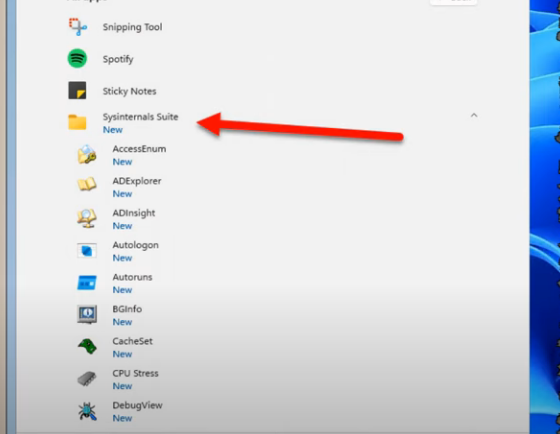
* Cliquer avec le bouton droit sur l’entête de la colonne



* Sélectionner Select Columns.
* Vous obtenez la liste des colonnes que l’on peut ajouter.

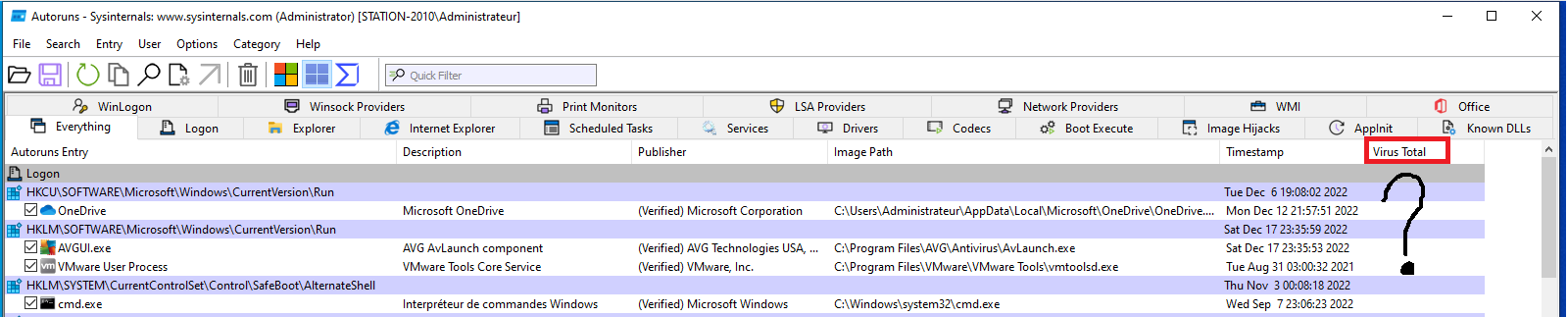


J’ai ajouté les deux colonnes indiquées ci-dessus. Sous Windows 11, les outils se trouvent sous le même Menu :

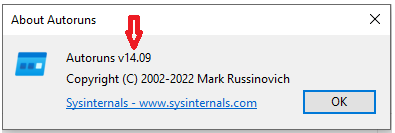
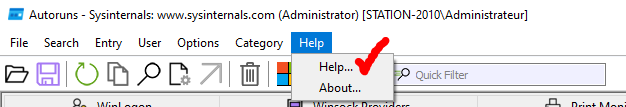


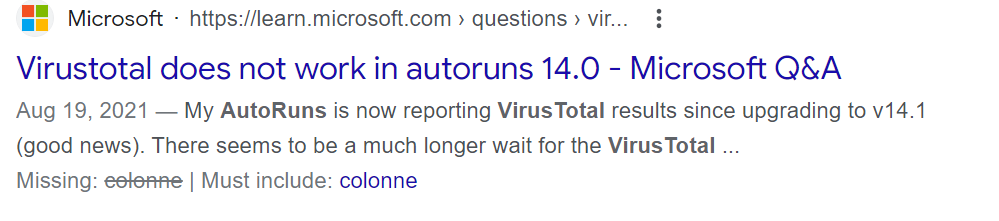
**Autorun**

C’est pour connaitre les programmes qui démarrent au démarrage de Windows.



Ma version :





# Virustotal est un antivirus en ligne où l’on peut soumettre un fichier ou une adresse web pour le faire analyser par 70 services différents. Je m’en sers régulièrement quand je reçois un lien ou un fichier que je n’attendais pas.

# Ce n’est pas une garantie que le fichier n’est pas malicieux, mais c’est un avis rassurant. Si un fichier est louche ou provient d’une source douteuse, il vaut toujours mieux ne pas l’ouvrir. Même chose si on a un doute. Les [arnaques sur le web sont de plus en plus élégantes](https://www.pascalforget.com/des-arnaques-de-plus-en-plus-elegantes/), y compris les [faux appels de service de Microsoft](https://www.pascalforget.com/appelmicrosoft/).

# Évidemment, on y pensera deux fois avant soumettre à l’antivirus VirusTotal des documents privés ou confidentiels. Les fichiers pourraient toujours être consultés par des chercheurs en virus.

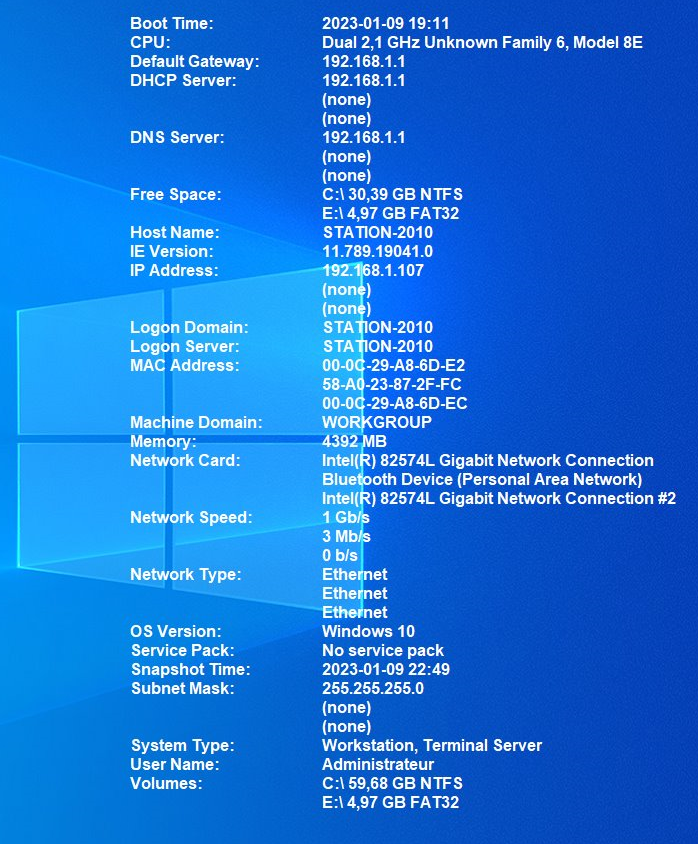
Dans Autorun, on peut vérifier un exécutable directement.

[**AdExplorer**](https://learn.microsoft.com/fr-fr/sysinternals/downloads/adexplorer)v1.51 (16 décembre 2021)

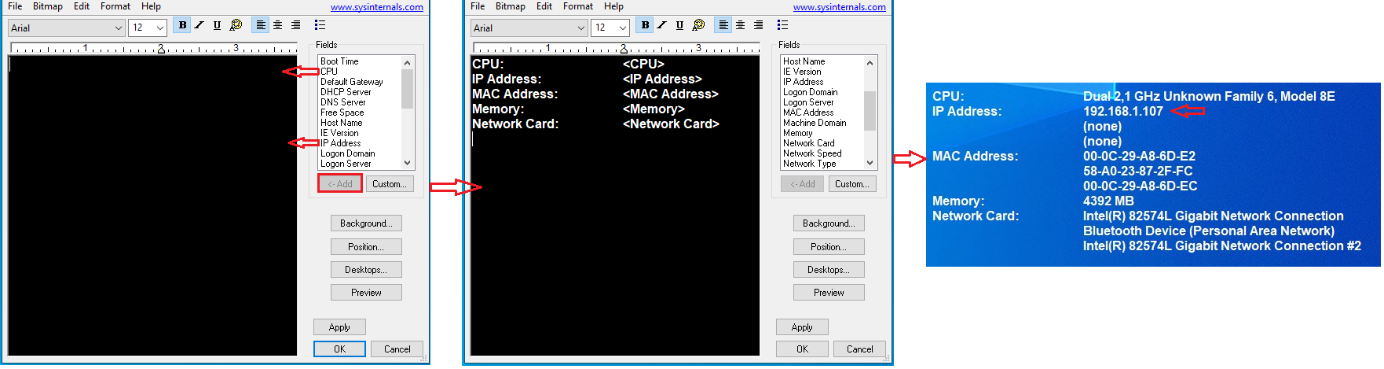
L’Explorateur Active Directory est une visionneuse et un éditeur Active Directory (AD) avancés.

[**BgInfo**](https://learn.microsoft.com/fr-fr/sysinternals/downloads/bginfo)v4.32 (29 septembre 2022)

Ce programme entièrement configurable génère automatiquement des arrière-plans de bureau qui incluent des informations importantes sur le système, notamment les adresses IP, le nom de l’ordinateur, les cartes réseau, etc. Très utile si quelqu’un veut avoir des informations sur sa machine, collées à l’écran :



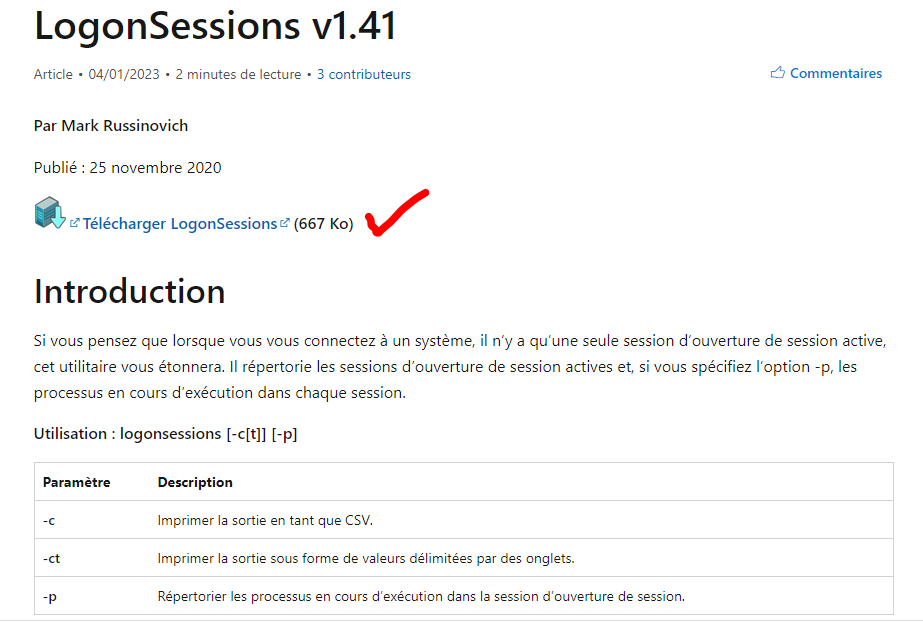
On peut effacer la configuration par défaut et personnaliser notre affichage. Par exemple, ce qui m’intéresse est les informations suivantes :



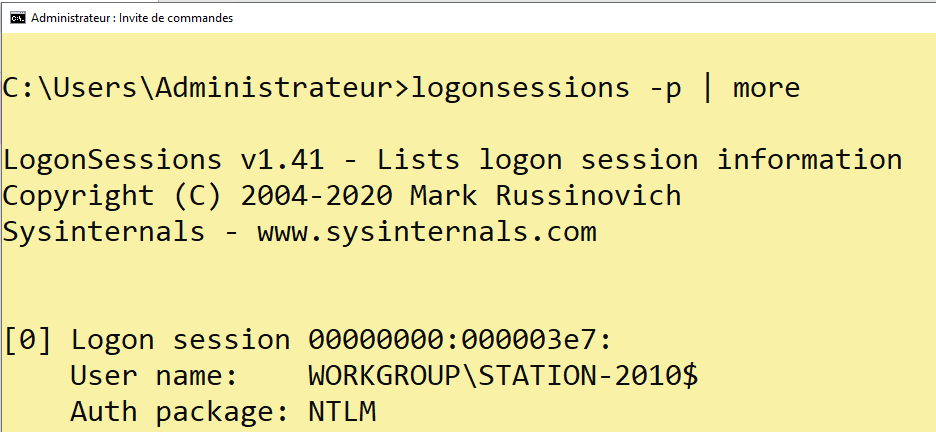
Dans le site suivant, on trouve tous les exécutables anciens (Avec les anciens systèmes) et nouveaux. Selon votre version, vous allez trouver une liste correspondante à votre version.

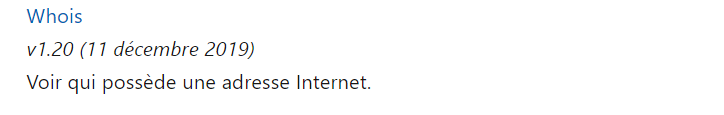
<https://learn.microsoft.com/fr-fr/sysinternals/downloads/>

Si vous remarquez un outil qui ne figure pas dans votre installation, et qu’il se trouve dans le site, vous pouvez l’ajouter. Comme : en ligne de commande.

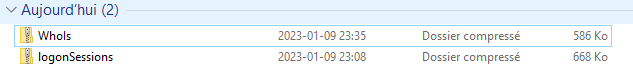


Pour le lancer :

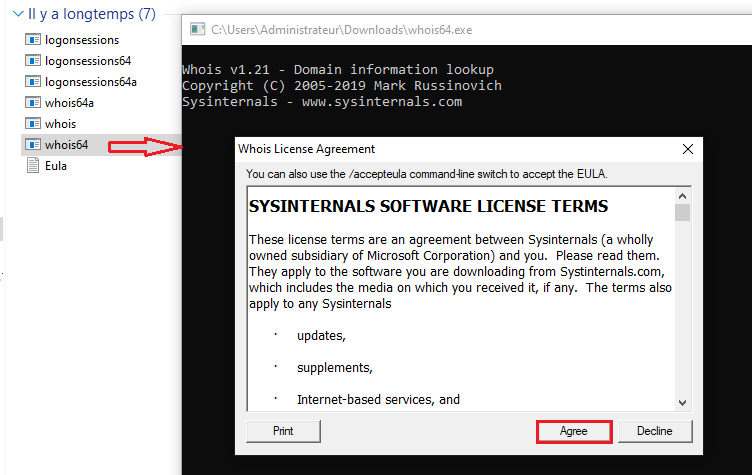




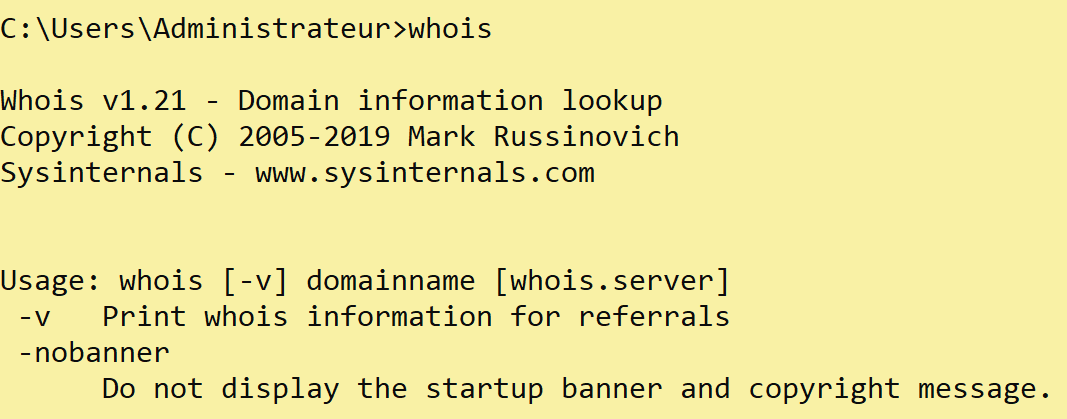
Vous télécharger le fichier zippé :



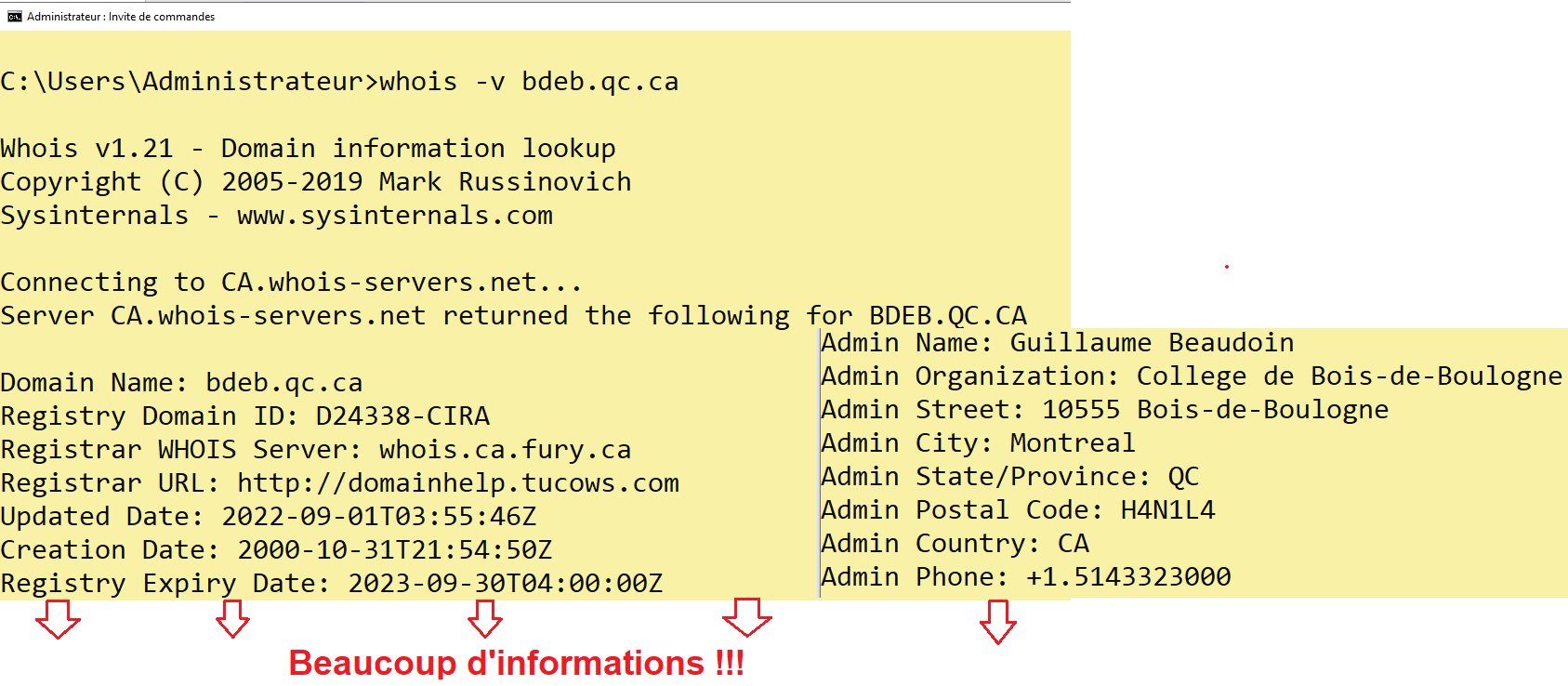
Vous décompressez le fichier et lancer la version 64 bits, comme le montre la figure suivante : acceptez la licence !



Quand vous le lancez, il va répondre et vous montre la syntaxe associée à la commande :



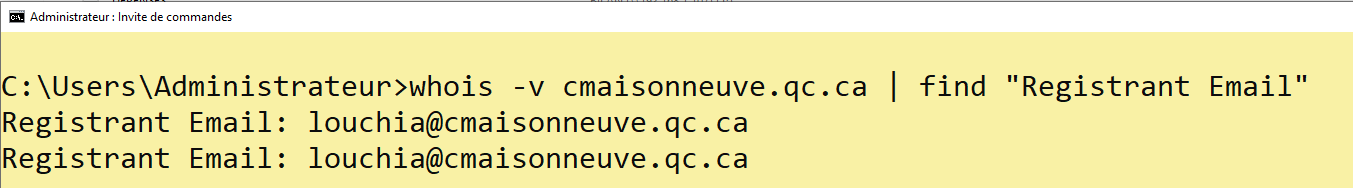
Elle donne énormément d’informations. Même le nom du technicien !

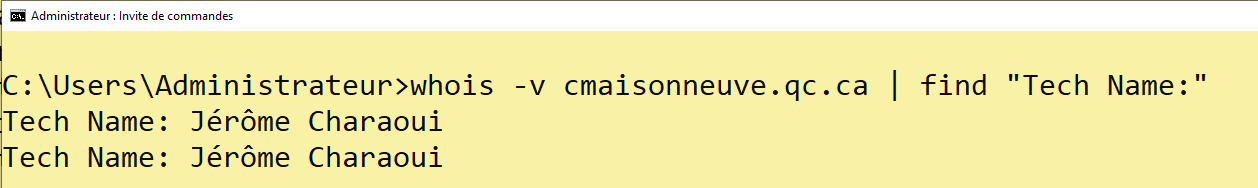


**Exercice (UTILISATION DE OUTILS SYSINTERNALS):**

Dans cet exercice, vous allez utiliser Sysinternals avec les différents exécutables. Pour l’installation, voir document ci-haut, et pour les programmes extra de Sysinternals vous les trouvez facilement dans la liste globale.

* Trouver les informations suivantes :

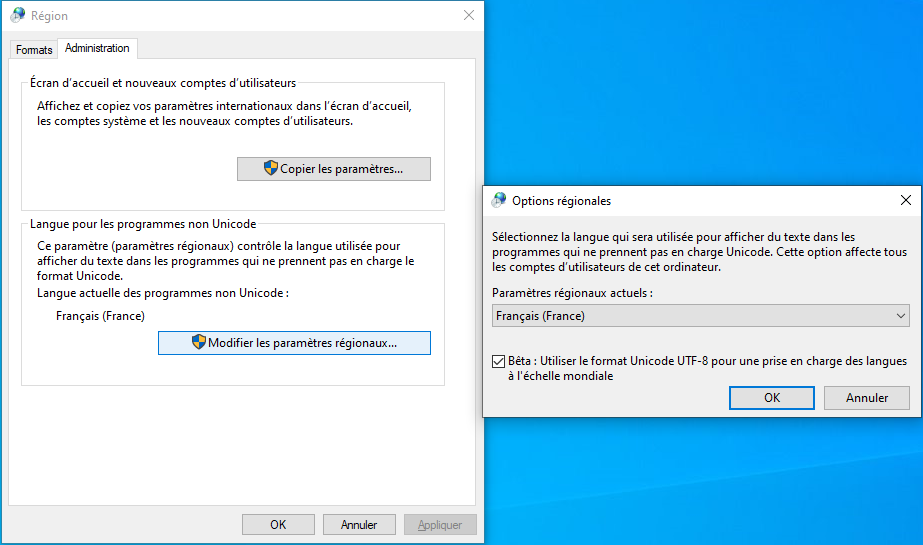




* Quel est le numéro de fax ?

……………………………………………………………..

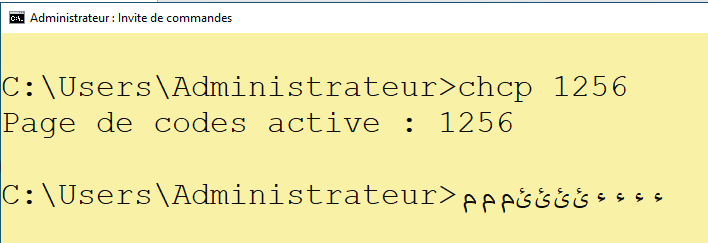
* Trouver comment activer le codage UTF-8 pour afficher tous les types de caractère, et les différents types d’accents (Aigu, circonflexe, …) 🡪intl.cpl. Ceci va vous permettre d’afficher le nom du technicien du collège Maisonneuve (Jérôme).



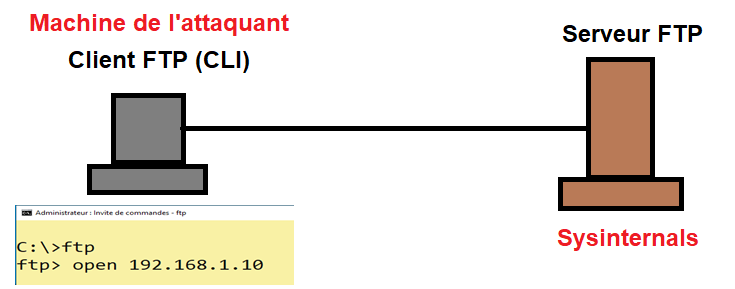
Placer les informations suivantes au milieu de l’écran !



Par exemple pour écrire en arabe dans un terminal cmd (De Windows), il faut lancer la page de code suivante :



* Dans votre système où est installé Sysinternals, configurer un serveur FTP.
* Connectez-vous avec un utilisateur nommé malicieux (L’utilisateur doit être créé) depuis une autre machine sur le serveur FTP. Utiliser une session en ligne de commande :



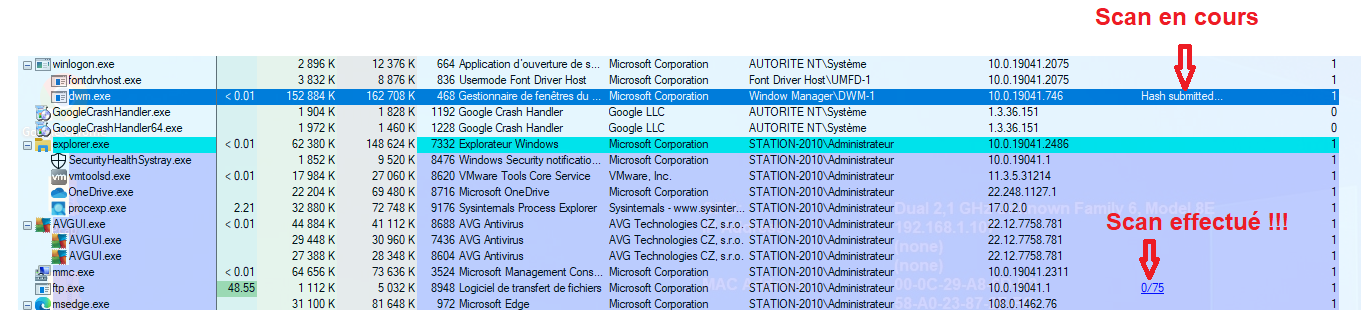
* Trouver l’outil qui permet de montrer l’utilisateur connecté avec FTP
* Trouver un ou deux moyens pour déconnecter l’utilisateur malicieux.
* Comment peut-on tuer le processus FTP de malicieux ?

Une des choses intéressantes à faire avec Process Explorer, est la vérification des fichiers, et s’ils présentent un risque d’infection (Malware).

Un résultat VirusTotal de 0/55 signifie que 55 produits antivirus ont vérifié le fichier et qu'aucun d'entre eux n'a rien détecté !

Cliquez sur le résultat/lien pour ouvrir le rapport détaillé dans un navigateur Web. Vous y trouverez quand l'analyse a été effectuée et d'autres informations utiles telles que les produits antivirus qui ont détecté quoi que ce soit et le type d'infection/malware possible.

* Vérifier quel processus avec VirusTotal.



<https://www.malekal.com/process-explorer-gestionnaire-taches-avance/#Comment_trouver_le_processus_lie_a_une_fenetre_avec_ProcessnbspExplorer>