

# 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 !

```
Windows10-Station
Administrateur : invite de commandes - winget install sysinternals

C:\Users\Administrateur>winget install sysinternals
La source 'msstore' nécessite que vous consultiez les contrats suivants avant de l'utiliser.
Terms of Transaction: https://aka.ms/microsoft-store-terms-of-transaction
La source nécessite que la région géographique à 2 lettres de l'ordinateur actuel soit envoyée au service principal pour fonctionner correctement (par exemple, « ÉTATS-UNIS »).

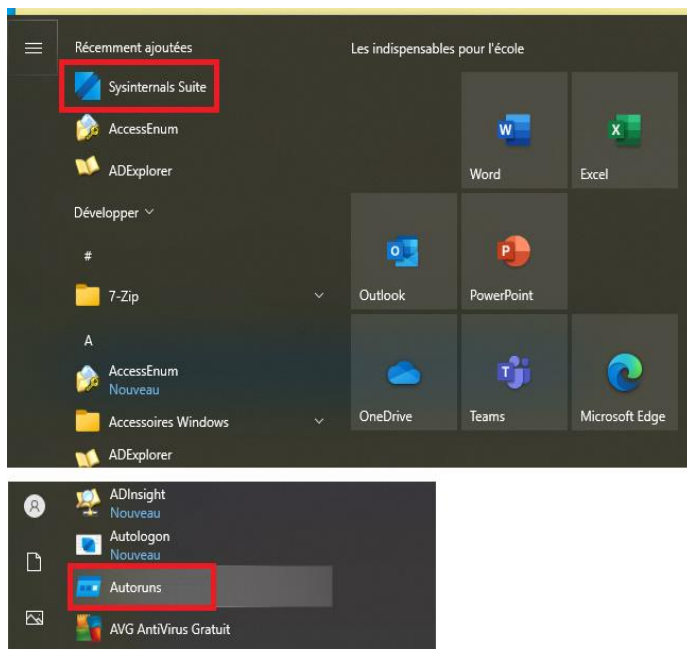
Acceptez-vous toutes les conditions des contrats sources ?
[Y] Oui [N] Non: Y
```

On arrive à la fin au message suivant :

```
Démarrage du package d'installation... Merci de patienter.
100%
Installé correctement
C:\Users\Administrateur>
```

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.

Windows10-Station x

Microsoft Store - Sysinternals | N | x +

learn.microsoft.com/fr-fr/sysinternals/downloads/microsoft-store

Google Chrome n'est pas votre navigateur par défaut Définir comme navigateur par défaut

Filtrer par titre

Accueil

▼ Téléchargements

Téléchargements

> Utilitaires de fichiers et de disques

> Utilitaires de mise en réseau

> Utilitaires de processus

> Utilitaires de sécurité

> Informations système

> Divers

Sysinternals Suite

Microsoft Store

Communauté

> Ressources

Termes du contrat de licence logiciel

FAQ sur les licences

Notes

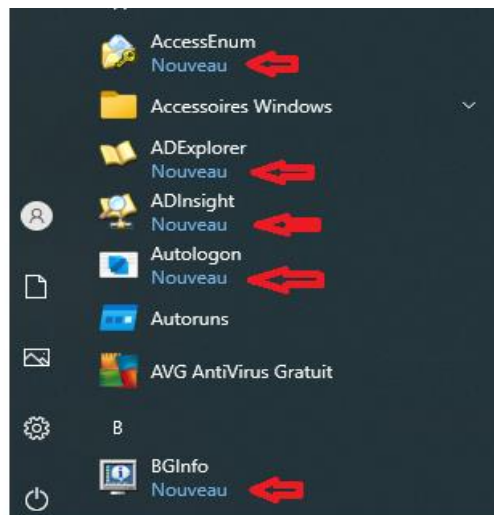
Windows 10 ne prend pas en charge les dossiers de menu Démarrer pour les packages MSIX, les outils ne sont donc pas regroupés dans un dossier Sysinternals Suite.

Tous les exécutables sont disponibles à partir du chemin via des alias d'exécution d'application Windows :

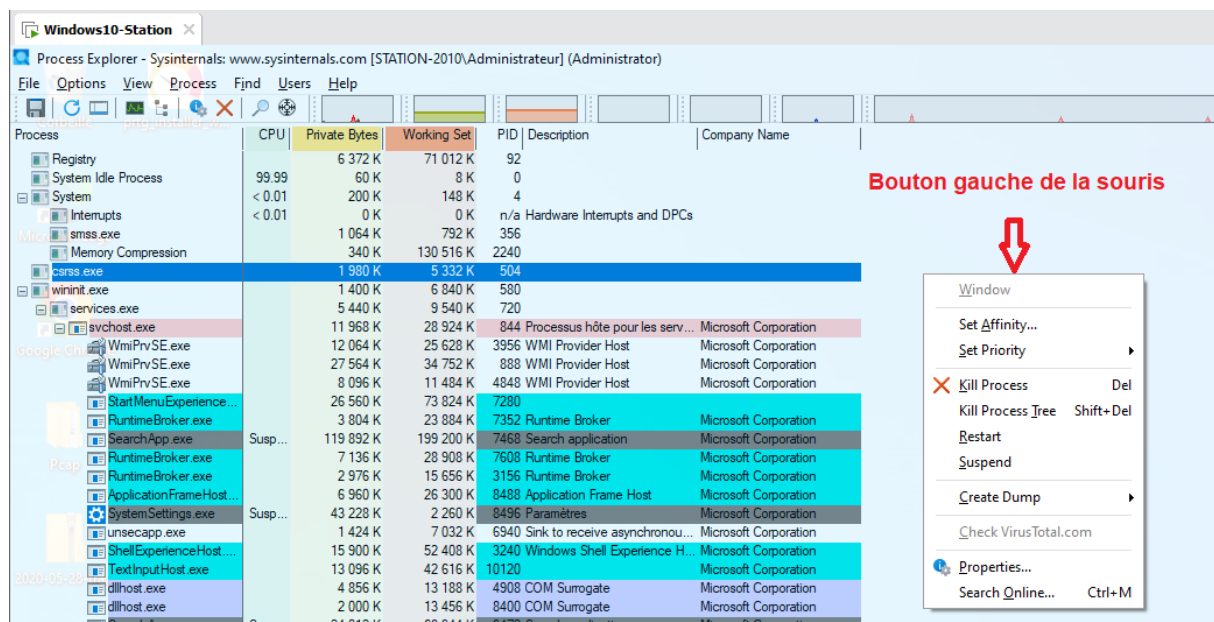
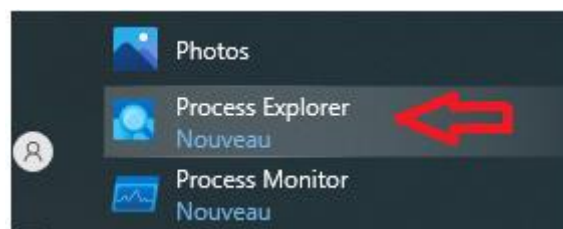
Microsoft.SysinternalsSuite\_8wekyb3d8bbwe "Sysinternals Suite" La liste des exécutables !

accesschk.exe	AccessEnum.exe	ADExplorer.exe	ADInsight.exe
adrestore.exe	Autologon.exe	Autoruns.exe	autorunsc.exe
Bginfo.exe	Cacheset.exe	Clockres.exe	Contig.exe
Coreinfo.exe	CPUSTRES.EXE	Dbgview.exe	Desktops.exe
disk2vhd.exe	diskext.exe	Diskmon.exe	DiskView.exe
du.exe	efsdump.exe	FindLinks.exe	handle.exe
hex2dec.exe	junction.exe	Listdlls.exe	livekd.exe
LoadOrd.exe	LoadOrdC.exe	logonsessions.exe	movefile.exe
notmyfault.exe	notmyfaultc.exe	ntfsinfo.exe	pendmoves.exe
pipelist.exe	procdump.exe	procexp.exe	Procmon.exe
PsExec.exe	psfile.exe	PsGetsid.exe	PsInfo.exe
pskill.exe	pslist.exe	PsLoggedon.exe	psloglist.exe
pspasswd.exe	psping.exe	PsService.exe	psshutdown.exe
psuspend.exe	RAVMap.exe	RDChman.exe	RegDelNull.exe
regjump.exe	ru.exe	sdelete.exe	ShareEnum.exe
ShellRunas.exe	sigcheck.exe	streams.exe	strings.exe
sync.exe	Sysmon.exe	tcpvcon.exe	tcpview.exe
Testlimit.exe	vmmmap.exe	Volumeid.exe	whois.exe
Winobj.exe	ZoomIt.exe		

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 :

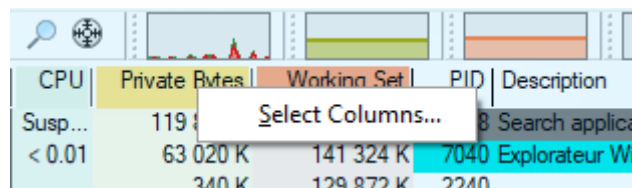


Prenons l'exemple de l'outil **Process Explorer** pour voir les processus et leurs PID, la description, le nom de la compagnie, la charge du CPU : interface graphique élaborée pour afficher les processus en cours et l'activité du système.

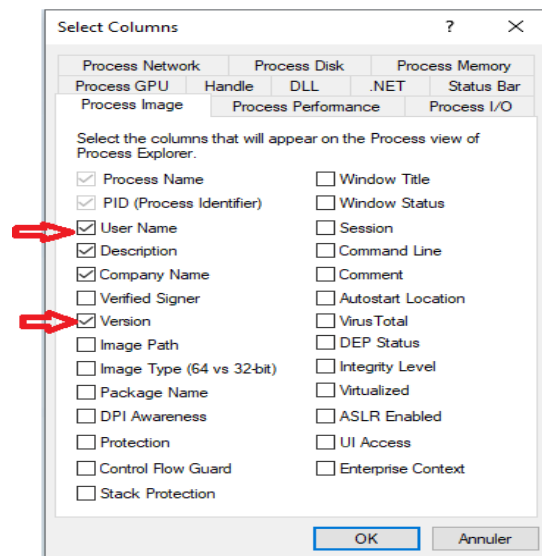


Il est vrai que le gestionnaire de tâches nous permet d'avoir ces informations aussi, mais Process Explorer est complémentaire. Pour ajouter d'autres colonnes et ainsi obtenir plus d'informations, procéder comme suit :

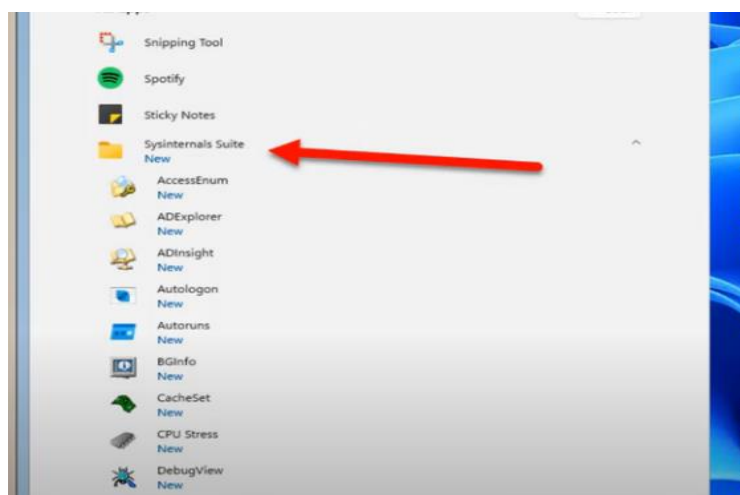
- ✓ Cliquer avec le bouton droit sur l'entête de la colonne



- ✓ Sélectionner Select Columns.
- ✓ Vous obtenez la liste des colonnes que l'on peut ajouter.

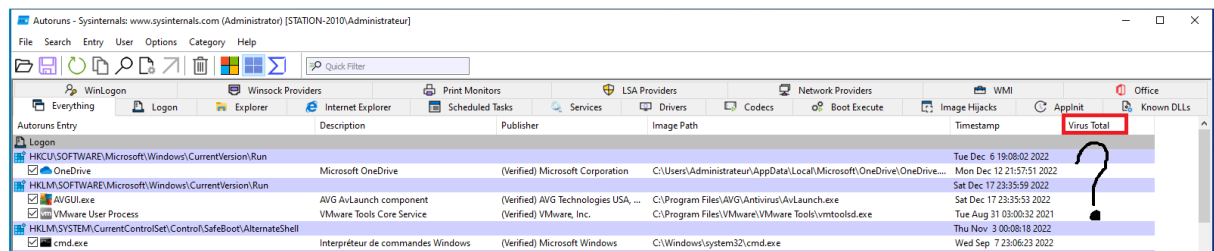


J'ai ajouté les deux colonnes indiquées ci-dessus. Sous Windows 11, les outils se trouvent sous le même Menu :

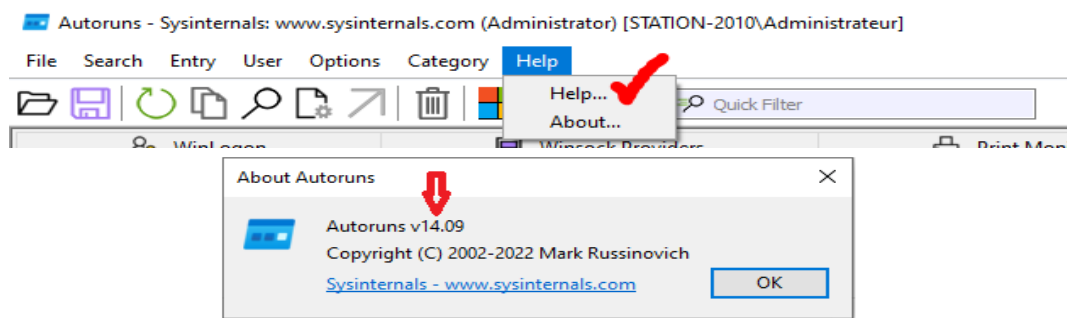


## Autorun

C'est pour connaître les programmes qui démarrent au démarrage de Windows.



Ma version :



Microsoft · <https://learn.microsoft.com/questions/vir...>

## Virustotal does not work in autoruns 14.0 - Microsoft Q&A

Aug 19, 2021 — My **AutoRuns** is now reporting **VirusTotal** results since upgrading to v14.1 (good news). There seems to be a much longer wait for the **VirusTotal** ...

Missing: colonne | Must include: colonne

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, y compris les faux appels de service de Microsoft.

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

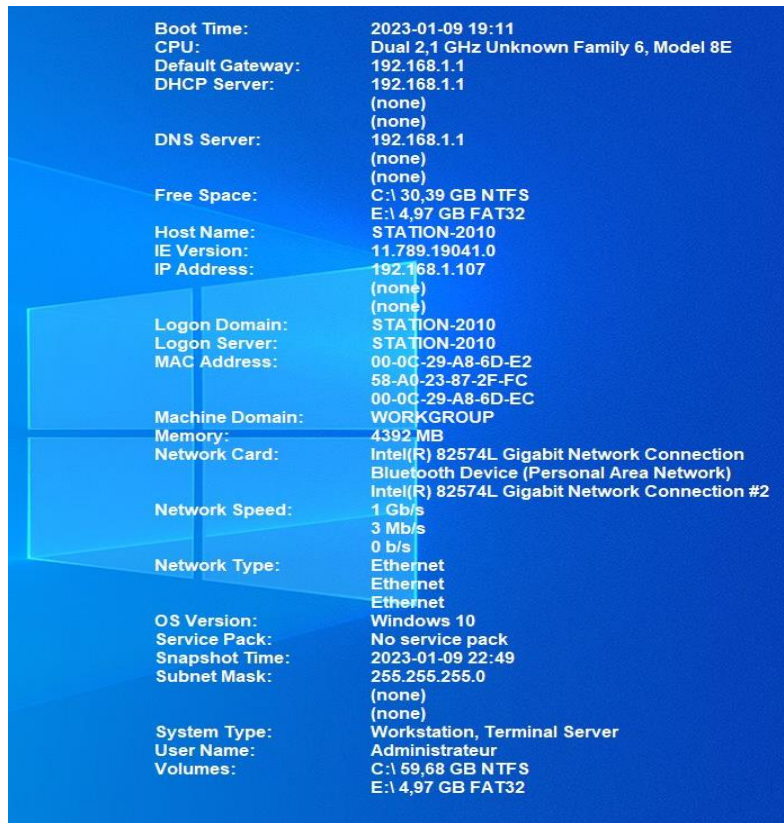
v1.51 (16 décembre 2021)

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

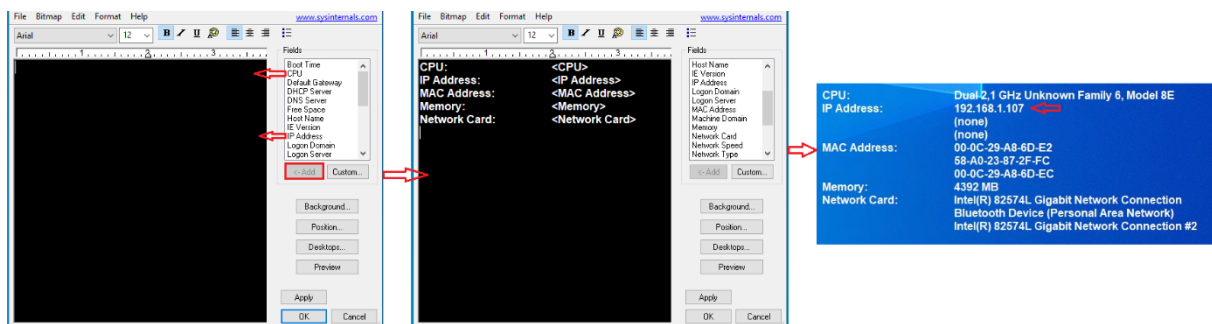
## BqInfo

v4.32 (29 septembre 2022)

Ce programme entièrement configurable génère automatiquement des arrières-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.



# LogonSessions v1.41

Article • 04/01/2023 • 2 minutes de lecture • 3 contributeurs

[Commentaires](#)

Par Mark Russinovich

Publié : 25 novembre 2020

 Télécharger LogonSessions  (667 Ko)

## Introduction

Si vous pensez que lorsque vous vous connectez à un système, il n'y a qu'une seule session d'ouverture de session active, cet utilitaire vous étonnera. Il répertorie les sessions d'ouverture de session actives et, si vous spécifiez l'option -p, les processus en cours d'exécution dans chaque session.

Utilisation : logonsessions [-c[t]] [-p]

Paramètre	Description
-c	Imprimer la sortie en tant que CSV.
-ct	Imprimer la sortie sous forme de valeurs délimitées par des onglets.
-p	Répertorier les processus en cours d'exécution dans la session d'ouverture de session.

Pour le lancer :

```
Administrateur : Invite de commandes

C:\Users\Administrateur>logonsessions -p | more

LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com



[0] Logon session 00000000:000003e7:
    User name:      WORKGROUP\STATION-2010$
    Auth package:   NTLM
```

## Whois

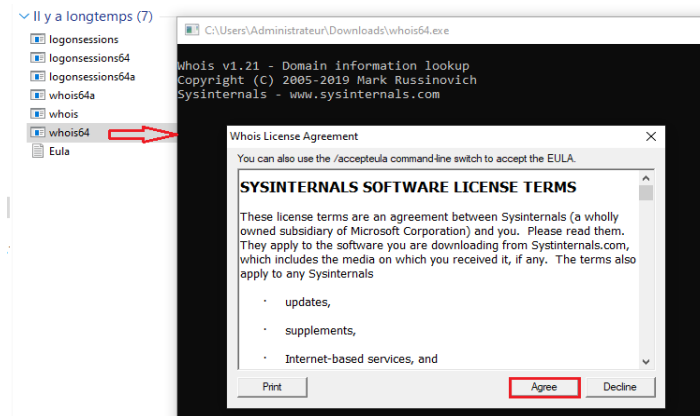
v1.20 (11 décembre 2019)

Voir qui possède une adresse Internet.

Vous télécharger le fichier zippé :

▼ Aujourd'hui (2)			
	Whois	2023-01-09 23:35	Dossier compressé 586 Ko
	logonSessions	2023-01-09 23:08	Dossier compressé 668 Ko

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 :

```
C:\Users\Administrateur>whois

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Usage: whois [-v] domainname [whois.server]
  -v    Print whois information for referrals
  -nobanner
        Do not display the startup banner and copyright message.
```

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

```
Administrateur : Invite de commandes

C:\Users\Administrateur>whois -v bdeb.qc.ca

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to CA.whois-servers.net...
Server CA.whois-servers.net returned the following for BDEB.QC.CA
Domain Name: bdeb.qc.ca
Registry Domain ID: D24338-CIRA
Registrar WHOIS Server: whois.ca.fury.ca
Registrar URL: http://domainhelp.tucows.com
Updated Date: 2022-09-01T03:55:46Z
Creation Date: 2000-10-31T21:54:50Z
Registry Expiry Date: 2023-09-30T04:00:00Z
Admin Name: Guillaume Beaudoin
Admin Organization: College de Bois-de-Boulogne
Admin Street: 10555 Bois-de-Boulogne
Admin City: Montreal
Admin State/Province: QC
Admin Postal Code: H4N1L4
Admin Country: CA
Admin Phone: +1.5143323000
```

↓ ↓ ↓ ↓ ↓

**Beaucoup d'informations !!!**

### 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 :

```
Administrateur : Invite de commandes

C:\Users\Administrateur>whois -v cmaisonneuve.qc.ca | find "Registrant Email"
Registrant Email: louchia@cmaisonneuve.qc.ca
Registrant Email: louchia@cmaisonneuve.qc.ca
```



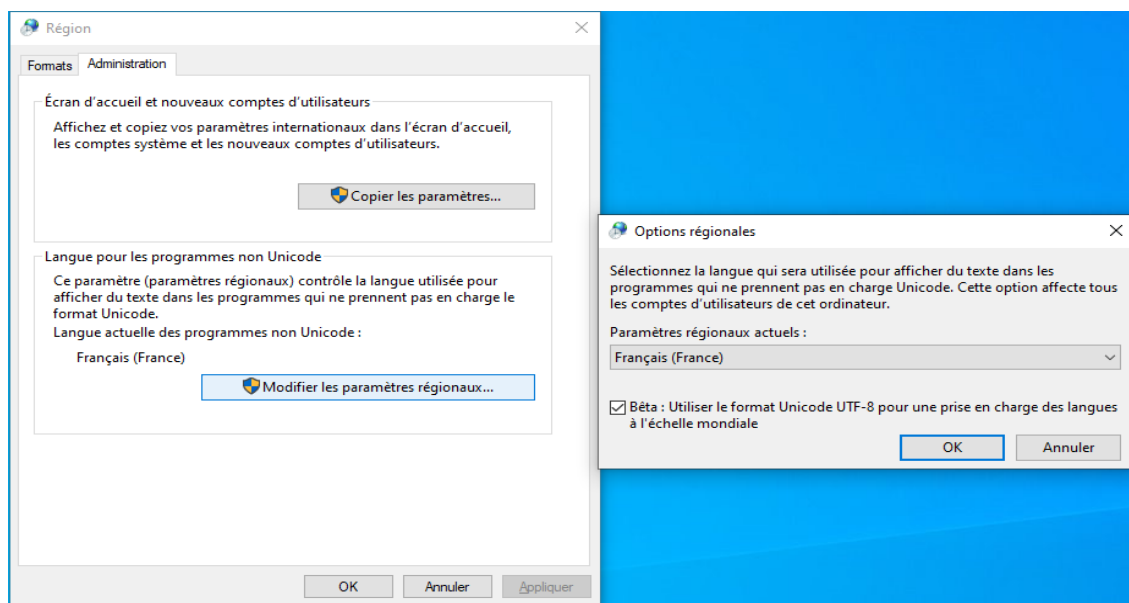
```
Administrateur : Invite de commandes

C:\Users\Administrateur>whois -v cmaisonneuve.qc.ca | find "Tech Name:"
Tech Name: Jérôme Charaoui
Tech Name: Jérôme Charaoui
```

- ✓ 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 :

```

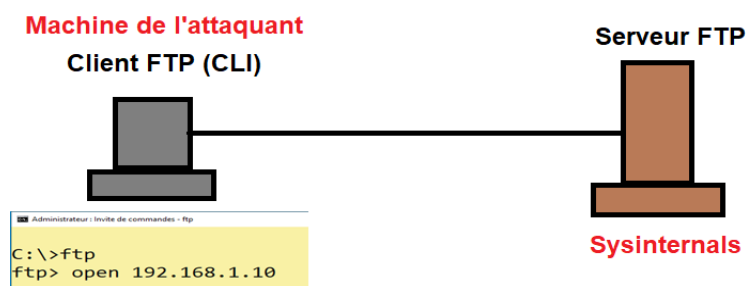
Administrateur : Invite de commandes

C:\Users\Administrateur>chcp 1256
Page de codes active : 1256

C:\Users\Administrateur> ۞۞۞۞۞۞۞۞۞۞

```

- ✓ 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/liens 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.

Scan en cours

Processus	MD5	SHA1	SHA256	Informations	Statut	Score
winlogon.exe	2 896 K	12 376 K	664 Application d'ouverture de s...	Microsoft Corporation	AUTORITE NT\Système	10.0.19041.2075
fontdrvhost.exe	3 832 K	8 876 K	836 Usermode Font Driver Host	Microsoft Corporation	Font Driver Host\UMFD-1	10.0.19041.2075
lsim.exe	< 0.01	152 884 K	162 708 K	468 Gestionnaire de fenêtres du...	Microsoft Corporation	Window Manager\UWM-1
GoogleCrashHandler.exe	1 904 K	1 828 K	1192 Google Crash Handler	Google LLC	AUTORITE NT\Système	1.3.36.151
GoogleCrashHandler64.exe	1 972 K	1 460 K	1228 Google Crash Handler	Google LLC	AUTORITE NT\Système	1.3.36.151
explorer.exe	< 0.01	62 380 K	148 624 K	7332 Explorateur Windows	Microsoft Corporation	STATION-2010\Administrateur
SecurityHealthSystray.exe	< 0.01	1 852 K	9 520 K	8476 Windows Security notificatio...	Microsoft Corporation	STATION-2010\Administrateur
ntmtoolsd.exe	< 0.01	17 894 K	27 060 K	8620 VMware Tools Core Service	VMware, Inc.	STATION-2010\Administrateur
OneDrive.exe	< 0.01	22 204 K	69 480 K	8716 Microsoft OneDrive	Microsoft Corporation	STATION-2010\Administrateur
process.exe	2.21	32 880 K	72 748 K	9176 Sysinternals Process Explorer	Sysinternals - www.sysinter...	STATION-2010\Administrateur
AVGUI.exe	< 0.01	44 884 K	41 112 K	8688 AVG Antivirus	AVG Technologies CZ, s.r.o.	STATION-2010\Administrateur
AVGUI.exe	< 0.01	29 448 K	30 960 K	7436 AVG Antivirus	AVG Technologies CZ, s.r.o.	STATION-2010\Administrateur
AVGUI.exe	< 0.01	27 388 K	28 348 K	8604 AVG Antivirus	AVG Technologies CZ, s.r.o.	STATION-2010\Administrateur
mmc.exe	< 0.01	64 656 K	73 636 K	3524 Microsoft Management Cons...	Microsoft Corporation	STATION-2010\Administrateur
ftp.exe	48.55	1 112 K	5 032 K	8948 Logiciel de transfert de fichiers	Microsoft Corporation	STATION-2010\Administrateur
msedge.exe	< 0.01	31 100 K	81 648 K	972 Microsoft Edge	Microsoft Corporation	STATION-2010\Administrateur

Scan effectué !!!

0/75

[https://www.malekal.com/process-explorer-gestionnaire-taches-avance/#Comment trouver le processus lie a une fenetre avec Process Explorer](https://www.malekal.com/process-explorer-gestionnaire-taches-avance/#Comment_trouver_le_processus_lie_a_une_fenetre_avec_Process Explorer)