

Rapport de laboratoire

PRSS – 9.1

Le Registre

2 JANVIER 2023

CLASSE SIG

Créé par : Julie Cobas



Table des matières

I. INTRODUCTION.....	1
II. EXERCICES DETAILLES	2
A. REGISTRE ET VALEUR DANS LA CLE DE REGISTRE DU PAPIER PEINT	2
1) Connexion sur le profil User1.....	2
2) Recherche et sélection d'une image comme arrière-plan du Bureau	2
3) Présentation de l'éditeur de registre Regedit.exe	3
4) Les différentes principales clés du Registre	4
5) Recherche de la clé du papier peint dans le Registre	4
6) Clés de registre complémentaires au papier peint.....	5
B. Fermeture d'une session et visualisation dans le Registre par l'Administrateur	6
1) Fermeture de la session du User1 et ouverture de la session Administrateur	6
2) Recherche rapide dans le Registre.....	6
C. Ouverture d'une session et visualisation dans le Registre en tant qu'Administrateur	7
1) Laisser la session User1 ouverte et basculer sur le profil Administrateur.....	7
2) Obtenir les SID des différents profils existants	7
D. Modification du papier peint directement dans le Registre	9
1) Affichage des informations principales Wallpaper	9
2) Nouvelle image et nouveau chemin d'accès.....	9
3) Modification de l'entrée de valeur de la clé WallPaper.....	10
4) Contrôle de la modification du fond d'écran dans la session User1 et corrections des erreurs	10
E. Exportation de la clé de Registre du papier peint	11
1) Sauvegarde du Registre actuel avant modifications.....	11
2) Exportation uniquement de la clé Desktop	13
3) Ouverture de la clé sous format .text dans le Bloc-Notes	13
4) Modification de la clé dans Bloc-Notes.....	14
5) Importation de la clé modifiée.....	15
6) Aperçue des modifications.....	16
F. Afficher les autorisations dans le Registre avec l'outil AccessEnum.exe	17
1) Installation de l'outil de Sysinternals AccessEnum.exe	17
2) Sélection et scan des clés du Registre.....	17
3) Tableau récapitulatif des autorisations dans le Registre	19
G. Observer enregistrement des modifications apportées dans le bloc-notes avec l'outil Process Monitor de Sysinternals.....	19

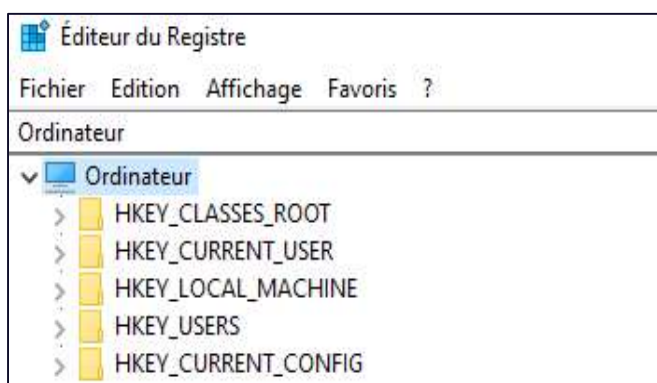
1) Installation de l'outil de Sysinternals Process Monitor.exe	19
2) Ouverture du programme Bloc-notes.....	20
3) Filtre et analyse des activités sur Process Monitor.....	20
H. Modification de la clé de Registre du Shell	21
1) Modification du type de fichier exécutable	21
2) Modification de l'apparence du Shell	22
3) Redémarrage et observations.....	23
4) Restauration.....	23
III. CONCLUSION	26
IV. RESSOURCES.....	27

I. INTRODUCTION

DEFINITION REGISTRE WINDOWS

Le Registre est une base de données hiérarchique centralisée qui sert à stocker des données auxquelles Windows fait référence en permanence durant son fonctionnement.

Il contient les paramètres de configuration du système d'exploitation, l'ensemble des programmes installés, les personnalisations de configuration et d'affichages enregistrées par chaque utilisateur, mais aussi les périphériques matériels reliés.



Le Registre de Windows est organisé en plusieurs sections que l'on appelle « ruches » dont chacune de celle-ci a hérité un rôle bien spécifique.

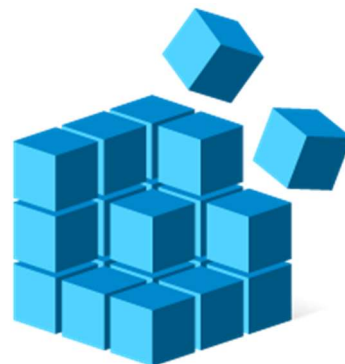
Chaque ruche du Registre est organisée sous une arborescence de clés et de sous-clés qui forment des conteneurs de sauvegarde de données.

Au sein de chaque clé est associée une valeur qui déterminent le comportement ou les paramètres de configuration du système ou du programme associé.

Cet outil présente de nombreux avantages pour l'organisation d'un parc informatique en combinant également l'outil de Stratégie de groupe :

- Stockage centralisé : facilité de gestion et de recherches
- Amélioration des performances : En réduisant les temps de chargement et de recherche des paramètres de configuration
- Gestion des droits d'accès : Contrôler et sécuriser les autorisations par typologie de groupes d'utilisateurs
- Sauvegarde : Importation et exportation de base de registre pouvant être réutilisé par la suite

Cet organisateur est un élément important du système d'exploitation qui doit être modifié avec précaution. Des modifications incorrectes du Registre peuvent entraîner des problèmes irréversibles qui peuvent causer une réinstallation de Windows et une perte générale des données.



II. EXERCICES DETAILLES

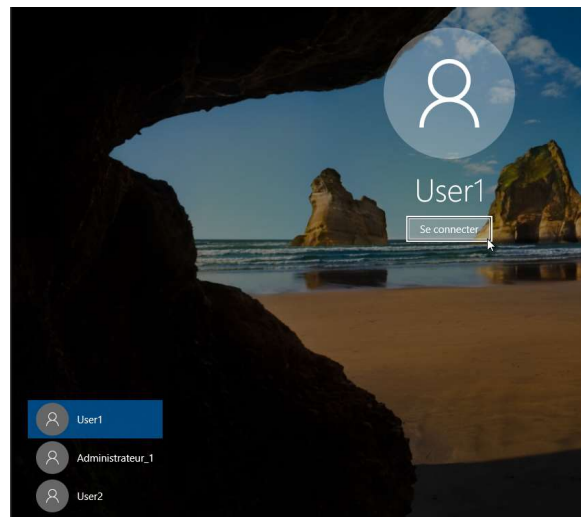
A. REGISTRE ET VALEUR DANS LA CLE DE REGISTRE DU PAPIER PEINT

Sujet : Modifier le papier peint du bureau de l'utilisateur user1 créé précédemment à l'aide des propriétés adéquates.

Dans quelle(s) clé(s) du Registre est enregistrée la valeur du papier peint ?

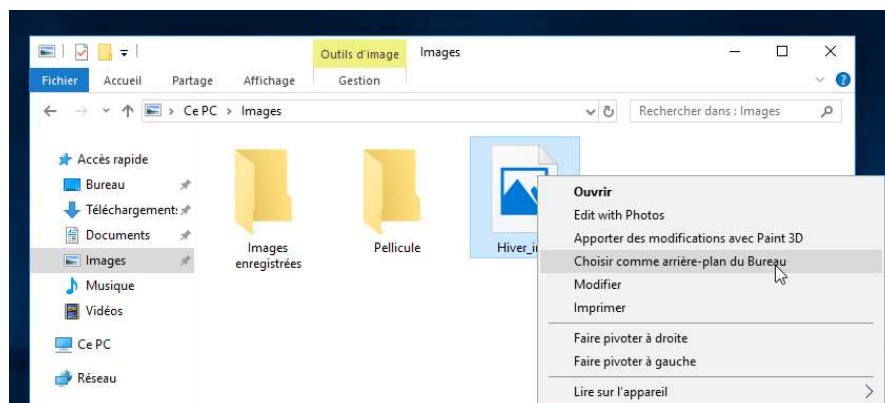
1) Connexion sur le profil User1

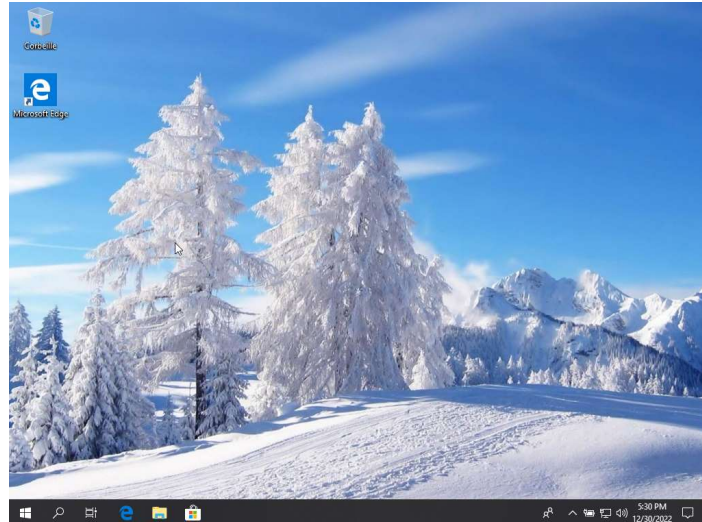
Dès la mise en tension de la Virtual Machine, se connecter en tant que User1 sur l'environnement Windows.



2) Recherche et sélection d'une image comme arrière-plan du Bureau

Rechercher une image sur Internet et la télécharger pour qu'elle figure dans le dossier « Images ». Ensuite, faire un clic-droit sur l'image choisie pour faire apparaître un menu déroulant et cliquer sur « Choisir comme arrière-plan du Bureau ».





Le papier peint de l'utilisateur 1 a été modifié. Pour observer dans quelle clé de registre la valeur du papier peint a été enregistré, nous allons utiliser le fichier éditeur de registre propre à Windows nommé Regedit.

3) Présentation de l'éditeur de registre Regedit.exe

Regedit est un utilitaire de l'environnement Windows permettant d'ajouter, modifier ou supprimer des clés et des valeurs dans la base de registre.



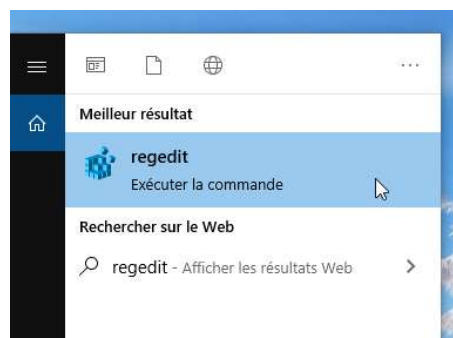
Regedit

Cet éditeur n'est pas le seul à pouvoir accéder au registre notamment :

- Le système via le GUI ou le PowerShell
- Un programme quelconque via une API (Excel par exemple)
- D'autres éditeurs de registre tiers (tels que Regedt32 ou reg.exe en ligne de commande)
- Par une Stratégie de Groupe (locale ou domaine)

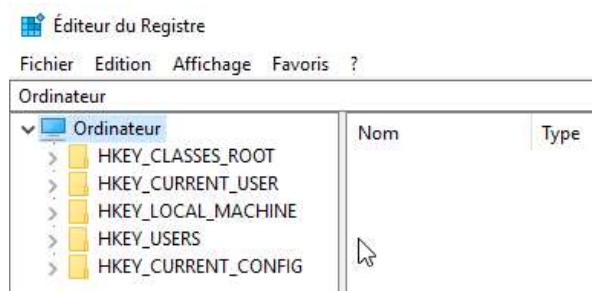
De plus, dans le but d'établir une sauvegarde ou de paramétrer un nouvel environnement Windows, il est possible d'importer ou exporter sous format texte l'ensemble du registre paramétré.

Afin d'obtenir l'éditeur de registre, taper « regedit » dans la barre de recherche du menu démarrage.



4) Les différentes principales ruches du Registre

Une fois activé, l'éditeur de registre de Windows affiche ses principales ruches :



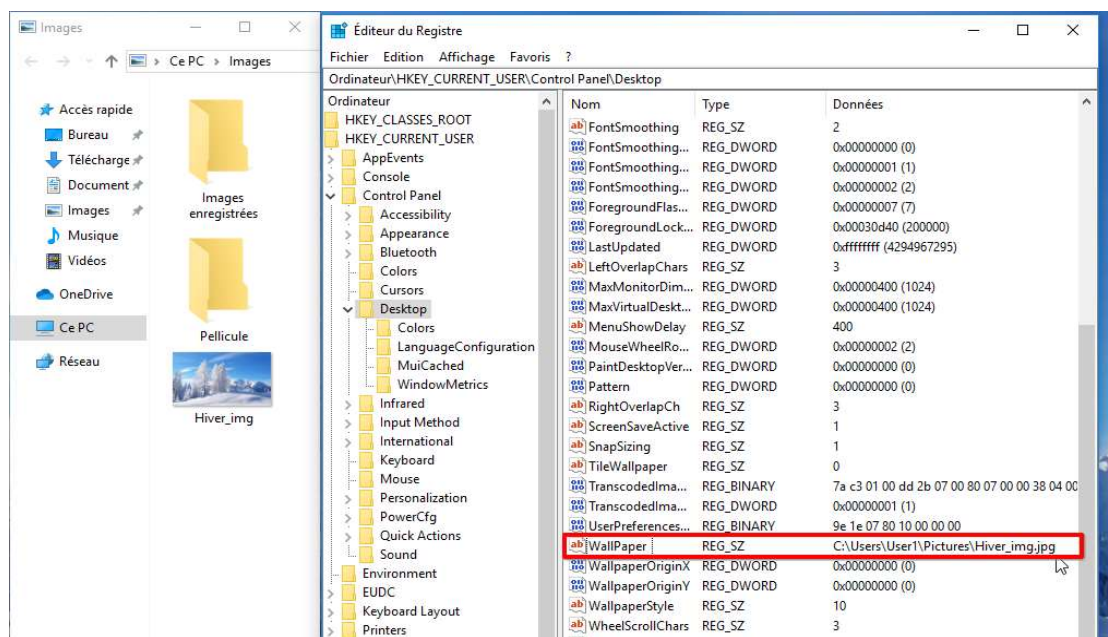
- **HKEY_CLASSES_ROOT** : Cette ruche correspond à une vue combinée entre la clé LOCAL_MACHINE\Software\Classes (registre de l'ordinateur locale) et à la clé HKEY_CURRENT_USER\Software\Classes (registre de l'utilisateur en cours). Ainsi, elle permet d'avoir accès à toutes les informations sur les types de fichiers, les actions associés à des programmes sur leur exécution d'ouverture ou leur cas d'utilisation quelques soient leurs emplacements de stockage de manière local ou sur le profil utilisateur courant.
- **HKEY_CURRENT_USER** : Cette ruche contient des informations sur les paramètres de configuration de l'utilisateur en cours via la sous-clé « Control Panel » et les programmes installés via la sous-clé « Software ». Cette ruche est principalement utilisée afin d'effectuer une bascule rapide des utilisateurs.
- **HKEY_LOCAL_MACHINE** : Cette ruche contient des informations générales exploitées par le système comme les paramètres du BIOS, les paramètres de démarrage et les paramètres de sécurité.
- **HKEY_USERS** : Cette ruche contient des informations sur tous les utilisateurs du système, y compris les paramètres de configurations et les programmes installés par chaque utilisateur.
- **HKEY_CURRENT_CONFIG** : Cette ruche contient des informations sur la configuration matérielle et logicielle actuelle de l'ordinateur. Elle se base sur l'utilisation des paramètres de configuration de l'ordinateur en cours d'utilisation tels que les paramètres de résolution d'écran ou de paramètres de performances.

5) Recherche de la clé du papier peint dans le Registre

En parcourant le registre d'après les informations cités sur les principales clés ci-dessus, le chemin d'accès se nomme la clé de registre suivante :

→ **Ordinateur\HKEY_CURRENT_USER\Control Panel\Desktop**

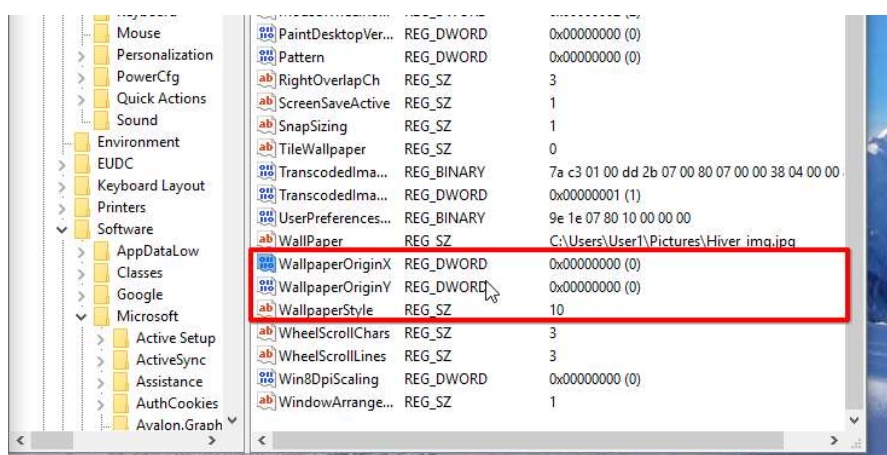
Cette clé contient des informations sur les paramètres de configuration du bureau de l'utilisateur en cours tels que la taille et la couleur ou l'image du fond d'écran, le placement et l'image des icônes, les paramètres de verrouillage de l'écran ou encore les effets visuels, etc.



Dans l'éditeur Regedit, on aperçoit les indications suivantes :

- **NOM** : c'est-à-dire le nom de valeur : WallPaper qui contient le chemin d'accès au fond d'écran et le nom du fichier jpg.
- **TYPE** : qui correspond au type de donnée stockée : REG_SZ veut dire stockage sous la forme de chaînes de caractères lisible par le programme de traitement de texte par défaut
- **DONNEE** : le chemin d'accès au programme convertir en chaîne de caractères.

6) Clés de registre complémentaires au papier peint



De plus, nous pouvons constater d'autres paramètres plus détaillés sur l'application du papier peint choisi sur l'écran :

- **WallpaperOriginX** : Position horizontale du fond d'écran indiquant la distance en pixels entre le bord gauche de l'écran et le bord gauche du fond d'écran qui peut être exprimé en positif ou en négatif (partira à droite). Le nombre entier est exprimé en hexadécimal.
- **WallpaperOriginY** : Même principe mais en position verticale.
- **WallpaperStyle** : Style d'affichage tels que centré, répété, étiré, etc. Ici, la valeur 10 est attribué à l'image ce qui signifie que le fond d'écran est redimensionné pour s'adapter à l'écran en maintenant les

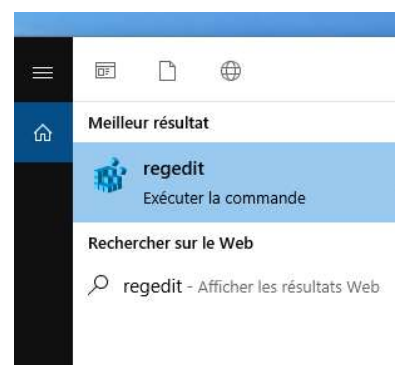
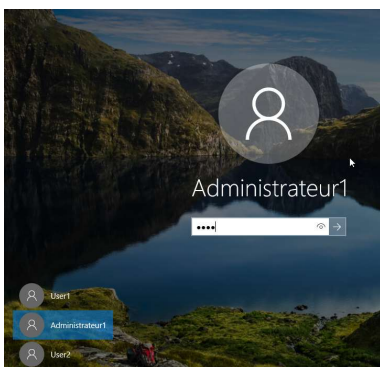
proportions de l'image d'origine. Voici un exemple des autres valeurs qui pourraient être utilisées par le système :

- 0 : Fond d'écran étiré. Si le fond d'écran est de proportions différentes de l'écran, il peut être distordu pour s'adapter à l'écran.
- 2 : Fond d'écran centré. Si proportions différentes, bandes noires apparaissent.
- 6 : Fond d'écran répété. Si proportions différentes, coupés ou étirés.

B. Fermeture d'une session et visualisation dans le Registre par l'Administrateur

Sujet : Fermer la session user1 et ouvrir une session en tant qu'Administrateur. Retrouvez-vous cette valeur dans le Registre ?

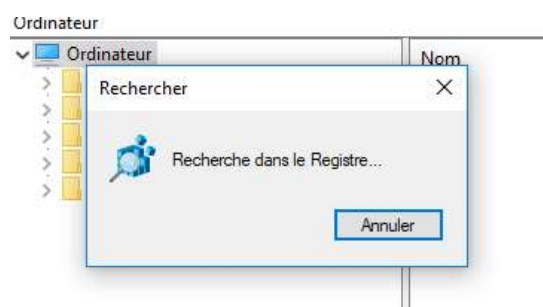
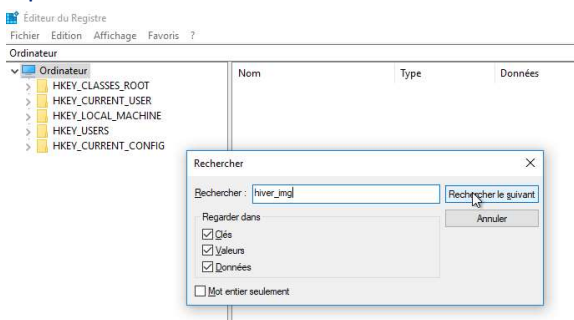
1) Fermeture de la session du User1 et ouverture de la session Administrateur



Après la fermeture de la session User1, ouvrir la session Administrateur et taper dans la barre de recherche du menu de démarrage Regedit.

2) Recherche rapide dans le Registre

Afin de rechercher le fichier jpeg correspondant au papier choisi, il est possible d'effectuer une recherche rapide à partir de la combinaison de touches suivantes CTRL + F. Un masque de recherche apparaît :

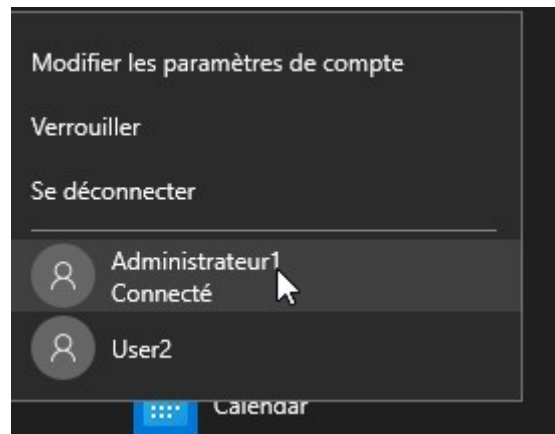


En passant au travers des différents répertoires, la recherche n'a mené à aucun résultat.

C. Ouverture d'une session et visualisation dans le Registre en tant qu'Administrateur

Sujet : Ouvrir la session user1 et utiliser la bascule rapide des utilisateurs pour ouvrir une seconde session en tant qu'Administrateur (user1 reste actif). Retrouvez-vous cette valeur dans le Registre ?

1) Laisser la session User1 ouverte et basculer sur le profil Administrateur



2) Obtenir les SID des différents profils existants

Pour rechercher dans la ruche du Registre HKEY_USERS le user1, différents SID apparaissent. Néanmoins, afin d'affiner les recherches, il faut affecter ces SID à chaque profil existant sur cet ordinateur virtuel.

Pour se faire, nous allons ouvrir l'invitation des commandes en tant qu'Administrateur et taper la commande suivante :

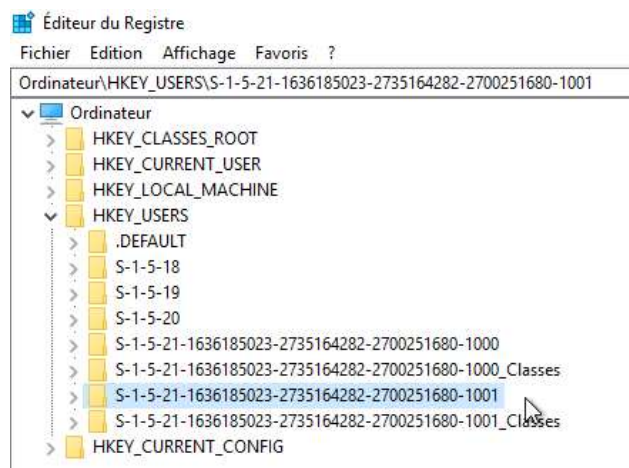
➔ *WMIC useraccount get name, sid*

```
Microsoft Windows [version 10.0.17134.112]
(c) 2018 Microsoft Corporation. Tous droits réservés.

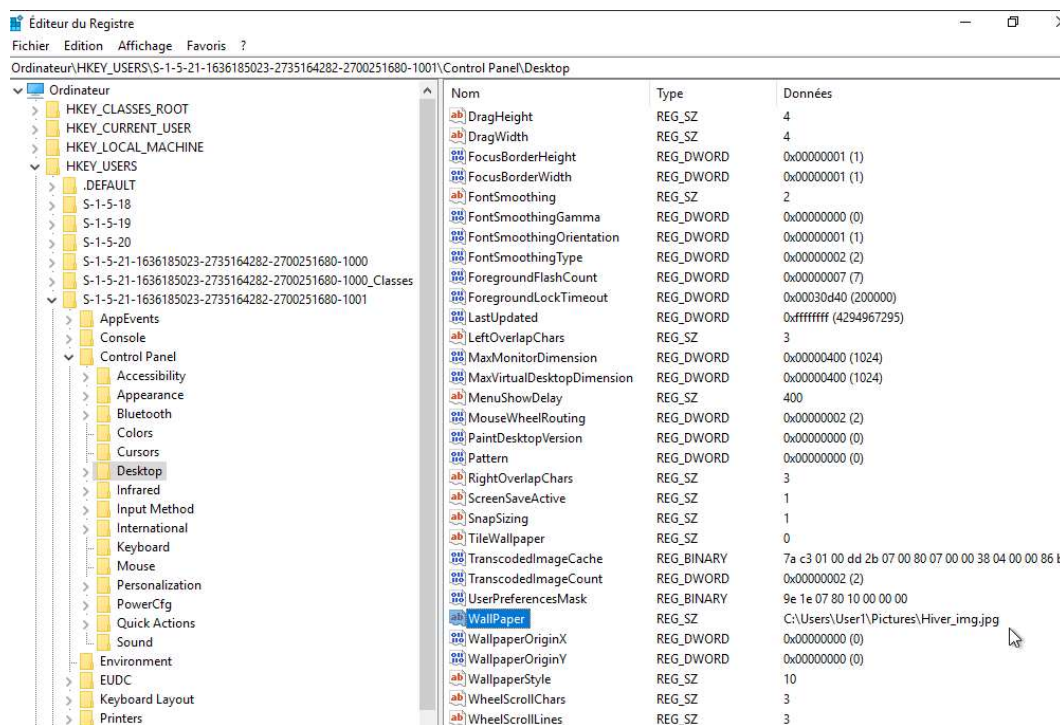
C:\Windows\system32>WMIC useraccount where name="username" get sid
Aucune instance disponible.

C:\Windows\system32>WMIC useraccount get name,sid
Name SID
Administrateur S-1-5-21-1636185023-2735164282-2700251680-500
Administrateur1 S-1-5-21-1636185023-2735164282-2700251680-1000
DefaultAccount S-1-5-21-1636185023-2735164282-2700251680-503
Invité S-1-5-21-1636185023-2735164282-2700251680-501
User1 S-1-5-21-1636185023-2735164282-2700251680-1001
User2 S-1-5-21-1636185023-2735164282-2700251680-1002
WDAGUtilityAccount S-1-5-21-1636185023-2735164282-2700251680-504
```

D'après cette recherche dans l'invitation des commandes, nous pouvons constater que le SID ressemble à l'ensemble des SID des profils mais fini par 1001.



Dans la ruche HKEY_USERS, le SID de l'utilisateur apparaît alors que celui-ci n'était pas présent lorsque la session de l'utilisateur était fermée comme vu précédemment.



En passant au travers des différentes sous-clés, on peut retrouver la valeur menant au papier peint choisi par l'utilisateur. Ainsi, la clé menant à cette information est la suivante :

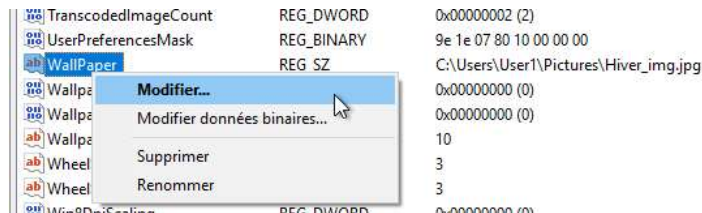
➔ HKEY_USERS\S-1-5-21-1636185023-2735164282-2700251680-1001\Control Panel\Desktop

D. Modification du papier peint directement dans le Registre

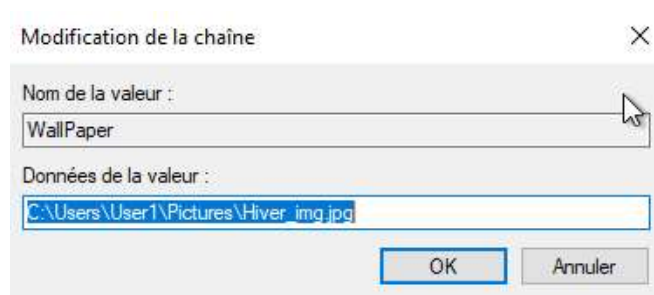
Sujet : Modifier la valeur du papier peint directement dans le Registre. Commentaires ?

1) Affichage des informations principales Wallpaper

Afin de modifier le fichier ou/et le chemin d'accès, cela conviendrait à modifier de la valeur Wallpaper. Pour se faire, faire un clic-droit sur Wallpaper faisant apparaître le menu déroulant et cliquer sur « Modifier ».

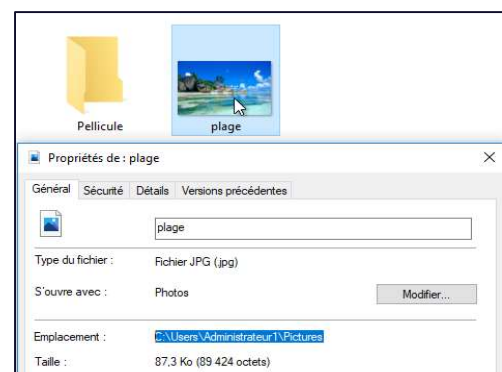
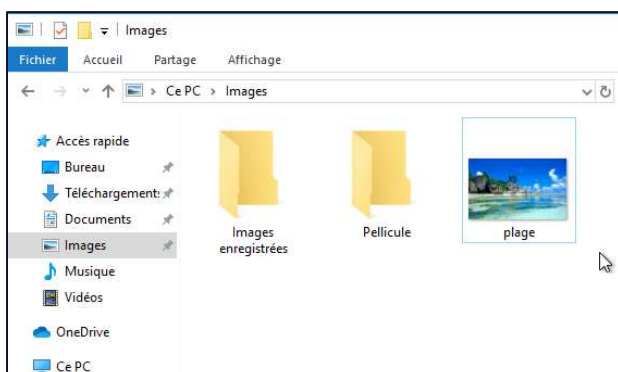


La donnée de la valeur s'affiche :



2) Nouvelle image et nouveau chemin d'accès

Après avoir télécharger au préalable une autre image sur Internet, il faudrait répertorier l'image choisie sur l'un des dossiers courants de l'Administrateur.



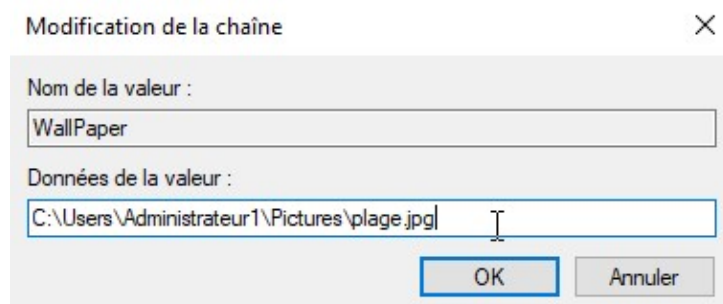
Ainsi, le chemin d'accès et le nom du fichier de la nouvelle image est le suivant :

➔ C:\Users\Administrateur1\Pictures\plage.jpg

Ce nouveau chemin sera la nouvelle entrée de valeur de Wallpaper.

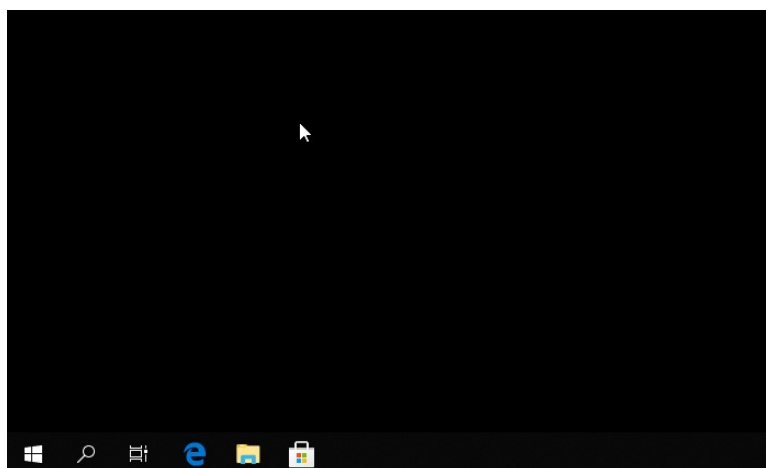
3) Modification de l'entrée de valeur de la clé Wallpaper

Après avoir saisi le chemin d'accès et le nom du fichier récupéré précédemment dans le champ « Données de la valeur », cliquer sur OK.



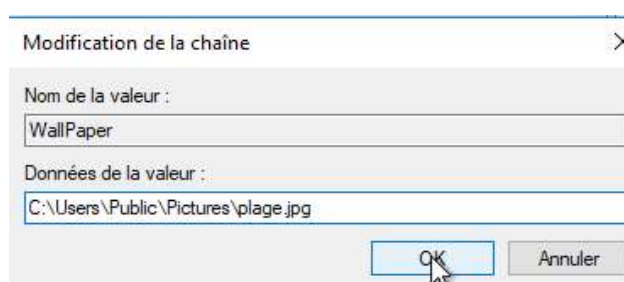
4) Contrôle de la modification du fond d'écran dans la session User1 et corrections des erreurs

Après avoir redémarrer la session de l'User1, on remarque le fond d'écran « hiver » a disparu laissant un écran noir s'afficher à la place.

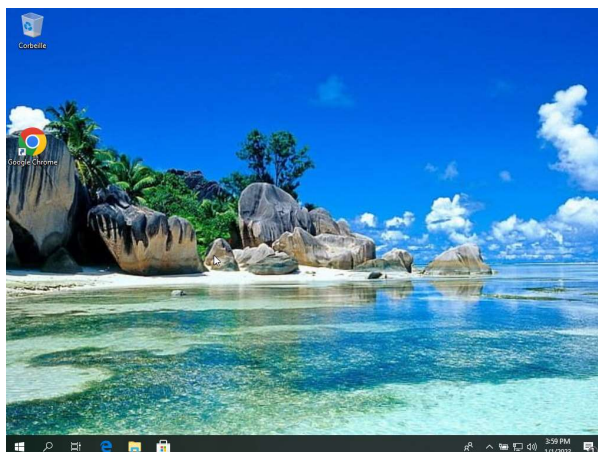


Afin de corriger ce problème, j'ai souhaité modifier le chemin d'accès afin qu'il soit non pas depuis un dossier de l'Administrateur mais directement déposé sur le dossier public accessible pour tout utilisateur.

Ainsi, la donnée de la valeur Wallpaper a donc été corrigée comme suit :



Après redémarrage de la session de l'User1, le fond d'écran se modifie correctement et affiche l'image choisie.



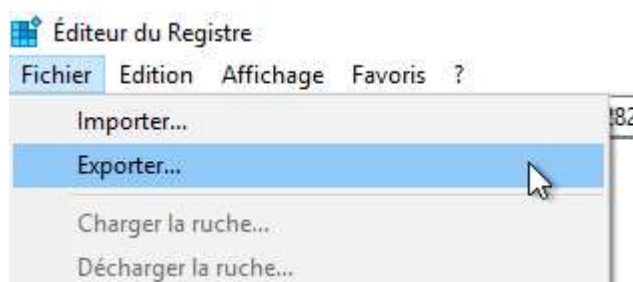
E. Exportation de la clé de Registre du papier peint

Sujet : Exporter la clé « papier peint », la modifier et l'importer dans le Registre. Commentaires ?

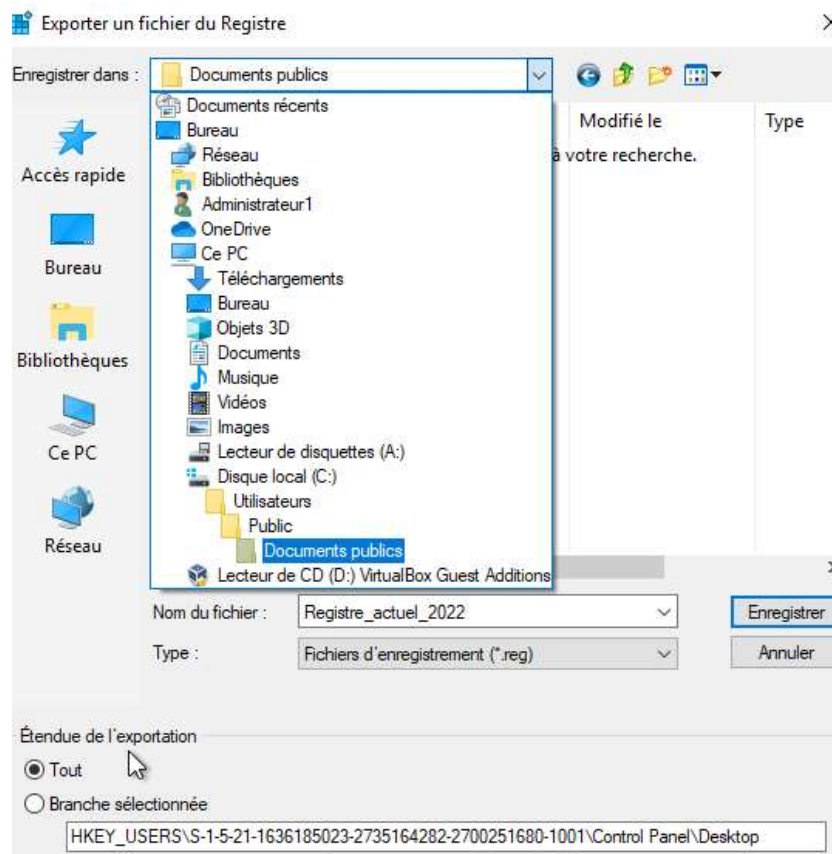
1) Sauvegarde du Registre actuel avant modifications

De manière général, il est recommandé d'effectuer une sauvegarde du registre avant de procéder à des modifications. En effet, la modification de certaines clés importantes peuvent affecter la performance et le fonctionnement général de l'ordinateur.

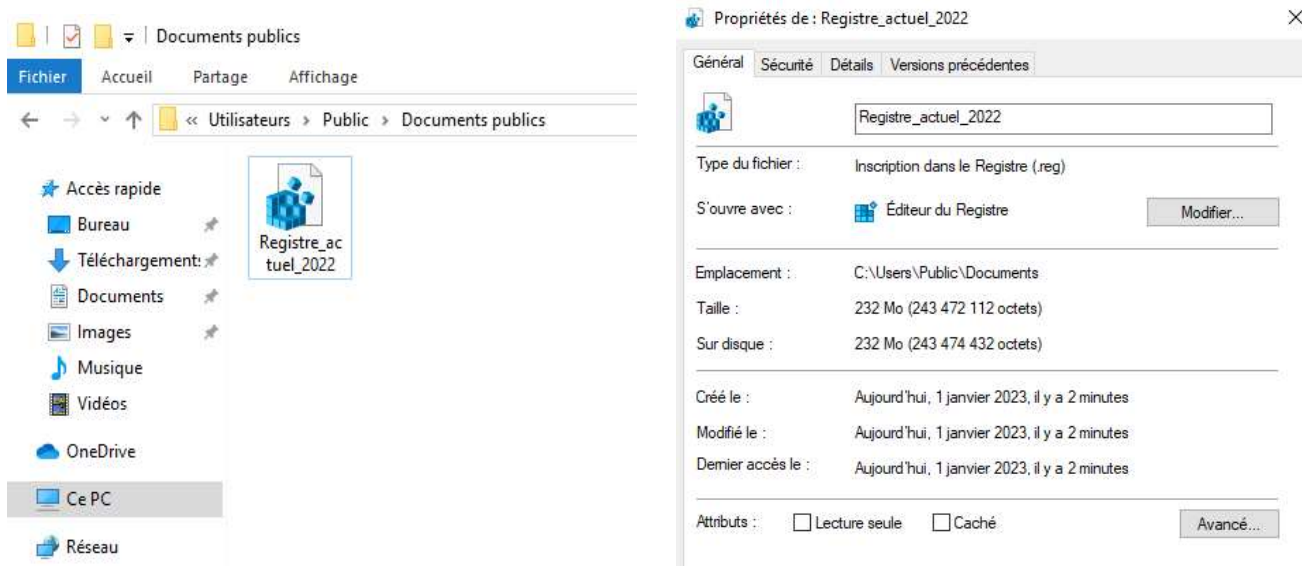
Pour commencer, cliquer sur l'onglet « Fichier » et sélectionner dans le menu déroulant « Exporter ».



Pour cette exportation, l'éditeur de Registre nous propose une « Etendue de l'exportation » sur la branche de la clé actuellement positionnée. Or, nous voulons tout d'abord effectuer une sauvegarde générale de toutes les clés actuelles.



Pour cela, corriger la coche sur « Tout » et nommer le nom du fichier à créer et enregistrer. J'ai souhaité enregistrer ce fichier une nouvelle fois dans la partie Public de l'ordinateur pour des questions pratiques.



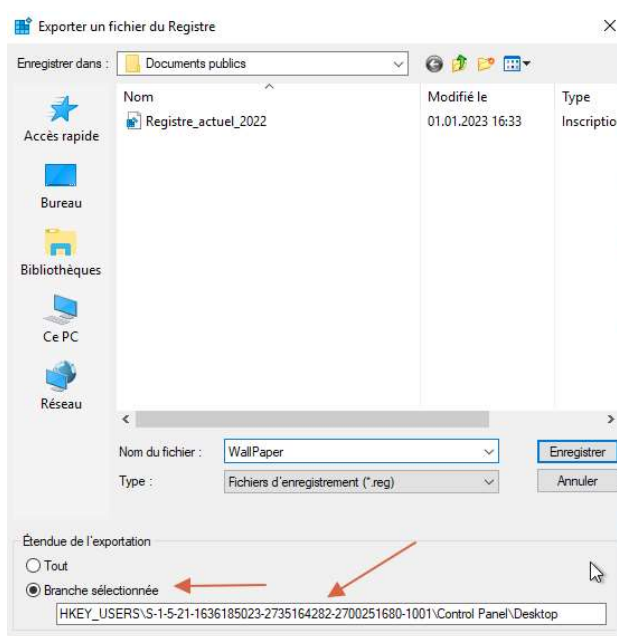
Le fichier de sauvegarde est maintenant créé sous la forme « Inscription dans le registre » avec l'extension « .reg ».

Maintenant, nous pouvons procéder à des modifications.

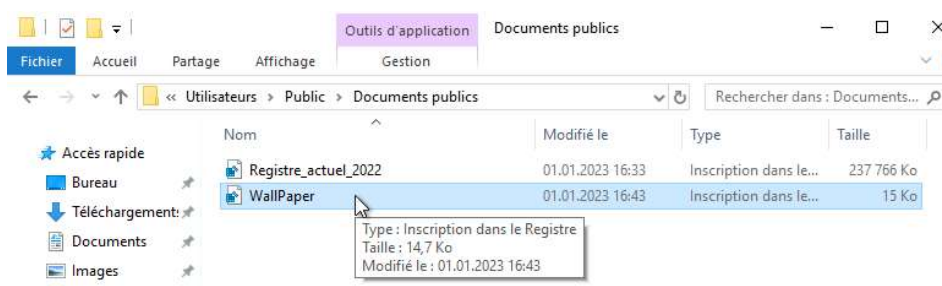
2) Exportation uniquement de la clé Desktop

Nous avons pu remarquer que les différentes informations concernant le fond d'écran se situe dans la sous-clé Desktop de l'utilisateur.

Ainsi, procéder une nouvelle fois à l'exportation. Cependant, nous allons ici exporter uniquement une Branche sélectionnée.



Un deuxième fichier de Registre est actuellement disponible au même chemin.



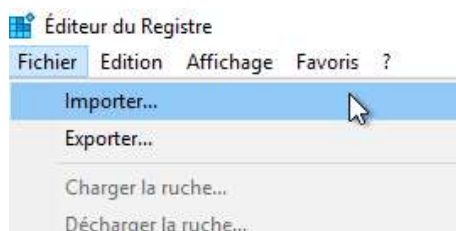
3) Ouverture de la clé sous format .text dans le Bloc-Notes

Afin de pouvoir modifier séparément la clé sans qu'elle soit directement importée dans le Registre, il est possible d'ouvrir le fichier .reg et de modifier manuellement des informations dans le programme Bloc-Notes de l'ordinateur.

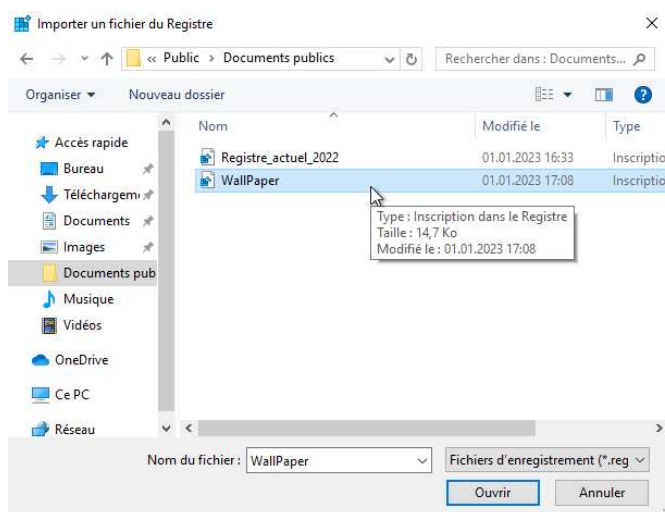
Comme expliqué précédemment, les entrées de valeurs seront la plupart exprimé sous forme hexadécimal et d'autres en caractères.

5) Importation de la clé modifiée

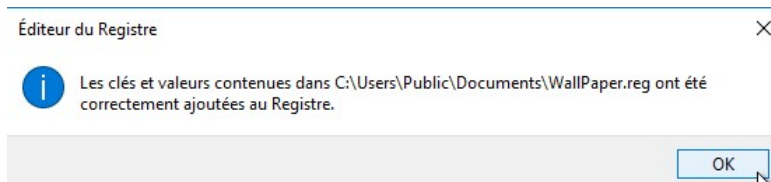
Pour importer la clé modifiée dans le programme Bloc-Notes, cliquer sur l'onglet « Fichier » et sélectionner dans le menu déroulant « Importer ».



Sélectionner ensuite le fichier « Wallpaper.reg » et cliquer sur « Ouvrir ».

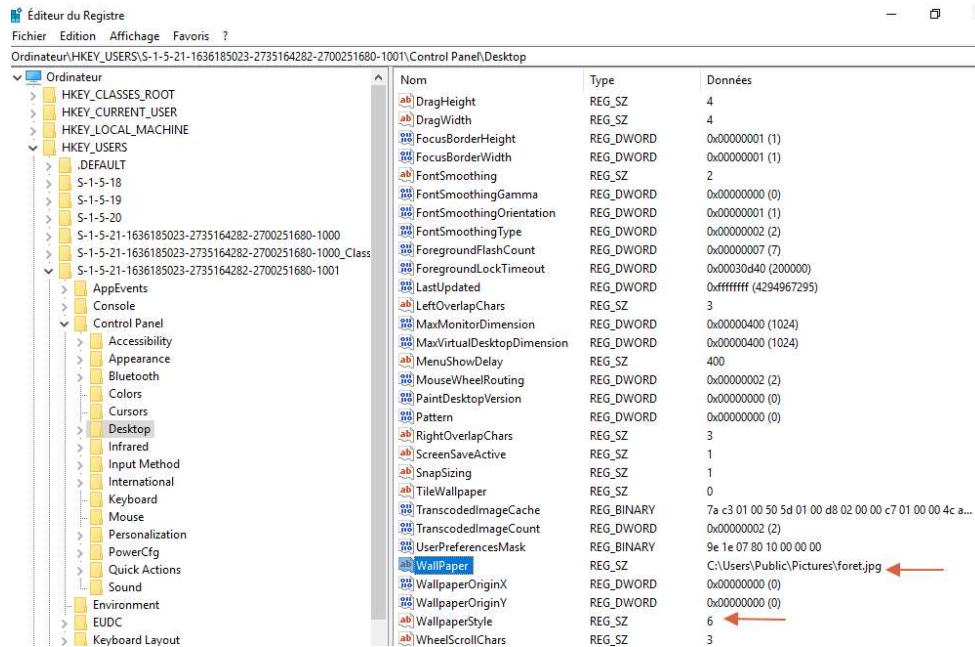


Un masque apparaît contenant ce message. L'importation a réussi sans problème particulier.

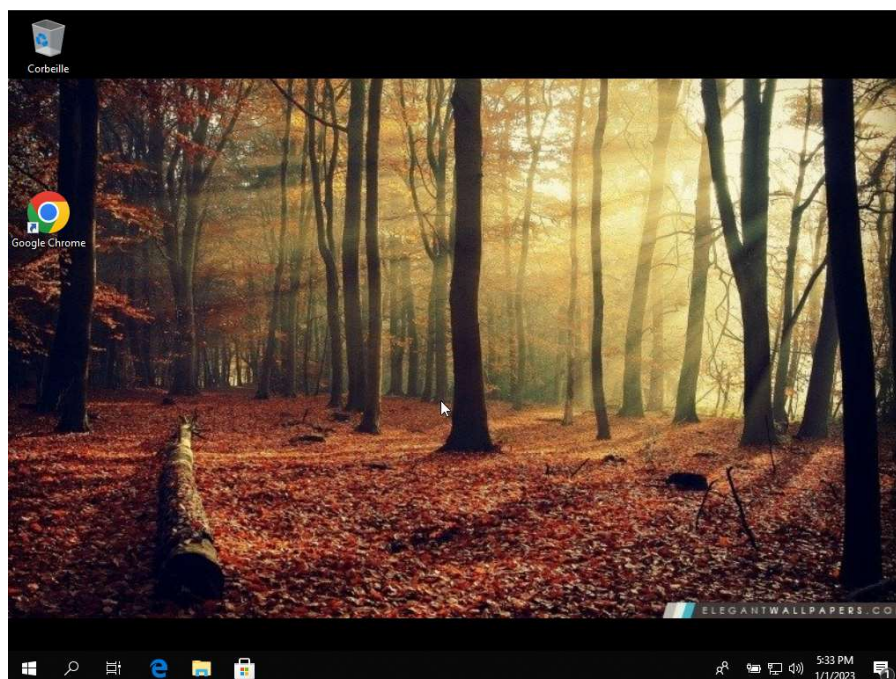


6) Aperçue des modifications

Suite à l'importation réussie de la clé modifiée, on retrouve les 2 modifications apportées directement dans le Registre.



En redémarrant la session de l'user1, on constate également que ces modifications ont été correctement appliquées.



F. Afficher les autorisations dans le Registre avec l'outil AccessEnum.exe

Sujet : A l'aide de l'outil AccessEnum.exe, afficher les autorisations sur les différentes clés du Registre.

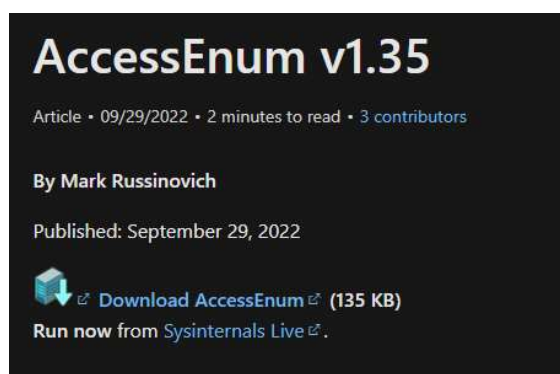
Chaque utilisateurs ou groupes d'utilisateurs ont des autorisation spécifiques associées aux clés de Registre. En effet, ces autorisations ont été créées afin d'assurer de la confidentialité des autres utilisateurs ou la sécurité du fonctionnement de l'ordinateur.

1) Installation de l'outil de Sysinternals AccessEnum.exe

AccessEnum est un outil de sécurité de Sysinternals de Microsoft utile pour les administrateurs de système et de sécurité qui souhaitent surveiller les autorisations d'accès sur leur réseau et s'assurer que les autorisations sont configurées de manière appropriée.

N'étant pas un fichier exécutable natif sur Windows, cet outil peut être téléchargé directement à cette adresse :

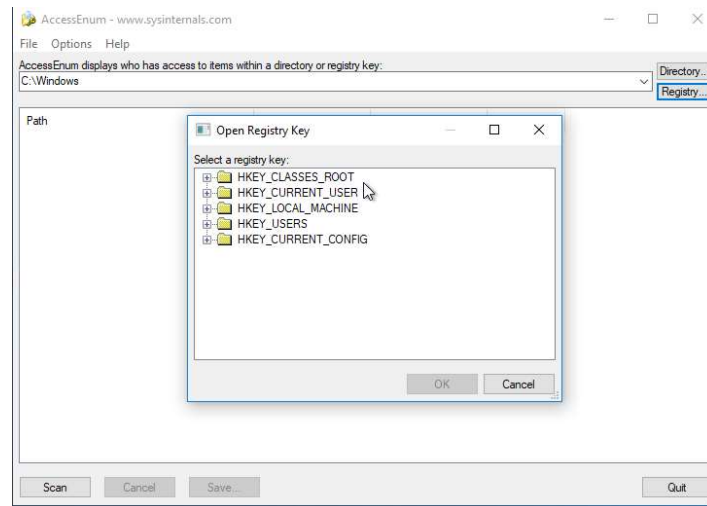
➔ <https://learn.microsoft.com/en-us/sysinternals/downloads/accessenum>



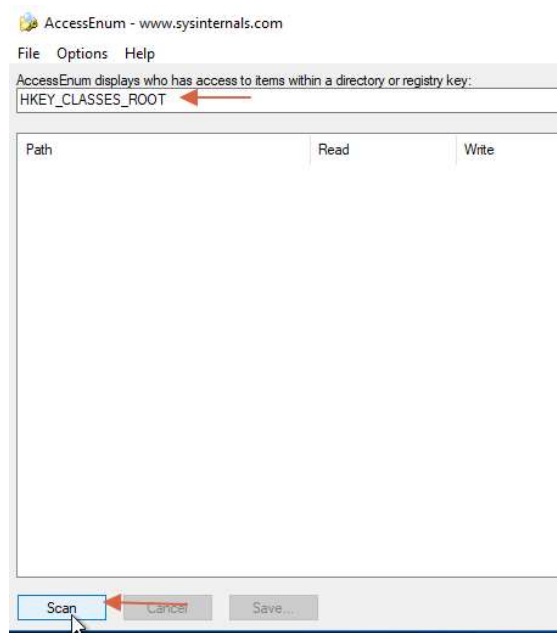
2) Sélection et scan des clés du Registre

Pour commencer, cliquer sur le bouton « Registry » pour accéder aux ruches du Registre.

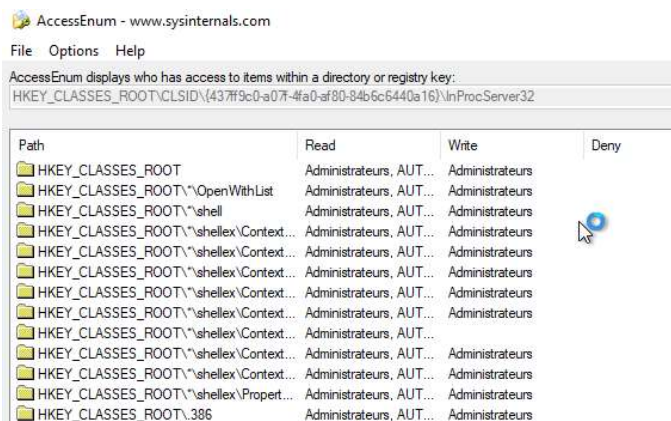




Les différentes ruches s'affichent. Pour connaître les autorisations pour chaque clé et sous-clé de celle-ci, sélectionner le dossier et cliquer sur OK.



La ruche HKEY_CLASSES_ROOT est sélectionnée. Cliquer sur Scan pour effectuer la recherche des autorisations.



Au fur et à mesure, les autorisations s'affichent par sous-clés. En majeure partie, en défilant, on remarque que cette ruche est principalement autorisée pour l'Administrateur du système.

3) Tableau récapitulatif des autorisations dans le Registre

De manière générale, des autorisations par groupes d'utilisateurs à travers les différentes clés et sous-clés du Registre sont prédéfinis par le système. Pour des questions de lisibilité, j'ai souhaité organiser ce tableau par ruches pour avoir un aspect plus globale des autorisations.

RUCHES DU REGISTRE	ADMINISTRATEURS		UTILISATEURS	
	READ	WRITE	READ	WRITE
HKEY_CLASSES_ROOT	✓	✓	✗	✗
HKEY_CURRENT_USER	✓	✓	✗	✗
HKEY_LOCAL_MACHINE	✓	✗	✓	✗
HKEY_USERS	✓	✓	✓	✗
HKEY_CURRENT_CONFIG	✓	✓	✓	✗

On peut constater que de manière générale les utilisateurs ne peuvent pas accéder aux clés de Registre et à l'inverse un Administrateur peut avoir l'ensemble des droits hormis certaines autorisations bloquées dans la ruche HKEY_LOCAL_MACHINE.

G. Observer enregistrement des modifications apportées dans le bloc-notes avec l'outil Process Monitor de Sysinternals

Sujet : Utiliser le programme Process Monitor (Sysinternals) pour déterminer la clé dans laquelle le bloc-notes (notepad.exe) enregistre ses paramètres par défaut d'édition (modifier la police via le menu Format/Police avant la fermeture de l'application).

1) Installation de l'outil de Sysinternals Process Monitor.exe

Process Monitor v3.92

Article • 10/26/2022 • 2 minutes to read • 9 contributors

By Mark Russinovich

Published: October 26, 2022

 [Download Process Monitor](#) (3.3 MB)

[Download Procmon for Linux \(GitHub\)](#)

Run now from Sysinternals Live

Process Monitor est un outil de Sysinternals de Windows permettant de voir en temps réel toutes les opérations de lecture et d'écriture de fichiers, de registre et de réseau effectuées par un processus ou par le système d'exploitation. Il affiche également des informations sur les processus en cours d'exécution, les événements de démarrage et d'arrêt de service, et les erreurs de système.

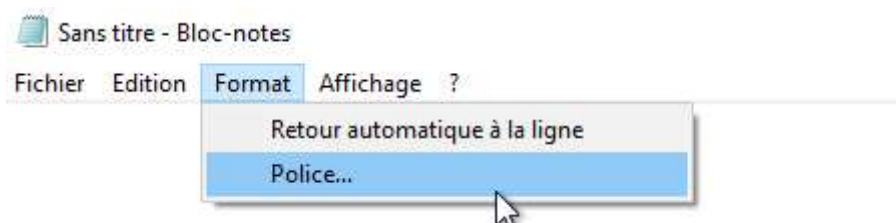
Il est possible de pouvoir le télécharger à cette adresse :

➔ <https://learn.microsoft.com/en-us/sysinternals/downloads/procmon>

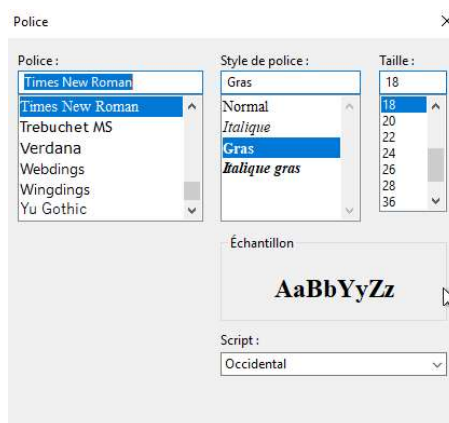
2) Ouverture du programme Bloc-notes

Avant d'ouvrir le Bloc-Notes, enclencher Process Monitor pour qu'il puisse déjà scanner l'ensemble des opérations qui vont suivre.

Ouvrir le Bloc-Notes et cliquer sur l'onglet « Format » et sélectionner dans le menu déroulant « Police ».

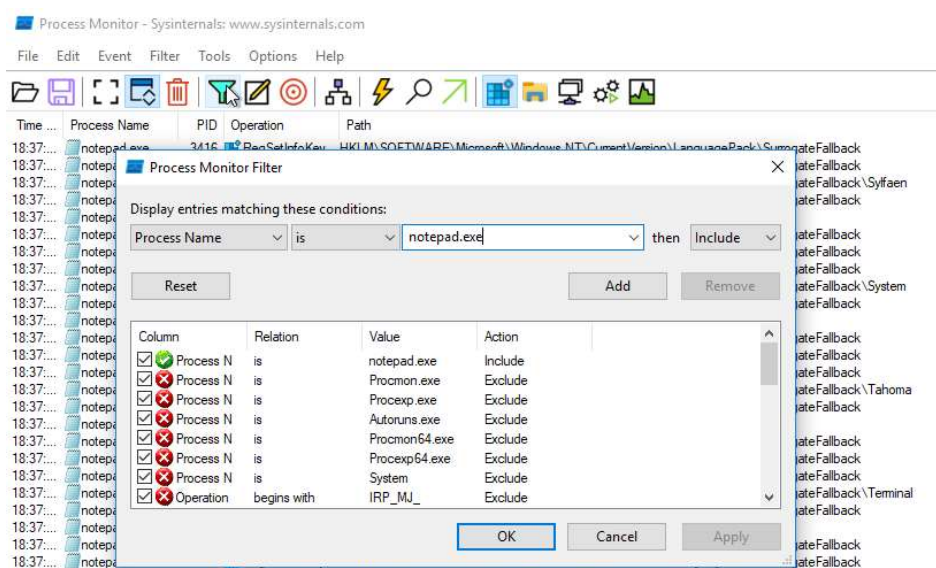


Modifier la police, le style de police et la taille.



Fermer l'application et observer ce qui s'est produit sur Process Monitor.

3) Filtre et analyse des activités sur Process Monitor



Après avoir scanner les activités, cliquer sur le bouton Capture pour figer les activités et ouvrir le Filtre pour effectuer une recherche plus précise en lien avec les opérations du programme Bloc-Notes appelé « notepad.exe ».

En majeure partie, on peut remarquer que l'ensemble des opérations viennent de la clé suivante :

➔ HKEY_CURRENT_USER\Software\Microsoft\Notepad
(HKCU)

19:34:...	notepad.exe	8692	RegQueryKey	HKLM\SOFTWARE\Microsoft\CTF\TIP
19:34:...	notepad.exe	8692	RegOpenKey	HKLM\SOFTWARE\Microsoft\CTF\TIP\{F89E9E58-BD2F-4008-9AC2-0F816C09F4
19:34:...	notepad.exe	8692	RegEnumKey	HKLM\SOFTWARE\Microsoft\CTF\TIP
19:34:...	notepad.exe	8692	RegCloseKey	HKLM\SOFTWARE\Microsoft\CTF\TIP
19:34:...	notepad.exe	8692	RegQueryKey	HKCU
19:34:...	notepad.exe	8692	RegCreateKey	HKCU\Software\Microsoft\Notepad
19:34:...	notepad.exe	8692	RegSetValue	HKCU\Software\Microsoft\Notepad\IfEscapement
19:34:...	notepad.exe	8692	RegSetValue	HKCU\Software\Microsoft\Notepad\IfOrientation
19:34:...	notepad.exe	8692	RegSetValue	HKCU\Software\Microsoft\Notepad\IfWeight
19:34:...	notepad.exe	8692	RegSetValue	HKCU\Software\Microsoft\Notepad\IfItalic
19:34:...	notepad.exe	8692	RegSetValue	HKCU\Software\Microsoft\Notepad\IfUnderline
19:34:...	notepad.exe	8692	RegSetValue	HKCU\Software\Microsoft\Notepad\IfStrikeOut
19:34:...	notepad.exe	8692	RegSetValue	HKCU\Software\Microsoft\Notepad\IfCharSet

H. Modification de la clé de Registre du Shell

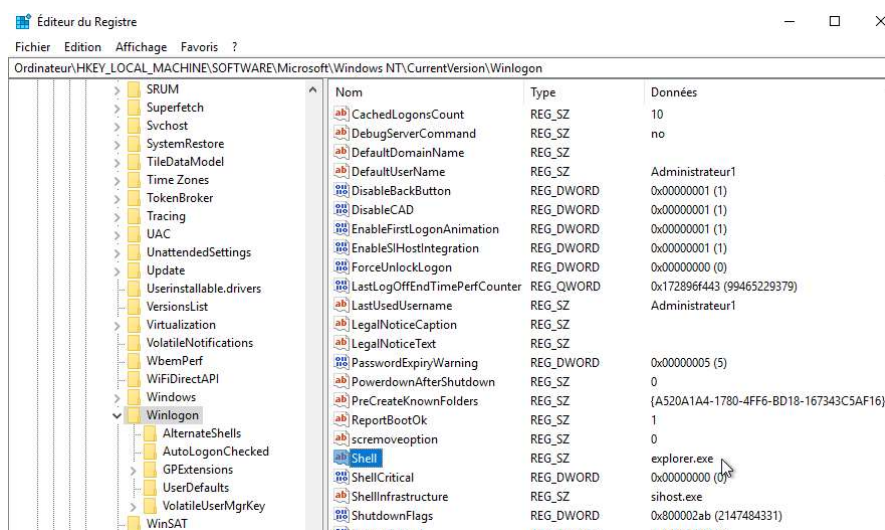
Sujet : Modifier le Registre de manière à ce que le Shell par défaut du login soit cmd.exe, caractères rouges sur fond bleu, plutôt que explorer.exe. Rétablir la situation !

Avant les modifications apportées, nous avons établi une sauvegarde du Registre. En cas de problèmes, elle pourra être utilisé afin de rétablir la situation.

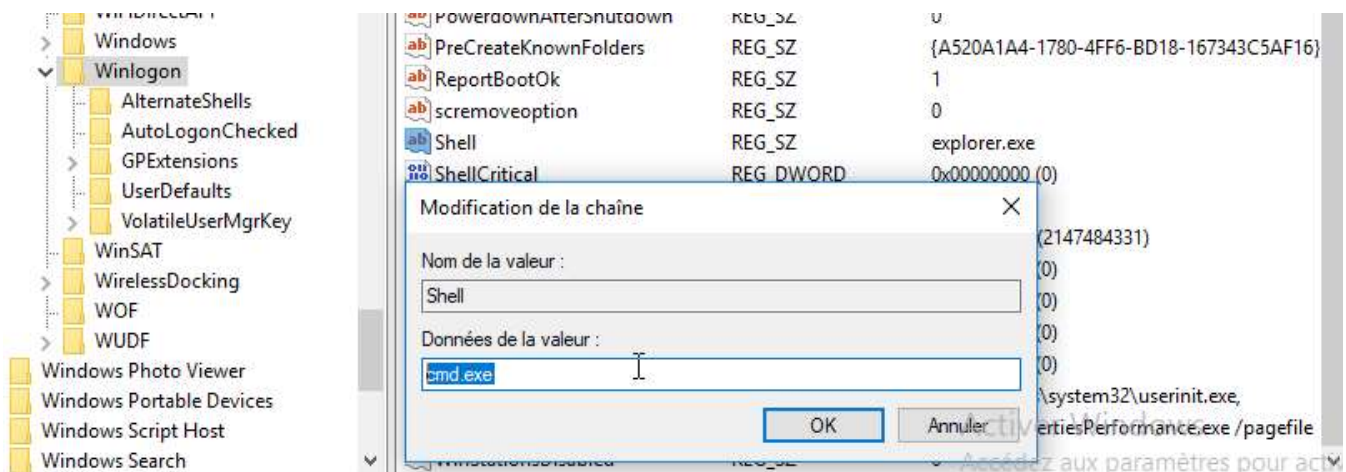
1) Modification du type de fichier exécutable

Pour accéder à la modification du lancement par défaut au login du fichier exécutable cmd.exe au lieu de explorer.exe, il faudra se rendre à la clé suivante :

➔ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon



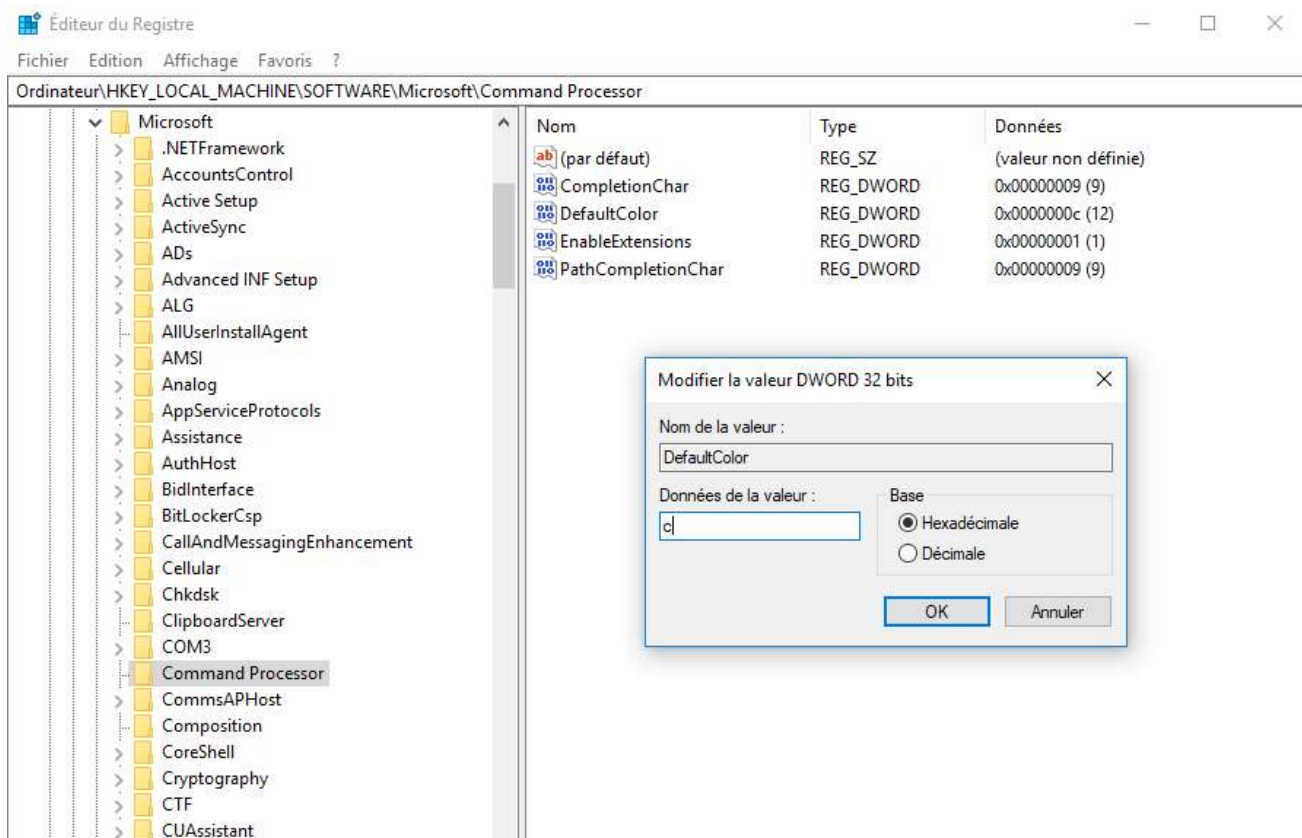
Ensuite, changer la donnée de la valeur « Shell » :



2) Modification de l'apparence du Shell

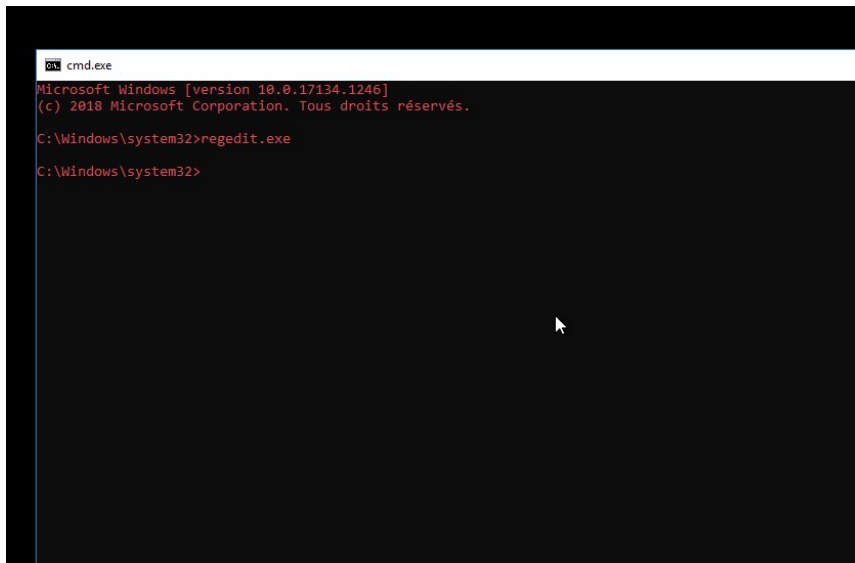
La clé utilisée pour modifier le fond de la couleur par défaut est la suivante :

➔ HKEY_LOCAL_MACHINES\Software\Microsoft\Command Processor



Dans la valeur DefaultColor, saisir la donnée C qui correspond à la couleur rouge en hexadécimal.

3) Redémarrage et observations



```
cmd.exe
Microsoft Windows [version 10.0.17134.1246]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>regedit.exe
C:\Windows\system32>
```

Au redémarrage, on peut observer que la session du profil Administrateur1 se lance automatiquement après le login et s'ouvre directement avec l'invitation des commandes.

On remarque la couleur rouge s'est bien appliquée.

4) Restauration

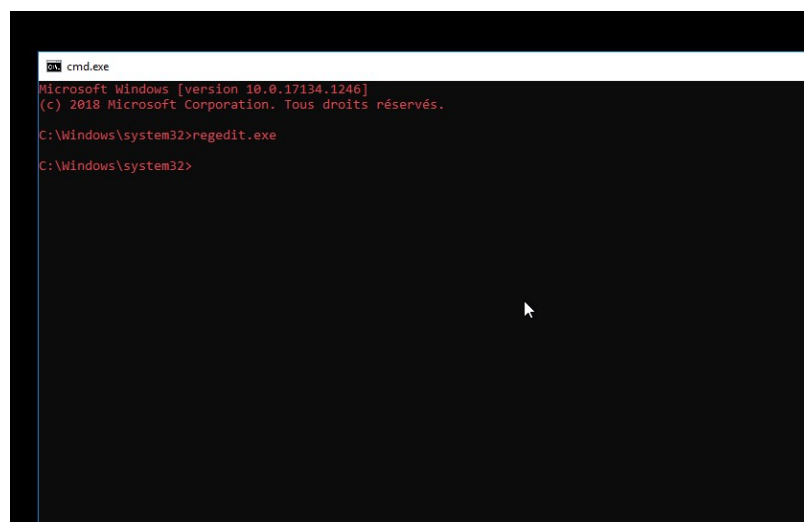
Pour restaurer les anciens paramètres pour revenir à une utilisation à la normale, il y a 2 manières de faire :

- Soit directement modifier manuellement dans Regedit les modifications effectuées
- Soit importer la dernière sauvegarde de Registre effectuée précédemment.

Pour ma part, je vais faire une démonstration de la 1^{ère} option.

Dans un premier temps, taper dans l'invitation des commandes :

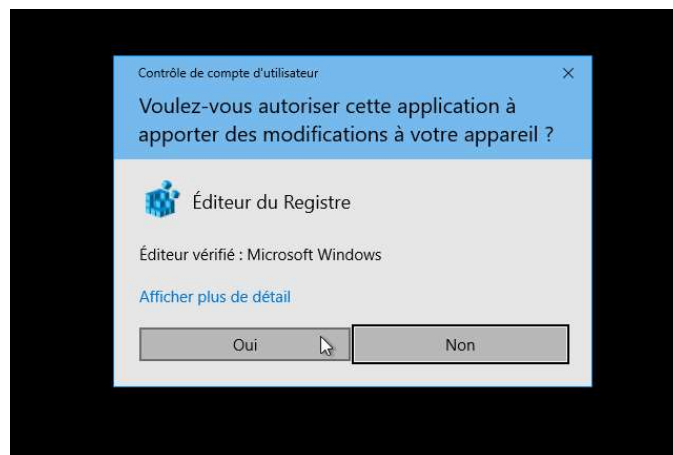
➔ Regedit.exe



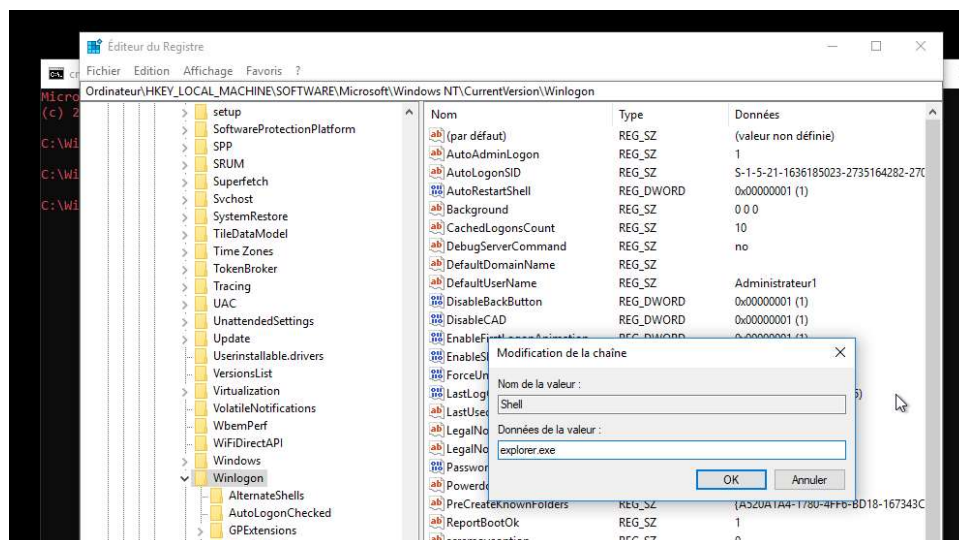
```
cmd.exe
Microsoft Windows [version 10.0.17134.1246]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>regedit.exe
C:\Windows\system32>
```

Une fois le fichier exécuté, la fenêtre d'autorisation s'enclenche et il est possible de revenir sur Regedit.



Ensuite, corriger directement la modification apportée à la valeur Winlogon en ressaisissant explorer.exe.

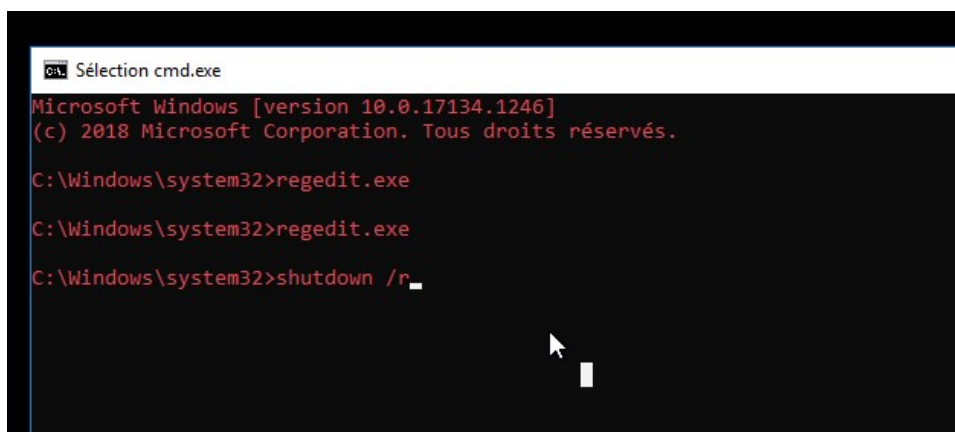


Cliquer sur OK.

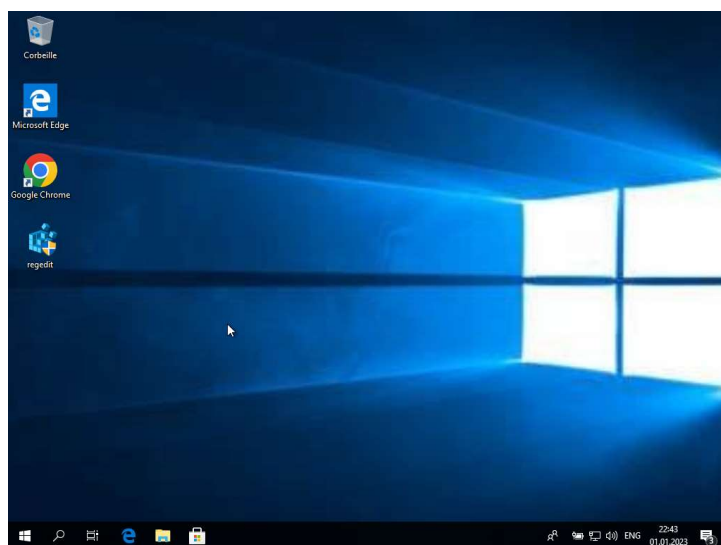
Faire de même pour remettre la couleur avec l'autre clé d'accès.

Quitter l'Éditeur de registre et revenir dans l'invitation des commandes et taper la commande suivante :

➔ Shutdown /r



L'ordinateur redémarrera normalement faisant apparaître le desktop du profil Administrateur1.



La situation a été rétablie.

III. CONCLUSION

Ce rapport a été pour moi une grande découverte sur le fonctionnement du Registre sur Windows.

Les différents exercices m'ont permis de comprendre et me familiariser avec les différentes ruches au fur et à mesure de les parcourir.

Malheureusement, je n'ai pas utilisé la Stratégie de Groupe pour effectuer ce travail et je pense qu'il aurait pu être un outil très intéressant à combiner avec Regedit pour définir des configurations prédéfinis et/ou bloqués pour un parc informatique pour de multiples utilisateurs.

IV. RESSOURCES

1. malekalmorte. Comment exporter/importer des clés du registre Windows [Internet]. malekal.com. 2020 [cité 1 janv 2023]. Disponible sur: <https://www.malekal.com/comment-exporter-importer-des-cles-du-registre-windows/>
2. malekalmorte. Process monitor : surveiller/capture l'activité système Windows ou d'une application [Internet]. malekal.com. 2022 [cité 1 janv 2023]. Disponible sur: <https://www.malekal.com/process-monitor-surveiller-activite-windows-application/>
3. markruss. AccessEnum - Sysinternals [Internet]. [cité 1 janv 2023]. Disponible sur: <https://learn.microsoft.com/en-us/sysinternals/downloads/accessenum>
4. Michael. Wallpaper bzw. Desktop Hintergrundbild per Registry setzen [Internet]. Windows FAQ. 2020 [cité 30 déc 2022]. Disponible sur: <https://www.windows-faq.de/2020/11/08/wallpaper-bzw-desktop-hintergrundbild-per-registry-setzen/>
5. Comment changer le papier peint du bureau dans Windows 10 sans activation [Internet]. [cité 30 déc 2022]. Disponible sur: <https://soundartifacts.com/fr/how-to/77-how-to-change-desktop-wallpaper-in-windows-10-without-activation.html#file-explorer>
6. Empêcher la modification du fond d'écran - Windows 10 [Internet]. [cité 30 déc 2022]. Disponible sur: <https://www.pcastuces.com/pratique/astuces/5536.htm>
7. Qu'est-ce qu'une clé de Registre [Internet]. [cité 30 déc 2022]. Disponible sur: <http://www.ordinateur.cc/syst%C3%A8mes/fen%C3%AAtres/224191.html>
8. Regedit : l'éditeur de registre, propre à Windows [Internet]. IONOS Digital Guide. [cité 30 déc 2022]. Disponible sur: <https://www.ionos.fr/digitalguide/sites-internet/developpement-web/regedit/>
9. AccessEnum : lister les droits des répertoires sous Windows | IT-Connect [Internet]. 2017 [cité 1 janv 2023]. Disponible sur: <https://www.it-connect.fr/accessenum-lister-les-droits-des-repertoires-sous-windows/>
10. Qu'est-ce que le registre Windows ? [Internet]. OneSafe Software FR. 2017 [cité 30 déc 2022]. Disponible sur: <https://onesafesoftware.com/software/fr/articles/quest-ce-que-le-registre-windows>
11. Qu'est-ce que la base de registre Windows ? | IT-Connect [Internet]. 2021 [cité 1 janv 2023]. Disponible sur: <https://www.it-connect.fr/quest-ce-que-la-base-de-registre-windows/>
12. Deland-Han. Registre Windows pour utilisateurs expérimentés - Windows Server [Internet]. [cité 1 janv 2023]. Disponible sur: <https://learn.microsoft.com/fr-fr/troubleshoot/windows-server/performance/windows-registry-advanced-users>
13. rédaction L. Comprendre le registre de Windows [Internet]. 01net.com. 2007 [cité 30 déc 2022]. Disponible sur: <https://www.01net.com/astuces/comprendre-le-registre-de-windows-351346.html>
- 14.