La base de registre Windows

SOMMAIRE

Première partie : Cours

Deuxième partie : Exploration du registre Windows

1. Lancer regedit et circuler dans l’arborescence

2. Effectuer une recherche de clé

3. Exemple : son système pour vider la corbeille

4. Exemple : Application par défaut pour ouvrir les GIF

5. Conclusion

C’est une base de données structurées qui contient tous les paramètres du système et des applications dans un fichier binaire (donc illisible).

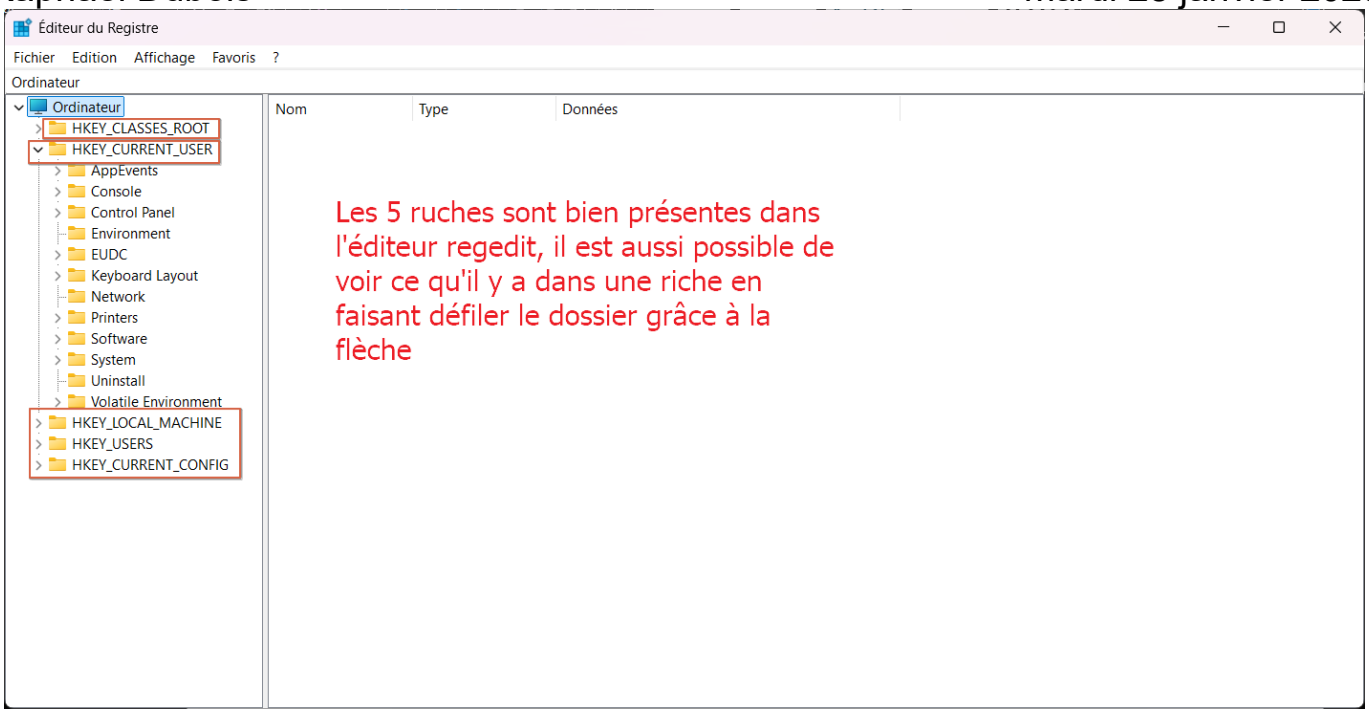
La base de registre est classée en 5 ruches

- HKEY_CLASSES_ROOT (HKCR) : Contient toutes les associations de fichiers et les informations sur les extensions.
- HKEY_CURRENT_USER (HKCU) : Contient la configuration de l’utilisateur courant. Fichier NTUser.dat de l’utilisateur .
- HKEY_LOCAL_MACHINE (HKLM) : Contient la configuration générale de Windows.
- HKEY_USERS (HKU) : Contient la configuration des utilisateurs Windows.
- HKEY_CURRENT_CONFIG (HKCC) : Contient la configuration de la machine (pilotes de périphérique, résolution…).

A part la HKCU, les autres sont stockées dans le dossier C:\Windows\System32\Config

Pour y accéder, on utilise l’éditeur Regedit.

1) Lancer regedit et circuler dans l’arborescence.

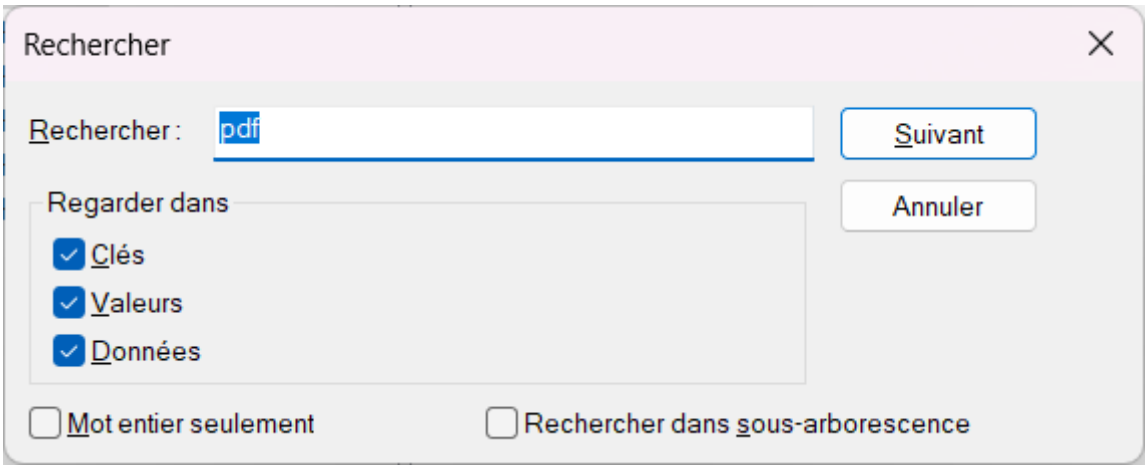


2) Effectuer une recherche de clé

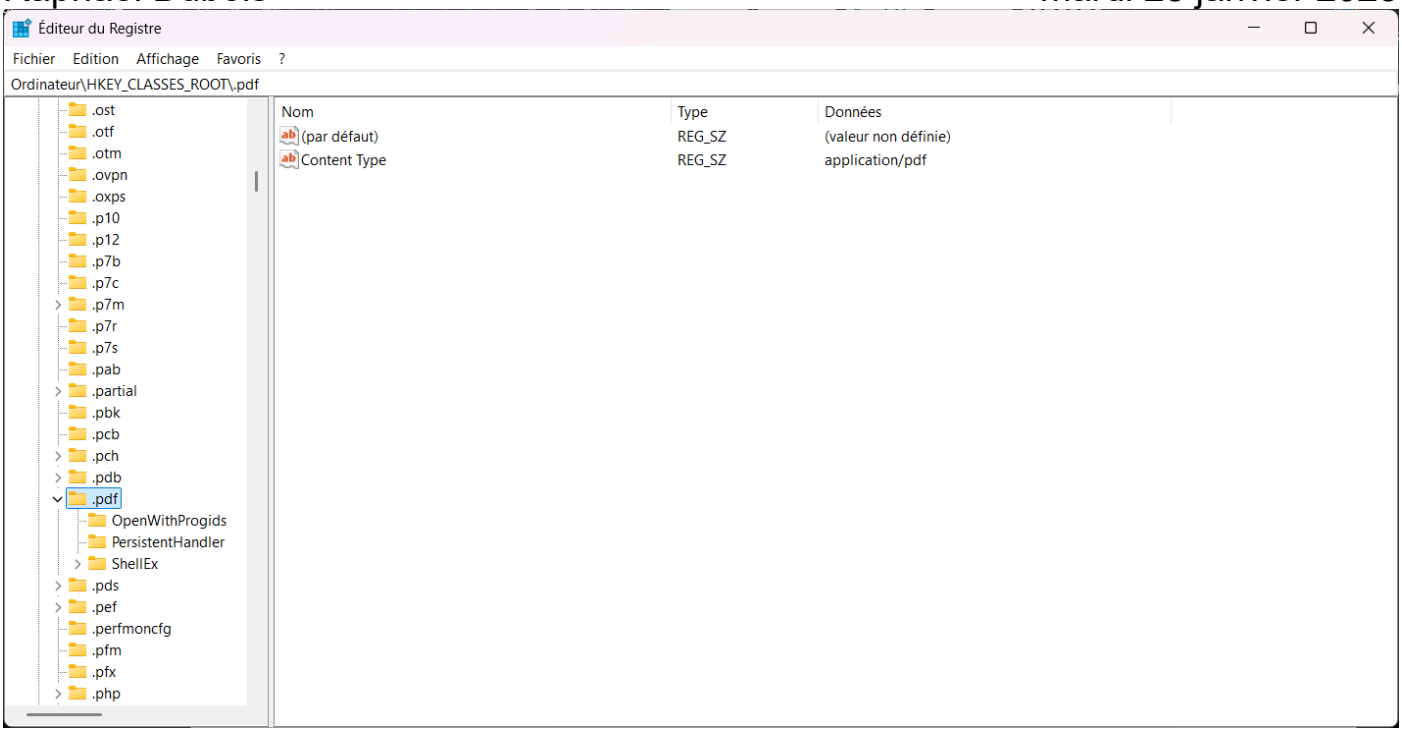
Avec quel logiciel seront ouverts les PDF ?

Comment fonctionne la recherche : à partir d'où, pour continuer, quelle touches…

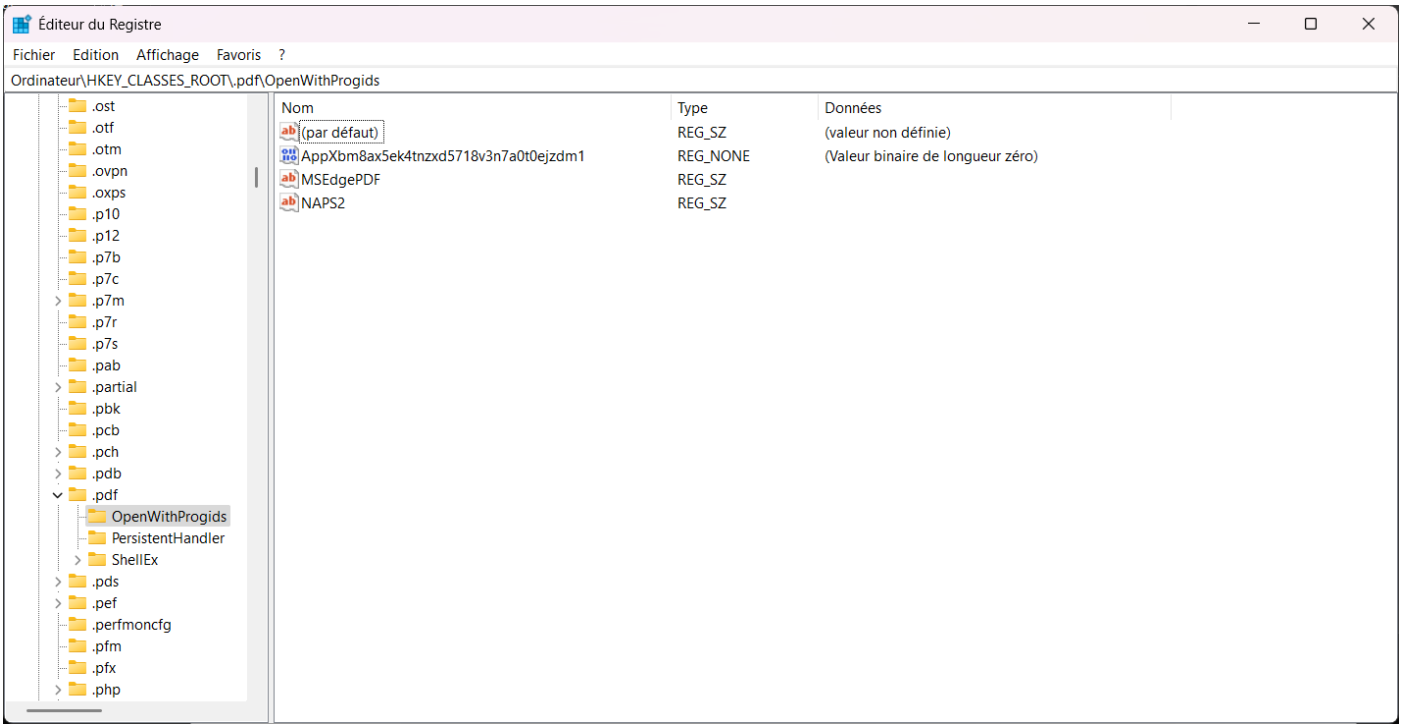
Pour effectuer une recherche, il suffit d'appuyer sur Ctrl + F pour afficher le menu suivant :



Il est possible d'effectuer une recherche dans les clés, les valeurs ou données. Dans notre cas notre cas nous allons simplement sélectionner les clés.



Une fois la recherche terminée, la recherche nous dépose directement sur la première clé, en commençant par la première ruche (HKEY_CLASSES_ROOT). Étant donné que cette ruche contient les associations de fichiers et les information sur les extensions, il est normal d'y retrouver notre format .pdf. Dans cette clé, on pourra y retrouver les logiciels qui permettrons d'ouvrir les pdf dans la sous clé « OpenWithProgid »

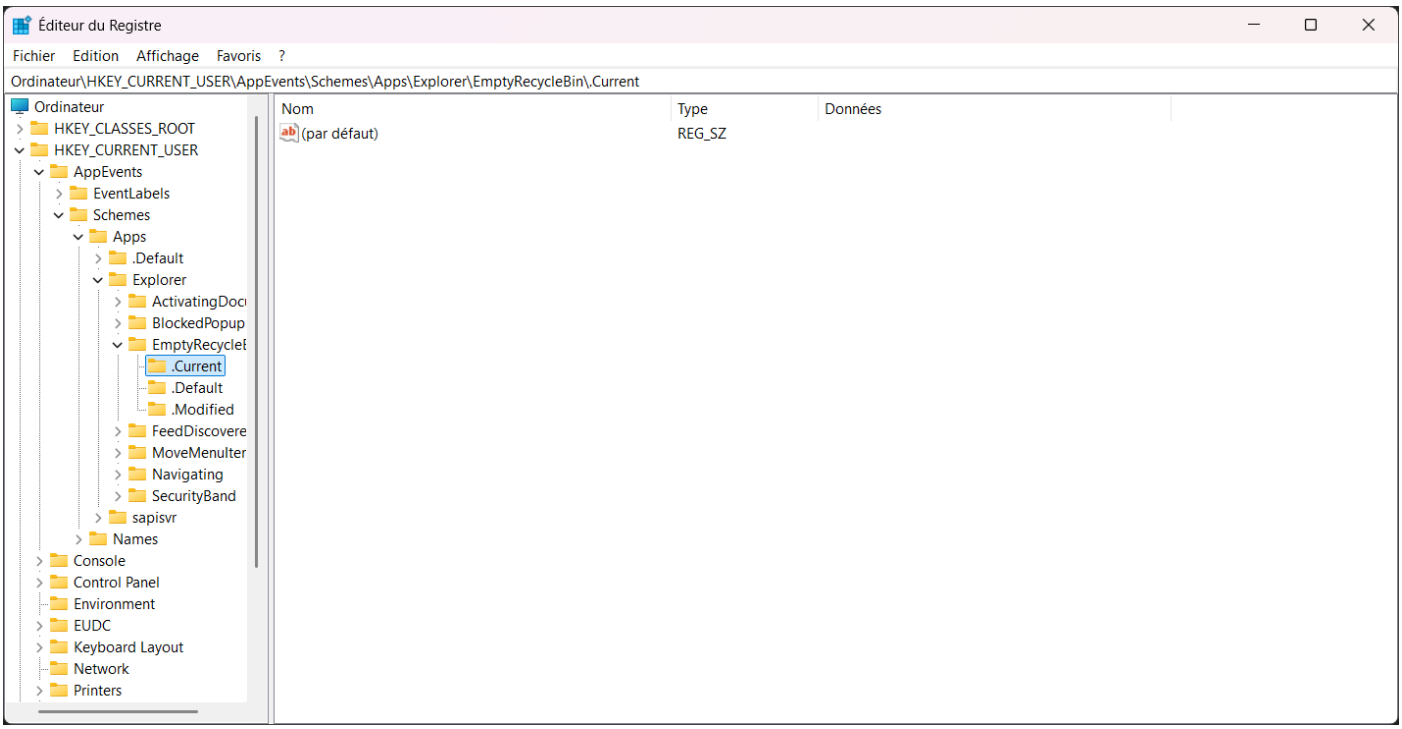


Ici nous observons qu'il est possible d'ouvrir les pdf avec « MSEdgePDF » qui correspond à Microsoft Edge et « NAPS2 » qui correspond à un logiciel de scanner.

Pour continuer la recherche dans une clé suivante, il suffit d'appuyer sur F3.

3) Exemple : son système pour vider la corbeille

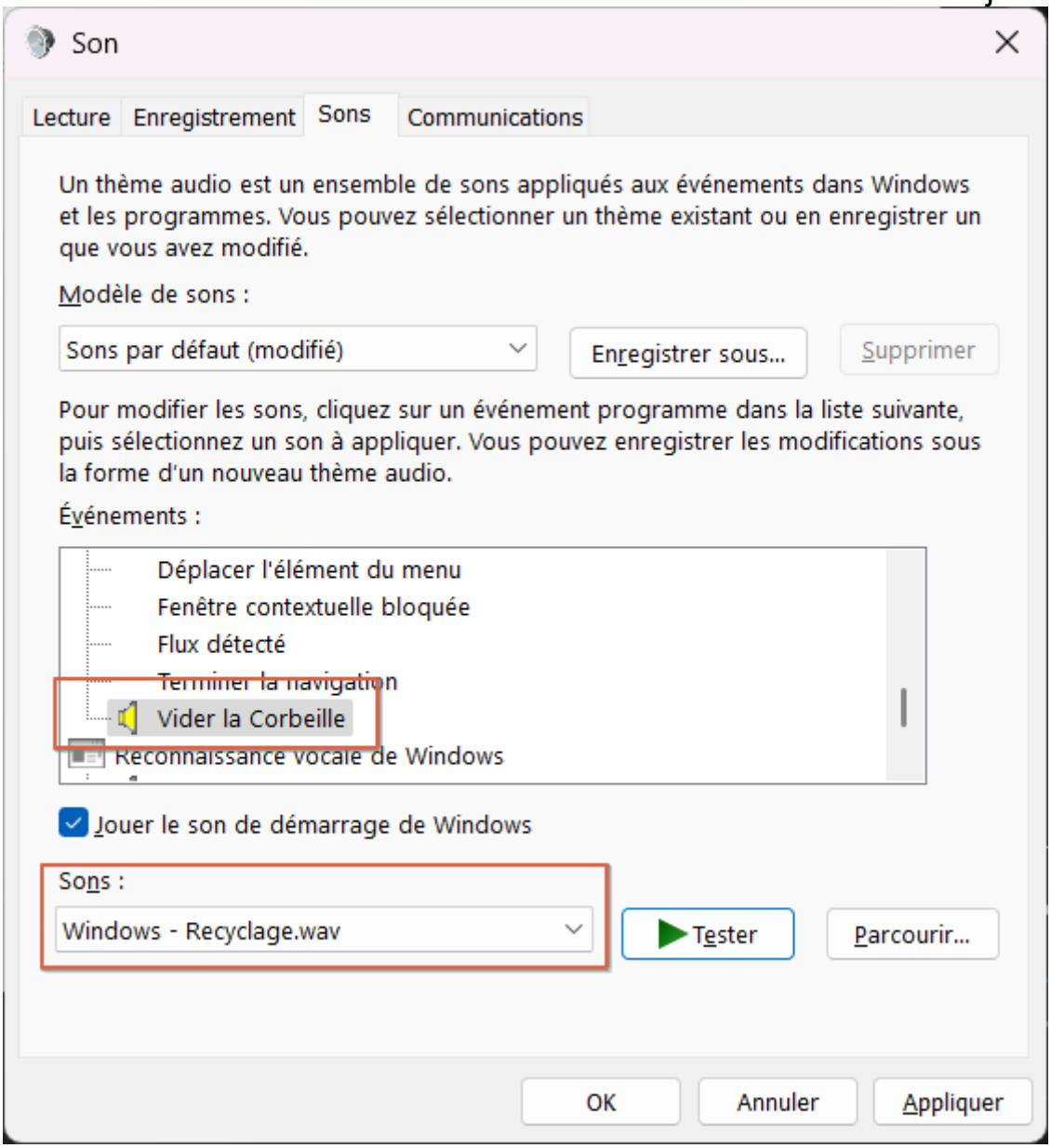
- Dans Regedit, aller dans HKEY_CURRENT_USER\AppEvents\Schemes\Apps\Explorer\EmptyRecycleBin\Current
- Pas de son par défaut.



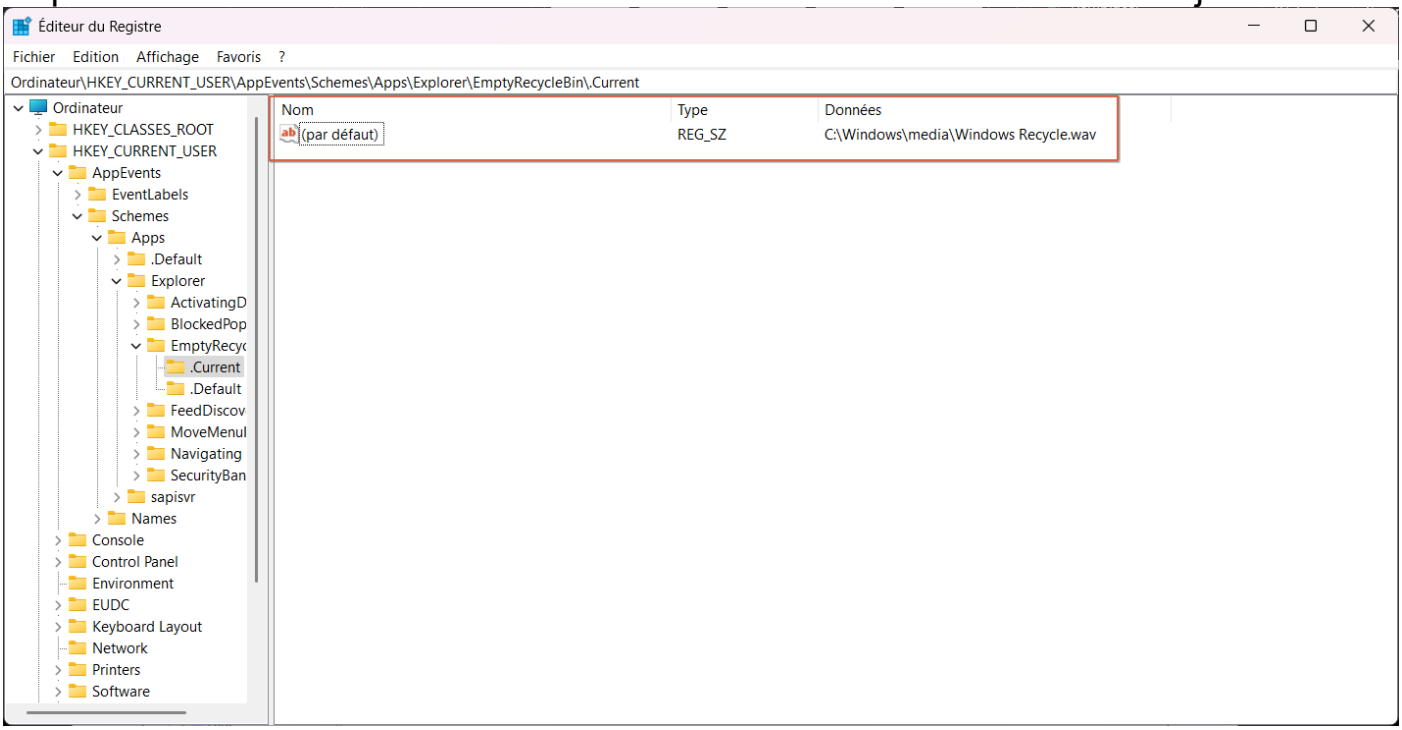
- Faire une sauvegarde du Registre.

Pour faire une sauvegarde, il suffit d'aller dans « fichiers » puis de cliquer sur « Fichiers » puis sur « Exporter » et puis il suffit de sélectionner un emplacement

- Dans Panneau de configuration et choisir un son pour vider la corbeille. Tester et appliquer.

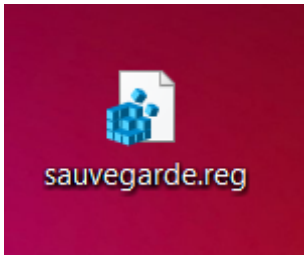


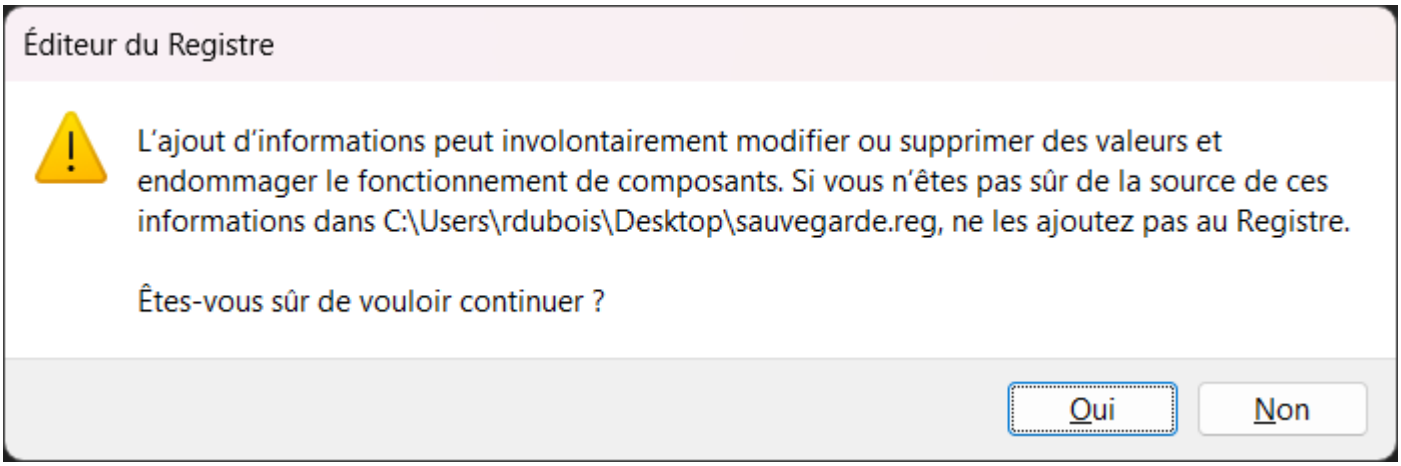
- Revenir dans Regedit et constater le changement.

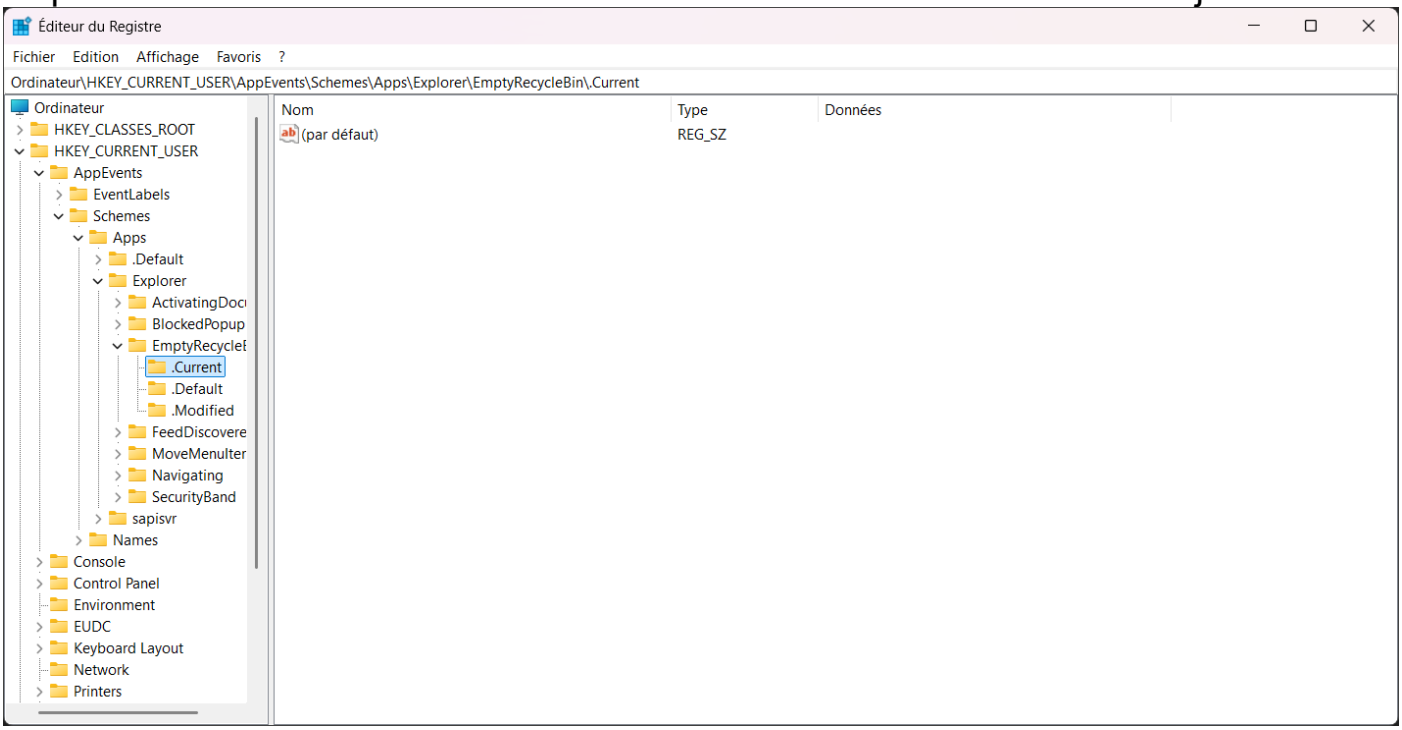


On peut constater que la valeur par défaut a changé et qu'elle contient maintenant un chemin vers le son choisi

- Remettre la sauvegarde et vérifier qu'il n'y a plus de son.



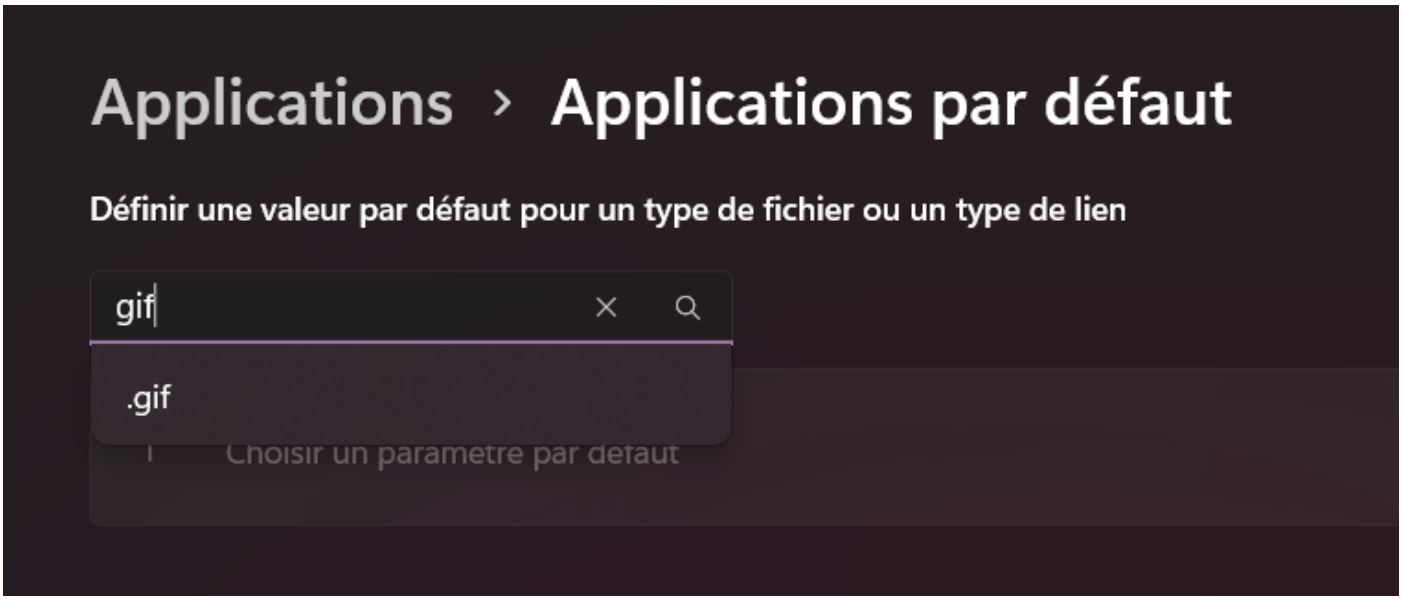




On peut remarquer qu'après avoir restauré la sauvegarde, la clé par défaut est de nouveau vide.

4) Exemple : Application par défaut pour ouvrir les GIF

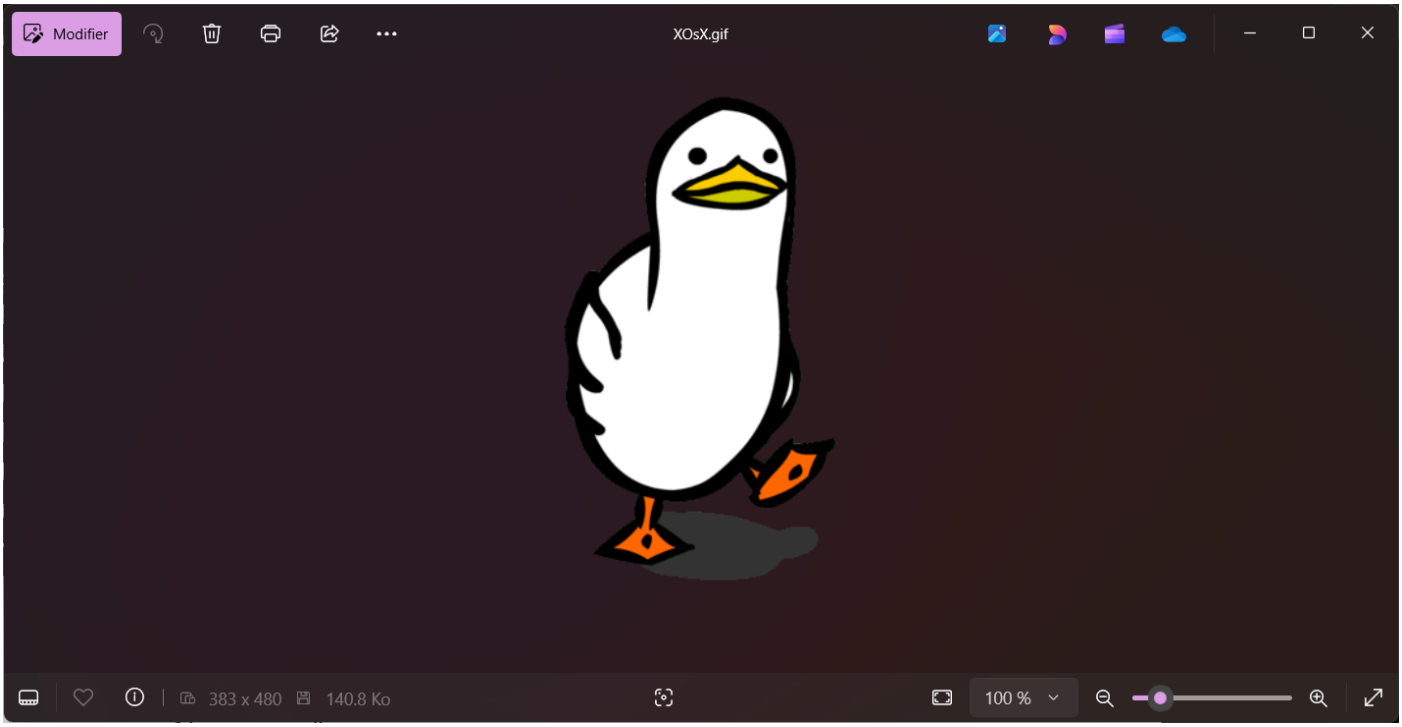
- Trouver l'application par défaut dans les paramètres Windows.





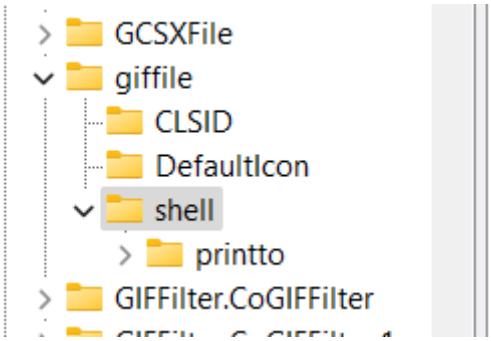
L'application pour ouvrir les fichiers .gif par défaut est l'application Photos de Windows

- Vérifier en cliquant sur un GIF.



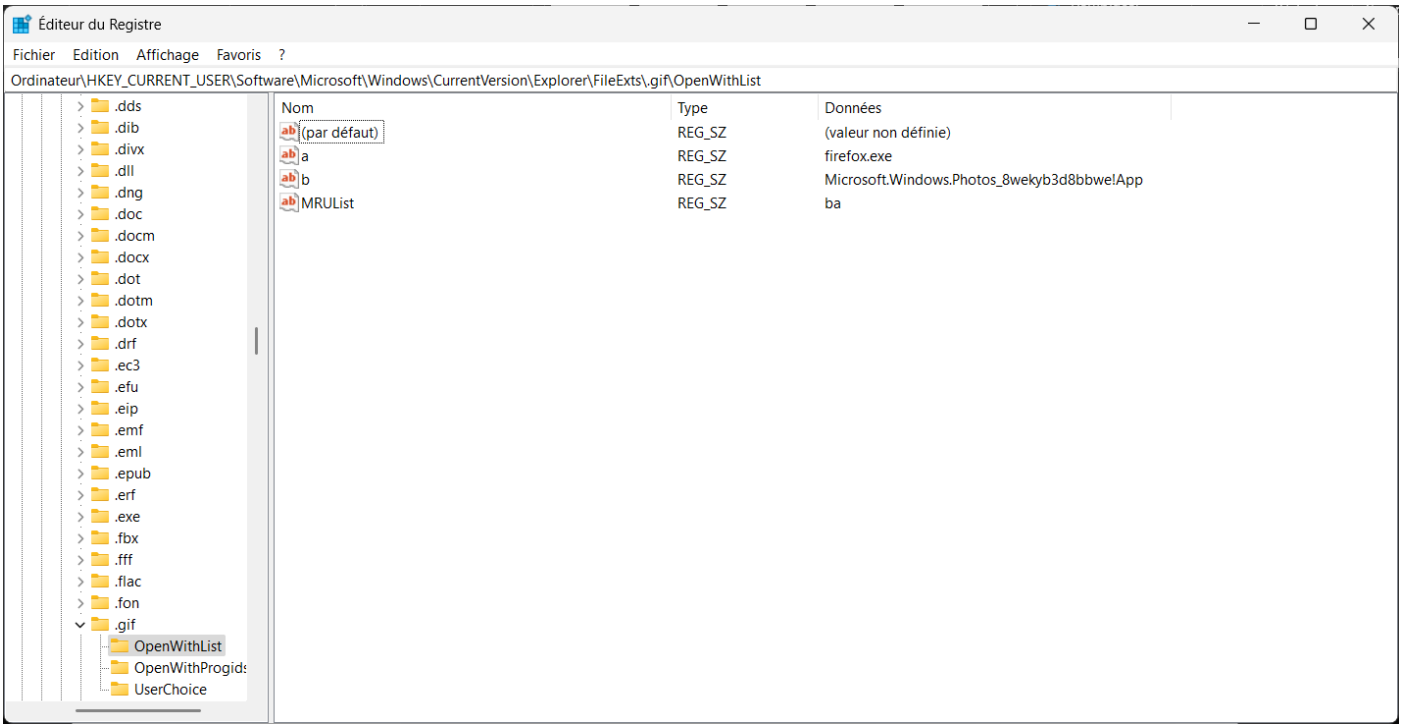
Le .gif s'ouvre bien avec cette application.

- Dans Regedit, aller dans HKCR\giffle\shell\open\command. Quelle est l'application définie par défaut ? Une hypothèse ?



On remarque ici que la clé n'est pas présente, c'est donc pas dans cet endroit la qu'on pourra voir les différents logiciels utilisés.

- Aller dans HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.gif\OpenWithList. Quels sont les logiciels définis pour ouvrir les gifs ? Et quel ordre sont-ils utilisés ? Conclusion ?



Ici nous avons bien les différents logiciels utilisés pour ouvrir les .gif. Ils sont chacun défini par une lettre, a, b, selon le moment auquel l'application a été définie par défaut. Cela signifie donc que si l'on modifie l'application par défaut pour les .gif, on pourra observer l'application avec la lettre « c » dans ce répertoire de clés.

La clé : « MRUList » contient l'ordre dans lequel les programmes sont exécutés. Dans notre cas, le programme b (étant l'application Photos de Windows) est exécuté avant le a (Firefox). Ce qui correspond bien à notre application par défaut.

5) Conclusion

En entreprise, sur les postes de travail et serveurs intégrés à un domaine Active Directory, on utilise les stratégies de groupe (GPO) pour déployer des paramètres de configuration. Cela permet d'agir directement sur le registre !