Le registry

Le système d'exploitation, les applications, le matériel et les utilisateurs ont besoin de nombreux paramètres que Windows les regroupe dans ce qu'il appelle le "registre".

A l'époque du DOS, quelques variables d'environnement et les fichiers ".INI" suffisaient pour mémoriser tous ces paramètres. Les variables d'environnement étaient initialisées par les fichiers CONFIG.SYS et AUTOEXEC.BAT. Ces derniers étaient lancés automatiquement au démarrage.
- CONFIG.SYS contenait des informations de configuration du DOS. Ce fichier ne sert plus depuis Windows 95.
- AUTOEXEC.BAT avait pour rôle le lancement automatique d'une série de commandes au démarrage. Ce système était encore utilisable sous Windows 9x.

Les premières versions de Windows proposaient dans leurs API (*interface pour programmes d'application*) des fonctions pour créer, lire et modifier des **fichiers ".INI"** Les applications peuvent par ce biais enregistrer des données réutilisables d'une session à l'autre. Les fichiers ".ini" sont des fichiers textes divisés en « sections » pouvant contenir chacune les définitions de plusieurs données, les « clés » de cette sorte de base de données.

Les noms de sections sont encadrés par des crochets [ ]

Le nom d'une clé est immédiatement suivi du signe égal et de la valeur à lui attribuer.

L'exemple ci-contre est le fragment d'un fichier dont le nom était MOUSE.INI.

```
[mouse]
Memory=HighMem
MouseType=SERIAL1
Device=Mouse
PhysicalButtons=2
[Display]
CursorDisplayDelay=0
[DOSPointer]
PointerSize=Small
PointerColor=Normal
...
```

Les concepteurs d'applications ont toujours la possibilité de créer ces fichiers .INI . Microsoft a laissé dans ses API les fonctions pour ce faire mais recommande aux développeurs d'utiliser une autre technique : le « registry »

Les fichiers ".INI" sont modifiables via SysEdit l'éditeur de configuration système accessible par la commande Démarrer > Exécuter … > sysedit
NB. La commande SysEdit utile pour Windows 95 et 98 est toujours disponible sur Windows 2000 et XP mais les fichiers WIN.INI et SYSTEM.INI ne servent plus qu'aux applications 16 bits. L'équivalent pour Windows XP est la commande MSCONFIG dont nous reparlerons ailleurs.

Les fichiers ".INI" sont facilement modifiables puisque rédigés en mode texte. Les applications sont libres de créer de tels fichiers aux emplacements de leur choix sur le disque. En général, chaque application place ses fichiers dans un répertoire qui lui est propre. Microsoft a cependant voulu réglementer tout cela en centralisant encore plus toutes les informations des applications sous le contrôle de Windows. C'est ainsi qu'est né ce que Microsoft appelle la « **Base de registre** » (**BDR**) ou ***registry***, un endroit où Windows rassemble des informations de toutes sortes.

Le registre devenu incontournable rassemble la plupart des paramètres du système :
- le matériel détecté lors de la séquence de boot
- les pilotes de périphériques
- les applications installées (dans quels répertoires, leurs options etc.)
- les informations propres au système d'exploitation
- les utilisateurs et leur profil quand il n'est pas stocké de manière centralisée sur un serveur
- …

Où se cache le registre ?

Le registre a ses données stockées dans plusieurs fichiers système.

Sous Windows 9x ce sont les fichiers USER.DAT et SYSTEM.DAT du répertoire \WINDOWS.

Windows Me possède un fichiers de plus : CLASSES.DAT.

Windows 2000 ou Windows XP rangent ce genre de fichiers dans les répertoires \WINNT ou WINDOWS\SYSTEM32\CONFIG et \DOCUMENTS AND SETTINGS\%USERNAME%. Vous y trouverez par exemple le fichier SAM, un fichier crypté qui concerne la sécurité des utilisateurs, mais aussi les fichiers SECURITY, SOFTWARE, SYSTEM, DEFAULT ou encore le fichier NTUSER.DAT .

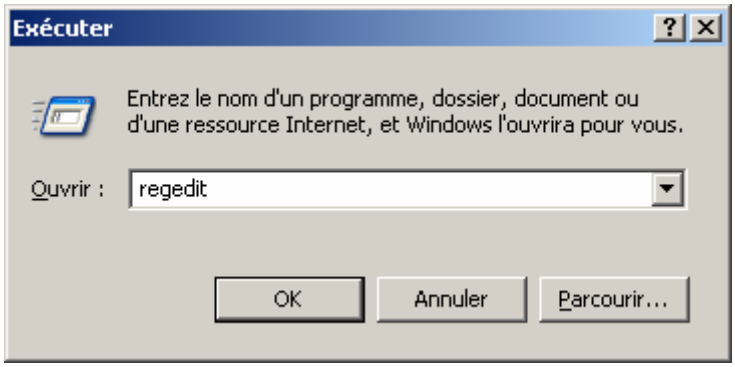
Peu importe finalement où se trouvent ces fichiers car même votre éditeur hexadécimal sera incapable de les ouvrir.

Ces fichiers sont aussi appelés "*hives*" ou "ruches" en français.

Comment consulter ou modifier le registre ?

Sur Windows 95, 98, Me et 2000, on a le choix entre deux programmes : REGEDIT et REGEDT32. La présentation des données diffère légèrement d'un programme à l'autre mais REGEDT32 offre l'avantage de permettre la consultation du registre en mode lecture seule ce qui réduit les risques.

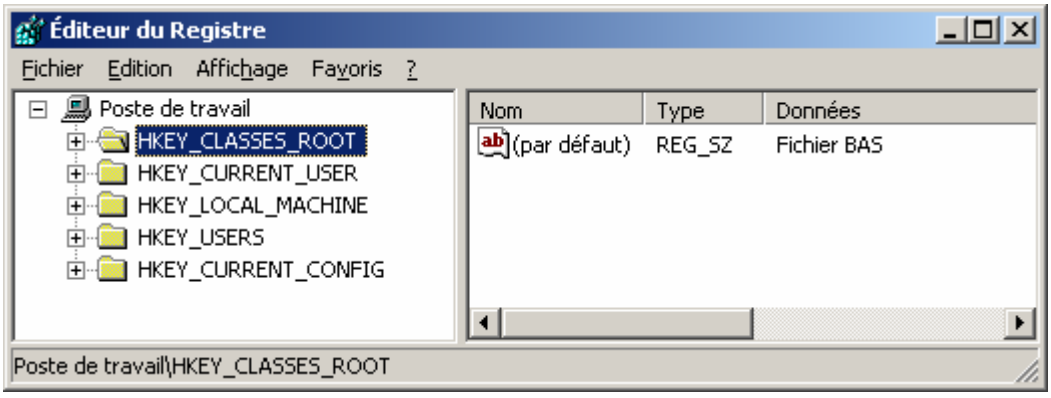
Depuis Windows XP, le seul moyen de consulter le registre et éventuellement le modifier est d'utiliser le programme REGEDIT. Si même vous appelez REGEDT32 c'est REGEDIT qui s'ouvrira. N'espérez pas trouver un raccourci vers ce programme ; il faut pour le lancer cliquer sur Démarrer puis Exécuter ... et taper REGEDIT. Cette contrainte est sans doute une façon de ne pas mettre ce programme à la portée du premier venu.



Parmi les centaines d'informations stockées dans le registre certaines sont vitales pour le système. Une fausse manœuvre risque d'endommager gravement le système au point de devoir tout réinstaller. Voici ce qu'indique l'aide de Windows XP à ce propos :

> *Les éditeurs du Registre permettent de contrôler et de modifier le Registre. Cependant, vous ne devriez pas avoir à le faire. … Il est fortement conseillé de ne pas modifier les paramètres du Registre vous-même.*

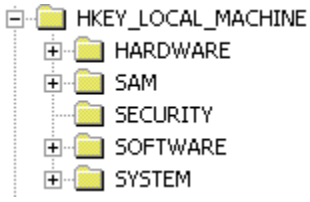
Vous êtes prévenu, nul autre que vous ne pourra être tenu responsable des conséquences de vos manœuvres sur un système qui devrait encore vous servir ensuite !



La structure du registre est arborescente

Le registre est organisé à la manière des répertoires et des fichiers.
A la racine, se trouvent cinq « HKEY » qui contiennent des sous-répertoires appelés "clés" qui se subdivisent en d'autres (sous-)clés etc. pour finalement aboutir à des valeurs (*values*).
A la base donc, cinq HKEY :
- Les deux premières sont bien réelles
    HKEY_LOCAL_MACHINE regroupe des informations relatives à la machine
    HKEY_USERS regroupe les informations spécifiques à chaque utilisateur
- Les trois autres HKEY ne sont que des raccourcis vers certains emplacements du registre.
    HKEY_CLASSES_ROOT regroupe les paramètres utilisés par les applications
    HKEY_CURRENT_USER conduit aux informations de l'utilisateur courant
    HKEY_CURRENT_CONFIG donne le profil matériel courant

HKEY_LOCAL_MACHINE



= Configuration matérielle et logicielle de la machine

On y trouve 5 clés :
- HARDWARE = la description du matériel et des pilotes qui le contrôle. Ces informations sont constituées lors de chaque démarrage de Windows. Elles ne sont pas enregistrées sur le disque.
- SAM = *Security Account Manager*, le gestionnaire de sécurité des comptes = les noms des utilisateurs, des groupes et les mots de passe. Ces informations correspondent au fichier C:\Windows\System32\Config\SAM qui est crypté bien entendu.
- SECURITY correspond au fichier C:\Windows\System32\Config\SECURITY
- SOFTWARE regroupe des informations plus accessibles. Chaque application y stocke les paramètres qui lui sont nécessaires : les préférences, les fichiers à enlever en cas de désinstallation etc.
- SYSTEM concerne les indications nécessaires au démarrage du système.

HKEY_USERS

= profils de tous les utilisateurs

HKEY_CURRENT_USER

= profil de l'utilisateur actuel : vous, vos préférences, vos logiciels, les fichiers récents que vous avez ouverts avec chacun d'eux etc. Ces informations sont entreposées dans le fichier C:\Windows\Documents and Settings\%username%\ntuser.dat

HKEY_CURRENT_CONFIG

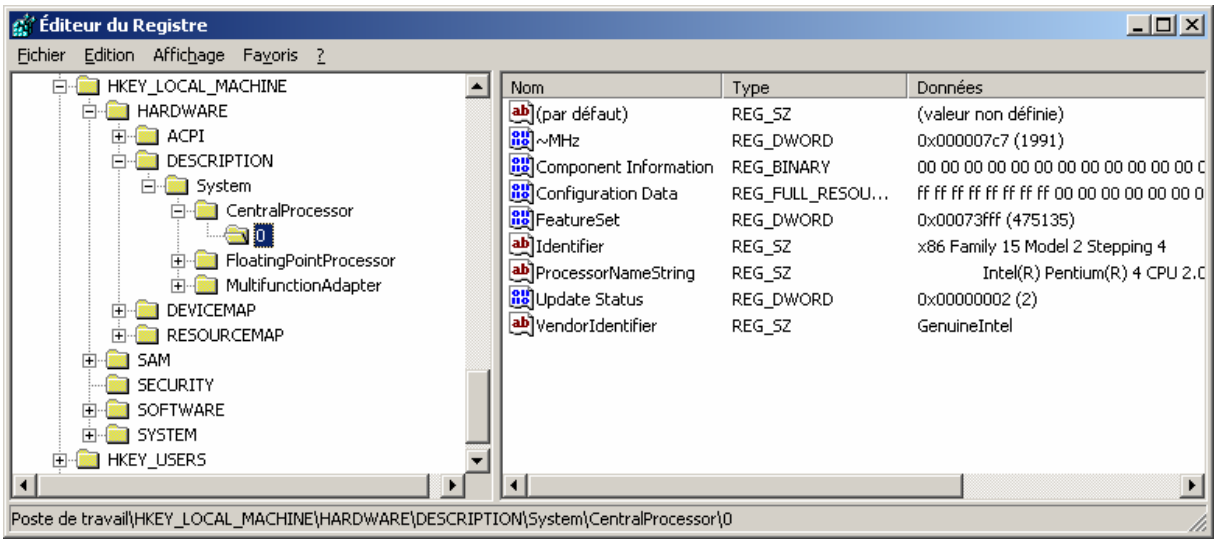
Pointe sur une sous-division de HKEY_LOCAL_MACHINE qui décrit le profil matériel courant : HKEY_LOCAL_MACHINE\System\CurrentControlSet\Hardware Profiles\Current

HKEY_CLASSES_ROOT

Ce répertoire regroupe toutes les extensions (.bat, .bmp, ….jpg, …, .wav, etc.) avec pour certaines d'entre elles les indications sur les applications associées. On y trouve aussi les noms des applications avec comme données des numéros de version et des CLSID (*Class identifier*) des numéros que les programmes se communiquent pour s'identifier notamment lors des liaisons et insertions d'objets. C'est ainsi que WORD sait à quel programme il doit faire appel quand on lui colle un tableau Excel ou que Internet Explorer trouve l'application pour afficher une animation Flash, jouer un air de musique ou une séquence vidéo.

Les valeurs

L'éditeur de registre REGEDIT rend parfaitement compte de l'organisation arborescente du registre. Le volet de gauche est semblable à celui de l'explorateur de Windows.
Les valeurs sont affichées dans le volet droit ; chacune comporte trois éléments : le nom, le type et la donnée.



Le type de données indique le format d'enregistrement des données. Elles sont enregistrées soit sous forme de chaînes de caractères, soit sous forme de codes binaires codés en hexadécimal.
Les noms de types commencent toujours par "REG_"

REG_SZ

String Zero = Simple chaîne de caractère s'achevant par un terminateur dont le code est 0

Exemple :

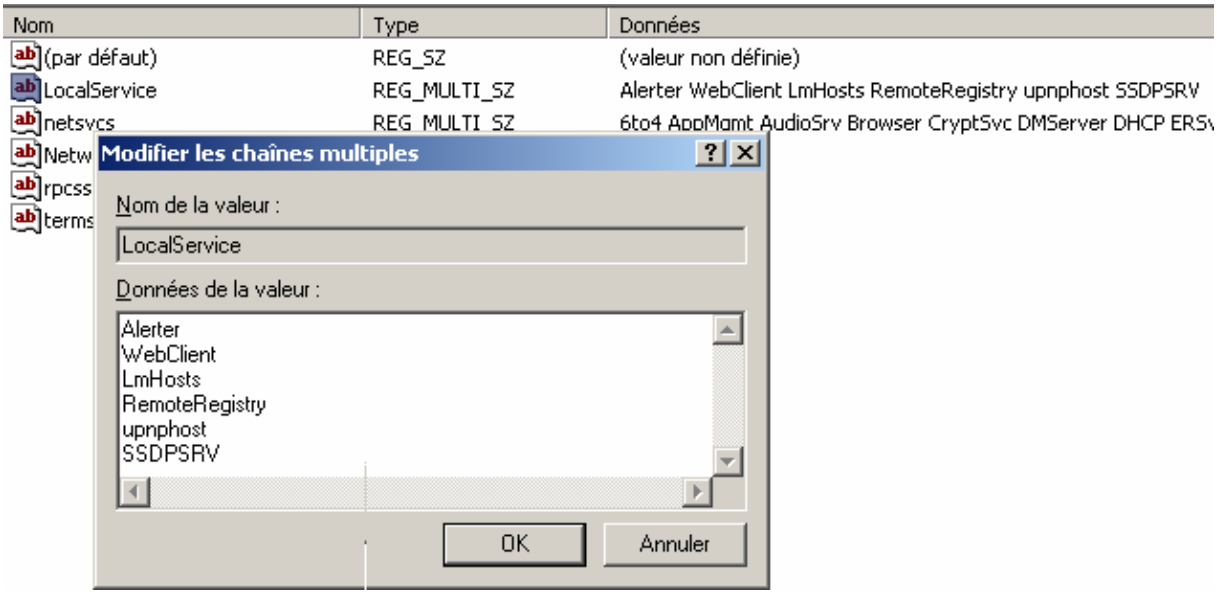
Nom	Type	Données
(par défaut)	REG_SZ	
COM1:	REG_SZ	9600,n,8,1

REG_EXPAND_SZ
Chaînes de caractère où peuvent être insérées des variables d'environnement

Exemple :

Nom	Type	Données
ProfilesDirectory	REG_EXPAND_SZ	%SystemDrive%\Documents and Settings

REG_MULTI_SZ
Une chaîne de caractères qui accepte plusieurs valeurs.



REG_DWORD Valeur binaire de 4 octets
REG_QWORD Valeur binaire de 8 octets
REG_BINARY Valeur binaire dont la taille est quelconque
REG_FULL_RESSOURCE DESCRIPTOR Un mode spécial propre à Windows XP
Exemple :

Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)
Policy	REG_BINARY	00
ZIP CodeW	REG_BINARY	00 00
MaxLogSizeKB	REG_DWORD	0x00000020 (32)
MinutesBeforeIdle	REG_DWORD	0x0000000f (15)
Configuration Data	REG_FULL_RESOURCE_DESCRIPTOR	ff ff ff ff ff ff ff ff 00 00 00 00 02 00 00 00

Sauvegarde du registre

Avant de supprimer des clés, veillez à faire une sauvegarde via la commande Exporter un fichier du registre … du menu Registre de l'éditeur REGEDIT. Le résultat sera un fichier ".reg" dont le contenu est visible avec n'importe quel éditeur de texte.
A l'inverse, il faut "Importer" ce fichier pour restaurer les valeurs effacées ou modifiées. Notez cependant que les valeurs qui se trouveraient dans la base de registre mais qui ne sont pas dans le fichier importé restent inchangées.

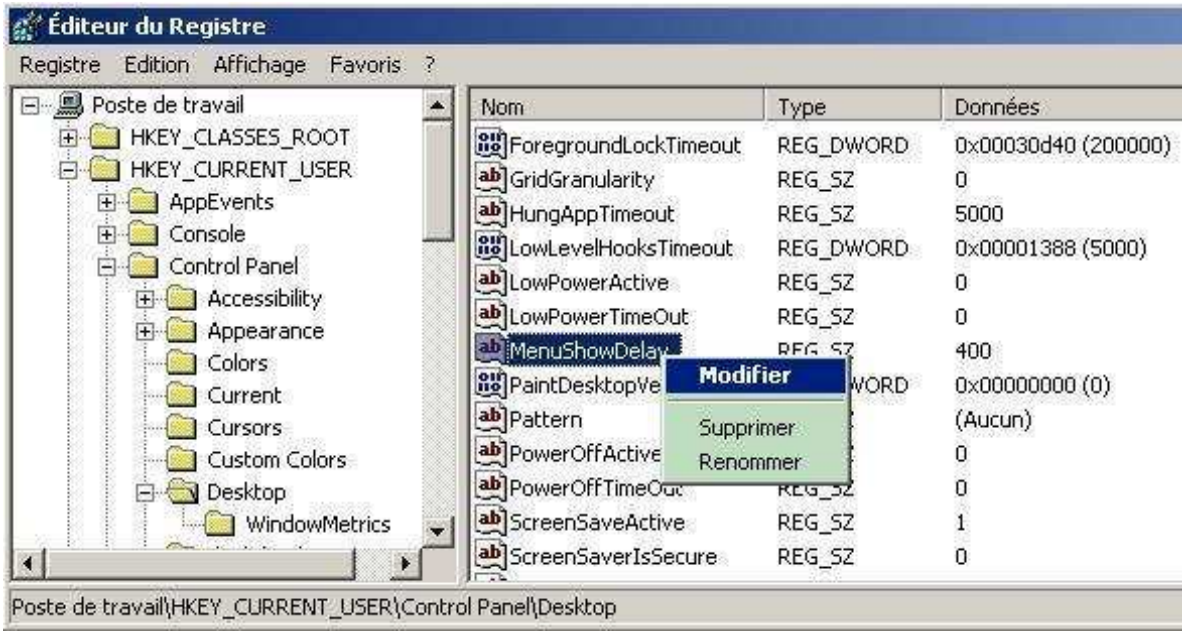
Exemples de manipulations pouvant être faites dans le registre :

Avec REGEDIT recherchez les informations suivantes :

- Le type, la version et la date d'édition de votre BIOS :
  `HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System`
- La liste des « ruches » chargées dans la base de registre :
  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist`
- Le numéro de licence de Windows :
  `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\`
  dans la fenêtre de droite lire ProductId (que l'on trouve plus simplement les propriétés système = clic droit sur Poste de travail > Propriété)
- Les programmes lancés automatiquement au démarrage :
  `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
  Espérons ne pas y trouver de spywares ni de virus !

Quelques bidouillages :

- Modifier la vitesse d'affichage des sous menu du menu démarrer :
  `HKEY_CURRENT_USER\Control Panel\Desktop` dans la fenêtre de droite recherchez l'entrée `MenuShowDelay` la valeur initiale est 400. Faites un clic droit sur le nom de la clé pour pouvoir la modifier. Essayez par exemple 20 au lieu de 400. Les délais devraient être 20 fois plus court après avoir redémarré Windows.



- Activer ou désactiver la fonction AutoRun du Cd-rom :
  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom`
  Mettre la valeur de `Autorun` à 0 ou à 1 pour enlever ou remettre cette option.

Curieux cette ressemblance entre les titres de la presse féminine et ceux de la presse informatique

Des recettes miracles pour perdre 3 kg en 10 jours ou la « révélation » de quelques trucs avec la promesse d'obtenir un PC plus performant sont des titres accrocheurs qui visent des publics différents mais laisseront perplexes les moins crédules !

Reconnaissons-le il y a dans le setup du BIOS et encore plus dans les innombrables variables du registre pas mal de points obscurs. N'espérez pourtant pas trouver la solution à vos angoisses dans des ouvrages du genre « **Truc et bidouilles pour les nuls** »

Le systèmes d'exploitation de Microsoft ne sont pas *"open source"*, la manière dont sont développés ces programme ou ce à quoi correspondent les variables n'est donc normalement pas documentés. Parfois, le nom de la variable laisse deviner son rôle ce qui rend possible la modification d'un détail ou l'autre ce que certains appellent des « astuces ».

Nettoyage du registre

Des programmes mal désinstallés, des virus mal soignés laissent des traces dans le registre. Bien que cela soit souvent sans conséquence cela laisse l'impression que le PC est encombré de trucs qui ne peuvent que le ralentir. Il existe donc des programmes qui vous proposent de nettoyer tout ça. Parmi ceux-ci Regcleaner gratuit sur www.telecharger.com devrait faire l'affaire.

… à suivre …

Liens externes vers ce sujet:

http://leregistre-fr.net/
http://mtoo.mvps.org/registre.shtml
http://www.zebulon.fr/articles/base-de-registre-1.php
http://fr.wikipedia.org/wiki/Base_de_registre#2_Hkey_de_base
http://www.secretswindows.com/