Le registre Windows
- Complément de cours -

Module R3

R&T 1ère année

EL HMAM Mohamed Saïd

Le registre Windows
- Complément de cours -

- Présentation
  - Accéder au registre
  - Arborescence du registre
- Mise à jour du registre
  - Exporter, créer, modifier, supprimer
  - Nettoyer le registre
  - Sauvegarder le registre
  - Clés à surveiller
- Outils
- Exemples

Définition

- Le registre c'est quoi ?

➢ Windows conserve toutes les informations relatives à la configuration du système, ces informations peuvent être visualisées dans une base de données appelée Registre.

➢ Le Registre contient :

✓ Les profils de chaque utilisateur de l'ordinateur.

✓ Les informations relatives au matériel du système, aux programmes installés et aux paramètres de propriétés.

Définition

- Windows utilise constamment les informations du registre dés le démarrage et lors de son fonctionnement.

- Windows inscrit les modifications dans le registre chaque fois qu'un utilisateur modifie une propriété du système à l'aide d'une boite de dialogue.

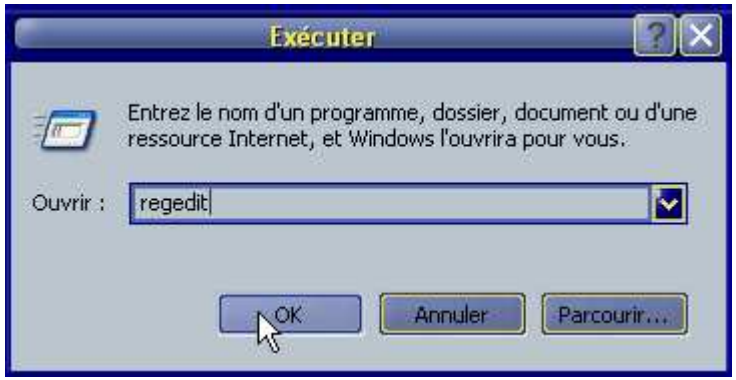
Définition

- Ces informations sont présentes dans divers fichiers appelés « ruches » et situés dans plusieurs répertoires :
  - C:\Documents and Settings\%USERPROFILE%\ (\%USERPROFILE%\ -> correspond au nom des sessions)
  - C:\Documents and Settings\%USERPROFILE%\Local Settings\Application Data\Microsoft\Windows\
  - C:\Windows\System32\Config\
  - C:\Windows\System32\Config\systemprofile\
  - C:\Windows\System32\GroupPolicy\
- Les principaux noms de ces fichiers : ntuser.dat, UsrClass.dat, default, SAM, SECURITY, software, system (accès impossible sauf via l'éditeur de registre)

Accéder au registre

- Les éditeurs du Registre permettent de contrôler et/ou modifier les données dans le registre. Il existe deux outils Windows présents sur le système : Regedit.exe et Regedit32.exe.
- Pour accéder au registre :

Menu Démarrer → Exécuter et tapez : regedit

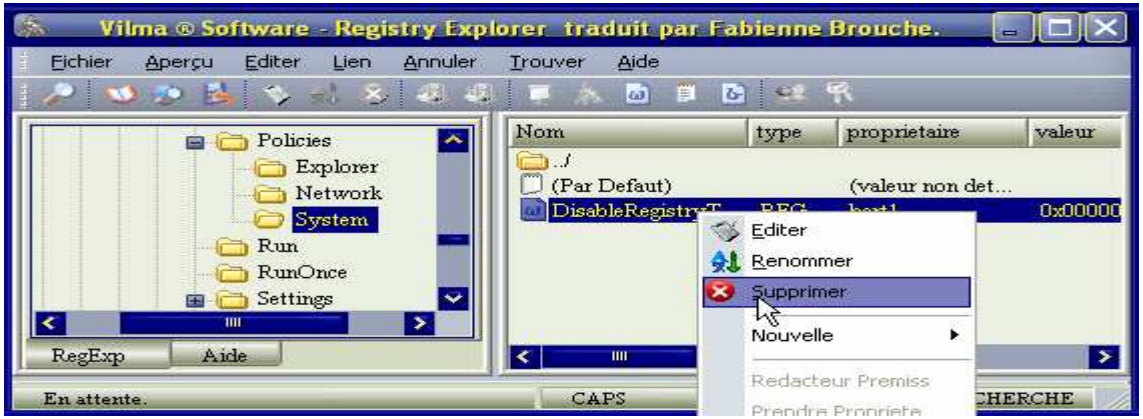


vous pouvez également ajouter un raccourci sur votre bureau, il suffit d'aller dans votre Explorateur à :

- C:\Windows\regedit.exe

Accéder au registre

- Dans de nombreux cas d'infections, les malwares installent des restrictions pour vous interdire d'accéder à votre registre.
  - Modifiez l'extension du programme (regedit.exe → .com)
  - Utilisez FixSwen.inf (Il est employé pour remettre en place (dans la base de registre) les associations relatives à l'exécution des fichiers exécutables (.exe, .com, .bat, .reg, etc.) altérées par le malware Swen pour paralyser le système.
  - Utilisez un autre éditeur de registre, Vilma



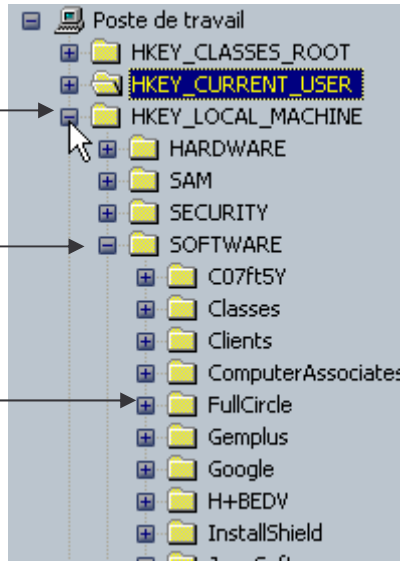
Arborescence du registre

- Le registre possède une structure hiérarchique ressemblant à la structure des répertoires de votre disque dur, l'exploration avec Regedit étant similaire à l'Explorateur Windows.

dossier

contenu (valeurs) du dossier sélectionné

Arborescence du registre

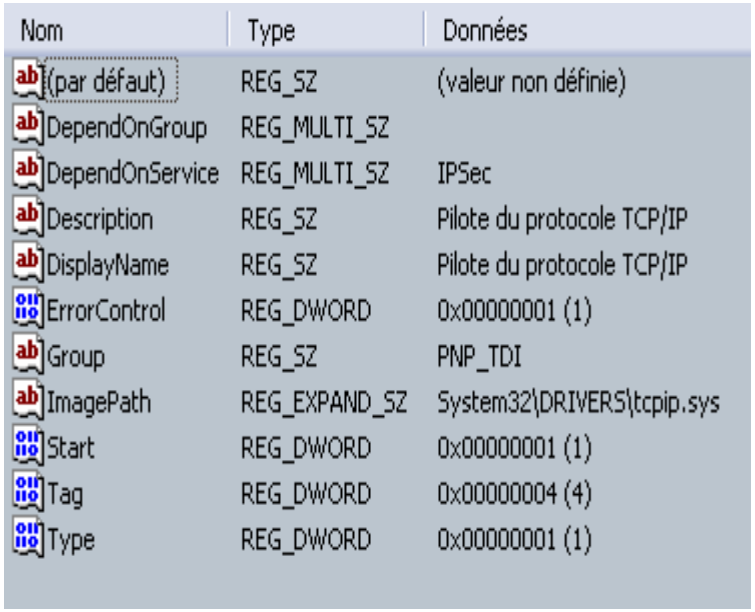


cliquez sur la clé désirée et examinez les valeurs énumérées dans la partie droite de la fenêtre

HKEY_LOCAL_MACHINE	Contient les informations relatives à l'ordinateur local : matériel, OS (type de bus, RAM, pilotes de périphérique, …
HKEY_CLASSES_ROOT	Contient les données de liaison d'incorporation d'objet (OLE) et d'association de classes de fichier (corr. des exécutions)
HKEY_CURRENT_USER	Contient le profil de l'utilisateur en cours de session (variable d'environnement, bureau,…)
HKEY_USER	Contient tous les profils utilisateurs chargés activement, y compris HKEY_CURRENT_USER
HKEY_CURRENT_CONFIG	Contient les informations sur le profil matériel utilisé par l'ordinateur local au démarrage (pilotes, …)

www.leregistre-fr.net

Arborescence du registre



Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)
DependOnGroup	REG_MULTI_SZ	
DependOnService	REG_MULTI_SZ	IPSec
Description	REG_SZ	Pilote du protocole TCP/IP
DisplayName	REG_SZ	Pilote du protocole TCP/IP
ErrorControl	REG_DWORD	0x00000001 (1)
Group	REG_SZ	PNP_TDI
ImagePath	REG_EXPAND_SZ	System32\DRIVERS\tcpip.sys
Start	REG_DWORD	0x00000001 (1)
Tag	REG_DWORD	0x00000004 (4)
Type	REG_DWORD	0x00000001 (1)

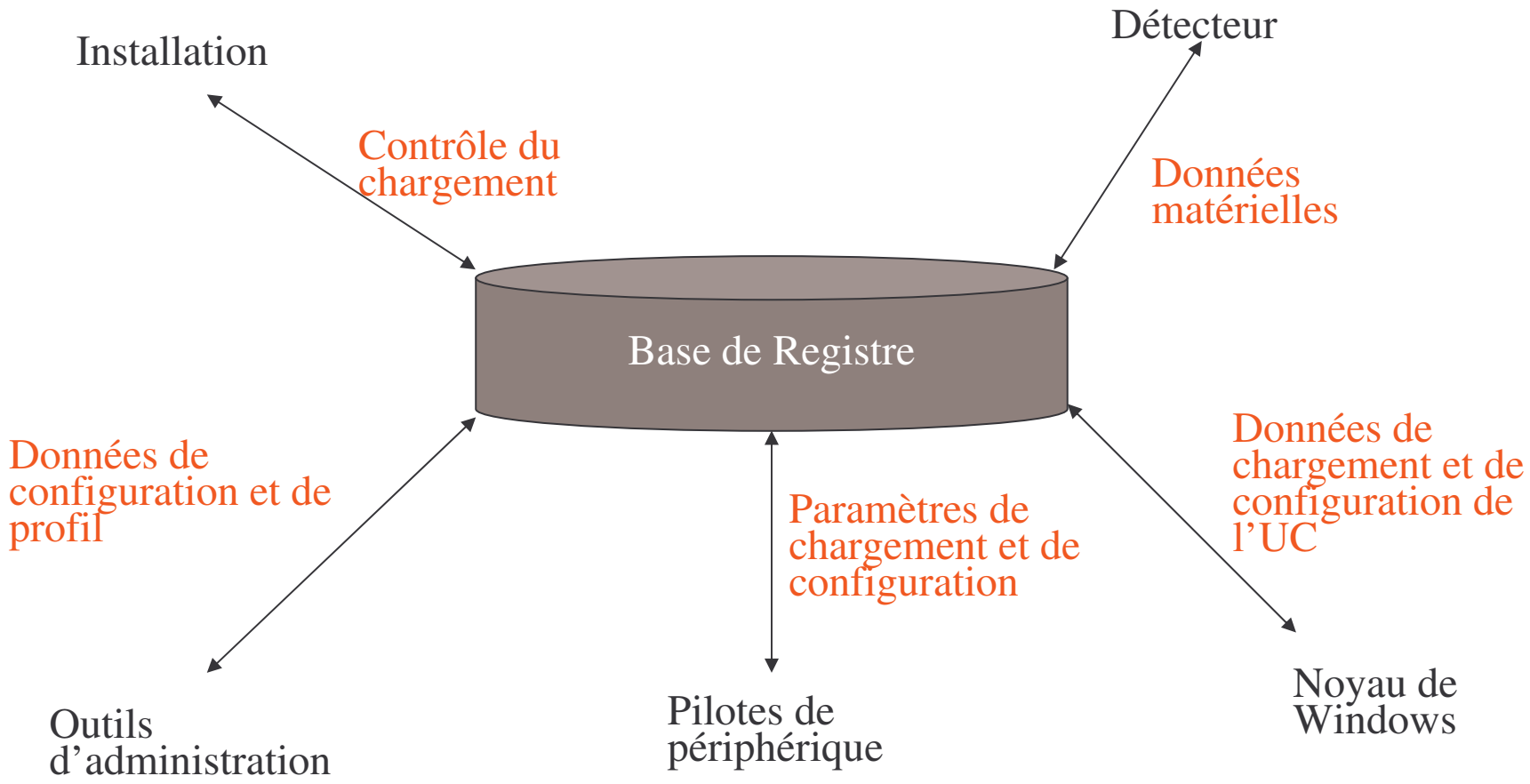
Chaque clé ou sous-clé du Registre peut contenir des données appelées « valeurs » . Une rubrique comprend trois parties : le nom de la valeur, le type de données de la valeur et la valeur elle-même.

- Il existe trois types de valeurs :
  - Chaînes
  - Binaire
  - DWORD
- Leur utilisation dépend du contexte.

Arborescence du registre

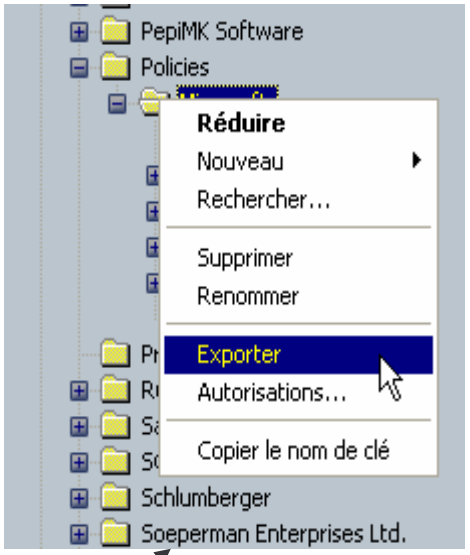
- Chaque valeur de base de registre est établie sous la forme de l'un des cinq types de données principales suivantes :
  - REG_BINARY (Contient la valeur sous forme d'une ligne de donnée binaire : informations concernant les composants matériels.)
  - REG_DWORD (Représente les données par un nombre de quatre octets et est couramment utilisé pour les valeurs booléennes (0 : désactivé, 1 : activé).)
  - REG_EXPAND_SZ (Ce type est une chaîne de données extensible dont la chaîne contient une variable qui sera remplacée quand elle est appelée par une application. Par exemple "%SystemRoot%" → répertoire actuel des fichiers système de Windows.
  - REG_MULTI_SZ (Ce type est une chaîne multiple, représente les valeurs qui contiennent des valeurs de liste ou multiples.)
  - REG_SZ (Ce type est une chaîne standard, représente des valeurs de texte contrôlables.)

Récapitulation



Exporter

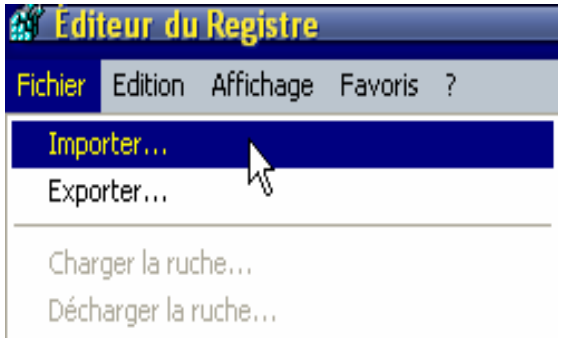
- Création d'un fichier avec une extension .reg.
- Ce fichier ainsi créé représente l'ensemble des informations de la clé ou de la sous-clé avec toutes les valeurs et les données que vous sélectionnez.
- Il est important de lui donner un nom "parlant" qui vous permettra par la suite de le retrouver si le besoin s'en fait sentir.



Pour exporter : dans la partie gauche du registre, faites un clic droit sur la clé en question puis choisissez ***Exporter***. Une fenêtre va s'ouvrir, choisissez le dossier dans lequel vous allez garder ce fichier puis enregistrez-le.

Importer

- La fonction ***Importer*** vous permet de fusionner le contenu d'un fichier registre avec une extension **.reg**.



Pour importer : Dans le menu du haut de l'Éditeur du registre, allez dans *Fichier* puis choisissez ***Importer....*** Une fenêtre va s'ouvrir, choisissez le dossier dans lequel vous allez récupérer le fichier puis cliquer sur *Ouvrir*. Votre fichier est enregistré dans votre registre.

Modifier

- Exemple : vous souhaitez remettre les infos-bulles par défaut dans Windows.

Rendez-vous à la clé **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced.** Cherchez le nom de la valeur : ***EnableBalloonTips*** et modifiez la donnée de la valeur, comme sur l'image ci dessous :

1 = pour réactiver l'option (remet les infos-bulles par défaut),
0 = pour désactiver l'option (désactive les infos-bulles).

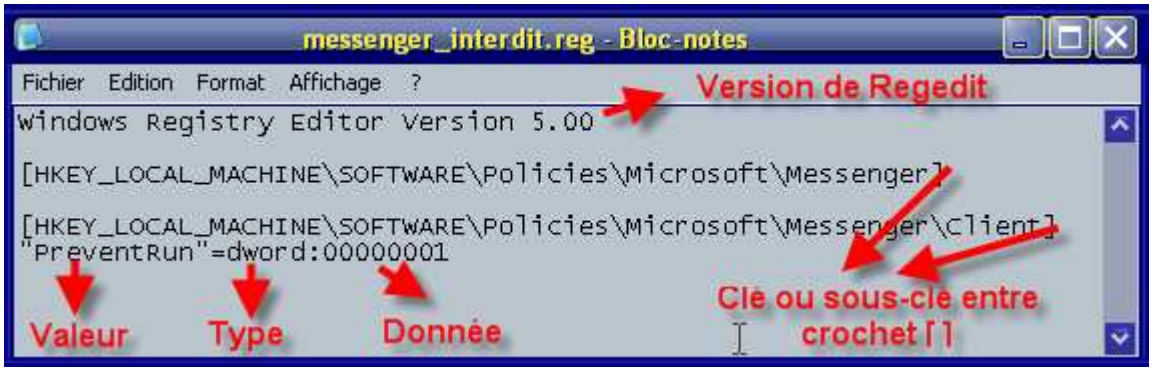
Créer

- Ajouter de nouvelles valeurs dans le registre ne s'improvise pas, il est important de consulter différents sites réputés afin de constater la véracité de cette valeur, son utilité, sa fonction, etc.

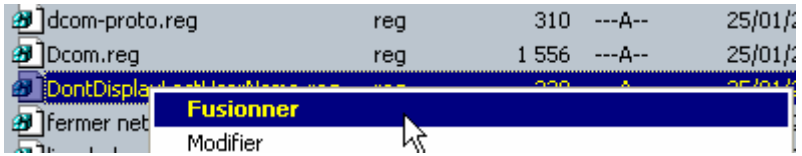
Pour créer :
une sous-clé → clic droit dans la partie gauche de regedit → inscrivez le nom de la nouvelle clé
une valeur → clic droit dans la partie droite de regedit → choisissez le type de valeur

Créer

- Création d'un fichier .reg.



- Clic droit dessus et choisir Fusionner dans le menu contextuel pour qu'il inscrive les valeurs dans le registre.



Créer

- On peut ajouter diverses clés les unes à la suite des autres et joindre un commentaire pour chacune des clés.

```
Windows Registry Editor Version 5.00

;-------------------------------------
;Optimisation du système le 10/10/2003
;-------------------------------------

;Désactivation de la visite guidée de Windows
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Applets\Tour]
"RunCount"=dword:00000000

;Arrêt plus rapide du système
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control]
"WaitToKillServiceTimeout"="3000"

;Conserver la connexion active lors du changement d'utilisateur
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"KeepRasConnections"="1"

; etc.
```

Supprimer

- Pour supprimer une valeur, il suffit d'attribuer le signe (moins) "-" à la valeur à supprimer :

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableRegistryTools"=-
```

- Pour supprimer une clé, il suffit d'attribuer le signe (moins) "-" devant le nom de la clé à supprimer et après le crochet [.

```
Windows Registry Editor Version 5.00

[-HKEY_LOCAL_MACHINE\Software\Symantec\Nom_de_la_cle]
```

Nettoyer le registre

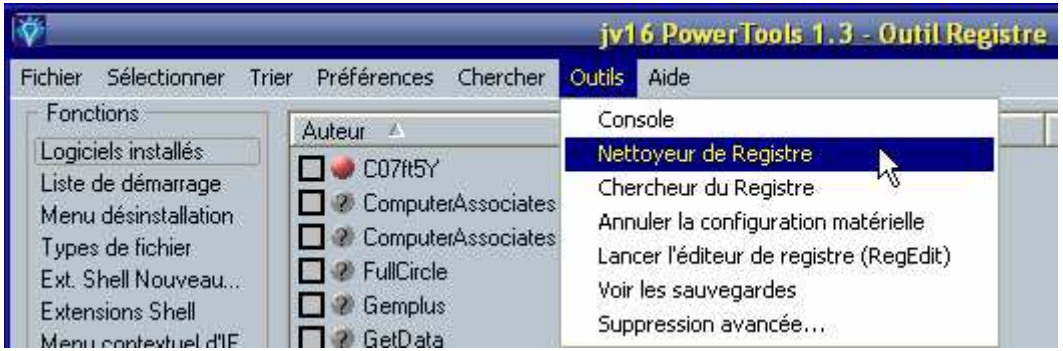
- Pourquoi faire le ménage dans le registre ?

  - Supprimer toutes les entrées qui n'ont plus de références sur votre système (ces entrées sont dites "obsolètes").

  - Il est difficile et fastidieux de nettoyer le registre manuellement, c'est pourquoi il est intéressant d'utiliser quelques outils spécialisés dans le domaine : JV16, RegCleaner, RegSeeker, RegSupreme, etc.

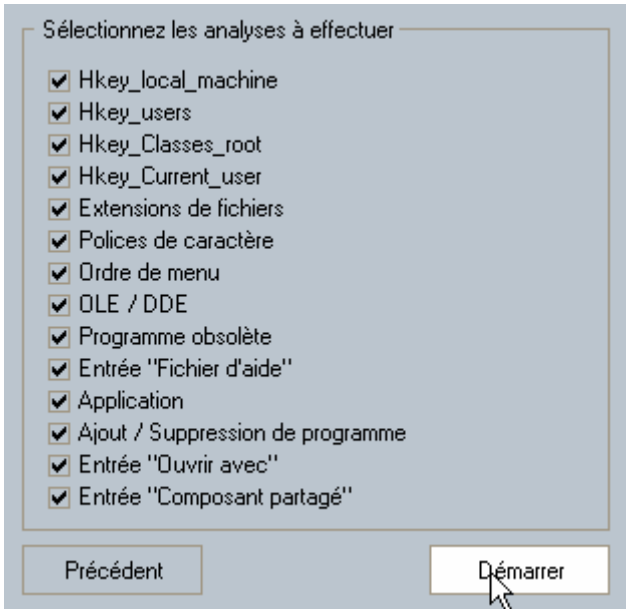
Nettoyer le registre

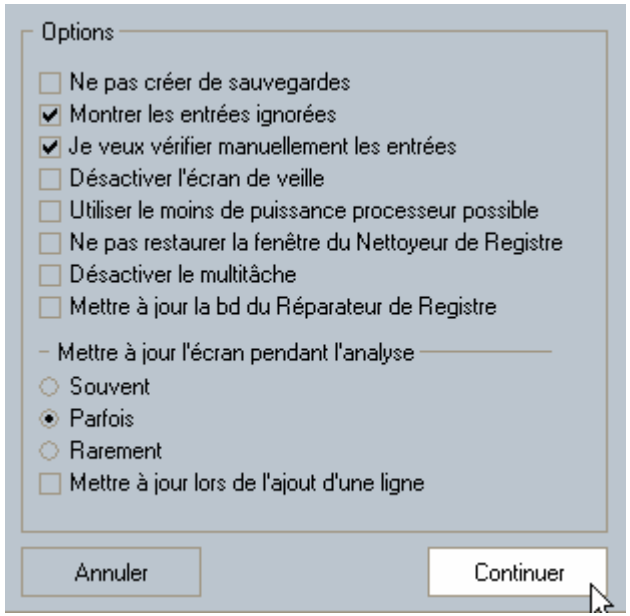
- JV16 PowerTools
  - Démarrer JV16 → Allez dans le menu "Outils" → Nettoyeur de registre.



Nettoyer le registre

- JV16 PowerTools
  - Les 2 écrans suivants permettent de paramétrer les options :





Nettoyer le registre

- JV16 PowerTools
  - Le scan des entrées de registre commence :

Nettoyer le registre

- JV16 PowerTools
  - Si vous souhaitez savoir où se trouve la ligne en question dans votre registre, cliquez sur "RegEdit" :

Regedit s'ouvre sur la clé, il suffit alors de vérifier la valeur dans la partie de droite pour contrôler.

Rechercher

- Cette fonction est la suite logique d'un nettoyage réalisé par logiciel car elle permet de vérifier la présence d'autres clés ou valeurs non supprimées par les logiciels de nettoyage automatique.

- La recherche commence :

Rechercher

- Pour une recherche sur l'ensemble du registre il faut se mettre sur poste de travail. Dès l'instant où regedit trouve une entrée, il s'arrête :

Si l'entrée que vous cherchez correspond au logiciel, vous pouvez supprimer la clé ou la valeur donnée. Ensuite, appuyez sur la touche F3 de votre clavier pour continuer votre recherche, et ainsi de suite jusqu'à ce que la recherche s'arrête.

- Outil presque identique à JV16 :
  - RegSeeker
  - RegSupreme

Sauvegarder

- Pourquoi sauvegarder le registre ?
  - Pour mettre le système à l'abri d'une défaillance et ainsi le restituer dans un parfait état de fonctionnement.
  - Dans la famille 2000/XP, il n'est pas possible de sauvegarder l'ensemble de la base de registre, la ruche SECURITY est inaccessible et certaines clés sont carrément interdites même en lecture.

Sauvegarder

- On trouve des utilitaires sur Internet : Erunt en fait partie.

  - Erunt copie simplement les ruches au format binaire qui se trouvent dans C:\Windows\System32\Config\ et le ou les fichiers des sessions : C:\Documents and Settings\%USERPROFILE%\ntuser.dat.

- Pour créer une sauvegarde, il est impératif que votre système soit en parfait état de fonctionnement, sain et exempt de tout malwares, sinon cela n'a aucun intérêt.

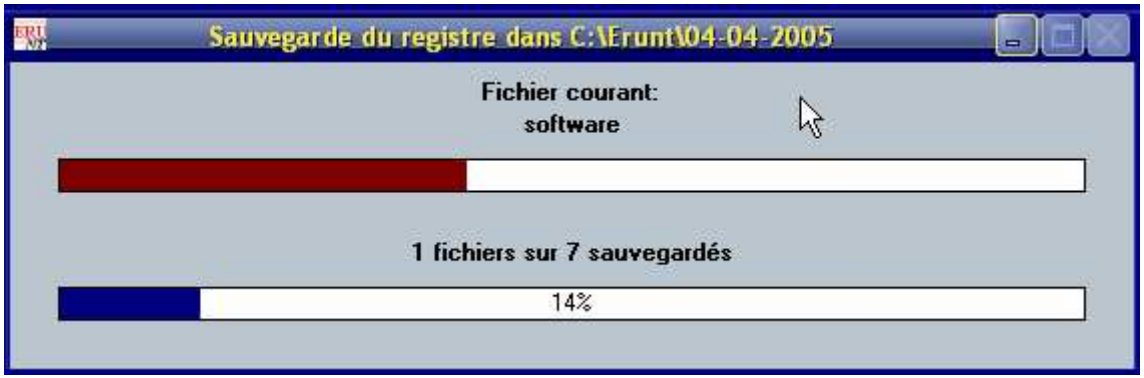
Sauvegarder

- La sauvegarde en image
  - Créez un dossier spécial pour vos sauvegardes (dans notre exemple C:\Erunt\) :

S'il existe plusieurs sessions, cochez la case destinée à cet effet.

Sauvegarder

- La sauvegarde en image
  - Cliquez sur "OK" → la sauvegarde commence :



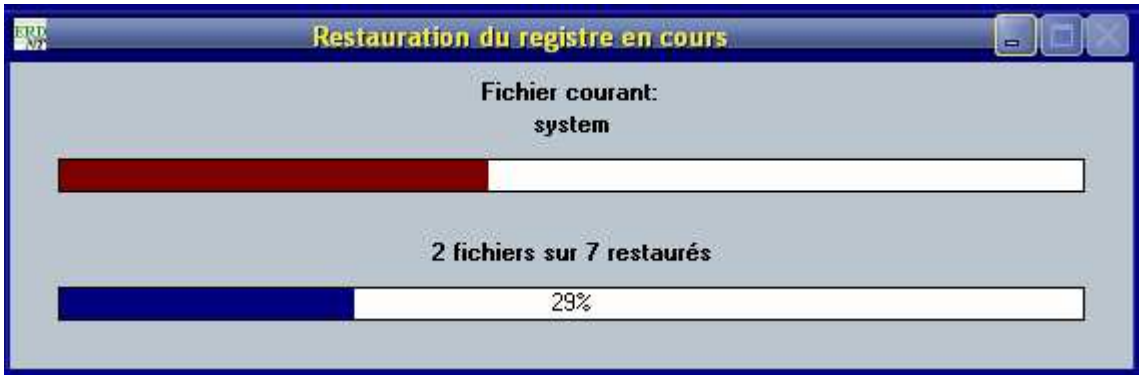
  - Erunt enregistre les fichiers :
ntuser.dat(ici 2), default, SAM, SECURITY, software, system dans le dossier :
C:\Erunt\(date de la sauvegarde)\

Sauvegarder

- La restauration en image
  - Ouvrez votre Explorateur à l'endroit où est créé votre sauvegarde, dans notre cas C:\Erunt\(date de la sauvegarde)\
    Cliquez ensuite sur ERDNT.EXE.

Sauvegarder

- La restauration en image
  - Cliquez sur "OK" → la restauration commence :



La restauration est terminée, redémarrez simplement votre ordinateur.

Sauvegarder

- Utilisez Erunt en cas de crash système
  - Démarrer votre système en mode console de récupération et copiez vos fichiers :

```
copy c:\Erunt\(date de la sauvegarde)\system c:\windows\system32\config\system
copy c:\Erunt\(date de la sauvegarde)\software
c:\windows\system32\config\software
copy c:\Erunt\(date de la sauvegarde)\sam c:\windows\system32\config\sam
copy c:\Erunt\(date de la sauvegarde)\security c:\windows\system32\config\security
copy c:\Erunt\(date de la sauvegarde)\default c:\windows\system32\config\default
copy c:\Erunt\(date de la sauvegarde)\Users\0000001\ntuser.dat c:\Documents And
settings\Session\ntuser.dat
```

- Outil presque identique à Erunt : NTREGOPT.

Clés à surveiller

- La liste des clés les plus connues où l'on peut trouver des entrées néfastes.

Démarrage automatique

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_USER\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_USER\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_USER\S-1223-etc\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_USER\S-1234-etc\Software\Microsoft\Windows\CurrentVersion\RunOnce

Clés à surveiller

Menu démarrer → Programmes → Démarrage

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

Application d'ouverture UserInit

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\UserInit
HKEY_LOCAL_MACHINESOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Appinit_Dlls

Clés à surveiller

Addons Explorer

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\shell Extension\Approved
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskSheduler
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell ServiceObjectDelayLoad
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explore\Browser Helper Object
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explore\ShellExecuteHooks

Démarrage de l'environnement

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\Shell

Clés à surveiller

Autres endroits susceptibles de contenir des entrées néfastes

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Windows\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Windows\Load
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Scripts\Logon
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Scripts\Logon

D'autres outils spécifiques qui aident à vérifier ces clés : HijackThis ou Autoruns,…

Quelques outils

- **RegMedic** :
  - Répare la base de registre aisément
  - Restaure aisément la base de registre sans avoir à réinstaller Windows.
  - Peut également désinstaller Internet Explorer et réinstaller tout autre programme.
  - Peut restaurer la base de registre du jour où vous avez installé Windows sans désinstaller aucun programme.
  - Enregistrer la base de registre à tous moment pour afin de la réparer plus tard en cas de problèmes et toujours sans avoir à formater le disque dur.

Quelques outils

- **Advanced Registry Tracer (plus intéressant)**
  - Permet de créer des images de la base de registre Windows afin de les comparer et de voir apparaître les modifications qui y ont été apportées.
  - Il est possible de ne comparer que certaines clés de la base de registre ou bien d'exclure une partie de l'arbre de l'opération de comparaison afin d'accélérer le processus.
  - Une option permet de restaurer une base de registre sauvegardée.

Quelques outils

- **RegCleaner (le plus connu)**
  - Nettoyer la base de registre de Windows : RegCleaner permet de faire le ménage dans la base de registre en supprimant les entrées inutiles.
  - Il affiche les clés qu'il n'est pas "trop risqué" de supprimer : logiciels, liste de démarrage, menu désinstallation, type de fichiers, nouveau fichier, intégration shell.
  - Les novices se contenteront d'utiliser les options de nettoyage automatique et les experts se permettront d'effacer en plus manuellement certaines entrées qu'ils considèrent obsolètes.

Quelques outils

- **Registry Tuner (En vogue)**
  - Modifiez votre base de registre avec l'aide d'un assistant.
  - Grâce à un classement par thème (différent du classement standard de la base de registre) les entrées sont facilement modifiables.
  - Pour chaque entrée documentée dans le programme, un commentaire vous indique les modifications à faire pour "tweaker" votre base de registre.
  - Plus de 350 entrées sont prédocumentées et il est possible d'en rajouter en les classant par catégories.

Quelques outils

- **Registrar Lite**
  - Éditeur de base de registre gratuit et plus puissant que regedit.
  - Registrar Lite se substitue à l'utilitaire "regedit" livré avec Windows en apportant plusieurs fonctionnalités :
    - Gestion de "Favoris" (clés souvent visitées)
    - Importation et exportation de clés de base de registre au format compatible .reg
    - Recherche/replacement en tâche de fond
    - Interface ergonomique ressemblant à l'explorateur Windows.

Exemple 1

- Administration :
  - Le but est de déployer facilement des applications ou des services sur un parc de machine plus ou moins important.

Exemple : Openoffice ou Msoffice offre la possibilité d'une installation au travers du réseau. Vous effectuez l'installation du serveur, puis une installation particulière (avec l'option -net ou /net) permet à l'application d'utiliser le serveur et d'installer sur le client qu'une version légère. De cette manière, vous évitez de charger l'espace disque des clients au détriment de communications réseaux.

Dans le cas général, l'application n'est pas écrite pour fonctionner en réseau et n'offre pas de possibilités de ce type.

Exemple 1

- Comment faire pour que les clients puissent utiliser l'application en réseau ?
  - Vous pouvez alors simplement mettre les fichiers sur votre serveur de fichiers (les clients y accèdent via un lecteur réseau). En partageant que les fichiers, il manque des instructions de l'installation classique.
  - Vous installez l'application une unique fois en prenant soin de sauvegarder la base de registre avant ET après l'installation.
  - Avec l'outil de votre choix, vous fabriquez un fichier REG qui correspond à la modification de la base de registre liée à l'installation effectuée (Attention, certaines clés vont faire référence à un chemin qui correspond à l'installation locale, il faut faire quelques petites modifications)

Exemple 1

- Comment faire pour que les clients puissent utiliser l'application en réseau ?
  - …
  - Vous éditez et modifiez dans les clés les chemins pour faire apparaître le lecteur réseau (votre serveur de fichiers où se trouve les fichiers de l'application).
  - Vous Exécutez le fichier REG sur l'ensemble des clients. Vous obtenez une application utilisable sur le réseau sans pour autant qu'elle opère des communications réseaux, seul le démarrage nécessite de la ressource réseau.

AVANTAGES : la mise à jour est effectuée qu'une seule fois. Les clients seront mis à jour facilement par un petit script qui exécutera le fichier REG correspondant aux mise à jour sans devoir ré-installer l'ensemble du parc.

Exemple 2

- Lorsqu'un fichier n'est pas associé à un programme il est difficile de le consulter il faut passer par "ouvrir avec", puis parcourir tous les programmes, en choisir un, confirmer ...

Nous vous proposons d'écrire un fichier REG qui va ajouter "Edit TXT" pour tous les fichiers dans le menu contextuel de l'explorateur Windows simplement en cliquant droit sur le fichier

- Dans quelle partie de la base de registre allez-vous travailler ?
- Pour quel type de fichiers souhaitez-vous offrir cette possibilités ?
- Que s'agit-il de faire ?
- Que proposez-vous ?
- Que devez-vous faire ?

Exemple 2

- Dans quelle partie de la base de registre allez-vous travailler ?
  - HKEY_CLASSES_ROOT
- Pour quel type de fichiers souhaitez-vous offrir cette possibilités ?
  - TOUS
- Que s'agit-il de faire ?
  - Proposez une nouvelle possibilité d'exécution du fichier à l'aide d'une commande SHELL
- Que proposez-vous ?
  - Edit TXT
- Que devez-vous faire ?
  - Exécuter notepad sur le fichier (%1 paramètre) pour l'ouvrir

Exemple 2

- Contenu du fichier

```
Résultat : EditTXT.reg
REGEDIT4


[HKEY_CLASSES_ROOT\*\shell]

[HKEY_CLASSES_ROOT\*\shell\Edit TXT]

[HKEY_CLASSES_ROOT\*\shell\Edit TXT\command]
@="notepad %1"
```

Exemple 3

- Créer un fichier REG pour lancer une application (programme créé par vous).

  Le fichier REG que vous devez écrire doit lancer le programme GetFileName (programme qui copie le chemin absolu du fichier dans le presse-papier) et doit "Récupère le nom" dans le menu contextuel de l'explorateur Windows en cliquant droit sur un fichier sur le fichier

  - Dans quelle partie de la base de registre allez-vous travailler ?
  - Pour quel type de fichiers souhaitez-vous offrir cette possibilités ?
  - Que s'agit-il de faire ?
  - Que proposez-vous ?
  - Que devez-vous faire ?

Exemple 3

- Dans quelle partie de la base de registre allez-vous travailler ?
  - HKEY_CLASSES_ROOT
- Pour quel type de fichiers souhaitez-vous offrir cette possibilités ?
  - TOUS
- Que s'agit-il de faire ?
  - Proposez une nouvelle possibilité d'exécution du fichier à l'aide d'une commande SHELL
- Que proposez-vous ?
  - Récupérez le nom
- Que devez-vous faire ?
  - Exécuter GetFileName.exe sur le fichier (%1 paramètre) pour l'ouvrir

Exemple 3

- Contenu du fichier

```
Résultat : GetFileName .reg
REGEDIT4


[HKEY_CLASSES_ROOT\*\shell]

[HKEY_CLASSES_ROOT\*\shell\Récupère le nom]

[HKEY_CLASSES_ROOT\*\shell\Récupère le nom\command]
@=" GetFileName.exe %1"
```

Fichiers .inf et .reg

- Quelles différences entre fichiers REG et fichiers INF ?
  - fichier REG permet de modifier, ajouter ou supprimer des clés de la base de registre,
  - fichier INF permet de modifier supprimer ou ajouter des clés de la base de registre MAIS AUSSI permet d'ajouter , copier des fichiers depuis un répertoire source vers un répertoire destination. Cela permet également de faire des modifications liés à l'installation.

Fichiers .inf

- Organisés en plusieurs sections associées à des fonctions particulières allant de la gestion des fichiers jusqu'à la modification de la base de registres en passant par les fichiers INI.
- Respectent les règles suivantes :
  - Les sections commencent avec un nom de section entouré de crochets.
  - la section [Version] identifie la compatibilité
  - L'utilisation de variable est possible en utilisant la syntaxe %nom_de_la_variable%. Les variables sont définies dans la section [Strings]. Pour utiliser le caractère % dans une chaîne, il faut utiliser la syntaxe suivante : %%

Fichiers .inf

Applications:

- Installation d'un driver (Détection d'un nouveau périphérique), ou d'un module Windows.
- Installation automatique d'un programme (notamment pour installer un programme à l'insu d'un utilisateur).
- Modification d'un INI ou d'une entrée dans la base de registre lors du script de connexion.

Fichiers .inf

Types de section **Description**

- **Add Registry :** Ce type de section permet d'ajouter des entrées dans la base de registres.
- **ClassInstall32 :** Ce type de section permet d'installer une nouvelle classe.
- **Copy Files :** Ce type de section permet de copier une sélection de fichiers
- **Delete Registry :** Ce type de section permet de supprimer des entrées dans la base de registres.
- **Delete Files :** Ce type de section permet de supprimer une sélection de fichiers.
- **DestinationDirs :** Cette section permet de définir le répertoire de destination de chaque sélection de fichiers.
- **Device :** Cette section donne les spécifications pour l'installation d'un périphérique.
- **EventLog Install :** Permet d'ajouter ou de supprimer un message d'évènement dans la base de registre.
- **Ini File to Registry :** Déplace une ligne ou une section d'un fichier INI vers la base.
- **Install :** Cette section permet d'identifier les sections du fichier INF.

Fichiers .inf

Types de section **Description**

- **Log Config :** Cette section permet de définir les paramètres du périphérique (IRQ, DMA, ...) à installer.
- **Manufacturer :** Cette section permet d'identifier le constructeur du périphérique à installer.
- **Rename Files :** Ce type de section permet de renommer une sélection de fichiers.
- **Service Install :** Cette section installe les services spécifiées dans la section Service.
- **Services :** Ce type de section permet d'ajouter ou de supprimer un service au système.
- **Strings :** Cette section permet d'initialiser les variables utilisées dans les autres sections.
- **Update INI Fields :** Ce type de section permet de modifier une partie d'une entrée dans une section d'un fichier INI.
- **Update INI File :** Ce type de section permet de modifier une entrée complète dans une section d'un fichier INI.

Fichiers .inf

Exemple :

- Section [CopyFiles] :
  - Permet de faire une sélection de fichiers à copier. Les répertoires sources et destination sont repris dans d'autres sections du fichier INF. Le nom d'une section de type "Copy files" doit apparaître dans la section [Install] avec l'étiquette CopyFiles.
- Syntaxe :
  - [file-list-section]
  - dst-file-name[,src-file-name][,tmp-file-name][,flag]

Fichiers .inf

Paramètres	Valeurs
dst-file-name	Nom du fichier de destination.
Src-file-name	Nom du fichier source. Ce paramètre n'est pas obligatoire si le nom de fichier source et le nom de fichier de destination sont identiques.
Tmp-file-name	Nom du fichier temporaire généré pendant l'installation, le vrai nom sera donné au prochain démarrage

Fichiers .inf

flag Optionnel. Ce flag est utilisé pour définir le mode de copie du fichier.

- COPYFLG_WARN_IF_SKIP (0x00000001) : Envoie un message si l'utilisateur annule la copie du fichier.
- COPYFLG_NOSKIP (0x00000002) : L'utilisateur ne peut pas annuler la copie.
- COPYFLG_NOVERSIONCHECK (0x00000004) : Ignore la version du fichier et écrase le fichier s'il est déjà existant.
- COPYFLG_FORCE_FILE_IN_USE (0x00000008) : Force la copie des fichiers en cours d'utilisation.
- COPYFLG_NO_OVERWRITE (0x00000010) : Ne remplace pas le fichier quand il existe déjà dans le répertoire de destination.
- COPYFLG_NO_VERSION_DIALOG (0x00000020) : Remplace le fichier qui existe dans le répertoire de destination uniquement si le nouveau fichier est une version supérieure.