Labo Windows: Opdracht 06: Het Register

Achtergrond

1. Inleiding

Het register van Windows is een soort van databank. Deze is noch relationeel, noch geïndexeerd. De gewone gebruiker komt normaal niet rechtstreeks in aanraking met het register. Het wordt echter voortdurend gebruikt door Windows en programma's die er al hun instellingen in opslaan.

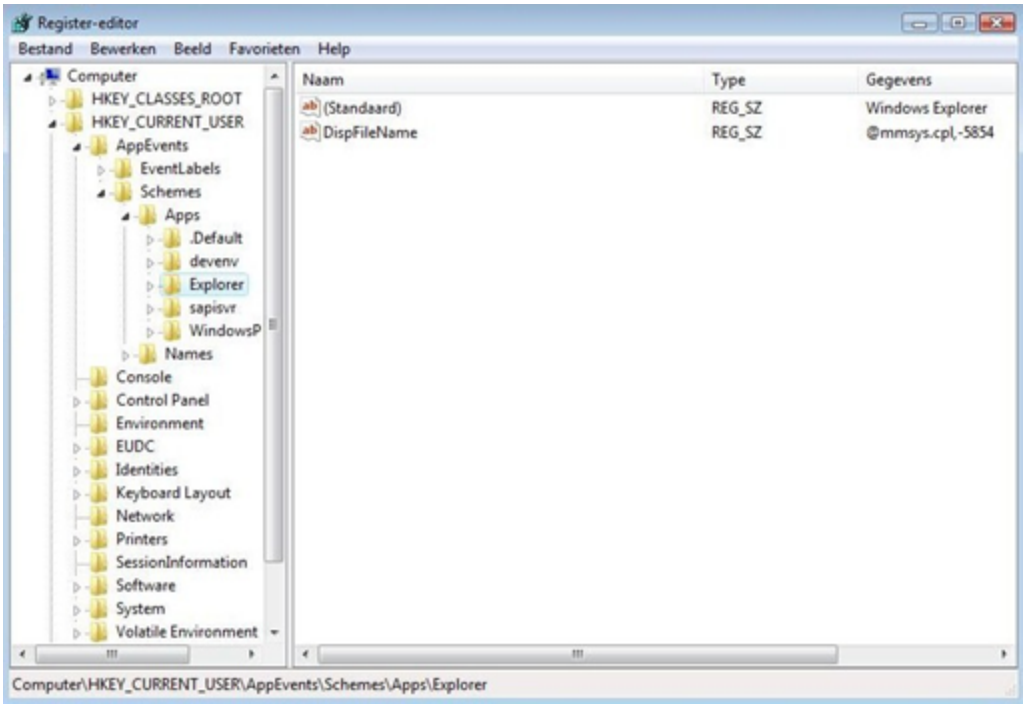
Windows beschikt over veel meer instellingen dan enkel deze die grafisch toegankelijk zijn. Veel van die instellingen zijn echter te gecompliceerd voor de doorsnee gebruiker. Om die instellingen te veranderen of te raadplegen moet men zelf in het register ingrijpen.

Veiligheid

Via het register kan men zowat alles aanpassen. Gelukkig is het goed beschermd om ongelukken te voorkomen. Enkel beheerders hebben toegang tot het volledige register, de gewone gebruiker heeft enkel toegang tot zijn instellingen. Maak steeds eerst een herstelpunt of een backup vooraleer iets te veranderen.

De registereditor

Het register kan geopend worden met de opdracht `regedit` via Start > Uitvoeren.



Figuur: De Windows registereditor

2. De opbouw

Het register bestaat uit vijf subtrees:

- `HKEY CLASSES ROOT`
- `HKEY CURRENT USER`
- `HKEY LOCAL MACHINE`
- `HKEY USERS`
- `HKEY CURRENT CONFIG`

Elk van deze subtrees heeft een set aan sleutels en waarden, bv:

```
HKEY CURRENT USER\Software\Microsoft\Windows\CurrentVersion\Policies
```

Betekenis van de subtrees

- `HKEY CLASSES ROOT`: bevat informatie over bestandstypen en dergelijke
- `HKEY CURRENT USER`: instellingen betreffende de huidige gebruiker
- `HKEY LOCAL MACHINE`: informatie over soft- en hardware op uw PC
- `HKEY USERS`: instellingen i.v.m. de afzonderlijke gebuikers
- `HKEY CURRENT CONFIG`: informatie over de huidige hardwareconfiguratie

De indeling

Het register heeft een ingewikkelde structuur met talloze lagen van sleutels en subsleutels. Onderaan in de statusregel van de registereditor wordt steeds het volledige pad weergegeven

van waar men zicht bevindt.

In het rechtste deel van de registereditor ziet men de instellingen van de huidige geselecteerde sleutel. Deze instellingen bevatten steeds een naam, het type en de feitelijke data.

Gebruikte datatypes

Voor de waarden van de sleutels worden er verschillende datatypes gebruikt:

- `REG SZ`: tekststrings
- `REG EXPAND SZ`: tekststrings die ook variabelen kunnen bevatten, bv. %systemroot%
- `REG MULTI SZ`: array van tekststrings
- `REG DWORD`: integer (4 bytes)
- `REG BINARY`: bitwaarde
- `REG FULL RESOURCE DESCRIPTOR`: gebruikt door hardwaredrivers om informatie te bewaren, deze waarde kan verschillende parameters bevatten
- `REG RESOURCE LIST`: enkel in het hardwaregedeelte, bevat meestal numerieke informatie over de gebruikte PC-bus

Opdeling

Het register kan opgedeeld worden in twee grote delen:

1. Machineinespecifiek: alle ingangen onafhankelijk van de gebruiker:
   `HKEY LOCAL MACHINE`, `HKEY CURRENT CONFIG` en `HKEY CLASSES ROOT`

2. Gebruikersspecifiek: alle ingangen afhankelijk van de gebruiker:
   `HKEY USERS` en `HKEY CURRENT USER`

Van de 5 opgenoemde subtrees zijn er eigenlijk maar twee echte, `HKEY USERS (HKU)` en `HKEY LOCAL MACHINE (HKLM)`. De andere zijn “links” *(verwijzingen)* naar `HKU` en `HKLM`.

HKCU: HKEY CURRENT USER

Deze subtree is een speciaal geval. Als een gebruiker inlogt worden zijn persoonlijke instellingen tijdelijk geladen in het register onder de `HKCU` subtree. Diezelfde gegevens vindt men ook in `HKU` SID value. De SID value heeft een waarde van `S-1-5-21` voor de huidige aangelogde gebruikers.

HKLM: HKEY LOCAL MACHINE

Deze sleutel bevat de volgende instellingen:

- `BCD00000000`
  Bevat de entry uit de Boot Configuration Data

- `Hardware`
  Wordt gecreëeerd tijdens de eerste keer opstarten, bevat dynamische informatie i.v.m. de hardware, bv: CPU-type, gebruikte poorten, naamgeving apparaten, . . .

- `SAM`
  Bevat informatie over de locale accounts wanneer men zich niet in een domein bevindt. SAM kan niet rechtstreeks bekeken worden.

- `Security`
  Bevat instellingen en rechten van de gebruikers

- `Software`
  Configuratie van Windows zelf, hier worden apparaten en services gedefinieerd, de laatste goede instelling staat hier ook

Register hives

Het register is zoals eerder vermeld een soort databank. Deze is opgebouwd uit verschillende bestanden die bewaard worden op de harde schijf (de hives). De meeste daarvan worden bewaard onder `%systemroot%\system32\config`.

De registerinstellingen van de huidige gebruiker staan in zijn `Documents and Settings` map. Er zijn twee versies: de hive en het logbestand (respectievelijk `ntuser.dat` en `ntuser.dat.log`).

De locatie van de andere hives:

Register hive	Bestand op schijf
HKEY_LOCAL_MACHINE\BCD00000000	%SystemDrive%\boot
HKEY_LOCAL_MACHINE\SAM	%SystemRoot%\System32\Config\Sam
HKEY_LOCAL_MACHINE\Security	%SystemRoot%\System32\Config\Security
HKEY_LOCAL_MACHINE\Software	%SystemRoot%\System32\Config\Software
HKEY_LOCAL_MACHINE\System	%SystemRoot%\System32\Config\System
HKEY_CURRENT_CONFIG	%SystemRoot%\System32\Config\System

3. Importeren en exporteren

Exporteren

Het register kan weggeschreven worden naar een bestand met `*.reg` als extensie. Het

volledige register van een verse Windows is zo'n 25 tot 30 MB groot. Daarom is het beter om afzonderlijke sleutels te exporteren. Zo kan men bijvoorbeeld zijn faxinstellingen opslaan en deze verplaatsen naar een andere PC.

Het registerbestand

Het geëexporteerde bestand bevat gewoon platte tekst. De eerste regel ervan toont de versie van de registereditor. Daaronder volgt de naam van de sleutel en de daarbijhorende gegevens, bijvoorbeeld:

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Fax\UserInfo]
"FullName"="Jan Janssens"
"FaxNumber"="093268899"
```

Importeren

Dit kan via het menu van de registereditor of door te dubbelklikken op het te importeren registerbestand. Let op: het importeren kan instellingen onheroepelijk veranderen. Maak best steeds eerst een herstelpunt of een backup van het register / jouw gegevens.

4. Voorbeelden

4.1 3D-text

Onderstaand voorbeeld stelt 3D-text schermbeveiliging in via het register. Onderneem de volgende stappen:

1. Controleer de huidige schermbeveiliginginstelling
2. Zoek naar deze tekst in het register
3. De sleutel die weergegeven wordt is:
   `HKEY CURRENT USER\Software\Microsoft\Windows\CurrentVersion\Screensavers\ssText3d`
4. Naast de tekstinhoud vindt men hier ook de fontgrootte, lettertype, . . .
5. Men kan hier nu rechtstreeks de registerwaarde veranderen door te kiezen voor “Tekenreeks bewerken"

4.2 Bestandsextensies

Om extensies van bestanden weer te geven (of te verbergen), volg je deze stappen:

1. Open de register-editor en blader naar:
   `HKEY CURRENT USER\Software\Microsoft\Windows\CurrentVersion\Explorer`
2. Kies daar voor de sleutel: `Advanced`
3. Verander de waarde van de sleutel `HideFileExt` naar `0` (of `1` om te verbergen)

4.3 Snelmenu

Nieuwe opties (bv. Naar map kopiëren) toevoegen aan het snelmenu gebeurt als volgt:

1. Open de register-editor en blader naar
   `HKEY CLASSES ROOT\*\shellex\ContextMenuHandlers`
2. Creëer daar een nieuwe sleutel met de naam `Copy To`
3. Bewerk de tekenreeks van het item (Standaard) en vul in:
   `{C2FBB630-2971-11d1-A18C-00C04FD75D13}`
4. Selecteer vervolgens de sleutel:
   `HKEY CLASSES ROOT\Directory\shellex\ContextMenuHandlers`
5. Maak daar dezelfde sleutel aan met dezelfde waarde
6. In je contextmenu staat nu een entry “Kopiëren naar map”

4.4 Startpagina Internet Explorer

De titelbalk van Internet Explorer wordt soms ongewild gewijzigd. Men kan dit herstellen of veranderen in het register:

1. Kies de volgende sleutel:
   `HKEY CURRENT USER\Software\Microsoft\Internet Explorer\Main`
2. Verander daar de waarde in “Start Page"
3. Start Internet Explorer op

4.5 Opstartbeheer

Na het inladen van Windows worden allerlei programma’s opgestart. Afhankelijk van de hoeveelheid hiervan kan dit je opstartprocedure aanzienlijk vertragen.

1. Kies de volgende sleutel:
   `HKEY CURRENT USER\Software\Microsoft\Windows\CurrentVerion\Run`
2. Verwijder de tekenreeksen die niet absoluut noodzakelijk zijn

5. Tweaken

Inleiding

Tweaken is het systeem zo optimaal mogelijk afregelen of volledig naar uw hand zetten zoals gewenst. Veel instellingen van Windows zijn echter niet rechtstreeks via een menu bereikbaar. Met speciale tweaktools kunnen soms zeer geavanceerde instellingen veranderd worden. Dit is vaak gemakkelijker dan het register zelf te editeren.

De tweaktools grijpen net zoals de registereditor rechtstreeks in op het register, tweaken kan daardoor gevaarlijk zijn. Maak dus steeds eerst een herstelpunt of een backup!

Voorbeelden

Enkele voorbeelden van wat bereikt kan worden m.b.v. tweaken:

- Mogelijke prestatiewinst (op uw systeem)
- Lijst recente documenten wissen bij afsluiten
- Swapbestanden verwijderen
- De laatst ingelogde gebruiker niet laten zien in het inlogvenster
- Instellen van transparatieëffecten
- Uitschakelen van irritante waarschuwingsballonnen
- Optimaliseren van netwerkverbindingen

Beschikbare tools

- Ultimate windows tweaker (gratis)
- Windows 7 manager (betalend)
- Tweak-7 (betalend – www.totalidea.com)
- ...

Handige website

Op www.pc-tools.com vindt men een zeer uitgebreid overzicht van de verschillende registerinstellingen (zowel voor Windows XP,Vista en 7)

- Windows besturingssysteem verbeteringen
- Windows tips en snelkoppelingen
- Netwerk en verbindingsverbeteringen
- Veiligheidsrestrities en systeem policies
- Hardware en aansluitingverbeteringen
- Verbeteringen voor Windows instellingen

LABO-GEDEELTE

Doelstellingen

- Opbouw register nagaan
- Instellingen van het register veranderen

Opgaven

6.1 Opbouw register

1. Meld je aan als beheerder en stel de screensaver van jouw virtuele computer in op 3D-tekst en zorg ervoor dat het woord “ikdoeict” weergegeven wordt.
2. Open de registereditor van uw virtuele PC en zoek naar de tree waar de gegevens staan van de huidige aangemelde gebruiker. Waar vind je die?
3. Kan je die ook op een andere plaats vinden?
4. Wat is de inhoud van de instelling `DisplayString` van de sleutel `ssText3d`? Gebruik hiervoor de zoekopdracht in de registereditor.
5. Verander deze tekst in het register in je eigen naam en bekijk opnieuw de waarde via het screensaver instelvenster. Wat is er gebeurd?
6. Onder welke subtree staat de sleutel `LastKnownGood`?

6.2 Instellingen veranderen

1. Zoek naar de sleutel die de lijst weergeeft met ingetikte URL's voor Internet Explorer van de huidige gebruiker. Maak die lijst leeg en controleer dit in de browser.
2. Verander de opgegeven MHz-waarde van uw CPU (`ProcessorNameString`), controleer dit via het configuratiescherm.
3. Zoek op in het register welke programma's bij het booten opgestart worden.

6.3 Exporteren/importeren

1. Exporteer alle gegevens van de huidige gebruiker naar een bestand, hoe groot is dit?
2. Exporteer alle gegevens van de sleutel `ssText3d` naar een bestand en geef dit bestand door aan uw gebuur. Laat uw gebuur de sleutel importeren. Wat is er gebeurd met de instelling van de screensaver?

6.4 Process Monitor

1. Download en installeer de tool Process Monitor (www.microsoft.com).
   Start het programma op en filter op het woord `ssText3d`
2. Verander nu via uw bureaublad/eigenschappen de instelling van uw schermbeveiliging naar 3D-tekst. Zet de tekst van de 3D-tekst op een andere waarde. Zoek dit in de output van de process monitor en noteer deze lijn in uw verslag.
   Welke filter heb je hiervoor gebruikt?

3. Start Wordpad op, en zoek met process monitor op waar hij de lijst met je recent gebruikte documenten ophaalt. Welke filter heb je hiervoor gebruikt?

6.5 Opbouw

1. Uit welke bestanden is het register opgebouwd?
2. In welk bestand vind je de persoonlijke data?