

# Windows - Registry

Die baumförmige **Registrierungsdatenbank** enthält Konfigurationsdaten von Betriebssystem und Programmen.

## Tools

**regedit.exe**

**Process Monitor (sysinternals.com)**

## Hauptschlüssel

HKEY_CLASSES_ROOT	HKEY_LOCAL_MACHINE\Software\Classes (Informationen über Dateitypen)
HKEY_CURRENT_USER	HKEY_USERS\SID des akt.Benutzers\ (Einstellungen des aktuellen Benutzers)
HKEY_LOCAL_MACHINE	Computerkonfiguration (Gerätemanager, Dienste, ...)
HKEY_USERS	Benutzerspezifische Einstellungen von allen angemeldeten Benutzern
HKEY_CURRENT_CONFIG	aktuelles Hardwareprofil unter HKEY_LOCAL_MACHINE

## Dateien

C:\Windows\System32\config\...

C:\Users\...\NTUSER.DAT HKEY\_CURRENT\_USER

## Datentypen eines Wertes

REG_SZ	Text
REG_BINARY	beliebig viele Bytes
REG_DWORD	32 bit
REG_QWORD	64 bit
REG_MULTI_SZ	mehrzeiliger Text
REG_EXPAND_SZ	Referenzen auf Text

## Beispiel

Schlüssel: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

Werteintrag: ProductName

Typ: REG\_SZ

Wert: Windows 7 Professional N