

Registryforensik

Relative Pfade

%UserProfile%	Pfad zum derzeitigen Benutzerprofil
%SystemDrive%	Laufwerksbuchstabe, auf dem Windows installiert ist, i.d.R. C:
%SystemRoot%	Pfad zum Windows Ordner, i.d.R. C:\Windows

Schlüssel & Werte

Ein Schlüssel enthält einen oder mehrere Werte sowie einen Zeitstempel des letzten Zugriffs

Jeder Wert hat 3 Felder:

Name	Eindeutig innerhalb eines Schlüssels
Typ	Datentyp des Wertes (s.u.)
Daten	kann leer oder null sein, Maximum 32767 Bytes, häufig in hexadezimaler Notation

Die wichtigsten Datentypen sind

REG_NONE	kein definierter Typ
REG_SZ	Fixe Länge und NULL-Char am Ende
REG_EXPAND_SZ	Variable Länge und NULL-Char am Ende
REG_BINARY	Binärdaten
REG_DWORD	Double-Word-Werte, häufig boolesche Werte
REG_LINK	Link
REG_MULTI_SZ	Liste von Strings

Struktur

Wurzelschlüssel

HKLM	HKEY_LOCAL_MACHINE	Hauptschlüssel
HKU	HKEY_HKU	Hauptschlüssel
HKCR	HKEY_CLASSES_ROOT	Verweis
HKCU	HKEY_CURRENT_USER	Verweis
HKCC	HKEY_CURRENT_CONFIG	Verweis

Verweise

HKCC	HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current
HKCU	HKU\S-1-5-21-xxx (SID)
HKCR	HKLM\SOFTWARE\Classes

HKU

Nutzerspezifische Einstellungen und Informationen für jeden aktiv geladenen Benutzer (Standardprofile und angemeldete Profile, keine abgemeldeten Nutzer)

.DEFAULT	Einstellungen, die Windows nutzt, bevor ein Nutzer sich eingeloggt hat
S-1-5-18	well-known SID für LocalSystem-Benutzer
S-1-5-19	well-known SID für LocalService-Benutzer, lokale Dienste, die den LocalSystem-User nicht benötigen
S-1-5-20	well-known SID für NetworkService-Benutzer, Netzwerkdienste, die den LocalService-Benutzer nicht benötigen
S-1-5-21- [...]	SID des derzeit angemeldeten Benutzers (Link von HKCU)
S-1-5-21- [...].Classes	Nutzerspezifische Dateiverknüpfungen

HKCU

Link auf HKU\[SID]

Spezifische Einstellungen und Informationen zum angemeldeten Benutzer (Umgebungsvariablen, Desktopeinstellungen, Netzwerkverbindungen, Drucker und Präferenzen)

AppEvents	Verknüpft Audiodateien mit Aktionen (z.B. Ton beim Öffnen eines Menüs)
Console	Daten zum Console-Subsystem (z.B. zum MS-DOS-Command-Prompt)
Control-Panel	Einstellungen der Systemsteuerung, u.a. regionale Einstellungen und Erscheinungsbild
Environment	Umgebungsvariablen, die Benutzer gesetzt haben
Keyboard-Layout	Installierte Tastaturlayouts
Network	Jeder Unterschlüssel ein Netzlaufwerk, Name des Schlüssels ist Laufwerksbuchstabe, enthält Konfigurationsdaten zum Verbinden
Printers	Präferenzen des Benutzers zum Drucken
Software	Nutzerspezifische Einstellungen zu installierten Programmen, je nach Programm Informationen zu Programmanbieter, Programm, Version, Installationsdatum und zuletzt zugriffene Dateien. Ablage nach HKCU\Software\Programmanbieter\Programm\Version
Volatile Environment	Umgebungsvariablen, die beim Login definiert wurden

HKLM

Spezifische Einstellugen des lokalen Rechners, die für alle Benutzer geladen werden.

HARDWARE	Speichert HW-Daten beim Systemstart, wird bei jedem Start erstellt und mit Informationen über Geräte, Treiber und Ressourcen gefüllt
SAM	Lokale Windows-Sicherheitsdatenbank über Benutzer- und Gruppeninformationen (Link zu HKLM\SECURITY\SAM)
SECURITY	Lokale Windows-Sicherheitsdatenbank (inklusive SAM)
SOFTWARE	Einstellungen zu Applikationen des Rechners (und Microsoft-Applikationen)
SYSTEM	Informationen zur Systemkonfiguration (z.B. Gerätetreiber und Dienste). Derzeitiges Hardwareprofil ist Link von HKCC. Mehrere Sätze mit Schema ControlSetxxx. HKLM\SYSTEM\Select zeigt aktuelle verwendetes Profil in CurrentControlSet.

HKCR

Link auf HKLM\Software\Classes & HKU\[SID]_Classes

- Zuweisungen für Dateierweiterungen
- OLE-Datenbank

- Einstellungen für registrierte Anwendungen für COM-Objekte
- Nutzer- und systembasierte Informationen

Setzt sich aus HKLM\SOFTWARE\Classes und HKU\[SID]_Classes zusammen. Falls identischer Wert, hat HKCU Priorität.

Beispiel: Was soll passieren, wenn eine .pptx-Datei geöffnet wird. HKCR macht einen erheblichen Teil der Registry und des Systemverhaltens aus

HKCC

Link auf HKLM\System\CurrentControlSet\Hardware Profiles\Current

Link zu den Konfigurationsdaten des derzeitigen Hardwareprofils. Informationen werden bei jedem Booten neu erzeugt und daher nicht physisch in der Registry-Datei gespeichert.

System
Software

Hives

User-Profile-Hives in %UserProfile%\NTUSER.DAT

Alle anderen Hives und Dateien in %SystemRoot%\System32\config

HKU\.DEFAULT	DEFAULT
HKLM\SAM	SAM
HKLM\SECURITY	SECURITY
HKLM\SOFTWARE	SOFTWARE
HKLM\SYSTEM	SYSTEM

Schlüssel HKLM\HARDWARE mit dynamischen Hive, wird beim Systemstart erstellt aber nicht gespeichert

Liste zu Standard-Hive-Files:

HKLM\SYSTEM\CurrentControlSet\Control\hivelist
Liste User-Hives: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

SID & SAM

Liste der SIDs

HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ProfileList
Pfad zu individuellen Profilen: ProfileImagePath

Aufbau der SID (S-1-5-21-[-...]-1002):

S	identifiziert den Schlüssel als SID
1	Revisionsnummer, Nummer der SID-Spezifikation
5	Autorität
21- [...]	Domänen-ID, identifiziert die Domäne oder den lokalen Computer, Wert ist variabel
1002	Benutzer-ID, relative ID (RID), >1000 für Profile die nicht standardmäßig generiert wurden

Wichtige Pfade

Autorun

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Pfade in Run bei jedem Systemstart, RunOnce nur einmal

MRU

HKU\<SID>\Software \Microsoft \Windows \CurrentVersion \Explorer ComDlg32 Zuletzt ausgeführte Anwendungen und deren Pfade sowie geöffnete oder geänderte Dateien

RecentDocs Unterschlüssel mit Dateierweiterungen, zuletzt geöffnete Dateien diesen Typs

RunMRU Aufrufe, die via Run durchgeführt wurden

UserAssist Werte von Objekten, auf der Nutzer zugegriffen hat (z.B. Optionen der Systemsteuerung, Dateiverknüpfungen und Programme)

ROT13 verschlüsselt, es gibt mehrere MRU-Listen in unterschiedlichen Listen

Geschützter Speicher

HKU\<SID>\Software \Microsoft \Protected Storage System Provider Verschlüsselte Passwörter für viele Anwendungen (Outlook Express, MSN-Explorer oder Internet Explorer)

Autovervollständigung oder Passwort merken

Internet Explorer

HKU\<SID>\Software \Microsoft \Internet Explorer

Download Informationen zu Downloads

Main Benutzereinstellungen (Search Bars, Startseite, etc.)

TypedURLs Zuletzt besuchte Seiten (z.B. EMail, Onlinebanking)

Microsoft Edge nutzt

HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_xxxxxx\MicrosoftEdge

Netzwerke

WLAN

HKLM\Software\Microsoft\Windows NT\CurrentVersions\NetworkCards Netzwerkgeräte (Beschreibung und GUID)

HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces/<GUID> Details zum Netzwerkgerät (IP, Gateway, Domain)

P2P

HKLM\System\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List Applikationen mit erlaubtem Zugriff auf ausgehende Verbindungen

Angeschlossene Geräte

HKLM\System\Mounted Devices Liste aller Geräte, die im System gemountet wurden

Mount eines Geräts bei Nutzerlogin

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 Enthält für jede DeviceClass-GUID

HKLM\System\CurrentControlSet\Control\DeviceClasses Unterschlüssel mit Geräten die verbunden waren oder sind.

DeviceInstance ist Pfad zu HKLM\System\CurrentControlSet\Enum.

Durch Export Zeitstempel für ersten und letzten Zugriff

Geräte im System mit Gerätebeschreibung und IDs

HKLM\System\CurrentControlSet\Enum\Angeschlossene USB-Geräte

USBSTOR

Antiforensische Maßnahmen

Zeitstempel fälschen Prüfsumme häufig nur auf Inhalt (Tool <http://www.petges.lu/home/download>)

Pagefile.sys In HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management den Wert ClearPagefileAtShutdown auf 1 setzen

Zeitstempel vermeiden HKLM\System\CurrentControlSet\Control\FileSystem Wert NtfsDisableLastAccessUpdate auf 1 setzen

Einträge löschen Verlauf IE oder zuletzt genutzte Dokumente

UserAssist abstellen HKU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist Wert NoLog vom Typ DWORD mit Wert 1 erstellen

Tools

FTK-Imager Erstellung von Abbildern, Kopien der Hive-Files (Live) (Files → Obtain Protected Files)

Registry-Editor Importieren und Exportieren von Dateien, Struktur laden und entfernen, Verbinden mit der Registry eines Remotecomputers, Berechtigungen ändern, Registry durchsuchen

RegShot Änderungen in der Registry aufzeichnen (Erstellen eines ersten Abbildes und Vergleich mit einem zweiten)

Forensic Registry Editor (fred) Untersuchung und Bearbeitung von HIVE-Dateien, vorgefertige Berichtsvorlagen

RegRipper Extrahieren von spezifischen Informationen, Automatisierung durch Plugins und Profile

DCODE Decodieren von Zeitstempeln (<https://www.dcode.fr/timestamp-converter>)