Betriebssysteme

Windows Registry

Physische Sicht:

Allgemeine Reg.-Daten:

- HKLM\SAM [Benutzer, Rechte] -> /windows/system32/config/SAM
- HKLM\BCD00000000 [Bootkonfiguration] -> [UEFI-Partition]
/EFI/Microsoft/Boot/BCD
- HKLM\SAM [Anmeldenamen, Kennwort-Hashes] -> /windows/system32/config/SAM
- HKLM\SECURITY [Benutzer, Rechte, Sicherheitsrichtlinien] ->
/windows/system32/config/SECURITY
- HKLM\SOFTWARE [allgemeine Softwareeinstellungen] ->
/windows/system32/config/SOFTWARE
- HKLM\SYSTEM [Gerätetreiber, Dienste] -> /windows/system32/config/SYSTEM
- HKU\DEFAULT [Standard-Profil von LOKAL SYSTEM] ->
/windows/system32/config/DEFAULT

Benutzerspezifische Reg.-Daten:

- HKCU\ [persönl. Nutzerprofil] -> /Users/[user]/NTUSER.DAT (-> [Forensik](#))
- USERCLASS.DAT [benutzerspez. Softwareeinstellungen] ->
/USERS/[user]/AppData/Local/Microsoft/Windows/

Kopie der Registry: befindet sich in /windows/repair/

Wiederherstellungspunkte:

in
/SystemVolumeInformation/_restore{GUID}/RP{x}/Snapshot/
(RP{x} steht für die einzelnen Wiederherstellungspunkte)

Logische Sicht (in REGEDIT):

- HKEY_CLASSES_ROOT (HKCR) - Zuweisung von Dateitypen und Dateiendungen zu Anwendungen, COM-Klassen
(Summe von HKLM\Software\Classes und HKCU\Software\Classes, wobei HKCU Vorrang hat)
- HKEY_CURRENT_USER (HKCU) - (Link auf aktuellen User in HKU)
- HKEY_LOCAL_MACHINE (HKLM) - Treiber, Dienste, globale Anwendungs- und Systemeinstellungen
- HKEY_USERS (HKU) - alle Userkonten inclusive HKCU und Systemuser (siehe unten)
- HKEY_CURRENT_CONFIG (HKCC) - aktuelle Hardwarekonfiguration (Link auf HKLM\System\CurrentControlSet\Hardware Profiles\Current)

HKCU eines anderen Benutzers laden / editieren:

Registry: HKU/ markieren, Datei -> Struktur laden, ntuser.dat aus dem betreffenden Userprofils laden.

Mit "Struktur entfernen" werden die Änderungen gespeichert.

Prinzip funktioniert bei Offline-Windows mit allen REG-Zweigen.

ID des angemeldeten Users ermitteln (HKCU): Dosbox: whoami /logonid

- in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList User-ID auswählen, in ProfileImagePath steht das jeweilige Userverzeichnis

Seite 1 / 2

Betriebssysteme

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run - Autostart des lokal Users
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce - Einmalstart lokal User

SID eines beliebigen anderen Users (username) ermitteln:
wmic useraccount where name='username' get sid

Systemkonten:

(S-1-5-18) - System

(S-1-5-19) - Lokaler Dienst

(S-1-5-20) - Netzwerkdienst

Abkürzung:

HKLM\System\CurrentControlSet (gibt es nur lokal) = HKLM\System\Select verrät, welches ControlSet das aktuelle ist.

HKEY_CLASSES_ROOT = HKLM\SOFTWARE\Classes

* ganzen Schlüssel mit Unterschlüsseln löschen:

[-Hkey_Local_Machine\Testschlüssel]

* einzelnen Wert löschen: **[Hkey_Local_Machine\Testschlüssel] "Testwert"=-**

Eindeutige ID: #1069

Verfasser: Uwe Kernchen

Letzte Änderung: 2024-03-22 14:19