Registryforensik

by Koll, Michael
https://github.com/michkoll/

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 zulegt zugegriffene 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\CurrenControlSet\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
HLKM\SECURITY	SECURITY
HKLM\SOFTWARE	SOFTWARE
HLKM\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: HLKM\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

Informationen aus SAM
`SAM\Domains\Account\Users\<Benutzernummer>\`

`F`	Enthält Informationen wie Datum der letzten Passwortänderung und Datum der letzten Anmeldung vom Nutzer mit der Id <Benutzernummer>

Wichtige Pfade

Systeminfo

`HKLM/Software/Microsoft/Windows NT/CurrentVersion/CurrentBuildNumber`	Windows Buildnummer (cmd: `systeminfo`)

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
`HKCU/Software/Microsoft/Windows/CurrentVersion/Explorer/MountPoints2`	Mount eines Geräts bei Nutzerlogin
`HKLM/System/CurrentControlSet/Control/DeviceClasses`	Enthält für jede DeviceClass-GUID Unterschlüssel mit Geräten die verbunden waren oder sind. `DeviceInstance` ist Pfad zu `HKLM/System/CurrentControlSet/Enum`. Durch Export Zeitstempel für ersten und letzten Zugriff
`HKLM/System/CurrentControlSet/Enum/<Enumerator>/<DeviceID>`	Geräte im System mit Gerätebeschreibung und IDs
`HKLM/System/CurrentControlSet/Enum/USBSTOR`	Angeschlossene USB-Geräte

Antiforensische Maßnahmen

`Zeitstempel fÃ¤lschen`	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/Contol/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, Berechtiungen 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`)

Windows 10-Forensik

by Koll, Michael
https://github.com/michkoll/

Allgemein

Buildnummer

Aktuelle Buildnummer über `systeminfo` (cmd.exe) oder `HKLM\Software\Microsoft\Windows NT\CurrentVersion\CurrentBuildNumber`

Zuletzt verwendete Elemente

`C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent`

Überwachter Ordnerzugriff

Überwacht und blockiert den schreibenden Zugriff auf vorhandene Dateien für nicht-vertrauenswürdige Applikationen.

Aktivieren

Windows Defender Security Center → Einstellungen für Viren- und Bedrohungsschutz → Überwachter Ordnerzugriff
`oder`
Gruppenrichtlinien: `Computerkonfiguration/Administrative Vorlagen/Windows/Windows Defender Antivir/Windows Defender Exploit Guard/Überwachter Ordnerzugriff`
`oder`
Registry (Besitzer vorher ändern): `HKLM\Software\Microsoft\Windows Defender\Windows Defender Exploit Guard\ControlledFolderAccess\EnableControlledFolderAccess` (DWORD) = 0x01

Erlaubte Anwendungen

`HKLM\Software\Microsoft\Windows Defender\Windows Defender Exploit Guard\ControlledFolderAccess\AllowedApplications`
Hinzufügen mit (PS): `Add-MpPreference -ControlledFolderAcessAllowedApplications «Anwendungspfad>"`

Geschützte Ordner

`HKLM\Software\Microsoft\Windows Defender\Windows Defender Exploit Guard\ControlledFolderAccess\ProtectedFolders`
Standardmäßig geschützte Ordner:
Documents|Pictures|Videos|Music|Desktop|Favorites (<username> und Public)

Ereignisse

Einzusehen über EventVwr oder Powershell:
`Get-WinEvent -LogName "Microsoft-Windows-Windows Defender/Operational Where-Object {$_.Id -in 1123,1124,5007}`
Ereignis-IDs:

`1123`	Blockiertes Ereignis
`1124`	Überwachtes Ereignis (Auditmodus)
`5007`	Änderung von Einstellungen

Jumplists

Mehr Informationen als MRU/MFU:

- Dateiname, -pfad
- MAC Zeitstempel
- Name des Volumes
- Zeitlicher Verlauf von Down- und Uploads
- Informationen bleiben nach Löschen der Datei erhalten

Speicherort

Erstellt vom Betriebssystem: `C:\User\<username>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations`
Erstellt von Softwareanwendungen:
`C:\User\<username>\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations`
Dateiname: `<AppId>.<automatic|custom>Destinations-ms`
Die AppId kann im ForensicsWiki nachgelesen werden `https://www.forensicswiki.org/wiki/List_of_Jump_List_IDs`

AutomaticDestination JL

Aufbau der Datei:
Header (32 Byte) mit Versionssnummer (3=Win10, 1=Win7/8), Anzahl Einträge, Anzahl gepinnte Einträge, Zuletzt zugewiesene Entry-ID, Anzahl der Aktionen
DestList-Entry:

`Prüfsumme`	Fehlerhafter Eintrag wird nicht angezeigt
`(New|Birth)`	Bei Änderung des Volumes geänderte New-ID
`Volume-ID`	
`(New|Birth)`	Generiert aus Bootzeit,Sequenznummer und
`Object-ID`	MAC-Adresse. Bei Änderung des Volumes neue New-ID
`NetBios Name`	nbtstat -n
`Entry ID`	Fortlaufende Nummer
`Access Timestamp`	letzter Zugriff
`Pinned Status`	angepinnt (ja/nein)
`Access Count`	Zugriffszähler
`variabel Unicode`	vollständiger Pfad zur Datei
`Länge Unicode`	Länge Unicodepfad

CustomDestionations JL

einfachere Dateistruktur, zusammengesetzte MS-SHLINK-Segmente
Anfang eines LNK-Segments: `4C 00 00 00 01 14 02 00 00 00 00 00 C0 00 00 00 00 00 00 46`
Ende: `AB FB BF BA`

QuickAccess/Schnellzugriff

Angepinnte Einträge im Schnellzugriff des Explorer.
Dateiname `5f7b5f1e01b83767.automaticDestinations-ms`

Tools

`JumpListExt for Windows 10`	grafische Oberfläche, nicht mehr stabil in aktuellen Versionen
`JLECmd`	`JLECmd.exe -f <JLFile> (-html|-csv|-json) <targetDir> (-ld)`

Windows 10 Applications

SystemApps

vorinstalliert, können nicht deinstalliert werden
`C:\Windows\SystemApps\<appname>`

WindowsApps

über Windows Store `C:\Windows\WindowsApps\<appname>`

Einstellungsdaten

`C:\Users\<username>\AppData\Local\Packages\<appname>`
Haupteinstellungen in Datei/Registry-Hive `settings.dat`

Anwendungsdaten

Gespeichert in ESE-DB-Datenbanken, Aufbau nicht vollständig bekannt, teilweise möglich mit `ESEDatabaseView` von Nirsoft

Fast Startup und Ruhezustand

Datei: `hiberfil.sys`

Zustände

`HIBR`	Im Ruhezustand
`RSTR`	Wird fortgesetzt
`WAKE`	Nach Fortsetzung

Forensische Bewertung

Änderung des Formats ab Win8

- Header bleibt auch nach Fortsetzen verfügbar
- Daten nur zwischen Versetzen in Ruhezustand bis zur Fortsetzung
- Vor Win8 zeitlich weit zurückreichende Daten
- Sichern der hiberfil.sys im laufenden Zustand keine forensisch relevanten Daten
- Größte Menge Daten `shutdown /h`
- HIBR2BIN ermöglicht dekomprimieren der Daten im neuen Format
- Fast Startup liefert keine interessanten Daten, da alle Applikationen beendet sind

Edge Browser / ESE-DB

Anwendungspfad

`C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdge`

ESE-Datenbank

Transaktionsflow

1. `Transaction in RAM (Log Cache)`
2. `Seiten aus DB in RAM (Page Cache)`
3. `Transaktion im RAM anwenden (LC⇄PC)`
4. `Aktualiserte Daten in Logdatei (LC→Datei)`
5. `Datenbank aktualisieren`

Dirty-DB

Datenbank, die nicht vollständig aktualisiert wurde.

`V01.chk`	Zeitpunkt der Transaktion
`*.log`	Transaktionsdaten, hexadezimale Dateinamen

Wiederherstellung mit esentutl

`esentutl /mh database.dat`	Überprüfung der Datenbank (Feld State=Dirty)
`esentutl /r database.dat`	Reparatur der Datenbank (Feld State=Clean)

WebCacheV01.dat

Pfade

→`C:\Users\<username>\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\` (enthält v.a. Verweise und Speicherorte)
→`C:\Users\<username>\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!<number>\MicrosoftEdge\`

Aufbau

Tabelle `Containers`

`ContainerId`	Referenz auf Tabelle `Container_n`
`Directory`	Pfad zum Verzeichnis mit zwischengespeicherten Daten
`SecureDirectories`	Zufällige Zeichenfolge, in 8er-Gruppen teilbar
`Name`	Containertyp (Cookies|Content|History|...)
`PartitionId`	Integritätslevel, (Protected= Internet=Low | lokal=medium)

Tabelle `Container_n`

`SecureDirectory`	Unterverzeichnis im Cachepfad
`Type`	z.B. In PrivateModus (siehe Chivers)
`AccessCount`	Anzahl wie oft URL referenziert wird
<Timestamps>	`Sync, Creation, Expiry, Modified, Accessed Time`
`URL`	Quelle der Informationen
`Filename`	Name der Cachedatei

Cache-Speicherort ermitteln

`SecureDirectories`	in 8er-Blöcke aufteilen
`SecureDirectory`	zeigt auf x-ten Block (in Container_n)
`Directory`	Zeichenfolge anhängen

Zeitstempel

`CreationTime`	Erstellungzeit der Cachedatei/-objekt
`ExpiryTime`	vom Webserver vorgegeben, Cache wird ungültig
`ModifiedTime`	vom Webserver, Zeitpunkt der letzten Änderung der Ressource
`AccessTime`	Letzter Zugriff des Nutzers auf Datei

Werkzeuge

Fazit: Tools gute Unterstützung, manuell bringt mehr

`IECacheView`	Zeigt Cachedateien von IE und Edge (Dateiname, -größe, -typ, URL, Zeitstempel, Cachedateipfad)
`BrowsingHistoryView`	Zeigt Browserverlauf mehrerer Browser

OneDrive

Anwendungspfad

`C:\User\<username>\AppData\Local\Microsoft\OneDrive\`

Registry

`HKU\Software\Microsoft\OneDrive\`

`.\`	`Version,UserFolder`
`.\Accounts\Personal`	`ClientFirstSignInTimestamp, UserCID, UserFolder`

Konfigurations- und Diagnostikdaten

Ausgehend vom One-Drive-Verzeichnis:

`.\logs\Personal\`	Down-\Uploadgeschwindigkeit,
`SyncDiagnostics.log`	Ausstehende Down-\Uploads, verfügbarer Speicherplatz lokal, UserCID (siehe REG), Anzahl Dateien und Verzeichnisse
`.\settings\Personal\`	bisher kein Parser, mit Hexeditor Dateinamen einsehen
`<usercid>.dat`	
`.\settings\Personal\`	Während Download temporär
`<uploads|downloads>.txt`	Daten wie Dateiname und UserCID

Logdateien

`.\logs\Personal\`
`*.aodl, *.odlsent, *.odl` enthalten Clientaktivitäten
Die Datei `ObfuscationStringMap.txt` enthält verschleierte Dateinamen, die in den Logs gefunden werden können.
Mögliche Aktionen in den Logs:

`FILE_ACTION_ADDED`	Datei lokal hinzugefügt
`FILE_ACTION_REMOVED`	Datei lokal entfernt
`FILE_ACTION_RENAMED`	Datei umbenannt

Arbeitsspeicher

Username und Passwort liegen im Klartext vor, nach Parameter `&passwd=` und `&loginmft=` suchen

Benachrichtigungen und Kacheln

Datenbank

`C:\Users\<username>\AppData\Local\Microsoft\Windows\Notifications`

`wpndatabase.db`	Datenbank (Signatur `53 51 4C 69 74 65 20 66 6F 72 6D 61 74 20 33`)
`wpndatabase.db-wal`	Writhe Ahead Log (Signatur `37 7F 06 82` oder `37 7F 06 83`)
`wpndatabase.db-shm`	Shared Memory File, keine spezifische Signatur

SQLite-Datenbank mit WAL-Verfahren: Änderungen in Datei, bei Erreichen des Checkpoints (manuell oder automatisch) synchronisiert. WAL-Dateien bei der Untersuchung einbeziehen (`PRAGMA wal_checkpoint`).

Struktur und Inhalt

Relevante Tabellen in `wpndatabase.db`

`NotificationHandler`	Anwendungen, die zu Benachrichtigungen berechtigt sind (Zuordnung über PrimaryID→ AppID,GUID)
`Notification`	Benachrichtigunginhalt → Payload

Kacheln

Datenbank wie Benachrichtigungen, Zeitstempel `ArrivalTime` und `ExpiryTime` Rückschlüsse auf Verwendung des Computers
Einige Anwendungen legen in dem DB-Verzeichnis Cacheordner an, die sehr lange zurückreichen

Cortana

`%localAppData%\Packages\Microsoft\Microsoft.Windows.Cortana_cw5n1h2txyewy`

Artefakte

→`.\AppData\Indexed DB\IndexedDB.edb`	11 Tabellen, Tabelle `HeaderTable` enthält `createdTime, lastOpenTime`
→`.\LocalState\ESEDatabase_CortanaCoreInstance\CortanaCoreDb.dat`	[Veraltet] `Geofences` mit Standortdaten, `Reminders` benutzerspezifische Erinnerungen, `Triggers` LocationTriggers, TimeTriggers, ContactTriggers
→`.\LocalState\DeviceSearchCache\`	keine Dokumentation, Infos über Programmeinträgen, -aufrufen, Zeitstempel und JL-Einträge
→`.\AC\INetCache\<randomnumber>`	vollständige HTML-Seite von Suchen über Cortana
→`.\AC\AppCache\<randomnumber>`	HTML- und JavaScript Dateien für Cortana-Suche
→`.\LocalState\LocalRecorder\Speech`	Aufgezeichnete Sprachbefehle
→`.\LocalState\Cortana\Uploads\Contacts`	Falls Synchronisierung mit Android, Kontaktdaten und Mobilnummern
→`9d1f905ce5044aee.automaticDestinations-ms`	URLs die über Cortane-Suche ausgelöst wurden
→`WebCacheV01.dat`	URLs die über Cortana aufgerufen wurden
→`%SystemDrive%\Windows\Prefetch\SEARCHUI.EXE-14F7ADB7.pf`	Letzte Ausführungszeit(en)
→`%SystemDrive%\Windows\appcompat\Programs\Amcache.hve`	Erstellungs- und Änderungszeitstempel der Anwendung

Deaktivieren von Cortana

Parameter in `HKLM\Software\Policies\Microsoft\Windows\Windows Search`

`AllowCortana`	`dword:00000000`
`DisableWebSearch`	`dword:00000001`
`AllowSearchToUseLocation`	`dword:00000000`
`ConnectedSearchUseWeb`	`dword:00000000`
`ConnectedSearchPrivacy`	`dword:00000003`

Betriebssystemforensik (allgemein)

by Koll, Michael
https://github.com/michkoll/

Betriebssystem

Architektur

Monolithisch (S.22)

`Geschwindigkeit`	schnell, minimaler Overhead; Funktionen optim. abgestimmt
`Sicherheit`	Risiko: ganzes BS im priv. Modus; Probleme einzerln Komp. Auswirkung auf ganzes BS
`Speichereffizienz`	Schlecht, ganzes BS im Speicher gehalten
`Wartbarkeit, Erweiterbarkeit`	Schlecht, da bei Änderungen viele Komponenten

Geschichtet (S.23)

`Geschwindigkeit`	Langsamer, da Funktionen Overhead, häufiger Kontextwechsel
`Sicherheit`	Teile des BS im User Mode, z.B. Treiber; Probleme Komponenten ↛ BS
`Speichereffizienz`	Gut, einzelne Module dynamisch nachgeladen und entladen
`Wartbarkeit, Erweiterbarkeit`	Besser, da Änderungen meist nur bei einzelnen Komponenten

Mikrokernel (S.24)

`Geschwindigkeit`	schlechte Performance, häufige Prozesswechsel und Interprozesskommunikation
`Sicherheit`	sicherheitskritischer Teil relativ klein; Dienste außerhalb Kern können Sicherheit und Stabilität nicht beeinflussen
`Speichereffizienz`	Gut, einzelne Module dynamisch nachgeladen und entladen
`Wartbarkeit, Erweiterbarkeit`	Sehr gut, einzelne Module können ausgetauscht werden (z.T. während Betrieb)

Ziele

Windows

Allgemein

Windows Stations, Desktops und Session (S.34)

Authentifizierung Session-orientiert, `Session` beinhaltet mehrere `Stations`, `Stations` beinhalten Desktops mit Fenstern und GDI-Objekten. Sicherheitsbeschreiber eines Objekts ist mit `Station` verbunden, darüber Kontrolle von Benutzer zum Desktop

Prozesse und Dienste

svchost.exe (Dienste) (S.138)

- mit `tlist` laufende Prozesse mit Diensten auflisten (`tlist -m svchost.exe -s`)
- mit `Process-Explorer` farblich gekennzeichnete Dienste → Properties → Services
- spezielle Programme wie z.B. `svchost-Analyzer`

Gestartete Dienste in Registry

`HKLM\System\CurrentControlSet\Services` als Unterschlüssel

Mandatorische Zugriffsregeln (S.153)

`No-<Write|Read>-Up`	Kein schreibender/lesender Zugriff von Prozessen mit niedrigem Level auf Objekte mit höherem Level (gleiches Level zugelassen)
`No-<Write|Read>-Down`	Kein schreibender/lesender Zugriff von Prozessen mit höherem Level auf Objekte mit niedrigerem Level (gleiches Level zugelassen)

Default: No-Write-Up (für alle Objekte), No-Read-Up (für Prozesse und Threads)

DACL (S.156)

Sicherheitsdeskriptor besteht aus `Header, SID Besitzer, SID Gruppe, DACL, SACL`
`DACL` besteht aus ACEs mit `<Allow|Deny>, SID User, ACE-Bitmapp`
Regeln DACL: Erst Einzel-ACE, dann Gruppe; Erst Verbote, dann Erlaubnisse; Reihenfolge von oben nach unten
`Hinweis`: Beim Ändern bzw. lesen aufpassen auf Gruppenzugehörigkeit (Jeder)

Registry