# $\frac{\text{Registry forensik}}{\text{by Koll, Michael}}$

### Relative Pfade

%UserProfile% Pfad zum derzeitigen Benutzerprofil Laufwerksbuchstabe, auf dem Windows %SystemDrive%

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:

Eindeutig innerhalb eines Schlüssels Name

Datentyp des Wertes (s.u.) Тур

kann leer oder null sein. Maximum 32767 Bytes, häu-Daten

fig 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

Binärdaten REG\_BINARY

REG DWORD Double-Word-Werte, häufig boolesche Werte

REG 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)	
G 4 F 04 F ] G1	M., t.,	

S-1-5-21-[...]\_Classe sutzerspezifische 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) Daten zum Console-Subsystem (z.B. Console zum MS-DOS-Command-Prompt) Control-Panel Einstellungen der Systemsteuerung, u.a.

ungsbild

Umgebungsvariablen, die Benutzer Environment

gesetzt haben

Keyboard-Layout Installierte Tastaturlayouts

Jeder Unterschlüssel ein Netzlaufwerk.

Name des Schlüssels ist Laufwerksbuchstabe, enthält Konfigurationsdaten zum

regionale Einstellungen und Erschein-

Verbinden

Printers Präferenzen des Benutzers zum Drucken Nutzerspezifische Einstellungen zu Software

installierten Programmen, je nach Programm Informationen zu Programmanbieter. Programm. sion, Installationsdatum und zulegt zugegriffene Dateien. Ablage nach HKCU\Software\Programmanbieter\-

Programm\ Version

Volatile Environment Umgebungsvariablen, die beim Login definiert wurden

#### HKLM

Network

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

Lokale Windows-Sicherheitsdatenbank über SAM Benutzer- und Gruppeninformationen (Link zu HKLM\SECURITY\SAM)

SECURITY Lokale Windows-Sicherheitsdatenbank (inklusive SAM)

SOFTWARE Einstellungen zu Applikationen des Rechners (und Microsoft-Applikationen)

Informationen zur SYSTEM 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 Systemyerhaltens aus

#### HKCC

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

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

Svstem Software

#### Hives

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

Alle anderen Hives und Dateien in %SystemRoot%\System32\config HKU\.DEFAULT DEFAULT

HKLM\SAM SAM

SECURITY HLKM\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):

Identifiziert den Schlüssel als SID

Revisionsnummer, Nummer der SID-Spezifikation

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>\

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 Unterschlüssel mit Dateierweiterungen, zuletzt RecentDocs

geöffnete Dateien diesen Typs

Aufrufe, die via Run durchgeführt wurden RunMRU UserAssist Werte von Objekten, auf der Nutzer zugegrif-

fen 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

Benutzereinstellungen (Search Bars, Startseite, Main

etc.)

Zuletzt besuchte Seiten (z.B. EMail, On-TypedURLs

linebanking)

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/ Netzwerkgeräte CurrentVersions/NetworkCards (Beschreibung

GUID)

HKLM/System/CurrentControlSet/ Details zum Netzw-Services/Tcpip/Parameters/ Interfaces/<GUID>

erkgerät (IP, Gateway, Domain)

und

P2P

HKLM/System/ControlSet001/ Services/SharedAccess/Parameters/ FirewallPolicy/StandardProfile/ AuthorizedApplications/List

Applikationen erlaubtem Zugriff auf ausgehende Verbindungen

#### Angeschlossene Geräte

HKLM/System/Mounted Devices Liste aller Geräte, die im System gemountet

HKCU/Software/Microsoft/ Windows/CurrentVersion/Explorer/

MountPoints2

HKLM/System/CurrentControlSet/ Control/DeviceClasses

Enthält für jede Forensic Registry DeviceClass-GUID Unterschlüssel mit Geräten die verbun-

Mount eines Geräts bei

wurden

Nutzerlogin

den waren oder sind. DeviceInstance Pfad zu HKLM/System/ CurrentControlSet/

Enum. Durch Export Zeitstempel für ersten und letzten Zugriff

HKLM/System/CurrentControlSet/Enum/Geräte im System mit <Enumerator>/<DeviceID>

und IDs

HKLM/System/CurrentControlSet/Enum/Angeschlossene USB-USBSTOR

Gerätebeschreibung

Geräte

## Antiforensische Maßnahmen

Zeitstempel fädlschen Prüfsumme häufig nur auf Inhalt

(Tool http://www.petges.lu/home/

download)

Pagefile.sys HKLM/System/ CurrentCOntrolSet/

Control/Session Manager/

Memory Management den Wert ClearPagefileAtShutdown auf 1

Zeitstempel vermeiden HKLM/System/CurrentControlSet/

> Contol/FileSvstem 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

Erstellung von Abbildern, Kopien der FTK-Imager

Hive-Files (Live) (Files → Obtain Pro-

tected Files)

Registry-Editor Importieren und Exportieren von

> Dateien, Struktur laden und entfernen, Verbinden mit der Registry eines Remotecomputers, Berechtiungen ändern,

Registry durchsuchen

Änderungen in der Registry aufzeichnen RegShot

(Erstellen eines ersten Abbildes und Ver-

gleich mit einem zweiten)

Untersuchung und Bearbeitung von HIVE-Dateien, vorgefertige Berichtsvor-EDitor (fred)

RegRipper Extrahieren von spezifischen Informatio-

nen, Automatisierung durch Plugins und

Profile

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

Auslesen von Hive-Files (https:

Access Data Registry Viewer //accessdata.com/product-download/

registry-viewer-1-8-0-5)

Auslesen von Hive-Files (https://www. RegView

gaijin.at/dlregview.php)

Fehler und Verbesserungen bitte melden:

https://github.com/michkoll/latex-template-cheatsheet/issues

## Windows 10-Forensik

## Allgemein

#### Buildnummer

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

#### Zuletzt verwendete Elemente

 $\label{lem:c:wisername} $$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  $\rightarrow$  Einstellungen für Virenund Bedrohungsschutz  $\rightarrow$  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

#### Automatic Destination 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-

Volume-ID II

(New|Birth) Generiert aus Bootzeit,Sequenznummer und Object-ID MAC-Adresse. Bei Änderung des Volumes

> neue New-ID nbtstat -n

NetBios Name nbtstat -n
Entry ID Fortlaufende Nummer

Access Count Fortiaurende Numm

Fortiaurende Numm

Fortiaurende Numm

fortiaurende Numm

angepinnt (ja/nein)

Zugriffszähler

variabel Unicode vollständiger Pfad zur Datei

Länge Unicode Länge Unicodepfad

#### Custom Destionations JL

einfachere Dateistruktur, zusammengesetzte
MS-SHLINK-Segmente
Anfang eines LNK-Segments: 4C 00 00 00 01 14 02 00 00
00 00 00 00 00 00 00 00 046
Ende: AB FB BF BA

### QuickAccess/Schnellzugriff

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

#### Tools

JumpListExt for grafische Oberfläche, nicht mehr stabil in ak-Windows 10 tuellen 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

 $(\texttt{LC} {
ightarrow} \texttt{Datei})$ 

5. Datenbank aktualisieren

#### Dirty-DB

Datenbank, die nicht vollständig aktualisiert wurde.

Zeitpunkt der Transaktion V01.chk

Transaktionsdaten, hexadezimale Dateinamen \*.log

Wiederherstellung mit esentutl

esentutl /mh database.dat Überprüfung der Datenbank

(Feld State=Dirty)

Reparatur der Datenbank esentutl /r database.dat

(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 Pfad zum Verzeichnis mit zwis-

Directory chengespeicherten Daten

SecureDirectories Zufällige Zeichenfolge. in 8er-

Gruppen teilbar

Name Containertyp (Cook-

ies|Content|History|...)

Integritätslevel, (Protected= Inter-PartitionId

net=Low | lokal=medium)

Tabelle Container\_n SecureDirectory

Unterverzeichnis im Cachepfad Type z.B. Ïn PrivateModus (siehe Chivers) Anzahl wie oft URL referenziert wird AccessCount

<Timestamps> Sync, Creation, Expiry, Modified, Accessed Time Quelle der Informationen URL

Filename Name der Cachedatei

Cache-Speicherort ermitteln

SecureDirectories in 8er-Blöcke aufteilen

zeigt auf x-ten Block (in Container n) SecureDirectory

Zeichenfolge anhängen Directory

Zeitstempel

CreationTime Erstellungzeit der Cachedatei/-objekt

vom Webserver vorgegeben, Cache wird ExpiryTime

vom Webserver, Zeitpunkt der letzten Än-ModifiedTime

derung der Ressource

AccessTime Letzter Zugriff des Nutzers auf Datei

#### Werkzeuge

Fazit: Tools gute Unterstützung, manuell bringt mehr

Zeigt Cachedateien von IE und Edge IECacheView

(Dateiname, -größe, -typ, URL, Zeit-

stempel, 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

<usercid>.dat Dateinamen einsehen

.\settings\Personal\ Während Download temporär Dat-<uploads|downloads>.txt en wie Dateiname und User-CID

#### 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:

Datei lokal hinzugefügt FILE\_ACTION\_ADDED 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

wpndatabase.db-wal Writhe Ahead Log (Signatur 37 7F 06 82 oder 37 7F 06 83)

Shared Memory File, keine speziwpndatabase.db-shm fische 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

Notification

Relevante Tabellen in wpndatabase.db

NotificationHandler Anwendungen, die zu Benachrichtigungen berechtigt sind (Zuordnung

über PrimaryID→ AppID,GUID) Benachrichtigunginhalt → Payload

#### Kacheln

Datenbank wie Benachrichtigungen, Zeitstempel Arrival Time 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\ 11 Tabellen, Tabelle HeaderTable IndexedDB.edb enthält createdTime.

lastOpenTime  $\rightarrow$ .\LocalState\ [Veraltet] Geofences mit Standort-

daten. Reminders benutzerspezifis-ESEDatabase che Erinnerungen, Triggers Loca-CortanaCoreInstance\ tionTriggers, TimeTriggers, Con-CortanaCoreDb.dat

tactTriggers

keine Dokumentation, Infos über  $\rightarrow$ . \LocalState\ DeviceSearchCache\ Programmeinträgen, -aufrufen,

Zeitstempel und JL-Einträge vollständige HTML-Seite von  $\rightarrow$ .\AC\INetCache\

<randomnumber> Suchen über Cortana

HTML- und JavaScript Dateien  $\rightarrow$ .\AC\AppCache\ <randomnumber> für Cortana-Suche

Aufgezeichnete Sprachbefehle  $\rightarrow$ .\LocalState\ LocalRecorder\Speech

→.\LocalState\Cortana\ Falls Synchronisierung mit An-Uploads\Contacts droid, Kontaktdaten und Mobil-

nummern

URLs die über Cortane-Suche aus- $\rightarrow$ 9d1f905ce5044aee.

automaticDestinations-ms gelöst wurden

URLs die über Cortana aufgerufen  $\rightarrow$ WebCacheV01.dat wurden

→%SystemDrive%\Windows\ Letzte Ausführungszeit(en) Prefetch\SEARCHUI.

EXE-14F7ADB7.pf

→%SystemDrive%\Windows\ Erstellungs- und Änderungszeitstempel der Anwendung app compat \ Programs \

Amcache hve

#### Deaktivieren von Cortana

Parameter in

HKLM\Software\Policies\Microsoft\Windows\Windows Search

AllowCortana dword:00000000 DisableWebSearch dword:00000001 AllowSearchToUseLocation dword:00000000 ConnectedSearchUseWeb dword:00000000 ConnectedSearchPrivacv dword:00000003

Fehler und Verbesserungen bitte melden:

https://github.com/michkoll/latex-template-cheatsheet/issues

## Betriebssystemforensik (allgemein)

by Koll, Michael

## 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 gehal-

ten

Wartbarkeit, Schlecht, da bei Änderungen viele Kom-

Erweiterbarkeit ponenten

## \_

#### Geschichtet (S.23)

Geschwindigkeit Langsamer, da Funktionen Overhead,

häufiger Kontextwechsel

Sicherheit Teile des BS im User Mode, z.B.

Treiber; Probleme Komponenten  $\nrightarrow$  BS

 ${\tt Speichereffizienz} \qquad {\tt Gut}, \quad {\tt einzelne} \quad {\tt Module} \quad {\tt dynamisch}$ 

 $nachgeladen\ und\ entladen$ 

Wartbarkeit, Besser, da Änderungen meist nur bei

Erweiterbarkeit einzelnen Komponenten

#### Mikrokernel (S.24)

Geschwindigkeit schlechte Performance, häufige Prozesswechsel und Interprozesskommunika-

tion

Sicherheit sicher Teil relativ klein;

Dienste außerhalb Kern können Sicherheit und Stabilität nicht beeinflussen

 ${\tt Speichereffizienz} \qquad {\tt Gut}, \quad {\tt einzelne} \quad {\tt Module} \quad {\tt dynamisch}$ 

nachgeladen und entladen

Wartbarkeit, Sehr gut, einzelne Module können aus-Erweiterbarkeit getauscht werden (z.T. während Be-

trieb)

#### Vorteile virtuelles BS

Sandbox verbesserte Sicherheit durch Abschottung; bessere Ausnutzung des Systems durch mehrere VMs; herstellen kompatibler Laufzeitumgebungen Ziele (S.12)

Unterstützung des Anwenders

Abstraktion der Hardware (Nummerierte Datenblöcke der HDD werden durch Reihenfolge, Verkettung und Verknüpfung zu Datei), Bereitstellen von Dienstfunktionen (Dateien öffnen, lesen, schreiben, schließen), Verheren irreleventer Dateile

Verbergen irrelevanter Details (Nummerierung Datenblöcke für

Anwender nicht sichtbar)

Optimierung der Rechnerauslastung Zuverlässigkeit Parallele Nutzung Rechnerkomponenten, mehrere Aufgaben quasiparallel Schutzmechanismus gegenseitig störender Prozesse, Abfangen von Ausnahmesituationen, Verhindern von blockieren-

den Prozessen

Portabilität Programme auf verschiedenen Plattfor-

men lauffähig

#### Nicht erfüllte Zuverlässigkeit

Prozess belegt zu viel Speicher, so dass andere Prozesse nicht ausgeführt werden können

Abbruch mit Ctrl+C funktioniert nicht, da Signal auf

Ignorieren steht

Prozess zieht alle Prozessorleistung, so dass andere Prozesse blockiert sind (unfaires Scheduling)

Aufgaben (S.14)

Programm- und Prozessverwaltung

Verwalten von

Betriebsmitteln

Steuern, Erzeugen, Starten, Entfernen von Prozessen; Laden von Programmen von HDD in RAM; Leerlaufprozess; Kommunikation und Synchronisation von Prozessen

Anwenderschnittstelle

Kommandoebene, graphische Bedienoberfläche, Systemaufrufe zwischen BS und Programmen Aufteilen der Betriebsmittel, Trennung Benutzerbereiche, Schutz, Prüfung Zugang

Verbindungen mit anderen Rechnern Begriffe

Parallel Gleichzeitige Abarbeitung von Prozessen,

jeder Prozess läuft auf eigener CPU

Quasiparallel Abwechselnde Abarbeitung, alle Prozesse

laufen auf gleicher CPU

Programm besteht aus Vorschriften/Anweisungen in

formaler Sprache; Ausführen zur Bewälti-

gung bestimmter Aufgaben

Prozess ablaufendes Programm mit konkreten Daten, besitzt Rechte, Registerinhalte und

Speicher;  $\operatorname{Zust\"{a}nde}$  running, ready oder waiting

Threads Untereinheit von Prozessen, teilen sich

denselben virtuellen Adressraum, Prozess-

wechsel schneller

Leerlaufprozess Prozessor führt ständig Befehlszyklen aus,

Leerlaufprozess verbraucht diese mit NOP-

Anweisungen

## Dateisystem

#### Zusammenhängende Belegung (S.104)

Belegungstabelle Datei, Start, Länge

## Verteilte Belegung verkettete Listen (FAT) (S.105)

Belegungstabelle Datei, Start

Hilfstabelle (FAT) Verweis auf nächste Adresse, Dateiende

mit EOF

#### Verteilte Belegung mittels Index-Liste (S.106)

Belegungstabelle

Datei, Index-DU

Index-DU

Verweise auf DUs (falls zu lang Verweis

auf weitere Index-DU)

## 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)
- $\bullet$  mit Process-Explorer farblich gekennzeichnete Dienste  $\to$  Properties  $\to$  Services
- spezielle Programme wie z.B. sychost-Analyzer

## Gestartete Dienste in Registry

HKLM\System\CurrentControlSet\Services als Unterschlüssel

#### laufende Prozesse PIDs und TIDs

mit Process Explorer; PID in Liste laufende Prozesse; TID Prozesseigenschaften  $\rightarrow$  Threads

#### Registryzugriffe von Prozessen

Mit Process Explorer und Process Hacker: Möglichkeit über Process Monitor Registryzugriffe zu protokollieren (Software installieren → mit Process Monitor analysieren)

#### Ausgeführte Dienste

z.B. über msc (services) oder Registry (siehe oben)

#### Mandatorische Zugriffsregeln (S.153)

No-<Write|Read>-Up Kein schreibender/lesender Zugriff von Prozessen mit niedrigem Level auf Objekte mit höherem Level (gle-

iches Level zugelassen)

Kein schreibender/lesender Zugriff No-<Write|Read>-Down 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 | Denv>. 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)

#### Festplatten und Drucker

Option 1 In regedit HKEY\_LOCAL\_MACHINE\SYSTEM exportieren, in RegRipper Report erstellen

Option 2 Systemwerkzeuge wie msinfo

## Forensische Anwendungsfälle

#### Suchen mit X-Ways

Image einbinden, Datei nach hex-Nach Hexwert in Bild Wert durchsuchen

Nach ASCII-String in Dokument

Dokument

in docx-Datei

Image einbinden, nach Text-Wert suchen mit ASCII-Codepage

Nach Unicode-String in Image einbinden, nach Text-Wert suchen mit Unicode-Codepage Image einbinden, Indexieren, Index

nach Text-Wert durchsuchen mit ASCII- oder Unicode-Codepage

#### Carving

Carving-Programm durchsucht Dokument von Anfang nach Anfangssignatur, Markierung, Suchen Richtung Ende nach Endesignatur; Bereich dazwischen in Datei kopieren

#### Schattenkopie

Volume-Shadow-Copy-Service (VSS) hält Dateien in mehreren Versionen, Versionen können über Eigenschaften  $\rightarrow$  Versionen eingesehen werden. Zur Analyse Schattenkopie mounten

#### Thumbs.db

Inhalte können mit Thumb.db-Viewer sichtbar gemacht werden (bildlich oder als Liste): Ungefähres Erscheinungsbild. Speicherort des Originals und Veränderungsdatum kann eingesehen werden

#### Überwachter Ordnerzugriff

(Details auf eigenem CheatSheet) Angriffsmöglichkeiten prüfen, dazu:

Ist überwachter Windows Defender, Registry oder Ordnerzugriff aktiviert? Gruppenrichtlinien

Standardverzeichnisse Falls aktiviert, sind diese geschützt Zusätzliche VerzeichnisseSchauen ob Verzeichnis hinzuge-

fügt (in Registry oder Windows

Defender)

UserCID

Schauen ob Anwendungen erlaubt Erlaubte Anwendungen sind (in Registry)

#### **Nutzung OneDrive**

Anhaltspunkte zur Nutzung

UserFolder

ClientFirstSignInTimestamp

UserCID

Logdateien

Schauen ob vorhanden Erster Login des Nutzers Falls vorhanden genutzt worden sein Infos zu Anzahl Dateien, Up-/Downloadgeschwindigkeit,

#### UNIX

#### Systemzustand

Werkzeuge verwenden Informationen aus /proc-Verzeichnis

Uptime /proc/cpuinfo Systemauslastung /proc/stat Speicherauslastung /proc/meminfo Version BS /proc/version /proc/filesystem Dateisysteme

Fehler und Verbesserungen bitte melden:

https://github.com/michkoll/latex-template-cheatsheet/issues