Registryforensik by Koll, Michael https://github.com/michkoll/		.DEFAULT S-1-5-18	Einstellungen, die Windows nutzt, bevor ein Nutzer sich eingeloggt hat well-known SID für LocalSystem- Benutzer	HARDWARE SAM	Speichert HW-Daten beim Systemstart, wird bei jedem Start erstellt und mit Informationen über Geräte, Treiber und Ressourcen gefüllt Lokale Windows-Sicherheitsdatenbank über
		S-1-5-19	well-known SID für LocalService- Benutzer, lokale Dienste, die den	SAM	Benutzer- und Gruppeninformationen (Link zu HKLM\SECURITY\SAM)
Relative Pfade		S-1-5-20	LocalSystem-User nicht benötigen well-known SID für NetworkService-	SECURITY	Lokale Windows-Sicherheitsdatenbank (inklusive SAM)
%UserProfile%	Pfad zum derzeitigen Benutzerprofil		Benutzer, Netzwerkdienste, die den LocalService-Benutzer nicht benötigen	SOFTWARE	Einstellungen zu Applikationen des Rechners (und Microsoft-Applikationen)
%SystemDrive%	Laufwerksbuchstabe, auf dem Windows installiert ist, i.d.R C:	S-1-5-21-[]	SID des derzeit angemeldeten Benutzers (Link von HKCU)	SYSTEM	Informationen zur Systemkonfiguration (z.B. Gerätetreiber und Dienste). Derzeitiges Hardware-
%SystemRoot%	Pfad zum Windows Ordner, i.d.R. C:\Windows	S-1-5-21-[]_Clas	-1-5-21-[]_Classe¥utzerspezifische Dateiverknüpfungen		profil ist Link von HKCC. Mehrere Sätze mit Schema ControlSetxxx. HKLM\SYSTEM\Select zeigt aktuelle verwendetes Profil in CurrentControlSet.

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

Тур Datentyp des Wertes (s.u.)

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

REG BINARY Binärdaten

REG DWORD Double-Word-Werte, häufig boolesche Werte

REG LINK Link

REG MULTI SZ Liste von Strings

Struktur

Wurzelschlüssel

				VCIDINGCII
HKLM	HKEY LOCAL MACHINE	Hauptschlüssel	Printers	Präferenzen des Benutzers zum D
HKU	HKEY HKU -	Hauptschlüssel	Software	Nutzerspezifische Einstellunge
HKCR	HKEY CLASSES ROOT	Verweis		installierten Programmen, je
HKCU	$HKEY_CURRENT_USER$	Verweis		Programm Informationen zu
HKCC	HKEY_CURRENT_CONFIG	Verweis		grammanbieter, Programm,
				on, Installationsdatum und
T 7	•			zugegriffene Dateien. Ablage

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 ieden aktiv geladenen Benutzer (Standardprofile und angemeldete Profile, keine abgemeldeten Nutzer)

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. regionale Einstellungen und Erschei-

nungsbild

Environment Umgebungsvariablen, die Benutzer ge-

setzt haben

Keyboard-Layout Installierte Tastaturlayouts

Network Jeder Unterschlüssel ein Netzlaufwerk.

> Name des Schlüssels ist Laufwerksbuchstabe, enthält Konfigurationsdaten zum

Verbinden

Drucken gen zu

e nach Pro-Versizulegt

 $HKCU\Software\Programmanbieter\-$ Programm\Version

Volatile Environment Umgebungsvariablen, die beim Login

definiert wurden

HKLM

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

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 SAMHLKM\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

 ${\tt HKLM \backslash Software \backslash Microsoft \backslash Windows NT \backslash Current Version \backslash Profile LiPownload}$

Pfad zu individuellen Profilen: ProfileImagePath

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

identifiziert den Schlüssel als SID S

1 Revisionsnummer, Nummer der SID-Spezifikation

5 Autorität

Domänen-ID, identifiziert die Domäne oder den lo-21-[...]

kalen Computer, Wert ist variabel

Benutzer-ID, relative ID (RID), >1000 für Profile 1002

die nicht standardmäßig generiert wurden

Wichtige Pfade

Systeminfo

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

CurrentBuildNumber

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

Werte von Objekten, auf der Nutzer zugegriffen UserAssist

hat (z.B. Optionen der Systemsteuerung, Datei-

verknüpfungen 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

Informationen zu Downloads

Main Benutzereinstellungen (Search Bars, Startseite,

etc.)

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

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 und

GUID)

Details zum Netz-

werkgerät (IP, Gate-

erlaubtem Zugriff auf

Mount eines Geräts bei

Verbin-

way, Domain)

Applikationen

ausgehende

HKLM/System/CurrentControlSet/ Services/Tcpip/Parameters/

Interfaces/<GUID>

P₂P

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

AuthorizedApplications/List

Angeschlossene Geräte HKLM/System/Mounted Devices

Liste aller Geräte, die im System gemountet

wurden

Nutzerlogin

dungen

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

MountPoints2

HKLM/System/CurrentControlSet/ Control/DeviceClasses

Enthält für jede DeviceClass-GUID Unterschlüssel

 $_{
m mit}$ Geräten die verbunden waren oder sind. DeviceInstance istPfad zu HKLM/System/ CurrentControlSet/ Enum. Durch Export

Zeitstempel für ersten und letzten Zugriff

HKLM/System/CurrentControlSet/Enum/Geräte im System mit

<Enumerator>/<DeviceID>

Gerätebeschreibung und IDs

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

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 Do-

kumente

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 Protec-

ted Files)

Registry-Editor Importieren und Exportieren von Datei-

en, Struktur laden und entfernen, Verbinden mit der Registry eines Remotecomputers, Berechtiungen ändern, Regis-

try durchsuchen

RegShot Änderungen in der Registry aufzeichnen

(Erstellen eines ersten Abbildes und Ver-

gleich mit einem zweiten)

Untersuchung und Bearbeitung von Forensic Registry EDitor (fred)

HIVE-Dateien, vorgefertige Berichtsvor-

Extrahieren von spezifischen Informatio-RegRipper

nen. 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

 $\label{lem:c:second} $$C:\Users<\ship\Data\Roaming\Microsoft\Windows\Recent $$$

Überwachter Ordnerzugriff

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

Aktivieren

Windows Defender Security Center \to Einstellungen für Virenund Bedrohungsschutz \to 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
-ControlledFolderAccessAllowedApplications

«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 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 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

 $(LC \rightarrow Datei)$

5. Datenbank aktualisieren

Dirty-DB

Datenbank, die nicht vollständig aktualisiert wurde.

Zeitpunkt der Transaktion V01.chk

Transaktionsdaten, hexadezimale Dateinamen *.log

Wiederherstellung mit esentutl

Überprüfung der Datenbank Registry esentutl /mh database.dat

(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 zwischen-

Directory gespeicherten Daten

Zufällige Zeichenfolge, in 8er-SecureDirectories

Gruppen teilbar

(Coo-Name Containertyp

kies|Content|History|...)

Integritätslevel, (Protected= Inter-PartitionId

net=Low | lokal=medium)

Tabelle Container n

Unterverzeichnis im Cachepfad SecureDirectory

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

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

ModifiedTime vom Webserver, Zeitpunkt der letzten Ände-

rung 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, Zeitstempel, Cachedateipfad)

Zeigt Browserverlauf mehrerer Brow-BrowsingHistoryView

OneDrive

Anwendungspfad

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

HKU\Software\Microsoft\OneDrive\

Version, UserFolder

ClientFirstSignInTimestamp, .\Accounts\Personal UserCID, UserFolder

Konfigurations- und Diagnostikdaten

Ausgehend vom One-Drive-Verzeichnis:

.\logs\Personal\ Down-\Uploadgeschwindigkeit,

Ausstehende Down-\Uploads, SyncDiagnostics.log verfügbarer Speicherplatz lokal, UserCID (siehe REG), Anzahl

Dateien und Verzeichnisse .\settings\Personal\ bisher kein Parser, mit Hexedi-<usercid>.dat tor Dateinamen einsehen

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

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

Writhe Ahead Log (Signatur 37 7F wpndatabase.db-wal

06 82 oder 37 7F 06 83)

Shared Memory File, keine spezifiwpndatabase.db-shm

sche 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 Benach-

richtigungen berechtigt sind (Zuordnung über PrimarvID→ Ap-

pID.GUID)

Benachrichtigunginhalt → Payload Notification

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\ 11 Tabellen, Tabelle HeaderTable IndexedDB.edb enthält createdTime.

lastOpenTime

 \rightarrow .\LocalState\ [Veraltet] Geofences mit Stand-ESEDatabase ortdaten, Reminders benutzerspezifische Erinnerungen, Triggers CortanaCoreInstance\

CortanaCoreDb.dat LocationTriggers, TimeTriggers, ContactTriggers

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

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

<randomnumber> chen über Cortana

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

Aufgezeichnete Sprachbefehle \rightarrow .\LocalState\

LocalRecorder\Speech

Uploads\Contacts

→.\LocalState\Cortana\ Falls Synchronisierung mit Android. Kontaktdaten und Mobilnum-

mern

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

automaticDestinations-ms gelöst wurden \rightarrow WebCacheV01.dat URLs die über Cortana aufgerufen

wurden →%SvstemDrive%\Windows\ Letzte Ausführungszeit(en)

Prefetch\SEARCHUI. EXE-14F7ADB7.pf

appcompat\Programs\

→%SystemDrive%\Windows\ Erstellungs- und Änderungszeitstempel der Anwendung

Amcache.hve

Deaktivieren von Cortana

Parameter in

HKLM\Software\Policies\Microsoft\Windows\Windows Search dword:00000000

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