HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCE

LEHRBRIEF

für das Modul

Betriebssysteme

Windows

Autor: Prof. Ronny Bodach

Bearbeitungsstand: 20.05.2022

Hinweise

Herausgeber:

Hochschule Mittweida - University of Applied Sciences
Fakultät Computer- und Biowissenschaften
Technikumplatz 17
09648 Mittweida
1. Auflage (20.05.2022)

Redaktionelle Bearbeitung: Prof. Ronny Bodach

Inhaltsverzeichnis

1 Betriebssystem Windows als Client

1.1 Lernziele

Nach Durcharbeiten dieses Kapitels sind Sie in der Lage, grundlegende Konzepte der Speicherung von Konfigurationsdateien in Windows zu verstehen. Sie kennen die Registry in ihrem Aufbau und wissen in welchen Dateien sie nach relevanten Informationen suchen müssen. Zusätzlich wissen Sie was Event Logs sind und Sie sind in der Lage das Windows Logsystem zu verstehen und zu nutzen.

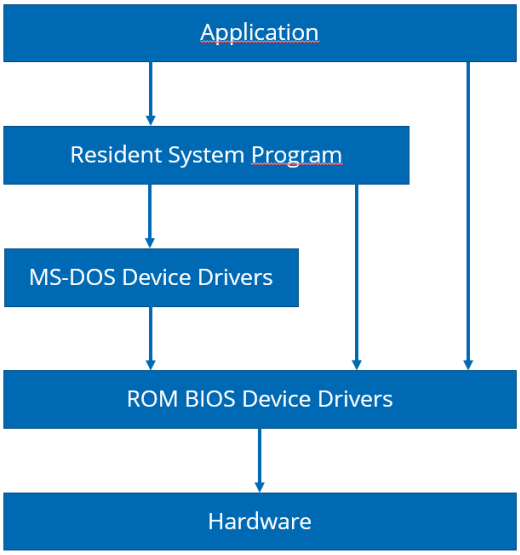
1.2 Einführung

1.2.1 Historie

1.2.1.1 MS-DOS

Das Microsoft Disk Operating System (MS-DOS) wurde am 12. August 1981 eingeführt und von Seattle Computer Products aufgekauft und als 86-DOS benannt. Weiterhin ist MS-DOS an IBM und 70 weitere Firmen lizensiert.

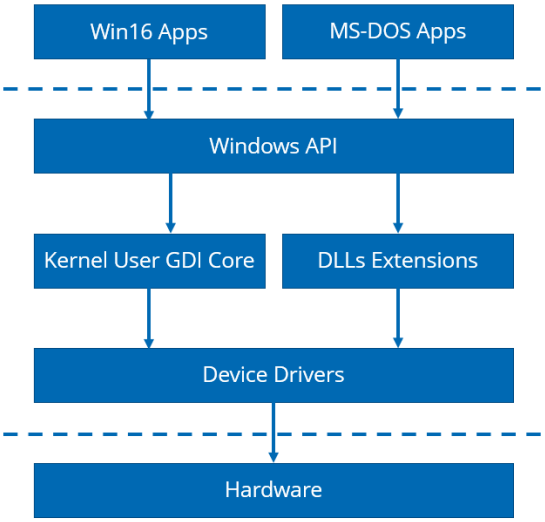
Von MS-DOS gibt es die Versionen eins bis sechs, welche nur für x86 Prozessoren geeignet sind. Weiterhin ist nur ein Single User Betrieb möglich und es gibt keine Rechte Staffelung. Das Multitasking wurde erst mit Version vier eingeführt. Außerdem gibt es nur ein Command Line Interface.

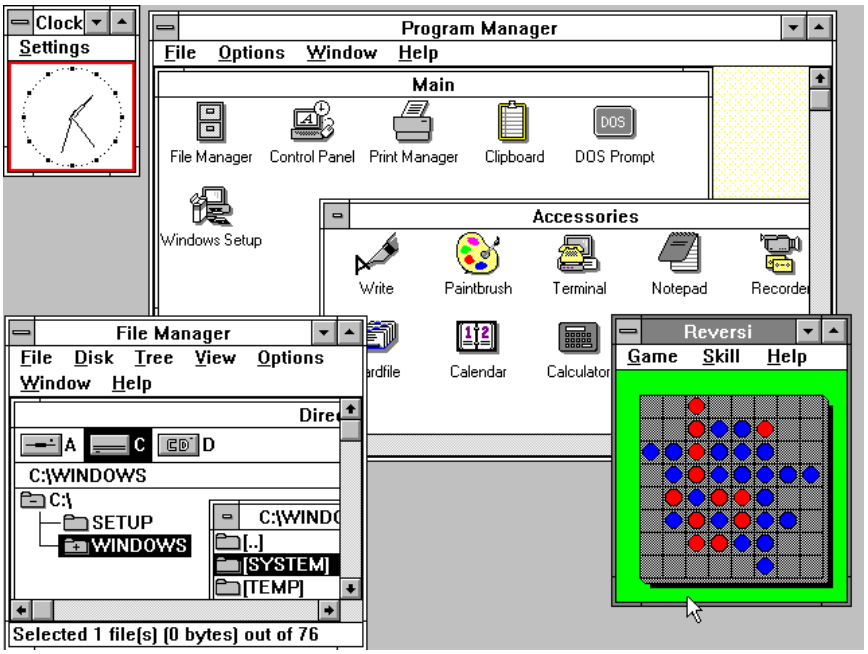


```
Seattle DOS version 3.1
Command v 3.10 (C)Copyright Microsoft Corp 1981, 1985
Copyright 1984, 1985 Falcon Technology, Inc.

Current date is Sun  1-07-2018
Enter new date (mm-dd-yy):
Current time is  0:36:35.75
Enter new time:

A>dir /w

 Volume in drive A is SEADOS31MAS
 Directory of  A:\

COMMAND  COM    ASSIGN   COM    ATTRIB   EXE    BACKUP   COM    BADSPOT  COM
CHKDSK   COM    DEBUG    COM    DISKCOPY COM    EDLIN    COM    EXE2BIN  EXE
FC       EXE    FDISK    COM    FIND     EXE    FORMAT   COM    GRAPHICS COM
JOIN     EXE    LABEL    EXE    LINK     EXE    MODE     COM    MORE     COM
MOVE     COM    PRINT    COM    RECOVER  COM    RENDIR   COM    RESTORE  COM
SHARE    EXE    SHIPDISK COM    SORT     EXE    SUBST    EXE    SYS      COM
TREE     COM    WHERE    COM
       32 File(s)    100352 bytes free

A>_
```

1.2.1.2 Windows 1-3

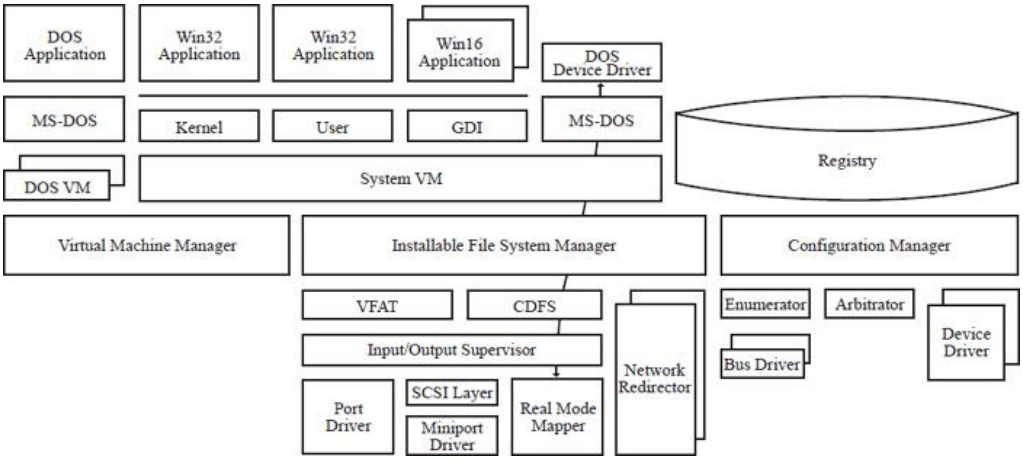
Die Einführung erfolgte 1990 und damit wurde eine graphische Oberfläche für MS-DOS implementiert. Weiterhin kam damit auch die spezielle Speicherverwaltung Virtual Memory Management. Um diese Art der Speicherverwaltung zu umgehen, kann der Protected Mode verwendet werden. Außerdem gibt es Arbeitsgruppen (Workgroups) für Peer-to-Peer Data Share.

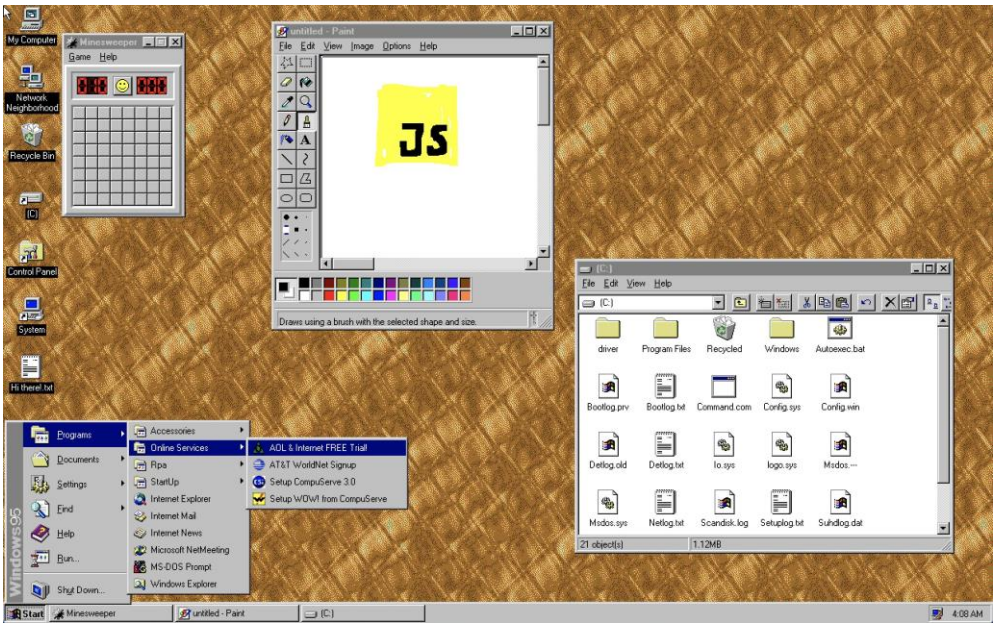




1.2.1.3 Windows 95

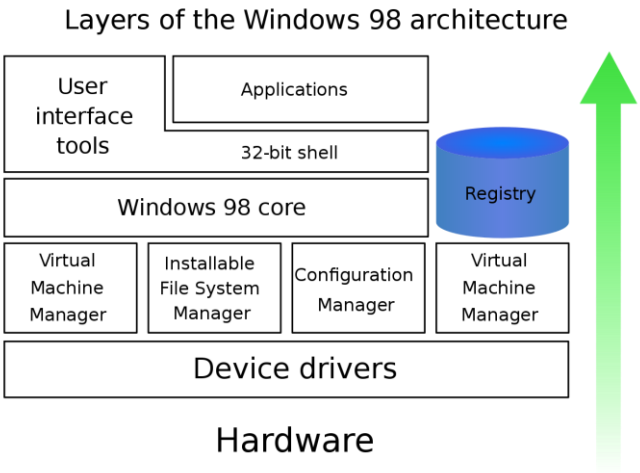
Windows 95 wurde im August 1995 eingeführt und basiert ebenfalls auf MS-DOS. Es bietet einen 32-Bit Support und ermöglicht Dateinamen mit einer Länge von 255 Zeichen. Weiterhin gibt es bei Windows 95 ein Startmenü und eine Taskbar. Windows 95 arbeitet standardmäßig mit dem TCP/IP-Stack und weist ebenfalls einen Internet Explorer sowie eine DirectX-API für Spiele auf.





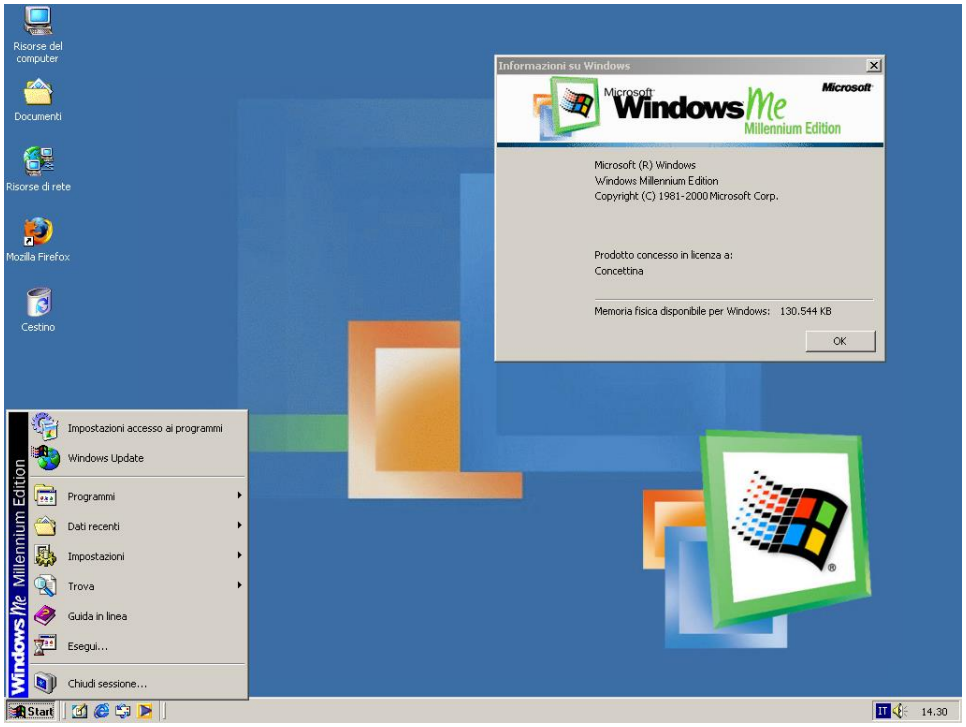
1.2.1.4 Windows 98

Die Einführung von Windows 98 erfolgte im Juni 1998. Es basiert auf dem eben vorgestellten Windows 95. Dabei wird mit einem Windows Driver Module gearbeitet. Bereits integriert sind der Internet Explorer und Outlook. Des Weiteren gibt es einen erweiterten USB-Support sowie eine Navigationshistorie, wobei vor- und zurückgeblättert werden kann.

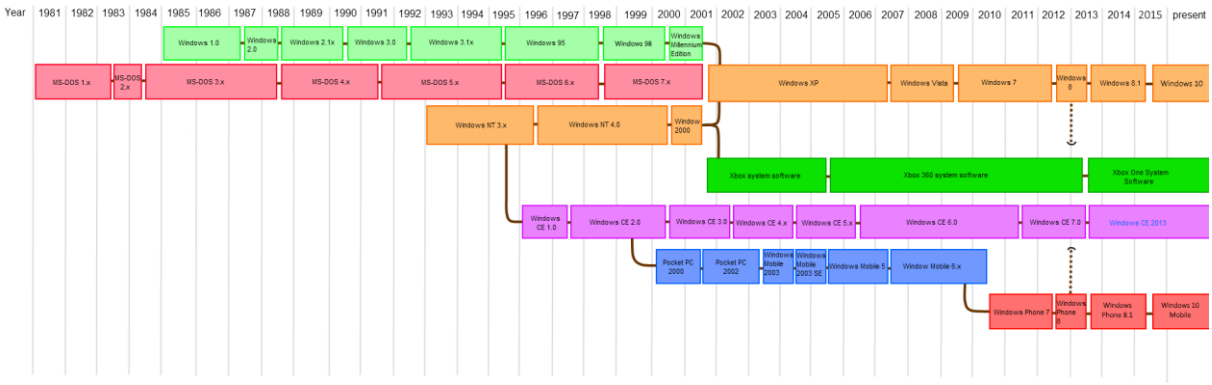


1.2.1.5 *Windows ME*

Windows ME wurde im September 2000 eingeführt. Es ist mit einem Windows Movie Maker, einem Windows Media Player und einem Windows DVD Player ausgestattet. Weiterhin erfolgt hier eine Optimierung der 9x Reihe. Zudem gibt es eine Plug and Play Ausrichtung, sodass API-Schnittstellen für Kameras und Scanner, USB-Storage Support, Universal Plug and Play (UPnP) und Network Crawling für lokal Shares implementiert sind.



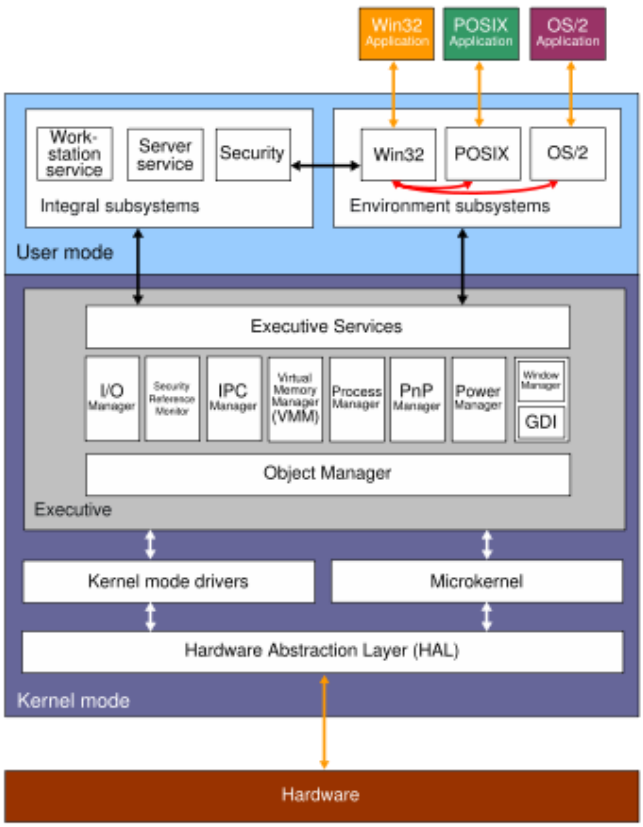
1.2.1.6 Windows NT

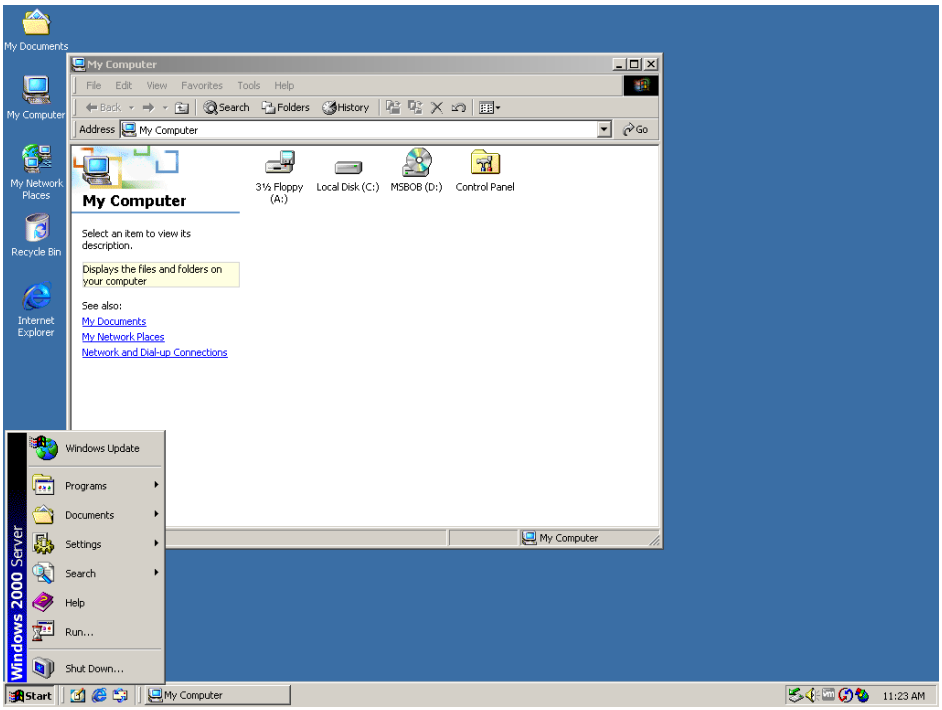


1.2.1.7 Windows 2000

Windows 2000 wurde im Februar 2000 eingeführt und implementiert die neue NT-Architektur. Diese Architekturbasis ist bis heute implementiert. Hiermit kam eine starke Businessorientierung und das Active Directory wurde eingeführt.

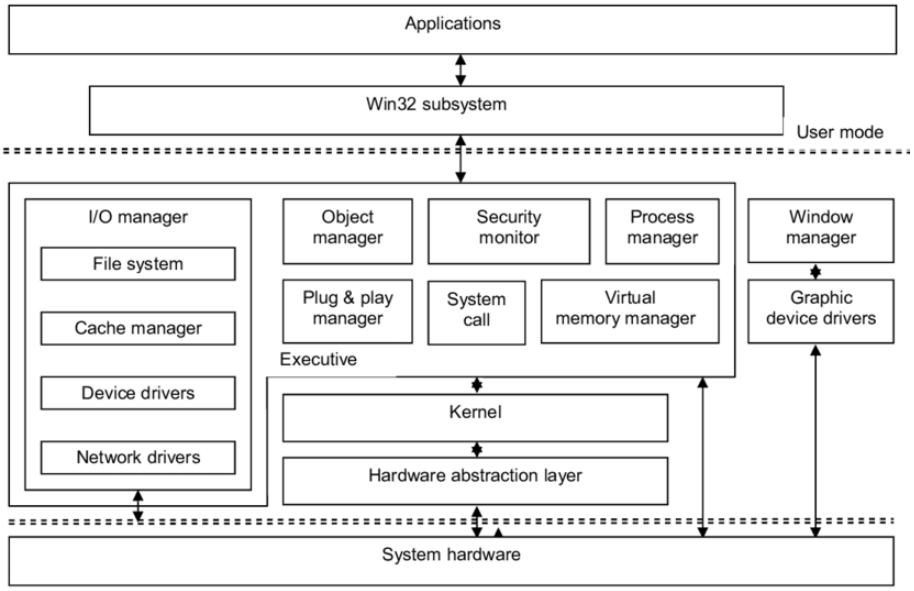
Weiterhin bietet Windows 2000 ein Encryption File System, ist Plug and Play Driver orientiert und besitzt ein Windows Driver Module. Zusätzlich gibt es einen Logical Disk Manager (Software RAID) und Accessability Features wie das Screen Keyboard.

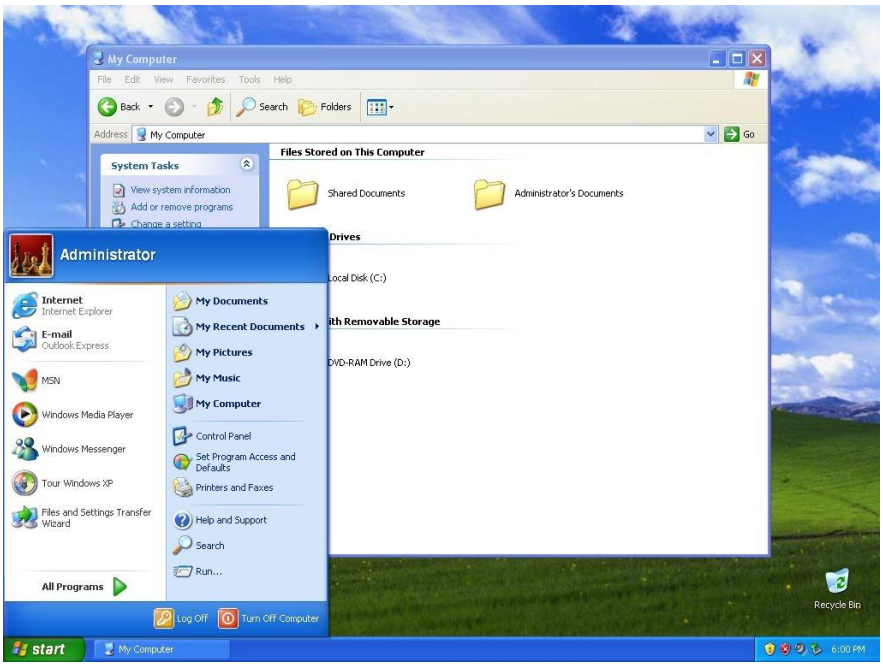




1.2.1.8 *Windows XP*

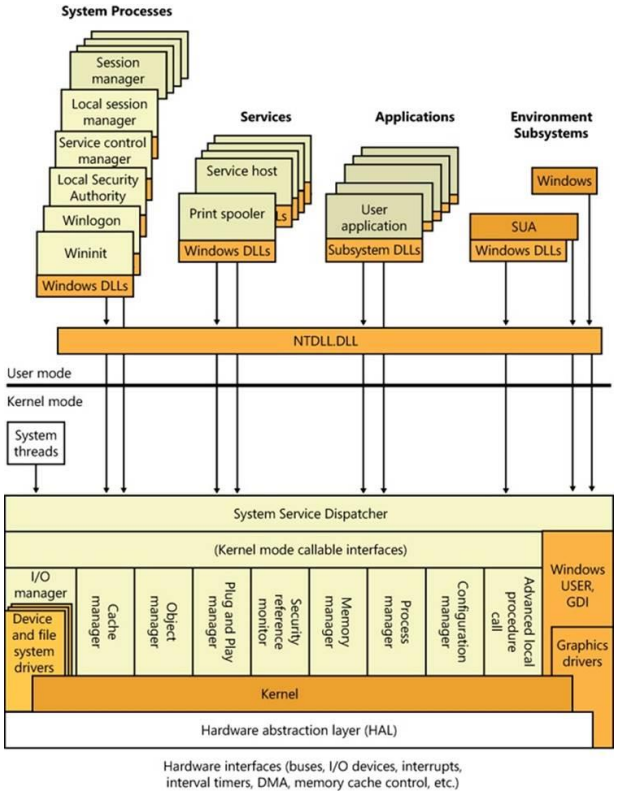
Windows XP wurde im Oktober 2001 veröffentlicht und besteht aus der Architektur von Windows NT und Programmen aus der 9x-Serie. Mit dieser Version wurde das Session Switching zwischen Nutzern eingeführt und ein Logout erfordert nicht mehr das Schließen der Programme. Weiterhin gibt es ein neues UI-Design und das prefetching von Programmen für das schnellere Starten wurde möglich.





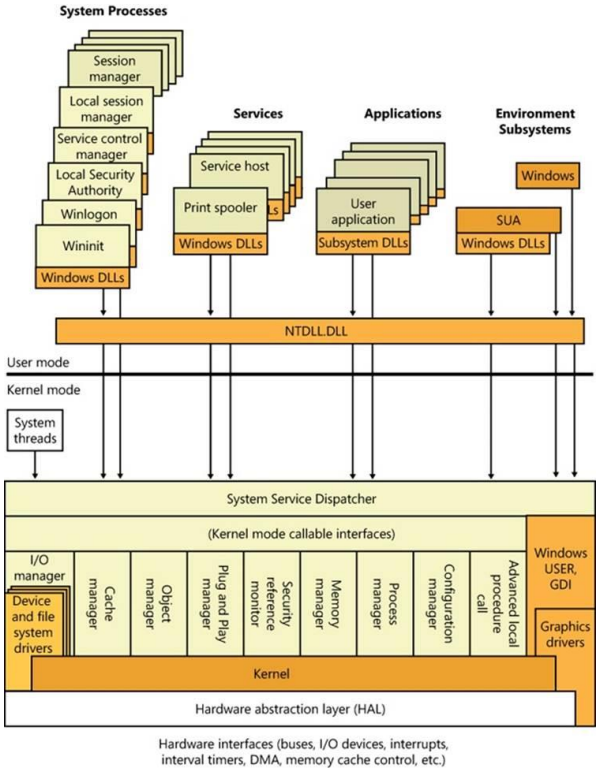
1.2.1.9 Windows Vista

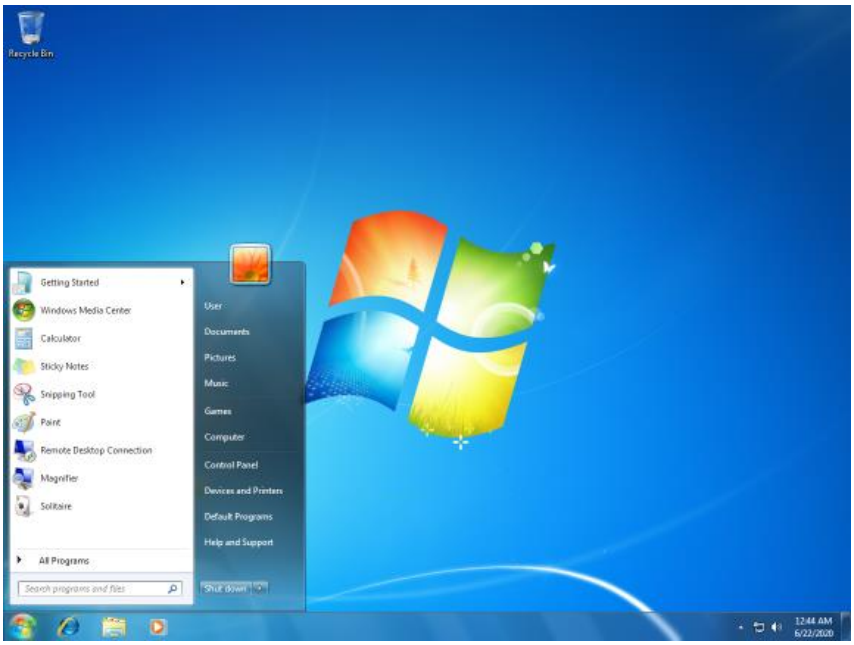
Windows Vista wurde im Januar 2007 veröffentlicht. Es bietet eine graphische UI mit Transparenz und User Account Control, wobei die Rechte des normalen Nutzers nach dem Unix Vorbild eingeschränkt werden. Weiterhin sind in dieser Version Komponenten wie der Windows Defender, Schattenkopien („shadow copy“) und die Spracherkennung integriert. Mit Windows Vista wurde ein voller IPv6-Support durchgesetzt sowie die BitLocker Drive Encryption, Code/Heap Integrity Checks und Address Space Layout Randomization.



1.2.1.10 Windows 7

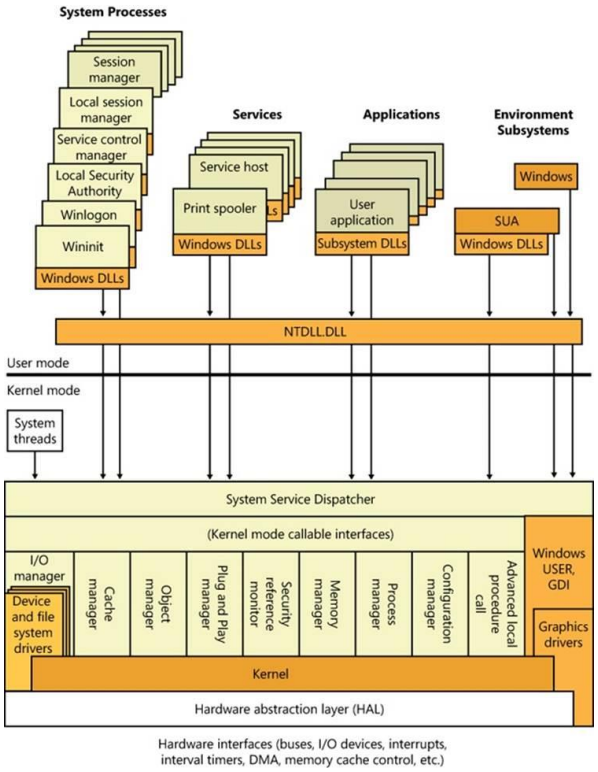
Windows 7 kam im Oktober 2009 heraus. Mit dieser Version wurde die Handschriftenerkennung integriert und die Performance in Bezug auf Multicore CPUs optimiert. Weiterhin ist in dieser Version die Windows Power Shell integriert und Windows 7 bietet eine Unterstützung für virtuelle Festplatten. Ein weiteres Merkmal ist, dass von Microsoft signierte Programme keine Sicherheitsfreigabe erfordern, sodass insgesamt weniger Sicherheits-Popups aufgerufen werden.





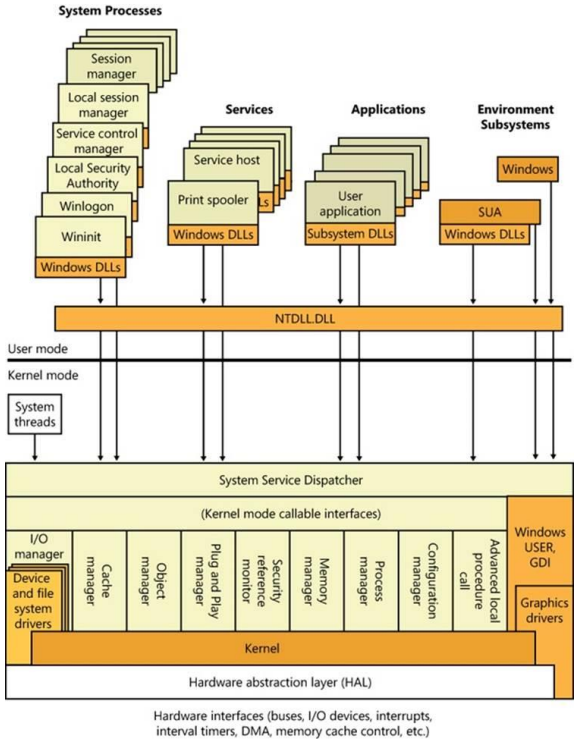
1.2.1.11 Windows 8

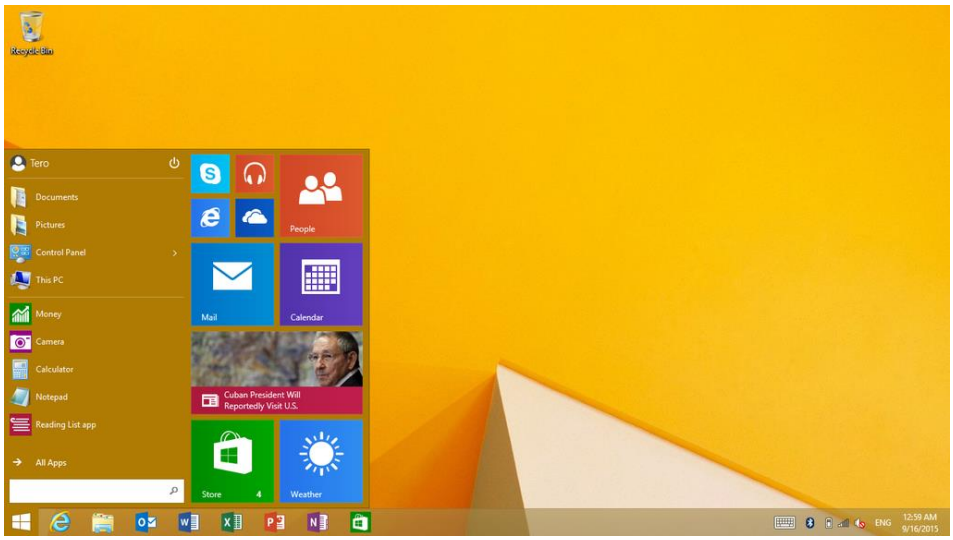
Windows 8 gibt es seit Oktober 2012. Das Userinterface wurde auf Touch optimiert. Außerdem gibt es ab sofort die UEFI Secure Boot Funktion. Des Weiteren wird Windows RT für die ARM Architektur verwendet und es gibt die Funktion Windows To Go (LiveUSB). In Windows 8 werden auch USB 3.0 sowie die PIN und Picture Authentication unterstützt. Mit dem Microsoft Account wird ebenfalls die Verwendung der Cloud unterstützt.



1.2.1.12 Windows 8.1

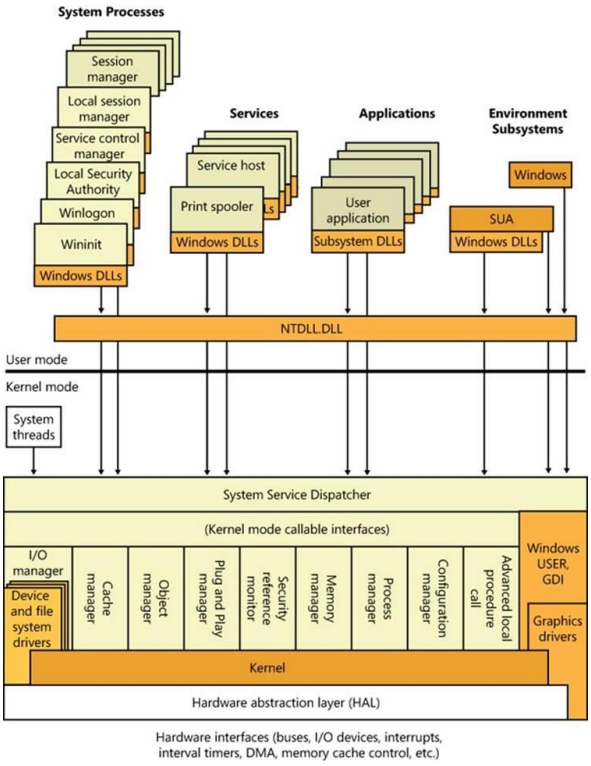
Windows 8.1 wurde im Oktober 2013 eingeführt. In dieser Version wurde vor allem auf Benutzerkritik eingegangen, um Mängel zu beheben. Aufgrund dessen wurde das Startmenü wieder nativ aktiv designed. Weiterhin wurde die Performance von Cloud-Diensten verbessert und der Dienst OneDrive integriert. Die Transparent Device Encryption erfolgt mit Bitblocker und der KeyStorage im Active Directory oder der Microsoft Cloud (MS-Cloud). Auch der Windows Defender wurde erweitert. In diesem Fall wurde ein Intrusion Detection System hinzugefügt.

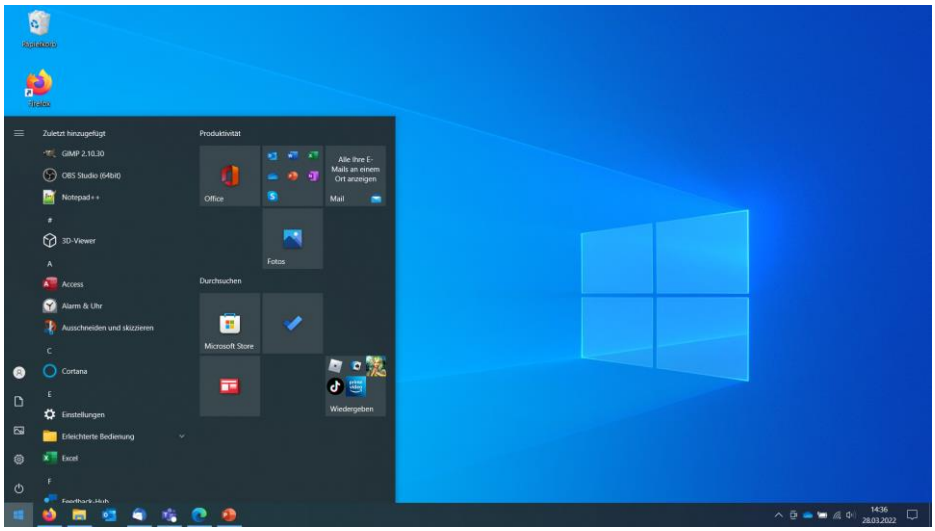




1.2.1.13 Windows 10

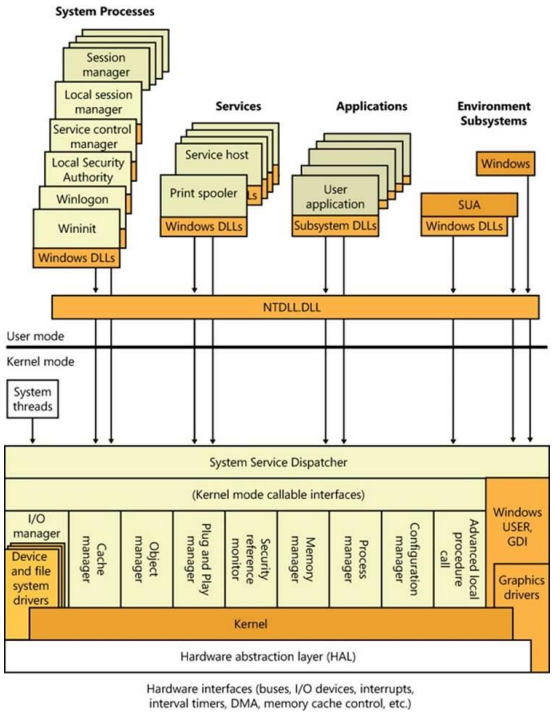
Windows 10 wurde im Juli 2015 veröffentlicht und mit dem Cortana Personal Assistant ausgestattet. Außerdem wurde Xbox Live integriert und Microsoft Edge als Webbrowser standardmäßig mit installiert. Windows 10 führt eine User Activity Analyse durch und setzt seinen Fokus auf die Werbung. Anwendungen können im Microsoft Store, dem Appstore von Microsoft, heruntergeladen werden. Außerdem wurde das UI für 2-in-1-PCs wie Microsoft Surface optimiert. Für die Authentifizierung besteht mit Windows 10 nun die Möglichkeit, diese mit der Gesichtserkennung durchzuführen. Weiterhin gibt es nun ein Windows Subsystem für Linux.





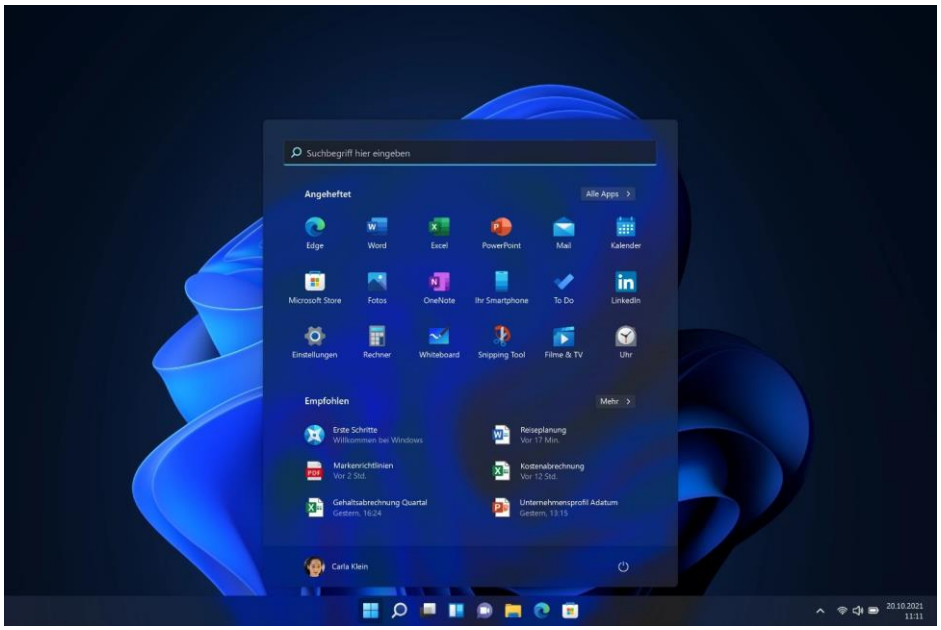
1.2.1.14 Windows 11

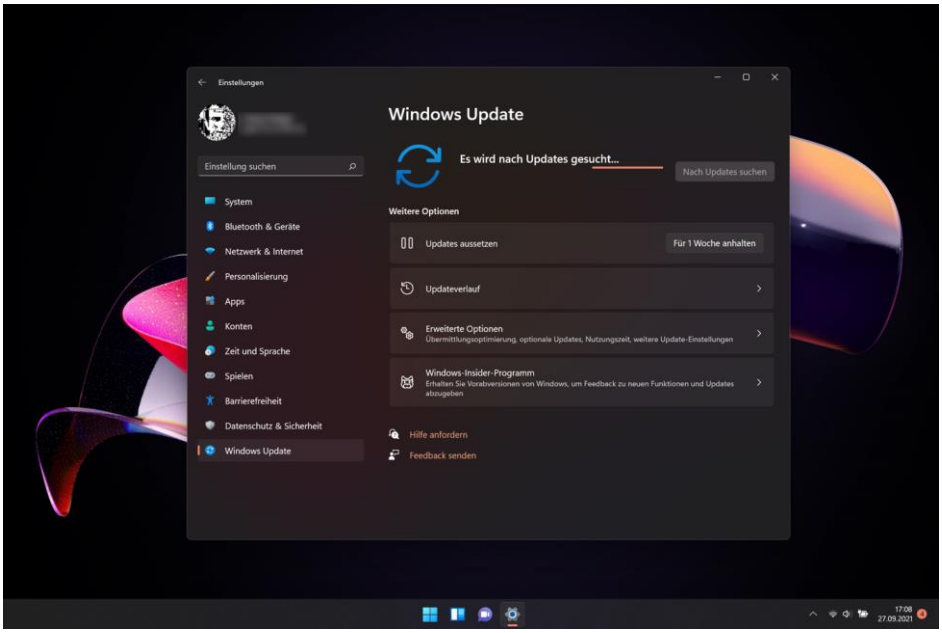
Windows 11 wurde im Oktober 2021 eingeführt. Es ist nur noch als 64 Bit System verfügbar. Außerdem gibt es UEFI nur noch in Kombination mit dem TPM (Trusted Platform Module) Chip. Android Anwendungen sind über das Subsystem verfügbar und Microsoft Teams ist automatisch in Windows 11 integriert. Weiterhin orientiert sich das Design von Windows 11 an dem von Apple und bietet auch wieder virtuelle Desktops, sodass geöffnete Programme übersichtlicher geordnet werden können.



Graphische Oberfläche

Die graphische Oberfläche von Windows 11 bietet den Dark Modus an. Weiterhin ist die Taskleiste zentriert, wobei hierfür Apple als Vorbild diente. Die Windows Tools haben ebenfalls ein neues Design bekommen. In der Praxis gibt es vermutlich als ein Mix aus Windows 7, 10 und 11. Des Weiteren sind die Desktop Widgets von Vista zurück und das Startmenü geht mit seinen Kacheln wieder eher in die Richtung von Windows 8. Die folgenden Abbildungen zeigen das Startmenü und die Einstellungen.





Android Apps

Windows 11 bietet eine native Unterstützung von Android Apps, wobei dies nur für US-Nutzer gilt (24.03.2022). Als bestätigte Appstores sind der Microsoft Store und der Amazon Appstore verfügbar. Weiterhin wichtig ist, dass die Subsysteme weiter ausgebaut werden. Mit Windows 11 kommt zudem auch ein Windows Subsystem für Android. Es lässt sich vermuten dann es bald auch auf Windows 10 installiert werden kann.

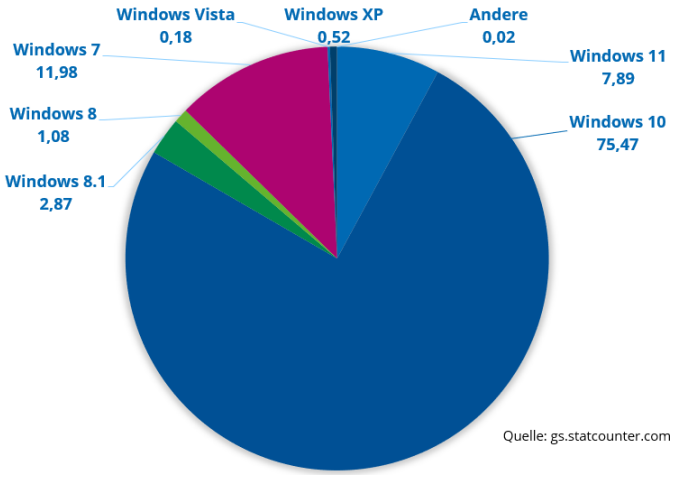
Fazit

Forensisch gesehen ist Windows 11 identisch zu Windows 10, wobei Windows 11 eher wie Windows 10.1 angesehen werden kann (wie damals Windows 8.1).

Es gibt lediglich graphische Änderungen von Farben, der Transparenz und Formen. Weiterhin sind leichte Layoutänderungen und die Veränderung der Subsysteme durchgeführt worden.

1.2.1.15 Windows Historie Zusammenfassung

Der Ursprung von Windows liegt in MS-DOS, woraufhin die Windows 9x-Serie folgte und anschließend Windows NT integriert wurde. Der Fokus wurde vor allem auf Upgrades im Bereich der Oberfläche, Touch und Mobil, Subsysteme für andere OS, Userdaten als neues Geschäftsfeld und Clouddienste gelegt. Die folgende Grafik zeigt den Anteil der verschiedenen Windows Versionen im Februar 2022:



1.2.2 Windows 10 Editionen

1.2.2.1 Lizenzschlüsselarten

In Windows 10 gibt es verschiedene Lizenzschlüsselarten. Dazu zählt unter anderem der Original Equipment Manufacturer (OEM). Hierbei installieren Hersteller von Hardware Windows als Betriebssystem schon vor und dieser Lizenzschlüssel ist dann an exakt diese Hardware gebunden.

Ein weiterer Lizenzschlüssel ist der Retail Key. Diesen kann man im Laden oder bei Händlern erwerben. Er ist an die Hardware der ersten Installation gebunden. Hierbei werden leichte Änderungen der Hardware toleriert.

Die Volumen Lizenz ist ebenfalls eine Art Lizenzschlüssel. Sie lässt sich mehrmals aktivieren, wobei das Volumen selbst die Häufigkeit festlegt, wie oft sie aktiviert werden kann.

1.2.2.2 Heimgebrauch

Die Edition Home wird für den normalen Benutzer empfohlen. Pro hingegen bietet sich für Heimnutzer mit erhöhtem technischem Bedarf an. Die ausgeprägteste Edition ist Pro für Workstations. Diese ist vor allem für Heimnutzer mit hohem Rechenbedarf vorgesehen.

Edition	Max RAM	Max CPUs	Max Cores	Hyper-V	Bitlocker	Long Term Service
Home	128GB	1	64	Nein	Nein	Nein
Pro	2TB	2	128	Ja	Ja	Nein
Pro for Workstations	6TB	4	256	ja	ja	Nein

1.2.2.3 Enterprise

Die Edition Education wird meist für Computer in Lehrinstituten eingesetzt, wohingegen Pro (Education) der Heim-Pro-Version entspricht und somit vom Lehrinstitut für den Privat-PC von Schülern und Studenten lizensiert ist. Die Edition Enterprise ist für den „normalen“ Arbeitscomputer vorgesehen. Die letzte Edition ist Enterprise LTSC, welche für den normalen Arbeitscomputer mit langem Security Support angedacht ist. Dies ist beispielsweise für auf Windows 10 speziell angepasste Software nötig.

Edition	Max RAM	Max CPUs	Max Cores	Hyper-V	Bitlocker	Long Term Service
Education	2TB	2	128	Ja	ja	Nein
Pro (Education)	2TB	2	128	Ja	Ja	Nein
Enterprise	6TB	4	256	Ja	Ja	Nein
Enterprise LTSC	6TB	4	256	ja	Ja	Ja

1.2.3 Systemarchitektur

1.2.3.1 Hardware Abstraction Layer

Die Hardware Abstraction Layer (HAL) bietet Schnittstellen für den Hardwarezugriff. Beispielsweise ist es bei Festplatten möglich, auf alle HDDs auf die gleiche Weise zuzugreifen. Dies ist unabhängig vom physikalischen Aufbau. Die Hardware Abstraction Layer ist zudem ein Teil vom Kernel und in der Datei NTOSKRNL.exe enthalten.

1.2.3.2 Kernel

Der Kernel ist der Kern des Betriebssystems. Bei Windows 10 handelt es sich um einen hybriden Kernel, welcher sich aus dem Selbstmanagement (Windows Manager) und dem Fremdmanagement (Inter Process Communication (IPC) Manager, Client/Server Subsystem) zusammensetzt. Der Kernel orientiert sich am Mach Microkernel.

1.2.3.3 I/O Manager

Der Input/Output Manager ist für die Kommunikation zwischen den Subsystemen zuständig. Er übersetzt die User-Mode read/write Befehle in I/O Request Packets und ist somit für das Schreiben und Lesen von Daten zuständig.

1.2.3.4 Cache Manager

Der Cache Manager arbeitet mit dem Memory Manager, dem I/O Manager und den I/O Drivers zusammen. Er ist für das Cachen von I/O Daten zuständig und arbeitet mit File Blocks.

1.2.3.5 Object Manager

Der Object Manager ist ein Gateway für Subsysteme. Er verwaltet den Zugang zu Ressourcen, wobei er sich sowohl um die physikalischen als auch um die logischen Ressourcen kümmert. Der Objekt Manager sieht alles als Objekt, da Windows NT ein Objekt-Orientiertes Betriebssystem ist.

1.2.3.6 Plug and Play Manager

Der Plug and Play Manager bietet Support für die Festplatte, den Game-Controller, das Audio-Device, Netzwerkkabel und vieles mehr. Er erkennt neue Geräte und kann den Zugriff für diese sowohl einrichten als auch beenden.

1.2.3.7 Security Reference Monitor

Der Security Reference Monitor setzt die Sicherheitsrichtlinien um. Außerdem bestimmt er, ob auf Ressourcen zugegriffen werden darf. Eine weitere Aufgabe des Security Reference Monitors ist die Auswertung der Access Control Listen (ACL).

1.2.3.8 Memory Manager

Der Memory Manager verwaltet den virtuellen Speicher. Er ist für die Memory Protection, das Memory Paging und den General-Purpose Allocator zuständig. Weitere Aufgaben sind das Parsen von PE-Executables und das atomare Ein- und Ausbinden von Anwendungen.

1.2.3.9 Process Manager

Der Process Manager verwaltet Prozesse und Threads. Außerdem ist er für das Starten und Beenden verantwortlich.

1.2.3.10 Configuration Manager

Der Configuration Manager für System Calls für die Registry durch und verwaltet die Registry Datenbank.

1.2.3.11 Advanced Local Procedure Call

Der Advanced Local Procedure Call ist für die Informationsleitung zwischen Subsystemen zuständig. Weiterhin wählt er ein Zielsubsystem aus und führt das Speicher Mapping innerhalb von Subsystemen durch. Weitere Aufgaben sind das direkte Weiterreichen von Daten per Pointer und das Vermeiden von Kopiervorgängen.

1.2.3.12 Graphics Drivers / Windows User GDI

Die Graphic Drivers und das Windows User GDI sind für das Zeichnen von Linien, Pixeln, Kurven und Kreisen zuständig. Außerdem führen sie die Farbverwaltung durch und stellen Bilder, Fenster und 3D-Objekte dar.

1.2.3.13 Kernel Mode Callable Interfaces

Die Kernel Mode Callable Interfaces stellen Schnittstellen für User-Mode-Prozesse zur Verfügung. Außerdem bilden sie eine Abstraktionsschicht, sodass Kernel oder Systemänderungen die API nicht ändern.

1.2.3.14 System Service Dispatcher

Der System Service Dispatcher mapped User-Space Adressen zu den entsprechenden System Call Funktionen.

1.2.3.15 NTDLL.DLL

NTDLL.DLL ist eine Schnittstelle für User-Prozesse. Sie ist hauptsächlich für das Mapping von Kernel-APIs in den User-Space zuständig.

1.2.3.16 Anwendungen

Es gibt verschiedene Kategorien von Anwendungen. Zu den Systemanwendungen gehören der Anmeldemanager, die Druckerwarteschlange, der Datei-Explorer oder ähnliches. Eine weitere Kategorie bilden die Benutzeranwendungen, zu welchen Anwendungen wie Power-Point oder Gimp2 gehören. Die letzte Kategorie bilden die Subsysteme wie Ubuntu, Android oder Ähnliches.

1.2.4 Zusammenfassung

In diesem Kapitel haben Sie die Historie und den Entwicklungsprozess des Microsoft Windows Betriebssystems erfahren.

Es wurde auf die einzelnen Betriebssystem Versionen und für Windows 10 auf die unterschiedlichen Lizenz-Editionen eingegangen. Damit sollte grob bekannt sein, welche Features mit welcher Version implementiert wurden. Darüber hinaus sollte die Vermarktungsstrategie von Microsoft der letzten Jahre deutlich geworden sein.

Zuletzt haben Sie die Windows-NT Architektur kennen gelernt. Hierbei wurde auf die einzelnen Komponenten eingegangen. Es wurde ein kurzer Überblick über deren Funktion gegeben.

1.3 Windows Systemeinrichtungen und Systemadministration

1.3.1 Installation

1.3.1.1 Systemvoraussetzung Windows 10

Bei Windows 10 müssen für die Installation bestimmte Systemvoraussetzungen gegeben sein:

- 1 GHz Prozessor oder schneller
- 2 GB Arbeitsspeicher
- 20 GB Festplattenspeicher
- Grafikkarte mit DirectX 9 oder höher und WDDM 1.0-Treiber
- Auflösung von 800x600
- Internetverbindung für Aktivierung
- UEFI v2.3.1 Errata B für Secure Boot
- Trusted Platform Module (TPM) 1.2 oder höher sowie ein Trusted Computing Group (TCG) kompatibles BIOS oder UEFI für Bitlocker

1.3.1.2 Installationsmöglichkeiten

Bei der Installation wird zwischen einer manuellen und einer automatisierten Installation unterschieden. Die manuelle Installation wird eher für den privaten Gebrauch oder Kleinunternehmen angewandt, wohingegen die automatisierte Installation in Behörden oder Großunternehmen eingesetzt wird.

Für die manuelle Installation wird ein Update von Windows 7, 8 oder 8.1 durchgeführt. Eine Wiederherstellung erfolgt mittels der Wiederherstellungspartition. Als Installationsmedium wird ein USB-Stick oder eine DVD gewählt.

Die zweite Möglichkeit ist die automatisierte Installation. Diese wird mithilfe von PXE-Boot (Installation über Intranet) durchgeführt. Diese Installationsvariante wird bevorzugt im Businessbereich verwendet. Falls dies bislang bei Ihnen nicht vorhanden ist, wenden Sie sich an Ihren Administrator.

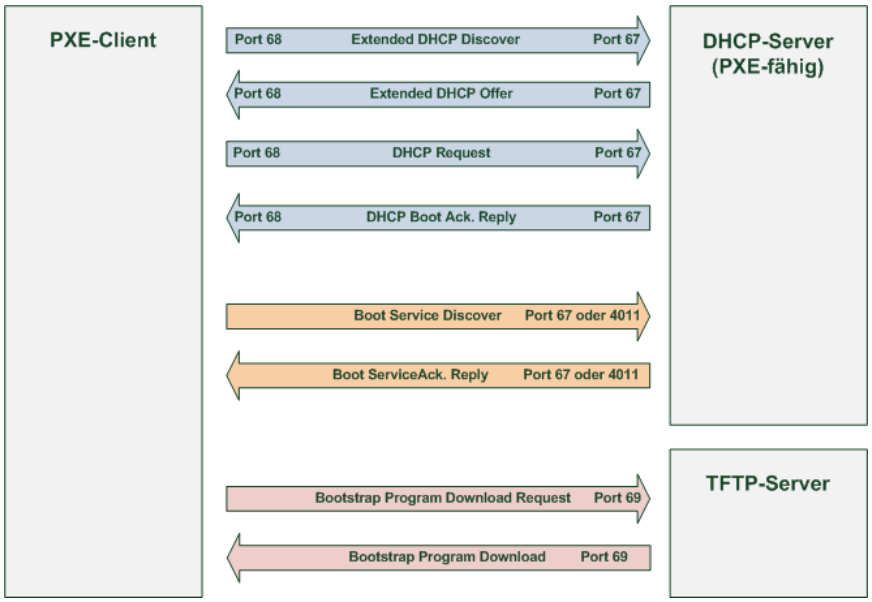
1.3.1.3 Installationsmedium (USB-Stick)

Hierfür wird das *MediaCreationTool* von Microsoft heruntergeladen und ausgeführt. Daraufhin wird „Installationsmedium für einen anderen PC erstellen“ ausgewählt. Anschließend erfolgt die Wahl der Windows Variante sowie die Auswahl des USB-Speichersticks, wobei dieser mindestens 8GB umfassen sollte.

Der USB-Stick wird am Ziel-PC angeschlossen und das Booten erfolgt direkt vom USB-Stick. Beim Booten muss das BIOS mit F12, F8 oder der Entf-Taste aufgerufen und der USB-Stick als Bootoption ausgewählt werden. Anschließend folgt man den Installationsanweisungen.

1.3.1.4 Installation über PXE

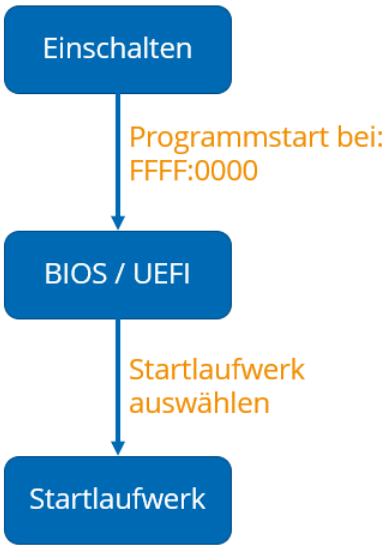
Bei der Installation über PXE handelt es sich um eine automatisierte Zero Touch Installation, womit die Windows-Installation und Konfiguration durchgeführt wird. Die Installation erfolgt über das Intranet, wobei auch Anwendungen mit installiert werden. Hierbei wird der Arbeitsplatz vordefiniert bereitgestellt. Außerdem reduziert die automatisierte Installation die Arbeitslast für den Nutzer und den Administrator.



Über den DHCP-Server erfolgt die Netzwerkkonfiguration des Clients und man erhält Informationen über den TFTP-Server. Der TFTP-Server hingegen stellt das Boot-Image zur Verfügung.

1.3.2 Bootvorgang

1.3.2.1 Startprozess Computer



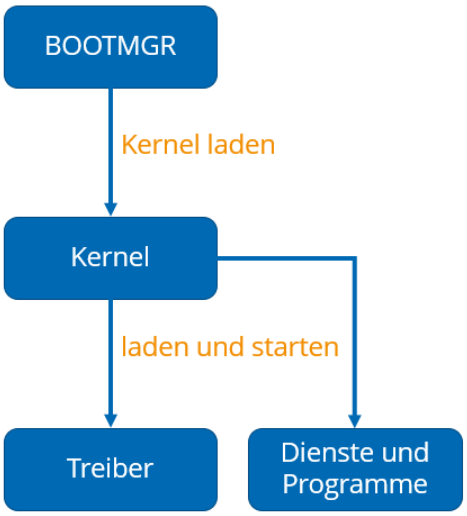
Beim Einschalten des Computers werden die PWR_SW-Pins kurzgeschlossen und die Hardware mit Strom versorgt. Der Programmstart ist bei FFFF:0000.

Das BIOS vollzieht entweder einen Kalt- oder ein Warmstart (Adresse 0000:0472 = 1234?) und führt eine Systemdiagnose (Power on Self Test = POST) durch. Außerdem erfolgt der Zugriff auf das Startlaufwerk (HDD, SSD, USB, DVD).

Das Startlaufwerk führt den Master Boot Record (MBR) aus. Daraufhin wird die Partitionstabelle ausgewertet und die primären Partitionen geladen. Dann folgt die Übergabe an den Boot Manager (NTLDR / BOOTMGR / grub2).

UEFI lädt den Boot Manager direkt und für die Übergabe an den Boot Manager durch.

1.3.2.2 *Windows NT Bootprozess*

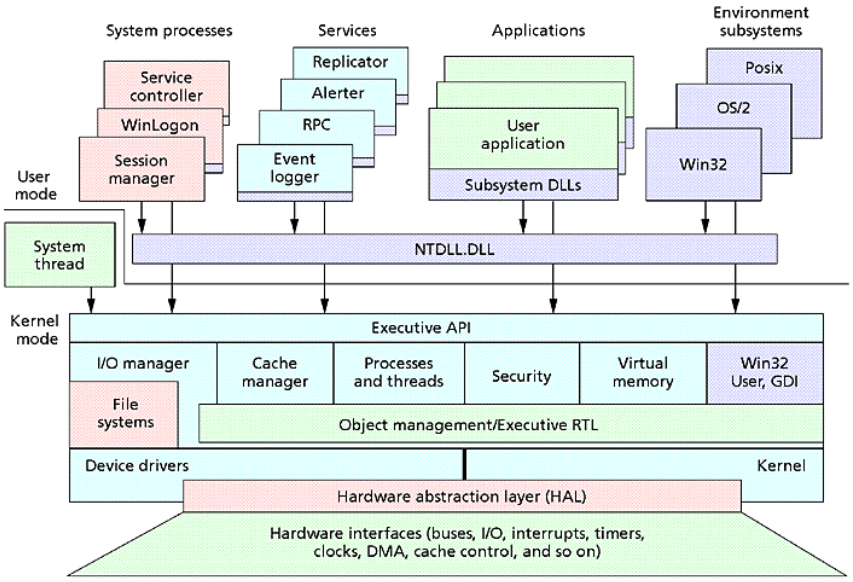


Der Bootmanager lädt den Kernel. Dafür werden die Boot-Konfiguration (Boot Configuration Data), der Core Device Driver (Hal.dll) und der Kernel (winload.exe / winload.efi) sowie die Registry wird geladen.

Der Kernel startet die Datei ntoskrnl.exe, welche auch als Kernel Image bezeichnet wird. Weiterhin führt der Kernel eine Hardwareabstraktion durch und ist für das Memory Management verantwortlich.

Der Kernel lädt zusätzliche Treiber wie Sound, Grafik oder die Eingabe. Außerdem startet er Dienste und Programme wie Windows Services, Subsysteme, den Explorer oder die GUI.

1.3.2.3 *Windows NT Architektur*



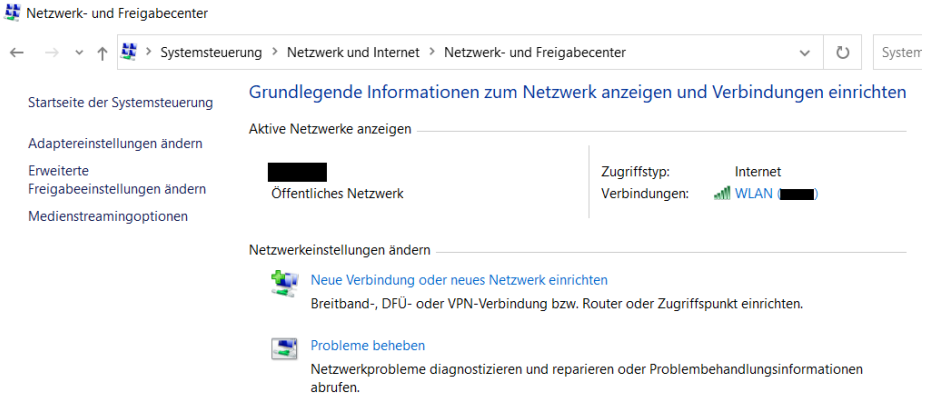
1.3.3 Systemverwaltung

1.3.3.1 Systemsteuerung

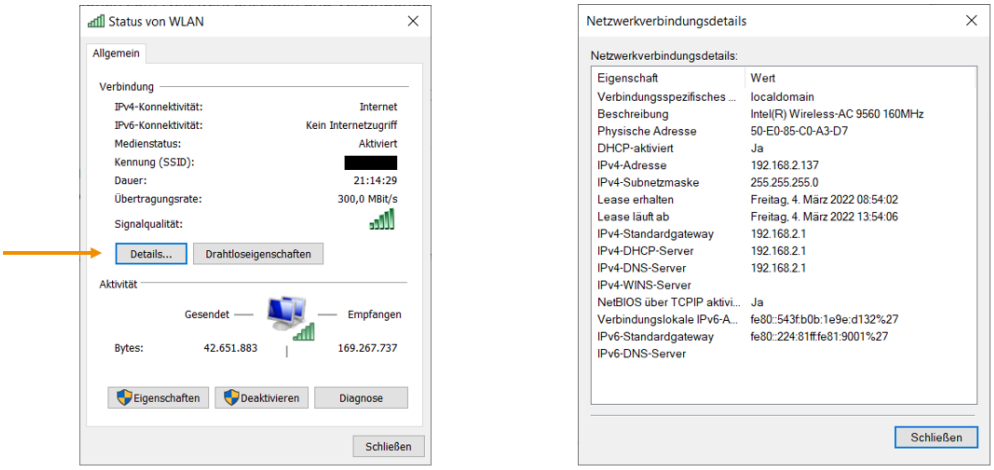
Die Systemsteuerung ist das zentrale Steuerpanel für den Endnutzer.

1.3.3.2 Netzwerkcenter

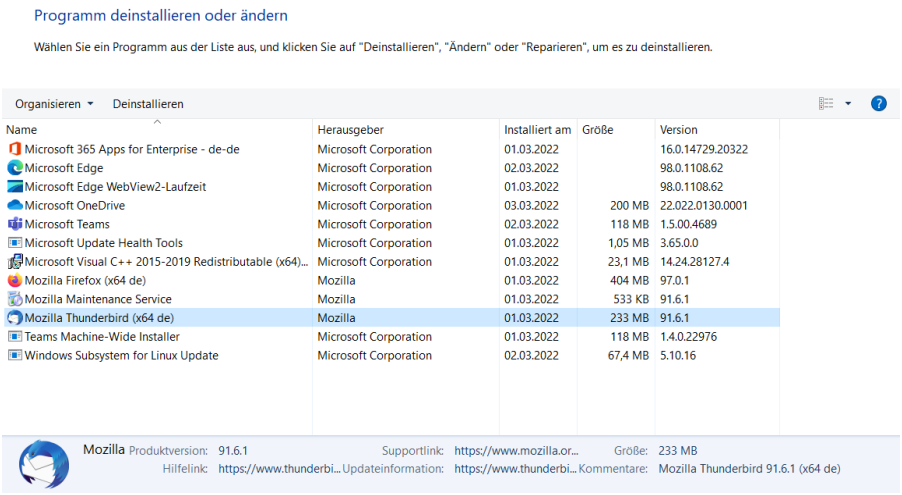
Das Netzwerkcenter ist für die Verwaltung der Netzwerkverbindungen zuständig. In dieser Abbildung ist ersichtlich, dass der Computer mit dem WLAN verbunden ist.



1.3.3.3 Verbindungsdetails



1.3.3.4 Programme installieren



Hier wird eine Übersicht über die Installierten Programme gegeben. Die Deinstallation kann hier ziemlich einfach durchgeführt werden. Weiterhin werden Programmdetails angezeigt. Dazu zählen Informationen wie der Hersteller, der Speicherbedarf, das Installationsdatum sowie die Version.

1.3.4 Konsolen

1.3.4.1 CMD (Windows Eingabeaufforderung)

CMD ist die historische Windows-Shell von OS/2. DOS-Befehle können eingegeben werden und Skripting ist möglich. Der „help“-Befehl wird für eine genauere Erläuterung verwendet. Unterstützte Befehle sind assoc, call, cd, color, copy, date, del, endlocal, for, format, ftype, goto, help, if, mkdir, popd, pushd, prompt, set, setlocal, shift, start, …

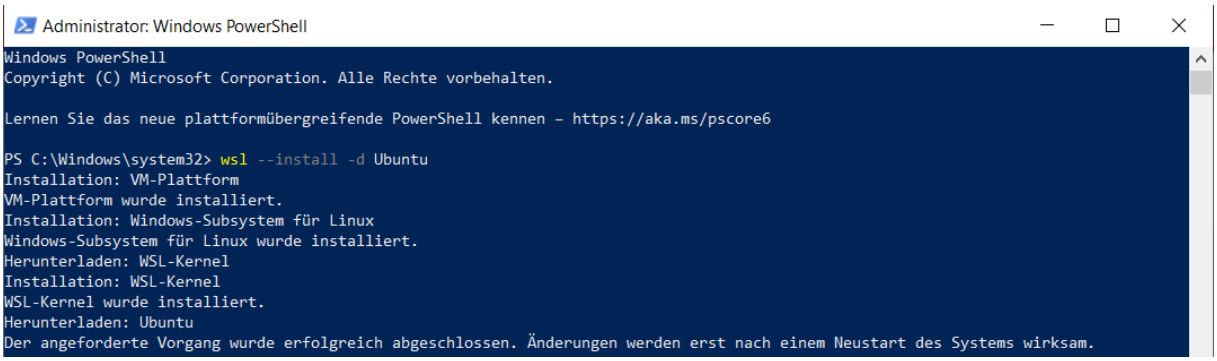
1.3.4.2 Power Shell

Die PowerShell ist seit Windows 7 vorinstalliert und wird für Skripte und die Konfiguration des Systems verwendet. Sie kann auf WMI-Klassen, COM-Objekte und das .NET-Framework zugreifen. Die cmdlets sind vordefinierte Befehle. Weiterhin kann der „get-help“ Befehl angewendet werden, um einen detaillierten Hilfstext anzeigen zu lassen.

1.3.4.3 Bash (Bourne-again-Shell)

Die Bash ist eine mächtige Shell aus der Unix-Welt. Sie ist skriptfähig und unterliegt dem Standard *IEEE POSIX P1003.2/ISO 9945.2 Shell and Tools standard conform*. Weiterhin ist sie unter einer GPL-Lizenz quelloffen. Vorteilhaft ist, dass die Bash umfangreich dokumentiert ist und viele Beispiele online verfügbar sind.

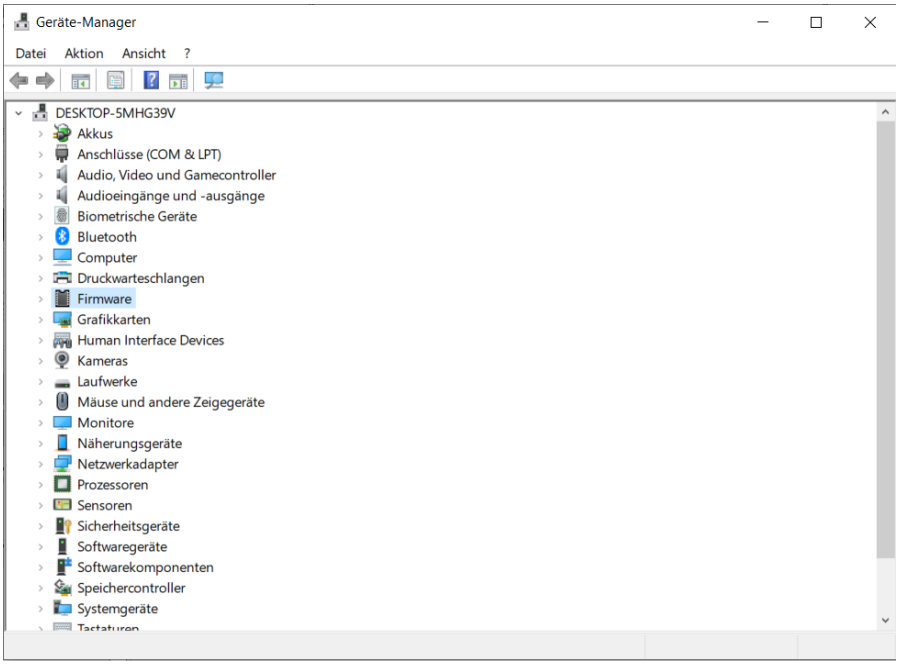
Die Nutzung der Bash erfolgt über WSL (Windows Subsystem for Linux) und die Installation erfolgt mittels der PowerShell:



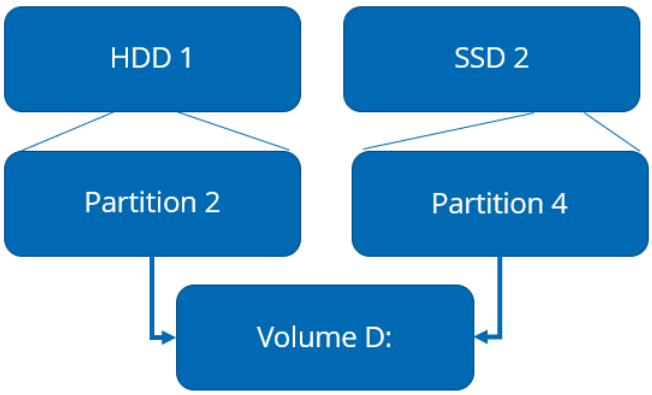
1.3.5 Geräte unter Windows

1.3.5.1 Gerätemanager

Der Gerätemanager liste alle aktuell angeschlossenen Geräte sowie alle bisher angeschlossenen Geräte auf. Außerdem verwaltet er den Gerätetreiber.



1.3.5.2 Laufwerke



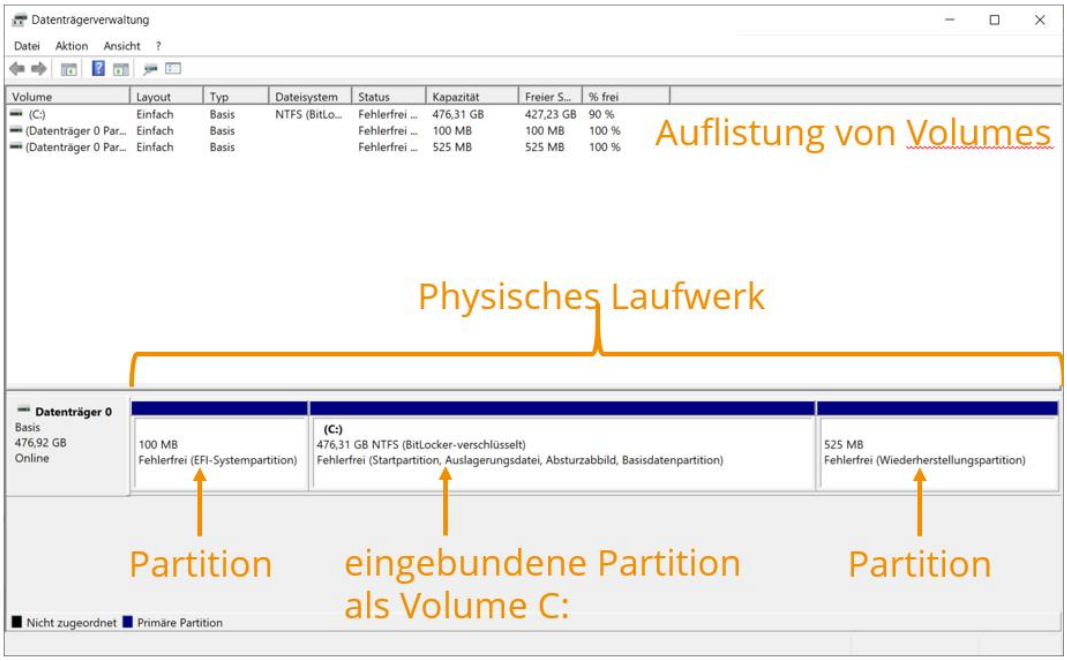
Physische Laufwerke sind die Hard Disk Drive (HDD), die Solid State Drive (SSD), die Digital Video Disk (DVD) und USB-Sticks

Logische Laufwerke hingegen sind die Partitionen, RAID Systeme und das Netzwerklaufwerk.

Volumes sind eine Zusammenfassung eines oder mehrerer logischer Laufwerke und sind im Dateiexplorer sichtbar.

1.3.5.3 Datenträgerverwaltung

Die Datenträgerverwaltung listet Datenträger, logische Laufwerke und Volumes auf. Die Verwaltung von Datenträgern erfolgt durch Partitionieren. Hingegen erfolgt die Verwaltung von Volumes durch Formatieren, Erstellen von RAID-Volumes und das Festlegen von Laufwerkbuchstaben.



1.3.5.4 Automatische Laufwerksbuchstaben

- A: Diskette 1
- B: Diskette 2
- C: Festplatte 1
- D:, E:, …
  - weitere Festplatten
  - interne Laufwerke (CD, DVD, Blue-Ray, …)
  - externe Datenträger (USB-Stick, DVD, …)
- … , X:, Y:, Z:
  - Netzwerklaufwerke

1.3.6 Dienste und Systemprozesse

1.3.6.1 Programmbezeichnungen

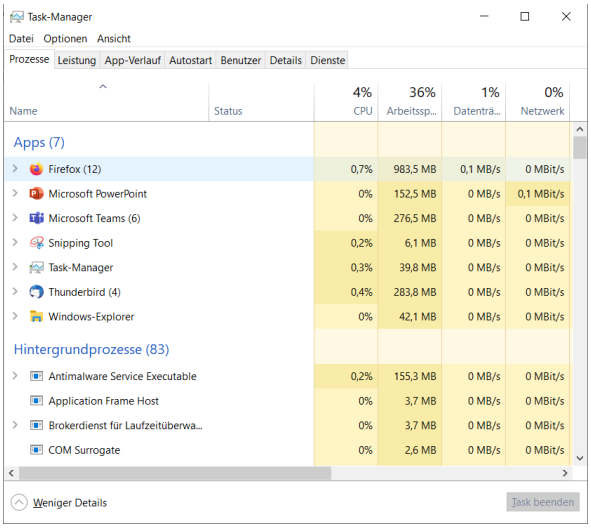
Dienste bezeichnen Anwendungen ohne eine graphische Oberfläche (GUI). Sie sind für periodische und zeitaufwendige Aufgaben geeignet.

Systemprozesse sorgen für die Funktionalität des Betriebssystems. Dafür stellen sie die Infrastruktur für Anwendungen bereit. Außerdem bilden sie eine Schnittstelle zwischen dem Nutzer und dem Betriebssystem.

Anwendungen bzw. App(lications) sind die Programme für den Endnutzer. Sie haben meistens eine graphische Oberfläche.

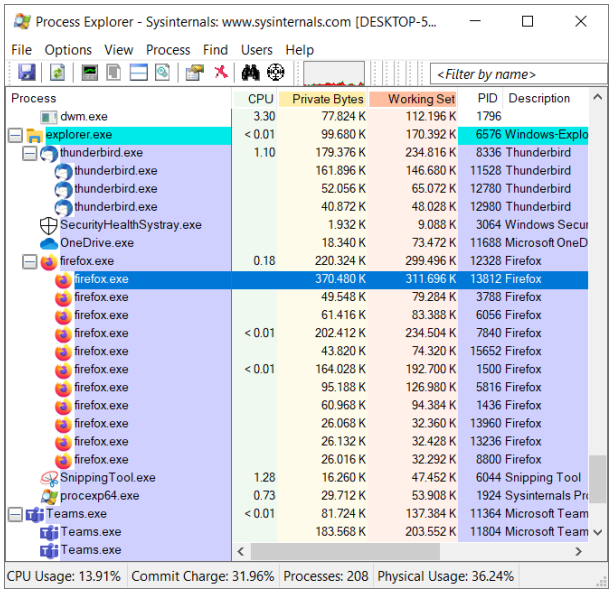
1.3.6.2 Taskmanager

Der Taskmanager listet Prozesse auf und kann über die Tastenkombination strg + shift + esc aufgerufen werden. Weiterhin kann der Taskmanager die Programmbeendung erzwingen, die Systemauslastung anzeigen, Autostartprogramme festlegen und Eingeloggte Benutzer anzeigen.



1.3.6.3 ProcessExplorer

Der ProcessExplorer ist kostenlos von Microsoft über die Sysinternals Suite verfügbar. Er liefert mehr Details über die Prozesse und kann die hierarchische Prozessstruktur anzeigen. Des Weiteren sind ein RAM Memory Dump sowie eine integrierte Virusüberprüfung über Virustotal verfügbar.



1.3.6.4 Wichtige Dienste

Dienst	Aufgabe
Idle-Prozess	Übernimmt Leerlaufzeit
Kernel	Arbeitet im Kernel-Mode
Registry	Verwaltet Registry Hive Data
Memory Compress	In-RAM-Compression zur Auslagerungsvermeidung
Windows Subsystem Prozess	Schnittstelle zwischen Subsystem und Windows
Windows Logon Process	Benutzeran- und -abmeldung
Explorer	Desktop- und Taskbaroberfläche
Desktop Window Manager	Rendern von Fenstern
Service Host Process	DLL-Prozesse bereitstellen

1.4 Systeminterne Spuren

1.4.1 Überblick

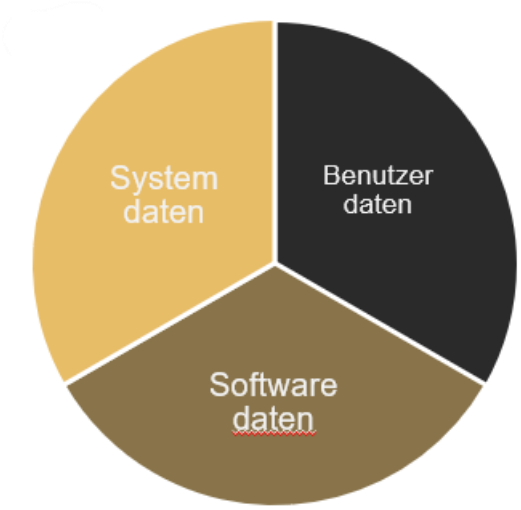
1.4.1.1 Allgemeine Informationen zu Windows

Das von Microsoft ursprünglich verwendete Dateisystem FAT wurde mehrfach erweitert und ab der Windows Version NT (NT steht für New Technology) mit dem Dateisystem NTFS (NT File System) abgelöst. Die Fortführung des FAT Dateisystem steht ebenfalls in Form des exFAT Dateisystems bereit. Auch CDFS / UDF wird unterstützt.

In Hinblick auf Architekturen unterstützt Windows zum einen die x64/iA64 Architektur, sprich ein 64 Bit System und zum anderen ARM64, ebenfalls ein 64 Bit System.

Mit der Einführung von Windows 95 im Jahre 1995 wurde auch eine bestimmte Kategorisierung von anfallenden Daten eingeführt. Windows Betriebssysteme teilen Daten in die drei Kategorien Systemdaten, Benutzerdaten und Softwaredaten auf. Die logische Trennung dieser Daten findet sich dabei an verschiedenen Stellen im Betriebssystemaufbau wieder.

1.4.1.2 Wichtige Verzeichnispfade



Die Systemdaten findet man im Windows Verzeichnis, welches je nach Betriebssystemversion als „WINDOWS“, „WIN“ oder „WINNT“ benannt ist. Softwaredateien befinden sich im Programm Verzeichnis je nach Betriebssystemversion und sind als „Programme“ oder „Program Files“ benannt. Die Benutzerdaten befinden sich im Benutzerdaten-Verzeichnis. Generauer gesagt, für die Windows Versionen Windows 95, 98 und ME im Verzeichnis „Eigene Dateien“, unter Windows NT, 2000 und XP im Verzeichnis „Dokumente und Einstellungen“ und unter Windows Vista, Windows 7, 8, 10 und 11 im Verzeichnis „Users“ in einem Benutzerverzeichnis benannt nach dem Benutzerkontonamen.

Weiterhin werden Einstellungen und anwenderspezifische Daten zu einzelnen installierten Softwareanwendungen in Unterverzeichnissen gespeichert. Unter Windows NT, 2000 und XP in den Unterverzeichnissen „\Anwendungsdaten“ und „\Lokale Einstellungen\Anwendungsdaten“ und unter Windows Vista, 2003, 2008, 2012, 2013, 7, 8 und 10 in den Unterverzeichnissen „\AppData\Local“, „\AppData\LocalLow“ und „\AppData\Roaming“.

Windows (64 Bit) Besonderheiten

Seit der Einführung von 64Bit Windows wird die 32 und die 64Bit-Software in unterschiedlichen Verzeichnissen installiert. Die 32Bit-Programme werden auf einem 64Bit-Betriebssystem in ein Programmverzeichnis installiert, welches den Präfix „(x86)“ besitzt. Diese Trennung wird auch auf der Systemebene durchgeführt. Hier gibt es in Windows 64Bit-Betriebssystemen ein zusätzliches Verzeichnis „SysWOW64“, in welchem sich die 32Bit-Systemkomponenten des Betriebssystems befinden. Daher sollten bei einer forensischen Untersuchung auch diese Verzeichnisse beachtet werden.

1.4.1.3 Spurenarten und Fundstellen

Informationen zu Einstellungen finden sich in der Registry oder auch Registrierungsdatenbank genannt. Außerdem lassen sich Artefakte in den Active Directory Richtlinien und den Einstellungen, welche sich in NTDS.DIT befinden.

Genutzte und gelöschte Dateien finden sich im Papierkorb (Recycle Bin), den Thumbnaildateien, den UAC (User Access Control) Virtual Store Verzeichnissen und der Index.dat (Network Share Access).

Ebenfalls lassen sich Informationen zur Protokollierung finden. Diese Informationen befinden sich in der Registry/Registrierungsdatenbank, in Event Logs (Protokollierung), in Recent (LNK-Dateien) und in Prefetch (Programmstarts) Dateien.

Außerdem gibt es Informationen zu flüchtigen oder veränderbaren Dateien. Diese Informationen befinden sich in Shadow Copies (Schattenkopien), den Windows Backup Files, den Memory Dateien (Hybernation, Pagefile, RAM-Kopien) und in Crash Dumps und Windows Error Reporting (WER).

1.4.2 Die Registrierungsdatenbank

1.4.2.1 Speicherung von Einstellungen in der Registrierungsdatenbank

Die in der Registrierung gespeicherten Daten werden in sogenannte Registrierungshives (englisch für Bienenstöcke) aufgeteilt und in Schlüsseln (Keys) mit Name Wert Paaren (Values) abgelegt. Ein Hive speichert damit einen Teilbaum der Registry. Alle Daten sind in einem Binärformat abgelegt.

Bei Windows NT4, Windows 2000 und späteren Versionen haben die Dateien das Windows NT Registry File (REGF) Format. Für Windows 95, 98 und Me sind die Dateien im Windows 9x Registry File (CREG) Format organisiert.

Ein Hive ist dabei nicht zwangsweise mit einem Haupt- oder Wurzelschlüssel identisch. So gibt es Wurzelschlüssel, die aus mehreren einzelnen Hives bestehen.

Die bereits genannte Trennung der drei Datenformen wird allerdings auch auf Ebene der Registrierung beibehalten. So existieren unterschiedliche Datenbanken in Form von Dateien im Verzeichnis „[Root-Laufwerk]/[Windows Verzeichnis]/System32/Config“. Die Registrierungsdatei für die Benutzereinstellungen befindet sich im jeweiligen Benutzerdaten Verzeichnis unter „[Root-Laufwerk]/[Benutzerdaten Verzeichnis]/[Benutzername]/“. Die Registrierungsdatei für die Benutzerkontenverwaltung wurde mit Windows NT eingeführt. In ihr werden die Einstellungen zu vorhandenen Benutzern des Betriebssystems gespeichert. Seit Windows 7 werden einige der Benutzerinformationen auch in einem weiteren Benutzerspezifischen Schlüssel gespeichert: „\AppData\Local\Microsoft\Windows\usrclass.dat“.

Die Tabelle zeigt eine Auflistung der verwendeten Registrierungsdateien und ihre korrespondierenden Hauptschlüssel:

Typ	Windows 95,98 und ME	Windows NT, XP und höher	korrespondierende Hives
Systemeinstellungen	SYSTEM.DAT	SYSTEM	HKEY_LOCAL_MACHINE/SYSTEM
Softwareeinstellungen	SOFTWARE.DAT	SOFTWARE	HKEY_LOCAL_MACHINE/SOFTWARE
Benutzereinstellungen	USER.DAT	NTUSER.DAT	HKEY_CURRENT_USER/HKEY_USERS
Benutzerkontenverwaltung	-	SAM	HKEY_LOCAL_MACHINE/SAM
Benutzerrechte und Richtlinien	-	SECURITY	HKEY_LOCAL_MACHINE/SECURITY

Von einigen Schlüsseln gibt es auch verlinkte bzw. gespiegelte Hauptschlüssel:

Der „HKEY_CLASSES_ROOT“ enthält Informationen über unterstützte Dateitypen des Rechners und die dazugehörigen Dateiendungen. Der Wurzelschlüssel ist bei den neueren Windows-Versionen seit Windows 2000 nicht real, sondern eine Kombination aus: „HKEY_LOCAL_MACHINE\Software\Classes“ und „HKEY_CURRENT_USER\Software\ Classes“.

Der „HKEY_CURRENT_CONFIG“ ist eine Spiegelung auf „HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current“.

Der „HKEY_CURRENT_USER“ ist eine Spiegelung von „HKEY_USERS\<Benutzer-SID>“, wobei <Benutzer-SID> die SID des aktuell am System angemeldeten Benutzers ist.

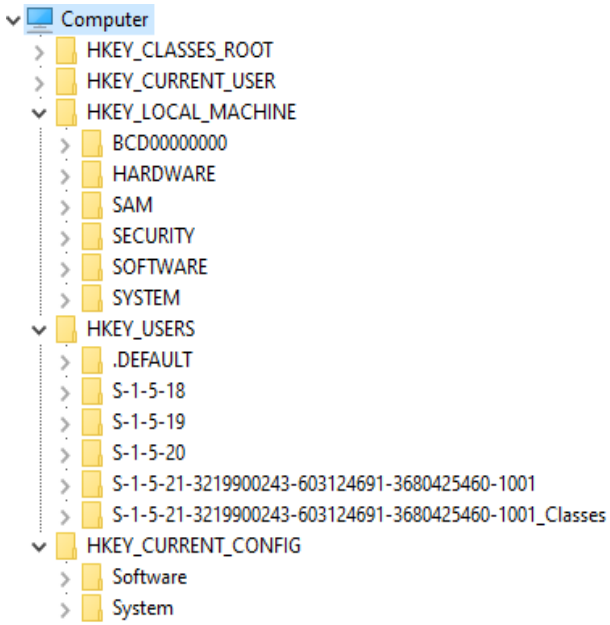
Weiterhin gibt es folgende Hives für Systemdienste:

- %systemroot%\System32\config\.DEFAULT
  - HKU\.DEFAULT und HKU\HKU\S-1-5-18 für User Local System
- %systemroot%\ServiceProfiles\LocalService\Ntuser.dat
  - HKU\HKU\S-1-5-19 für User Local Service
- %systemroot%\ServiceProfiles\NetworkService\Ntuser.dat
  - HKU\HKU\S-1-5-20 für User Network Service

Weitere Hives wären:

- \Device\HarddiskVolume1\Boot\BCD
  - HKLM\BCD00000000 Konfiguration für den Bootloader

In der folgenden Abbildung wird noch einmal die Struktur der Hives dargestellt:



Es existieren oft Kopien von Hives, welche sich an einer anderen Stelle befinden. Beispiele für diese sogenannten Supporting Files sind „system.alt“, welches eine Kopie des system Hives darstellt. Weiterhin gibt es „.log“, welches die Logs zu den einzelnen Hives enthält und „.sav“, worin Kopien der Hives während des Bootvorgangs enthalten sind.

In der Registry kann jeder Wert eine theoretische Größe von 1024 kB haben. Dabei sind folgende Datentypen bei den aktuellen Versionen möglich:

- REG_BINARY: Roher Binärcode
- REG_DWORD: binärer 32-bit Integer-Wert
- REG_QWORD: binärer 64-bit Integer-Wert
- REG_SZ: Unicode-String
- REG_EXPAND_SZ: Eine Zeichenkette variabler Länge die Umgebungsvariablen wie %systemroot% enthält,die beim Lesezugriff expandiert werden.
- REG_MULTI_SZ: Multi-Parameter-String, dessen einzelne Elemente durch Standard-Trennzeichen abgetrennt werden
- REG_FULL_RESOURCE_DESCRIPTOR: Ein Wert der eine kodierte Beschreibung der Hardware-Ressource enthält, z.B. eines Laufwerkes, Chipsatzes usw.

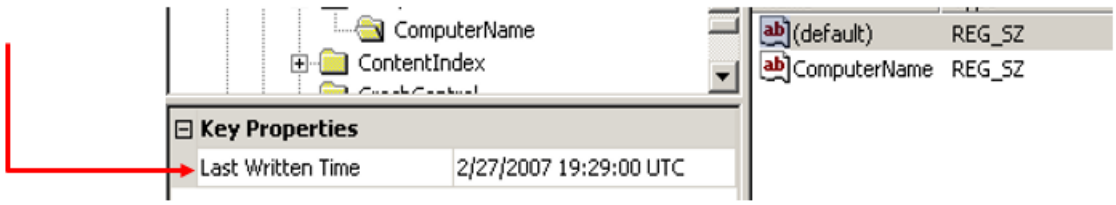
1.4.2.2 Speicherorte

Die Folgenden zusätzlichen wichtigen Informationen zu Registrierungsschlüsseln können für eine forensische Auswertung herangezogen werden:

Klasse	Eintragungen
Timezone Informationen	Zeitzonen Informationen
Netzwerk Historie	WLAN / LAN Informationen (Adapter/Settings – IP)
	Firewall Settings
	SSID's und MAC Adressen
	Zeitstempel von Verbindungen
USB Storage / Geräte	Volume Serials
	Volume Namen
	Laufwerksbuchstaben
	Zeitstempel von Verbindungen
	USB User ID's
	Geräteidentifikationen
Most Recent Used	Last Visited Used MRU (Executables)
	Open Save MRU (Dokumente)
	Run MRU (Start Commands)
User Assist Keys	Programm und Datei Starts vom Desktop
Shell Bags	Informationen zu geöffneten Verzeichnissen
Cached User Credentials	Gespeicherte Domainpasswörter (SYSTEM/SECURITY)
Dienste und Treiber	Systemdienste und Systemtreiber Einstellungen

1.4.2.3 Forensisch bedeutsame Registry Informationen

Jeder Registrierungsschlüssel enthält einen Wert namens „LastWrite“. Dieser enthält den Zeitstempel der letzten Änderung des Keys. Hierbei ist zu beachten, dass der Zeitstempel die Nanosekunden seit dem 01.01.1601 zählt. Wichtig ist außerdem, dass der Zeitstempel sich immer auf die letzte Änderung des Keys bezieht und nicht auf die Änderung der einzelnen Values. Wird eine Value geändert, so ändert sich aber die LastWrite Time des Keys.



Zeitstempel und Zeitzoneninformationen

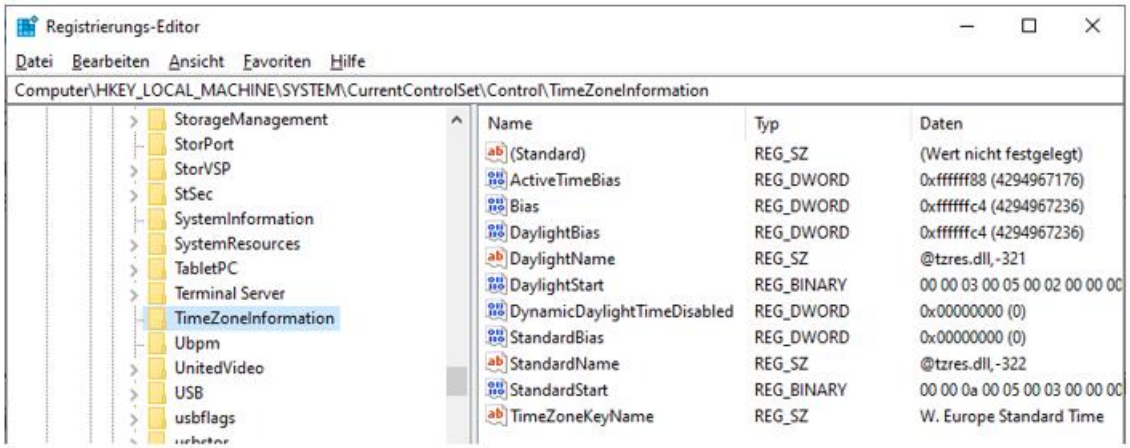
Die Deutung von Zeitstempeln ist nur mit zusätzlichen Informationen bezüglich der systeminternen Zeit bzw. der Zeitzone möglich. Diese Informationen findet man im Hive „HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation“.

Bezüglich der Zeitzone gibt es einige Informationen, welche von Bedeutung sind. Dazu zählt die UTC. Dies ist die Weltzeit und wird überall dort für Zeitangaben genutzt, wo eine weltweit einheitliche Zeitskala benötigt wird. Ebenfalls von Bedeutung ist die Local Time, welche die lokale Zeit angibt. Die Standard Time ist eine gesetzlich definierte Zeitzählung. Dies ist heutzutage meist die dem Längengrad entsprechende Zeitzone, die sich von UTC um eine ganze Zahl von Stunden unterscheidet. Weiterhin gibt es noch die Daylight Time, welche der Sommerzeit entspricht.

Für die Berechnung der Zeitzoneninformationen stehen folgende Formeln zur Verfügung:

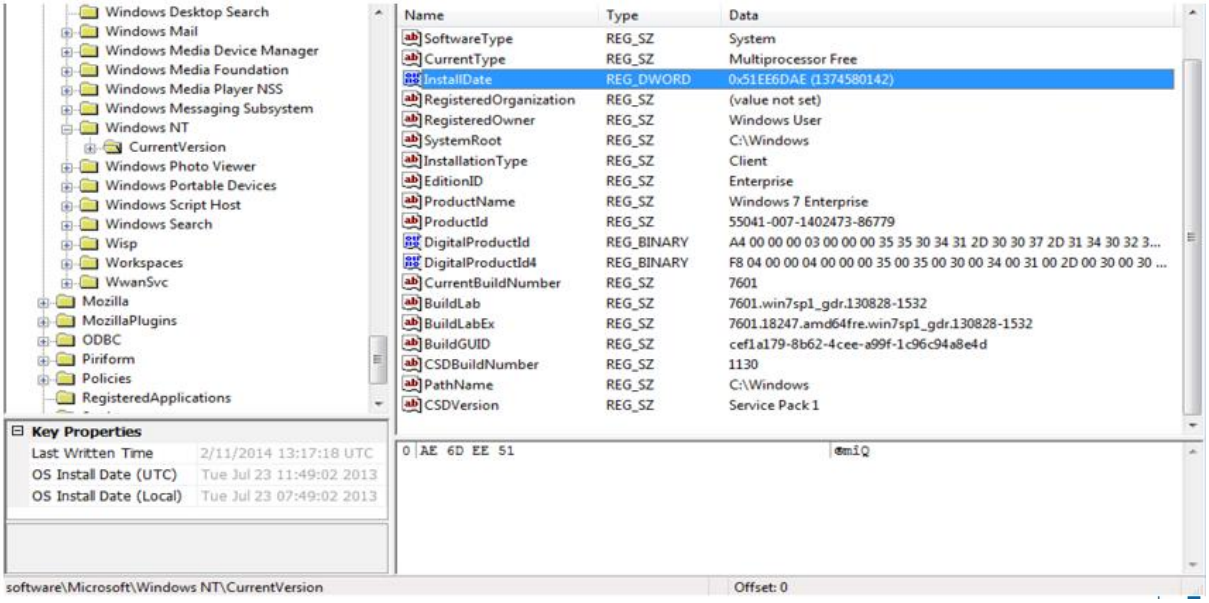
- UTC = Local Time + ActiveTimeBias
- Local Time = UTC - ActiveTimeBias
- Standard Time = Bias + StandardBias
- Daylight Time = Bias + DaylightBias

Die Werte, welche für die Berechnung benötigt werden, sind der ActiveTimeBias, der Bias, der DaylightBias und der StandardBias. Diese Informationen befinden sich alle im angegebenen Hive zur TimeZoneInformation.

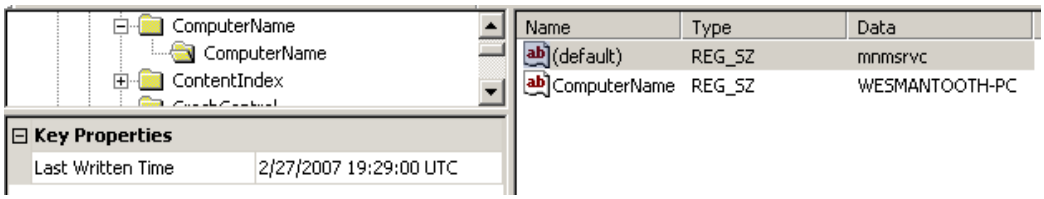


Operating System Version und Computerinformationen

Informationen zur Operating System Version befinden sich im Hive „HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion“.



Informationen zum Computer befinden sich im Hive „SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName“.



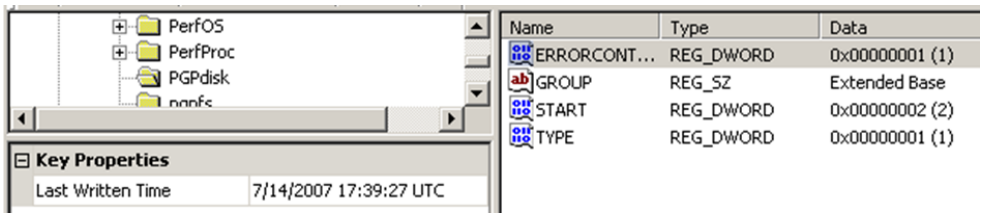
Autorun Locations

Die einzelnen Windows Versionen verfügen über eine Reihe von Autorun Locations. Hierbei werden ausgeführte Programme automatisch beim Systemstart ausgeführt. Informationen dazu befinden sich in folgenden Hives:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
- HKLM\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\SYSTEM\CurrentControlSet\Services (Typ 0x02 = Start)

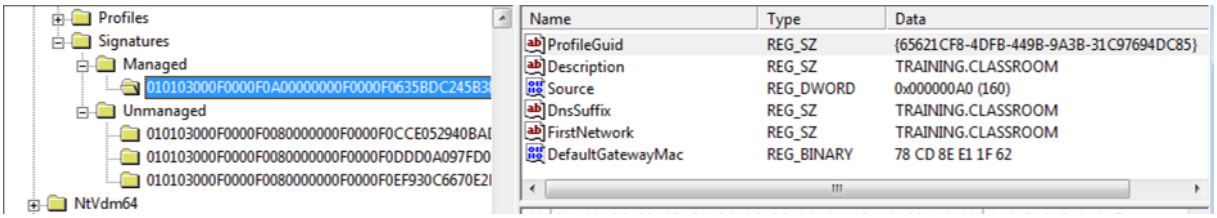
Weiterhin gibt es die Möglichkeit, Programme auch bei der Benutzeranmeldung am Computer automatisch auszuführen. Informationen dazu befinden sich in folgenden Hives:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Windows\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Runonce



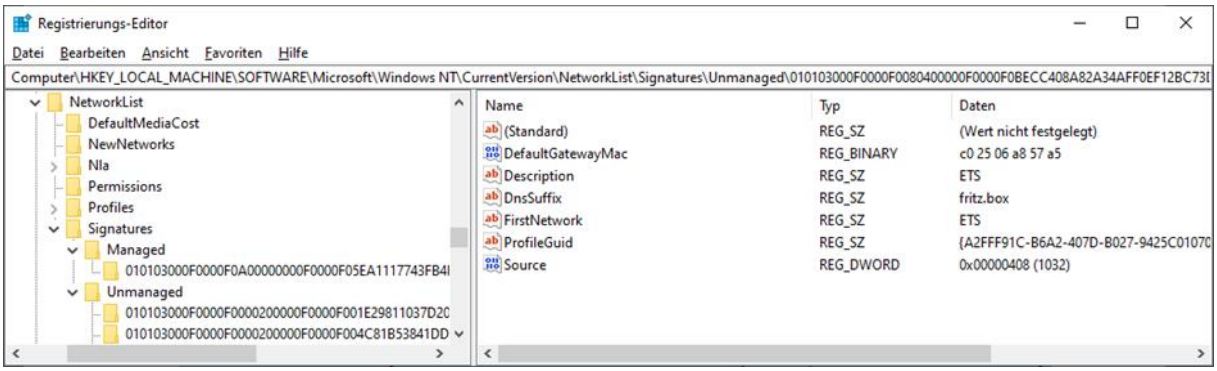
Netzwerkverbindungen – Managed by a Domain (Vista/7/8/10)

Informationen zu Netzwerkverbindungen welche unter Windows Vista, 7, 8 und 10 von eine Domain gemanaged werden, findet man im Hive „HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed“. Der DnsSuffix ist hier die Domain, FirstNetwork die SSID, DefaultGatewayMac die Media Access Control (MAC) Adresse des Gateways und die Last Written Time die letzte Verbindung mit dem Netzwerk.



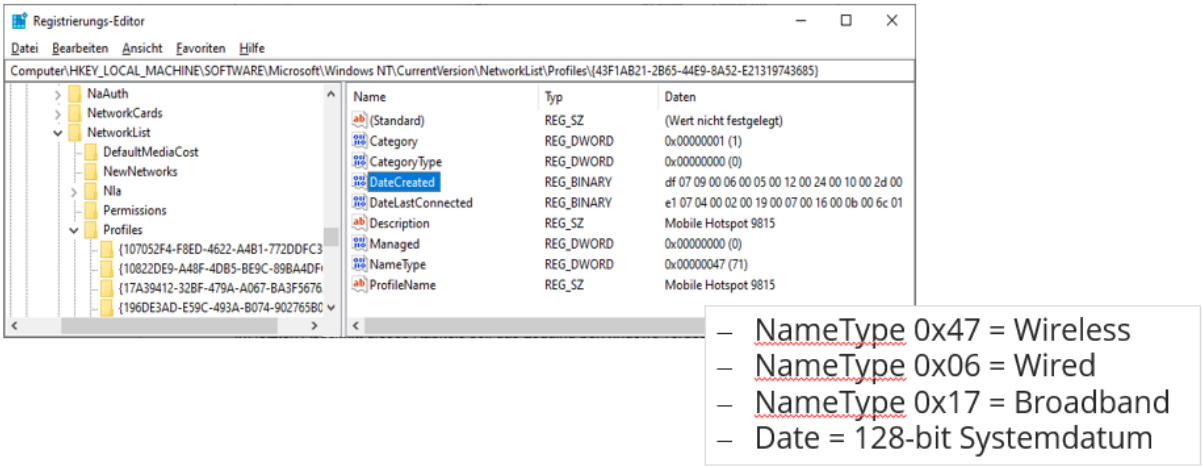
Netzwerkverbindungen – NotManaged by a Domain (Vista/7/8/10)

Informationen zu Netzwerkverbindungen, welche unter Windows Vista, 7, 8 und 10 nicht von einer Domain gemanaged werden, findet man im Hive „HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged“.



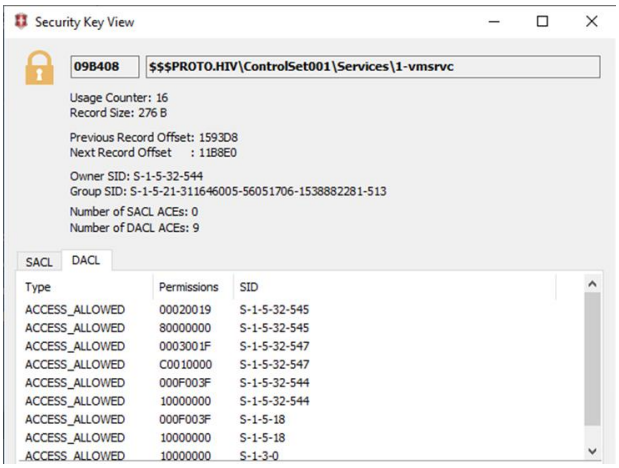
Netzwerkadapter

Informationen zum Netzwerkadapter findet man bei Windows XP im Hive „HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\{GUID}“. Bei Windows Vista, 7 und 8 liegen diese Infos im Hive „HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles“.



1.4.2.4 Zugriffsberechtigungen auf Registry Daten

In der Registry werden für Registrierungsschlüssel die SID (Security Identifier) des Besitzers und der Berechtigten, welche den Schlüssel erzeugt haben oder verändern dürfen gespeichert, um so unterschiedliche Zugriffsberechtigungen zu gewährleisten.



1.4.2.5 Registrierungsdatenbank 64 Bit Support

Für den Support von 32Bit-Softwareanwendungen wurden auf 64Bit-Umgebungen extra Schlüssel eingeführt. Diese sind in der SOFTWARE Registrierungsdatei unter dem Hive HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node zu finden. Die Informationen, welche für 32Bit-Anwendungen relevant sind, werden notwendigerweise im 64Bit Format abgelegt.

1.4.3 Betriebssystemartefakte

1.4.3.1 Genutzte und gelöschte Dateien – Der Papierkorb

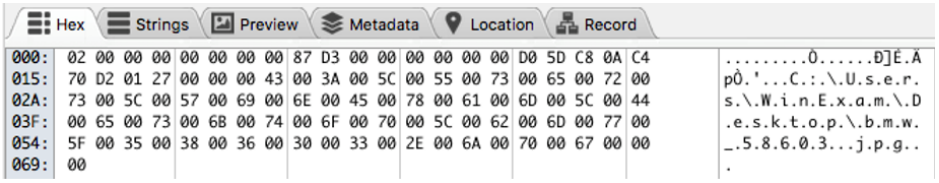
Viele kennen den Papierkorb als $Recycle.Bin, jedoch wird dieser oft auch als $RECYCLE.BIN angezeigt. Das „$“ bedeutet, dass der Papierkorb zum System gehört, aber aus Tests können wir erkennen, dass sich $Recycle.Bin auf dem Windows-Laufwerk befindet (normalerweise 'C:\') und $RECYCLE.BIN normalerweise auf ein Laufwerk geschrieben wird, dass an ein Windows-System angeschlossen ist, sprich beispielsweise ein sekundäres Laufwerk auf einem Computer oder ein externes Laufwerk, das an einen Computer angeschlossen ist.

Im $Recycle.Bin befinden sich Unterverzeichnisse mit langen alphanumerischen Bezeichnungen der SID (Security Identifier), mit der jeder Benutzer auf dem Computer identifiziert wird. Dies ist wichtig, da jeder Benutzer einen eigenen Papierkorb hat. Der Papierkorb ist im Wesentlichen ein spezieller Ordner. Im Papierkorb werden mehrere Dateien angezeigt. Die Dateien haben unkonventionelle Namen und beginnen entweder mit $I oder $R. Unter Windows XP werden die im Papierkorb gelöschten Dateien im Ordner "Recycler" unter der spezifischen SID des Benutzers abgespeichert. Dort gibt es eine INFO2-Datei, die einen Index aller gelöschten Dateien sowie den ursprünglichen Pfad, die Dateigröße und den Zeitpunkt, zu dem die Datei gelöscht wurde, enthält. Die gelöschten Dateien werden umbenannt in das Format DC#IndexNummer#.Extension.

Dateien, die mit $I beginnen, sind im Wesentlichen die Metadaten für die bestimmte gelöschte Datei. Im Gegensatz zu früheren Windows-Versionen hat die $I-Datei keine feste Größe von 544 Byte und ist nur so groß, wie sie sein muss. Die Metadaten Datei ist wie folgt aufgebaut:

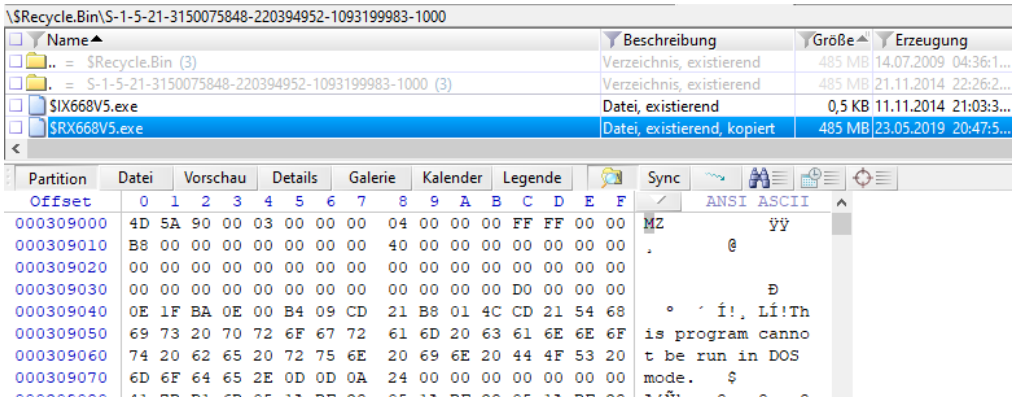
Offset	Size	Data Description
0	8	Header
8	8	Deleted File Size
16	8	Date/Time File Deleted
24	4	File Name Length
28	Variable Length	File Name And Path

Ein Beispiel für gelöschte Dateien:



Description	Hex Value	Interpreted Data
Header	0200000000000000	2
Deleted File Size	87D3000000000000	54151
Date/Time Deleted	D05DC80AC470D201	2017-01-17 13:17:24 (UTC)
File Name Length	27000000	39
File Name And Path	43003A005C0055007300 6500720073005C005700 69006E00450078006100 6D005C00440065007300 6B0074006F0070005C00 62006D0077005F003500 3800360030003300 2E006A00700067 00	C:.\.U.s.e.r.s.\.W.i.n.E.x.a.m. \.D.e.s.k.t.o.p.\.b.m.w._. 5.8.6.0.3...j.p.g

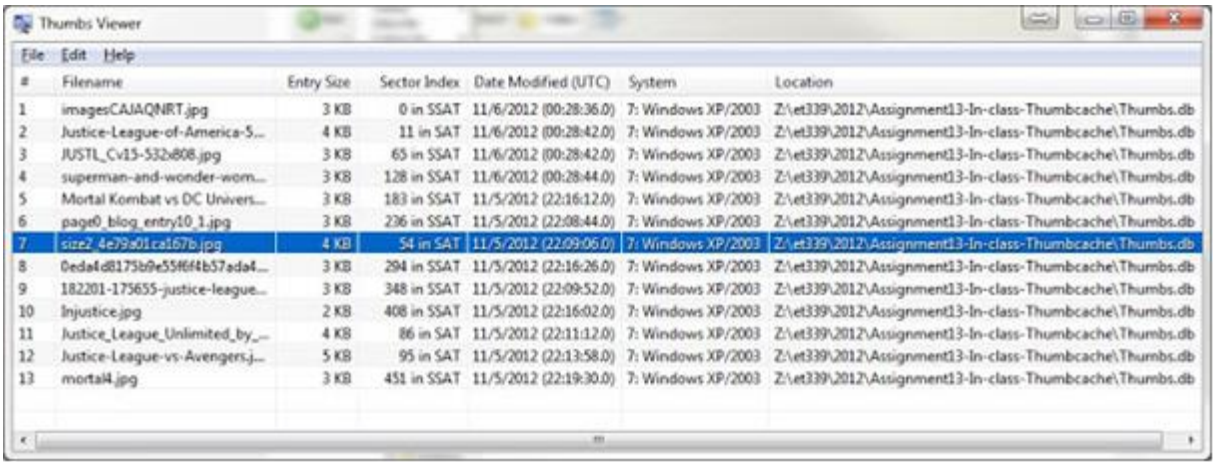
Die Dateien, die mit $R beginnen, sind der Inhalt der tatsächlichen in den Papierkorb verschobenen Dateien. Mit anderen Worten, die Dateien die aus diesem Konto gelöscht wurden.



1.4.3.2 Thumbs und Thumbcache

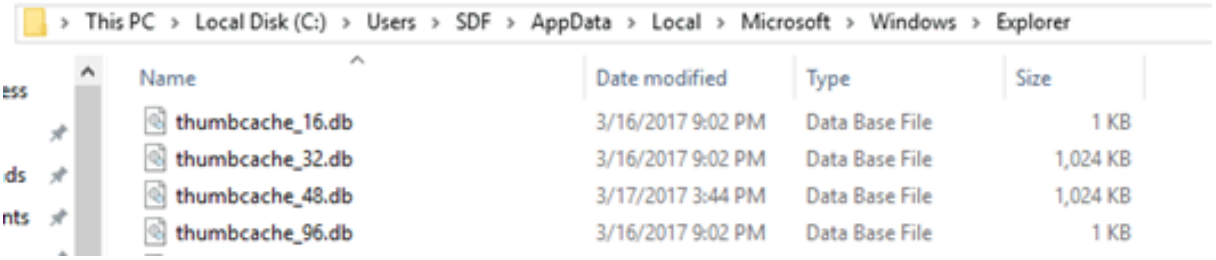
Der Windows-Thumbcache und die Thumbs.db-Datei sind eine hervorragende Quelle für grafische Beweise für Untersuchungen zu Dateikenntnis und Dateinutzung. Thumbcache-Bilder sind versteckte Systemdateien, die kleinere Bilder von Multimediadateien darstellen und dazu dienen, dem Benutzer eine grafische Ansicht der Dateien in einem bestimmten Verzeichnis zu ermöglichen. Thumbcache-Dateien werden zentral für jedes Benutzerkonto gespeichert. Diese Beweise können als stummer Zeuge für einen Benutzer dienen, der Bilder ansieht, oder als Aufzeichnung von Bildern, die einmal auf einem System vorhanden waren.

Thumbs Dateien sind die bis Window XP genutzten Datendateien mit Vorschaubildern, die zugleich auch den Dateinamen enthielten. Die thumb.db Dateien waren nicht zentral abgelegt, sondern befanden sich in den jeweiligen Verzeichnissen mit den Daten.

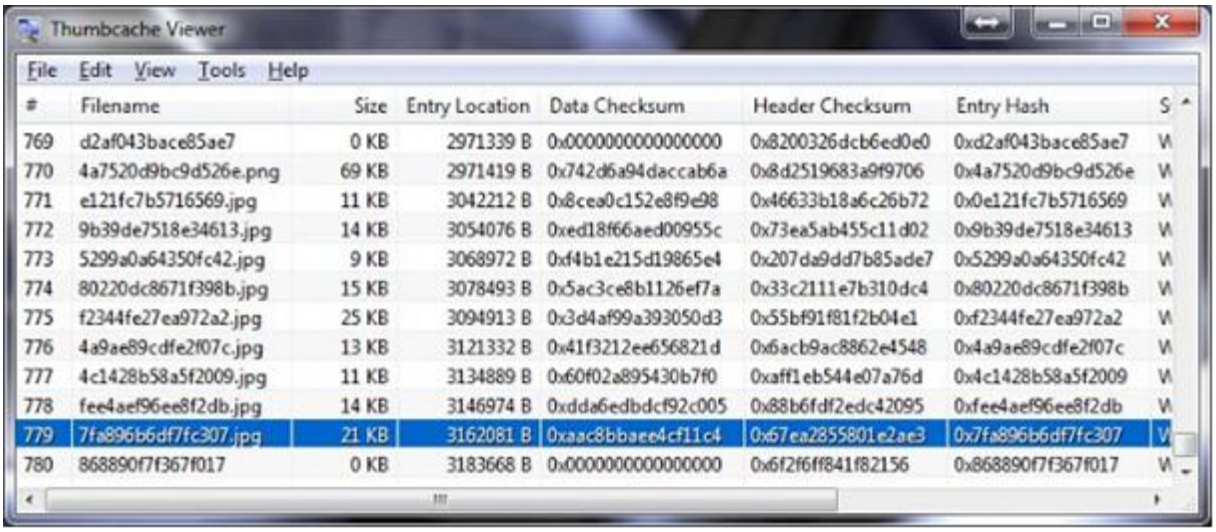


#	Filename	Entry Size	Sector Index	Date Modified (UTC)	System	Location
1	imagesCAJAQNRT.jpg	3 KB	0 in SSAT	11/6/2012 (00:28:36.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
2	Justice-League-of-America-5...	4 KB	11 in SAT	11/6/2012 (00:28:42.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
3	JUSTL_Cv15-532x808.jpg	3 KB	65 in SSAT	11/6/2012 (00:28:42.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
4	superman-and-wonder-wom...	3 KB	128 in SSAT	11/6/2012 (00:28:44.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
5	Mortal Kombat vs DC Univers...	3 KB	183 in SSAT	11/5/2012 (22:16:12.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
6	page0_blog_entry10_1.jpg	3 KB	236 in SSAT	11/5/2012 (22:08:44.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
7	size2_4e79a01ca167b.jpg	4 KB	54 in SAT	11/5/2012 (22:09:06.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
8	0eda4d8175b9e55f6f4b57ada4...	3 KB	294 in SSAT	11/5/2012 (22:16:26.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
9	182201-175655-justice-league...	3 KB	348 in SSAT	11/5/2012 (22:09:52.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
10	Injustice.jpg	2 KB	408 in SSAT	11/5/2012 (22:16:02.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
11	Justice_League_Unlimited_by_...	4 KB	86 in SAT	11/5/2012 (22:11:12.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
12	Justice-League-vs-Avengers.j...	5 KB	95 in SAT	11/5/2012 (22:13:58.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db
13	mortal4.jpg	3 KB	451 in SSAT	11/5/2012 (22:19:30.0)	7: Windows XP/2003	Z:\et339\2012\Assignment13-In-class-Thumbcache\Thumbs.db

Ab Windows Vista hat Microsoft die Verwendung von Thumbs.db-Datenbankdateien auf Verzeichnisebene auf das Speichern von Miniaturbildern in einer einzelnen Ordnerstruktur umgestellt, in der einzelne Dateien gespeichert sind, die alle angezeigten Elemente basierend auf der ausgewählten Symbolgröße enthalten. Thumbcache-Dateien sind direkt an jeden Benutzer gebunden und werden in einem separaten Benutzerverzeichnis gespeichert. Der Speicherort des Thumbcaches unter Windows 7, Windows 8 und Windows 10 ist C:\Users\Benurtzername\AppData\Local\Microsoft\Windows\Explorer.

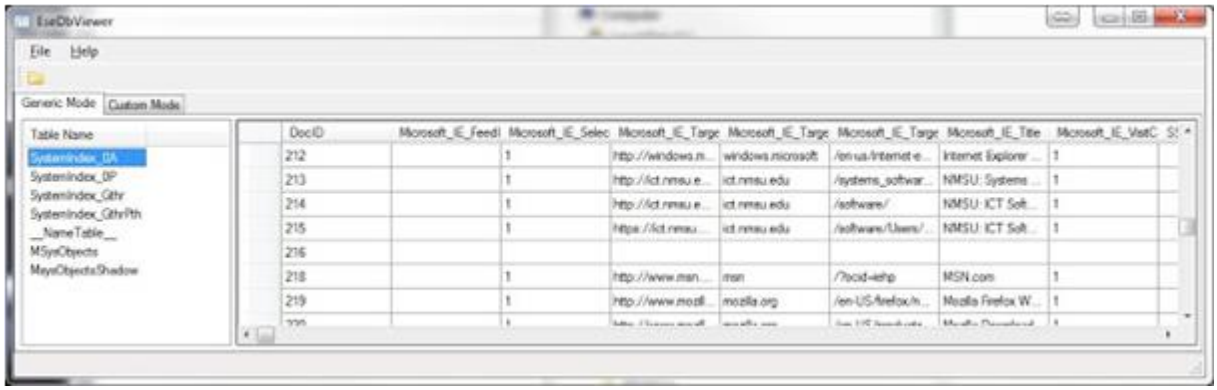


Die in den Thumbcache-DB-Dateien gespeicherten Thumbnails werden in verschiedenen Formaten gespeichert, z. B. wird original.jpg als .jpg und original.png als .png gespeichert. Sie behalten jedoch nicht den ursprünglichen Namen bei, sondern werden in eine Unicode Zeichenfolge umbenannt, die ThumbnailCacheID genannt wird.



#	Filename	Size	Entry Location	Data Checksum	Header Checksum	Entry Hash	S
769	d2af043bace85ae7	0 KB	2971339 B	0x0000000000000000	0x8200326dcb6ed0e0	0xd2af043bace85ae7	W
770	4a7520d9bc9d526e.png	69 KB	2971419 B	0x742d6a94daccab6a	0x8d2519683a9f9706	0x4a7520d9bc9d526e	W
771	e121fc7b5716569.jpg	11 KB	3042212 B	0x8cea0c152e8f9e98	0x46633b18a6c26b72	0x0e121fc7b5716569	W
772	9b39de7518e34613.jpg	14 KB	3054076 B	0xed18f66aed00955c	0x73ea5ab455c11d02	0x9b39de7518e34613	W
773	5299a0a64350fc42.jpg	9 KB	3068972 B	0xf4b1e215d19865e4	0x207da9dd7b85ade7	0x5299a0a64350fc42	W
774	80220dc8671f398b.jpg	15 KB	3078493 B	0x5ac3ce8b1126ef7a	0x33c2111e7b310dc4	0x80220dc8671f398b	W
775	f2344fe27ea972a2.jpg	25 KB	3094913 B	0x3d4af99a393050d3	0x55bf91f81f2b04e1	0xf2344fe27ea972a2	W
776	4a9ae89cdfe2f07c.jpg	13 KB	3121332 B	0x41f3212ee656821d	0x6acb9ac8862e4548	0x4a9ae89cdfe2f07c	W
777	4c1428b58a5f2009.jpg	11 KB	3134889 B	0x60f02a895430b7f0	0xaff1eb544e07a76d	0x4c1428b58a5f2009	W
778	fee4aef96ee8f2db.jpg	14 KB	3146974 B	0xdda6edbdcf92c005	0x88b6fdf2edc42095	0xfee4aef96ee8f2db	W
779	7fa896b6df7fc307.jpg	21 KB	3162081 B	0xaac8bbaee4cf11c4	0x67ea2855801e2ae3	0x7fa896b6df7fc307	W
780	868890f7f367f017	0 KB	3183668 B	0x0000000000000000	0x6f2f6ff841f82156	0x868890f7f367f017	W

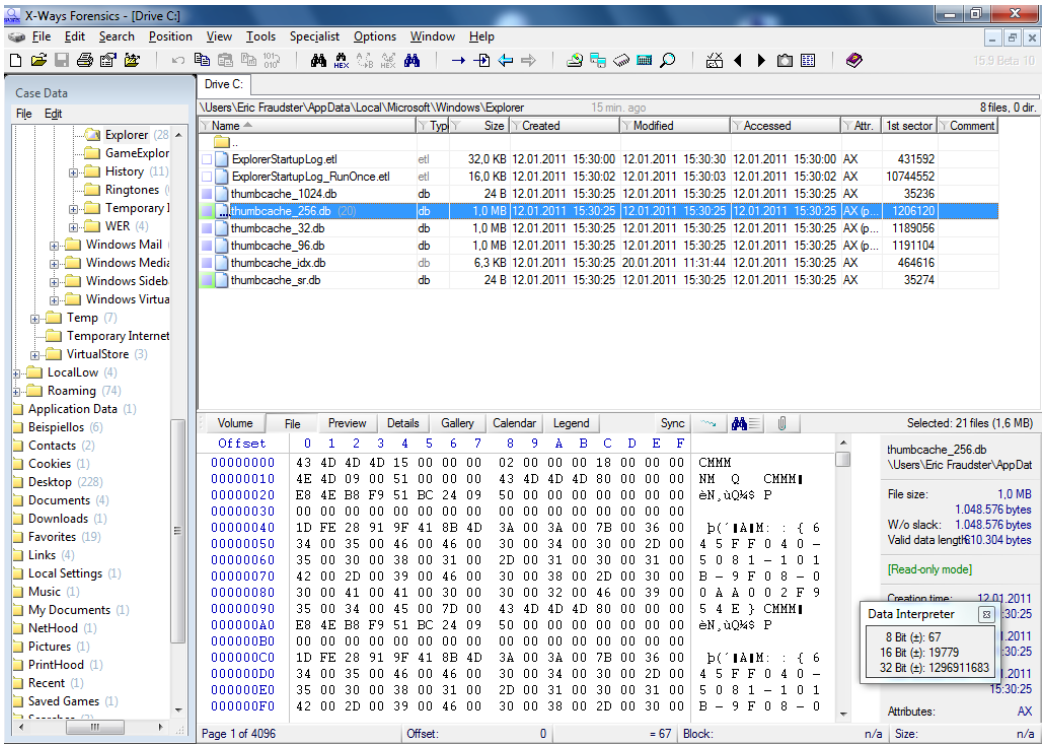
Leider enthält die Thumbcache-Datenbank keine Informationen, mit denen Thumbnails einfach mit ursprünglichen Dateinamen oder Speicherorten verknüpft werden können. Eine Möglichkeit dies zu tun, ist die Verwendung der Windows-Suchdatenbank (Windows.edb). Die Windows.edb speichert die ThumbnailCacheID als Teil seiner Metadaten für indizierte Dateien. Die Tabelle mit dem Namen SystemIndex_0A enthält sowohl die Pfad- und Dateinamenangabe wie auch das verknüpfte Programm und die ThumbnailCacheID.



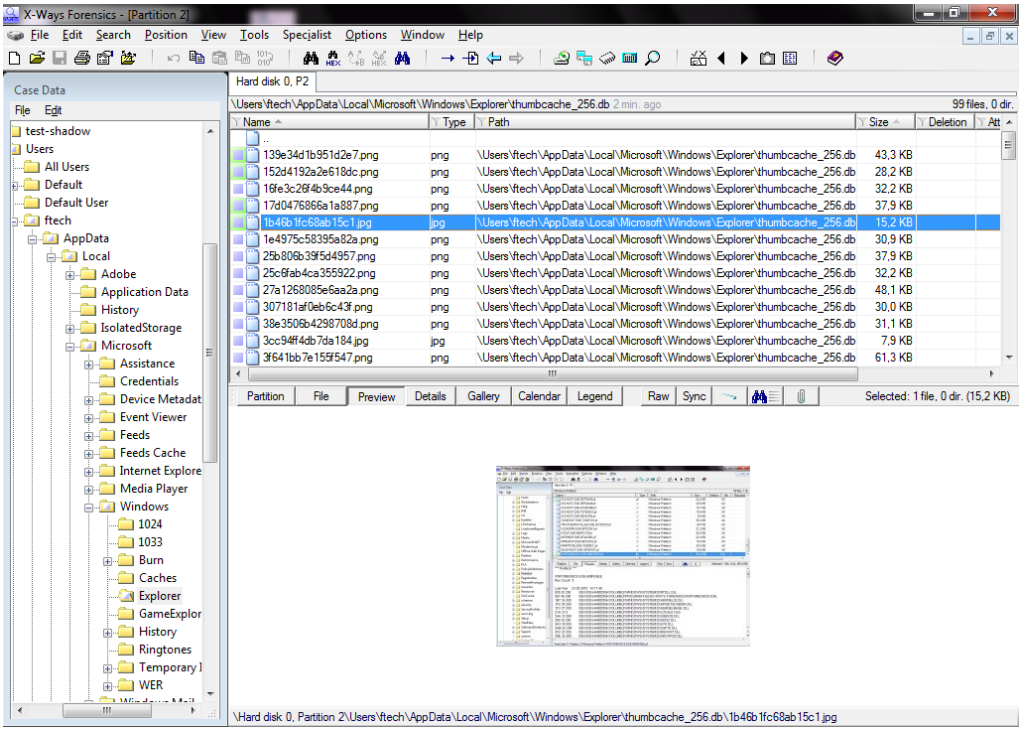
Der Speicherort für die EDB Datei ist „C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb“. Um die Daten in der EDB Datei einsehen zu können, sind spezielle Tools nötig. Dafür kann man den Thumbcache Viewer (//thumbcacheviewer.github.io/) oder auch den ESDB Viewer (//www.woanware.co.uk/forensics/esedbviewer.html) verwenden.

Sofern ein Verzeichnis mit Bildern im Netzwerk aufgerufen wird, werden reguläre Thumbs.db Dateien geschrieben. Dies Verhalten ist unter Windows 7, 8 und 10 feststellbar. Außerdem kann die Thumbcache Erzeugung per Registry deaktiviert werden.

X-Ways analysiert Thumb.db und ThumbCache Dateien beim Dateiüberblick erweitern in eingebetteten Dateien und extrahiert hierbei die Vorschaubilder und ThumbCacheID:



Zudem kann X-Ways die Windows.edb Datei lesen. Eine Zuordnung von ThumbCacheID zu Vorschaubildern wird von X-Ways jedoch nicht unterstützt.



1.4.4 Benutzerkontenzugriffssteuerung

1.4.4.1 User Access Control (UAC)

Mit der Einführung von Windows Vista wurde den Windows Betriebssystemen ein neues Sicherheitsfeature hinzugefügt. Es handelt sich dabei um die User-Access-Control (UAC). Die UAC soll den Zugriff von Anwendungen auf die Programm- und Systemverzeichnisse ohne administrative Kennung verhindern. Dies bedeutet, dass keine Software, ob Browser oder Festplattentool, Zugriff auf diese durch die UAC geschützten Bereiche nehmen darf, es sei denn, die jeweilige Software wird mit Administratorrechten ausgeführt (rechte Maustaste – Ausführen als Administrator).

Es gibt allerdings nach wie vor Anwendungen, die durch ihre Implementierung gegen diesen Grundsatz verstoßen und anwendungsspezifische Nutzerdaten im eigenen Programmverzeichnis ablegen. Diese Anwendungen werden dabei durch das Betriebssystem ermittelt und alle Schreib/Lese Operationen werden auf ein virtuelles Programmverzeichnis umgeleitet. Dieses befindet sich im jeweiligen Benutzerverzeichnis des angemeldeten Benutzers unter „…\AppData\Local\VirtualStore“. Dieses Verzeichnis hat daher eine wichtige Bedeutung für die Untersuchung und sollte immer mit in Augenschein genommen werden.

Auch im Bereich der Registrierung hat die UAC ihren Einfluss genommen. User ohne Administrator-Berechtigung können nicht in den Registrierungshive HKEY_LOCAL_MACHINE/SOFTWARE schreiben. Schreibzugriffe in diesen Bereich werden umgebogen nach HKEY_CURENT_USERS\Software\Classes\VirtualStore\Machine\Software und werden für den Benutzer transparent zugeordnet. Die virtuellen Registrierungsschlüssel werden jedoch nicht in die Datei NTUSER.DAT geschrieben, sondern in das Anwendungsdatenverzeichnis unter „\AppData\Local\Microsoft\Windows\usrclass.dat“. Bei der Auswertung von Registrierungsinformationen sind diese Ablageorte daher mit zu untersuchen.

1.4.5 Remote Desktop Nutzung

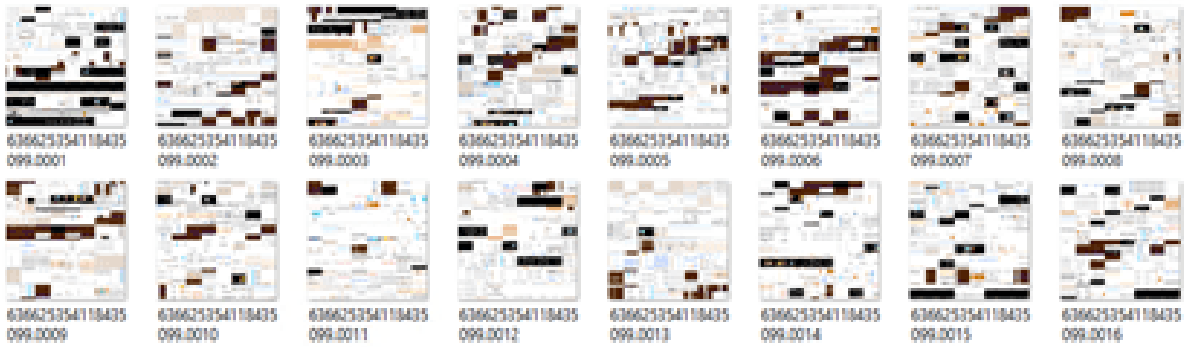
1.4.5.1 Betriebssystemspezifika Windows

RDP Cache Forensik

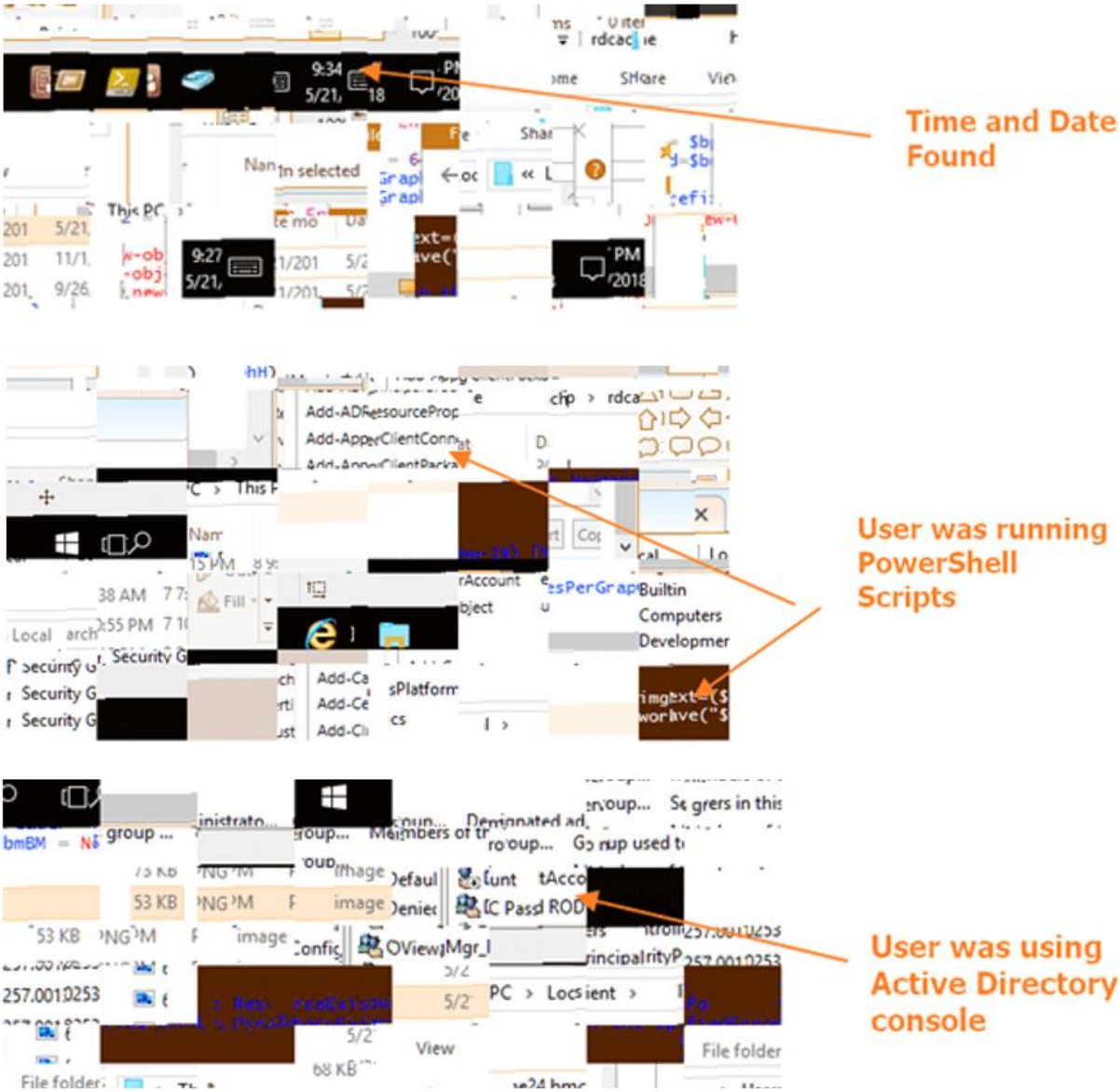
Angriffe auf Windows Netzwerke werden häufig mittels RDP (respektive Terminal Server) durchgeführt. Dabei wird ein RDP Initialangriff für Seitwärtsbewegungen (Lateral Movements) verwendet. Verwendet man den Windows „mstsc“-Client, erbringt dies zusätzliche Artefakte. Dazu zählen die automatischen Cache-Dateien und die enthaltenen Bereiche des Computerbildschirms aus der Angreifersicht. Solche Cachedateien können als weiterer Beweisgegenstand für die Forensik hinzugezogen werden. Zu finden sind diese genannten Artefakte unter dem folgenden Pfad: „C:\Users\XXX\AppData\Local\Microsoft\Terminal Server Client\Cache“.

Für die RDP Cache Forensik benötigt man Werkzeuge für die Extraktion der gespeicherten Bilder und Cache Dateien. Hierfür kommen Tools wie „bmc-tools“ von ANSSI-FR in Frage.

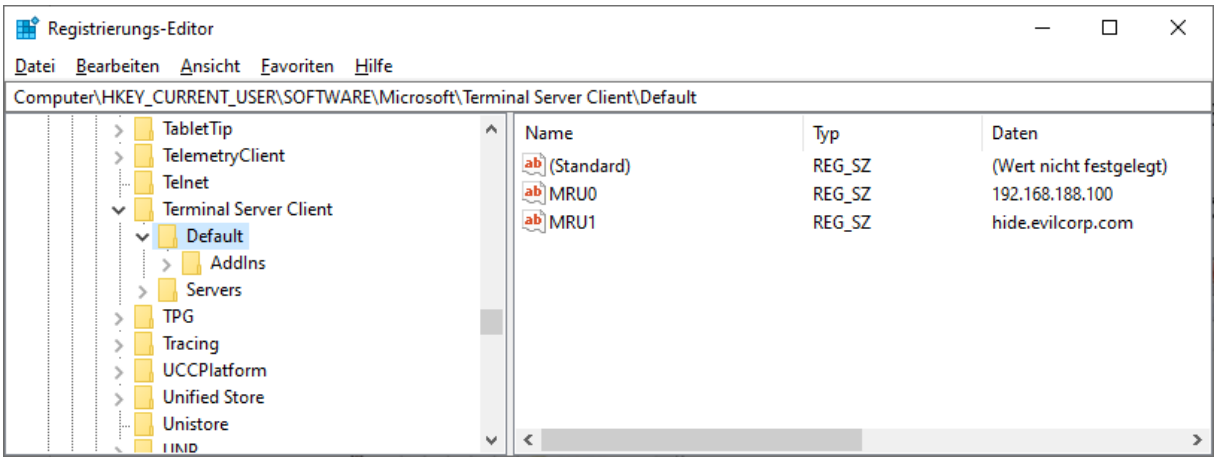
Weiterhin werden Bitmaps mit einer Größe von 64x64 extrahiert. Solche Teile sind nur als Puzzle Teile einsetzbar, können jedoch trotzdem wichtige Hinweise bieten.



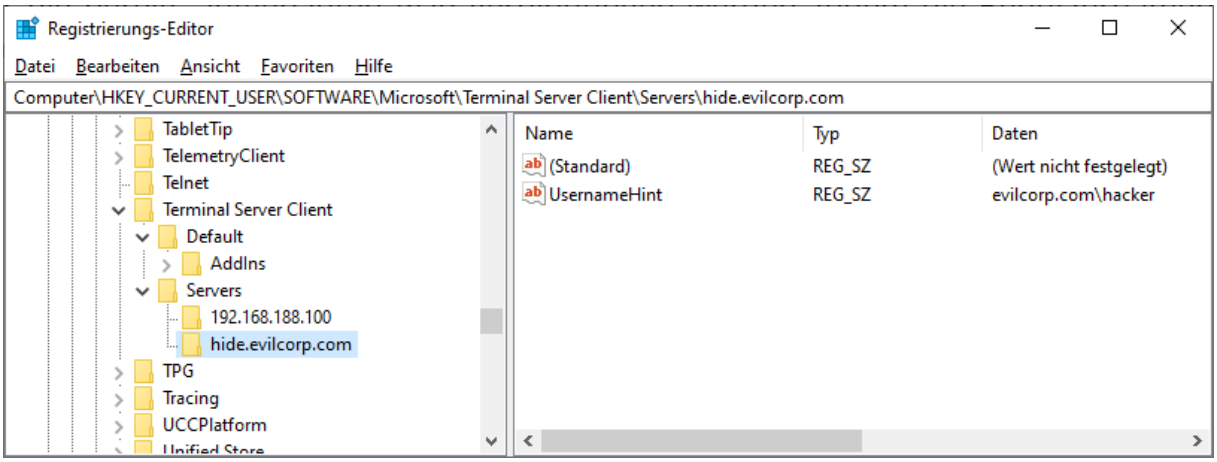
Einige Beispiele, was an Hinweisen über diese Puzzle Teile gefunden werden kann, sind im Folgenden dargestellt:



Zusätzlich zu den Cache Dateien befinden sich in der Registry die MRU Eintragungen der RDP Server, die genutzt wurden: „HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default“.



Für die bereits aufgebauten RDP Verbindungen werden zudem die Benutzernamen der Anmeldung *(UsernameHint)* gespeichert im Schlüssel: „HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers“.



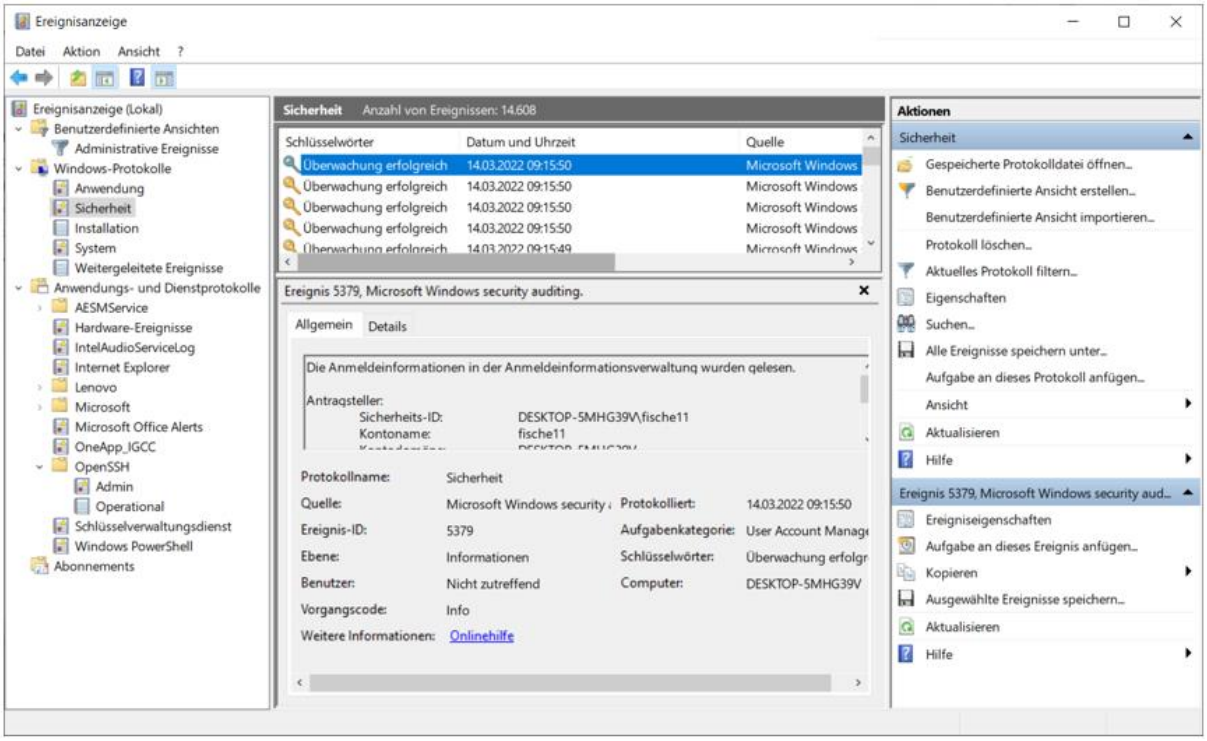
1.4.6 Zusammenfassung

Der Teil 1 der Windows spezifischen Daten ist damit erarbeitet. Die so zu ermittelnden Informationen der einzelnen Bereiche geben jeweils Hinweise auf Dateizugriffe und Dateinutzung am Windows System. Das Zusammenspiel der hier einzeln vorgestellten Windows Artefakte ergibt am Ende ein Gesamtbild der Nutzung von Computersystemen, welche eine wesentliche Rolle in einer forensischen Computeruntersuchung spielen kann.

Im Teil 2 werden wir auf den Punkt externe Datenträgernutzung eingehen, schauen uns Zeit- und Zugriffsanalysen näher an.

1.5 Windows Logging und Accounts

1.5.1 Windows Logging – Ereignisanzeige



Beim Event-Logging geht es um die Protokollierung von Ereignissen und Fehlern was insbesondere für Systemadministratoren interessant ist. Diese Dateien sind geeignet, um ein Anwendernutzungsprofil zu erzeugen. Dabei geht es vor allem um Informationen wie Computernutzungszeiten (alle logs), WLAN-Verbindungen (DHCP-Client), Dateienlöschung (NTFS-Log), den Netzwerkshare (SMB-Client, SMB-Server) und angeschlossene Geräte.

1.5.2 Windows Logging – EVT und EVTX

Das Logging unter Windows unterschiedet sich fundamental vom Logging unter anderen Betriebssystemen wie etwa UNIX. Anstelle von Textdateien mit beschreibenden Einträgen werden binäre Log Dateien geführt, in denen den einzelnen Ereignissen Eventcodes zugeordnet sind. Bei Windows 2000, XP und 2003 wird das Event Log in EVT-Dateien abgelegt. Seit Windows Vista wurde das Format auf das Windows XML Event Log im EVTX-Format geändert.

1.5.2.1 EVT-Dateien

Die Log Dateien sind in *„%System%\system32\config“* abgelegt. Bei Windows 2000, XP und 2003 gibt es die drei Log Dateien Application.evt**,** System.evt und Security.evt. Bei den Server Betriebssystemen kommen noch die Log Dateien DNS Server.evt**,** Directory Service.evt und File Replication Service.evt hinzu.

Aufbau der Log Dateien

Jedes Log besteht aus dem Header Record und einem Body. Der Body wiederum besteht aus Event Records, dem Cursor Record und freiem Speicher. Der Body bildet einen Ringspeicher. Das bedeutet, ist dieser voll, wird der älteste Eintrag vom neuesten überschrieben. Der Cursor Record zeigt auf die Stelle zwischen dem ältesten und dem neuesten Event Record. Sollte noch freier Speicher existieren, so kann dieser ausgenullt sein, Slack enthalten oder mit Padding gefüllt sein.

1.5.2.2 EVTX-Dateien

Ab Windows Vista wurde das EVT Log durch das Windows XML Event Log, kurz EVTX Format, ersetzt. Bei Windows Vista, Windows 7, Windows 8 und Windows 10 liegen die Log Dateien in: *%SystemRoot%\system32\winevt\logs*. Es gibt wesentlich mehr Log Dateien (Win 7 > 60; Win 10 > 250):

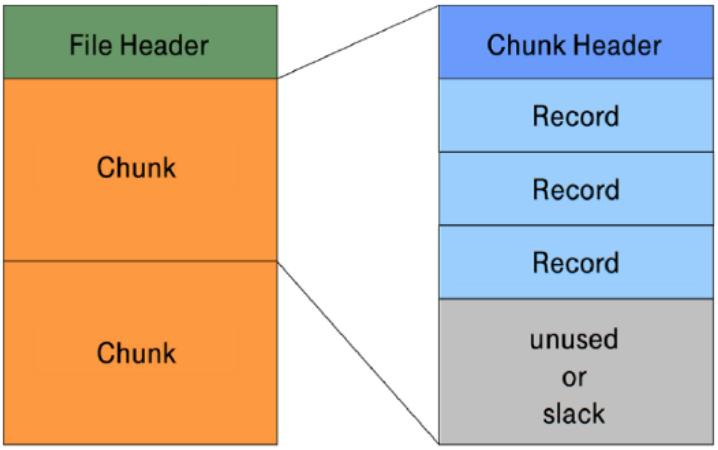
- Application.evtx
- System.evtx
- Security.evtx
- .....

Für eine forensische Untersuchung sind dabei öfters folgende Dateien interessant:

- HardwareEvents.evtx
- InternetExplorer.evtx
- Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
- Microsoft-Windows-PowerShell%4Operational.evtx
- Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx
- ....

Aufbau der EVTX-Dateien

EVTX Dateien bestehen aus einem File Header und sind danach in Chunks aufgeteilt. Jeder Chunk enthält einen Chunk Header und mehrere Records, nach den Records kann ein Slack folgen.



Der EVTX-File Header hat folgenden Aufbau, wobei er immer 4096 Bytes lang ist, aber nur die ersten 128 Byte verwendet werden.

Offset	Größe	Beschreibung
0x0000	8	Signatur 'ElfFile'
0x0008	8	Ältester Chunk
0x0010	8	Aktueller Chunk
0x0018	8	Nummer des nächsten Records
0x0020	4	Länge des verwendeten Headers in Bytes (immer 0x80)
0x0024	2	Minor Version (immer 1)
0x0026	2	Major Version (immer 3)
0x0028	2	Länge des Headers in Bytes (immer 0x1000)
0x002A	2	Anzahl der Chunks
0x002C	76	Unbekannt (ausgenullt)
0x0078	4	Flags
0x007C	4	Prüfsumme

Ein Chunk ist immer 64 KiB groß. Jeder Chunk hat eine Signatur 'ElfChnk'. Der Chunk Header ist wie folgt aufgebaut:

Offset	Größe	Beschreibung
0x0000	8	Signatur 'ElfChnk'
0x0008	8	Nummer des ersten Log Records
0x0010	8	Nummer des letzten Log Records
0x0018	8	Nummer des ersten File Records
0x0020	8	Nummer des letzten File Records
0x0028	4	Offset Tabelle (immer 0x80)
0x002C	4	Offset des letzten Records
0x0030	4	Offset des nächsten Recodrs
0x0034	4	Prüfsumme über die Daten
0x0038	68	Unbekannt
0x007C	4	Prüfsumme über den Header
0x0080	64x4	String Table
0x0180	32x4	Template Table

Jeder Event Record hat wieder einen Header. Der ist wie folgt aufgebaut:

Offset	Größe	Beschreibung
0x0000	4	Signatur 0x2a, 0x2a, 0x00, 0x00
0x0004	4	Record Länge in Byte
0x0008	8	Nummer des Records
0x0010	8	Time Created Zeitstempel
var.	var.	Binär XML Stream
var.	4	Record Länge in Byte

Die EVTX Logs können, wie die EVT Logs, mit bestimmten Viewern menschenlesbar dargestellt werden. Bei EVTX Logs ist dabei auch eine Darstellung in XML möglich:
XML-Schema nach der Dekodierung:

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="EventLog" />
    <EventID Qualifiers="32768">6013</EventID>
    <Level>4</Level>
    <Task>0</Task>
    <Keywords>0x80000000000000</Keywords>
    <TimeCreated SystemTime="2019-12-21T14:38:40.938225200Z" />
    <EventRecordID>17189</EventRecordID>
    <Channel>System</Channel>
    <Security />
  </System>
  <EventData>
    <Data>720306</Data>
    <Data>60</Data>
    <Data>-60 W. Europe Standard Time</Data>
  </EventData>
</Event>
```

Die binäre XML-Kodierung erfolgt in den 3 Schritten Tokenization und Binärisierung, Substitution und Templates.

1. Tokenization und Binärisierung

Beispiel:
`aus <EventID>1234</EventID>`

wird

```
#OpenStartElementTag#
EventID
#CloseStartElementTag#
1234
#EndElementTag#
```

Binärisierung mit Tabelle:

Value	Meaning	Example
0x00	EndOfBXmlStream	
0x01	OpenStartElementTag	< name >
0x02	CloseStartElementTag	< name >
0x03	CloseEmptyElementTag	< name />
0x04	EndElementTag	</ name >
0x05	Value	attribute = “value”
0x06	Attribute	attribute = “value”
0x0c	TemplateInstance	
0x0d	NormalSubstitution	
0x0e	OptionalSubstitution	
0x0f	StartOfBXmlStream	

2. Schritt Substitution

Strings die komprimiert dargestellt werden können, werden durch entsprechende Formate substituiert.

Beispiel:
`<EventID>1234</EventID>`

Aus 4 Byte String 1234 wird ein 2 Byte unsigned Int.

3. Schritt Templates

Oft ähneln sich aufeinanderfolgende Events. Dann werden nur die Unterschiede zum vorherigen Event gespeichert, wie eine Differenz, oftmals nur Zeitstempel.

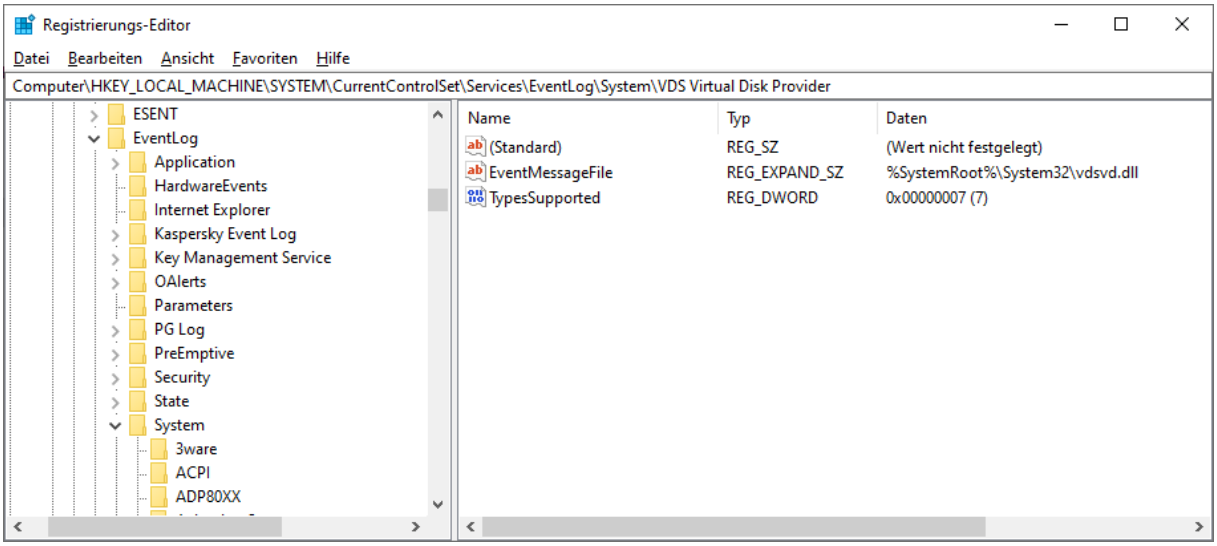
Eine manuelle Dekodierung ist sehr mühsam aber bei gecarvten Fragmenten etwa unumgänglich.

1.5.2.3 Untersuchen von EVT- und EVTX-Log-Dateien

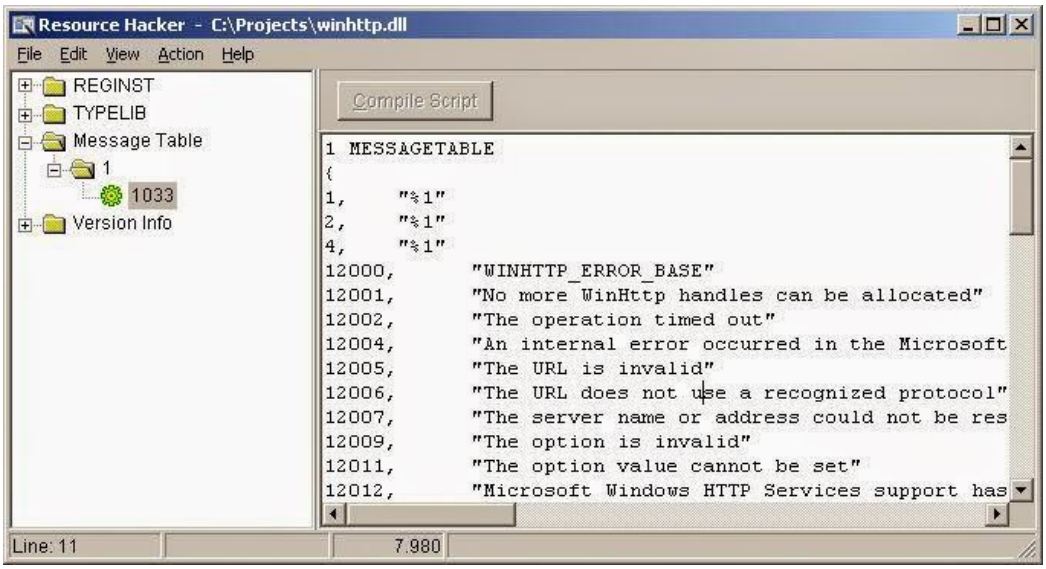
Die EVT- und EVTX-Log Einträge enthalten nur sehr wenig menschenlesbaren Kontext. Die Einträge werden erst durch einen Viewer, wie den Microsoft Event Viewer, verständlich indem die variablen Daten aus den Event Records mit vordefinierten Log Templates, die in den System DLLs und EXEs als Ressourcen abgelegt sind, verknüpft werden.

Wenn der Event Viewer (oder ein anderer Interpreter) die Log Einträge darstellt, müssen die DLLs, die das Message Template enthalten, gefunden werden. Die Zuordnung Event nach DLL geschieht über die Registry und ist für jedes Log (System, Security, Application, etc) spezifisch.

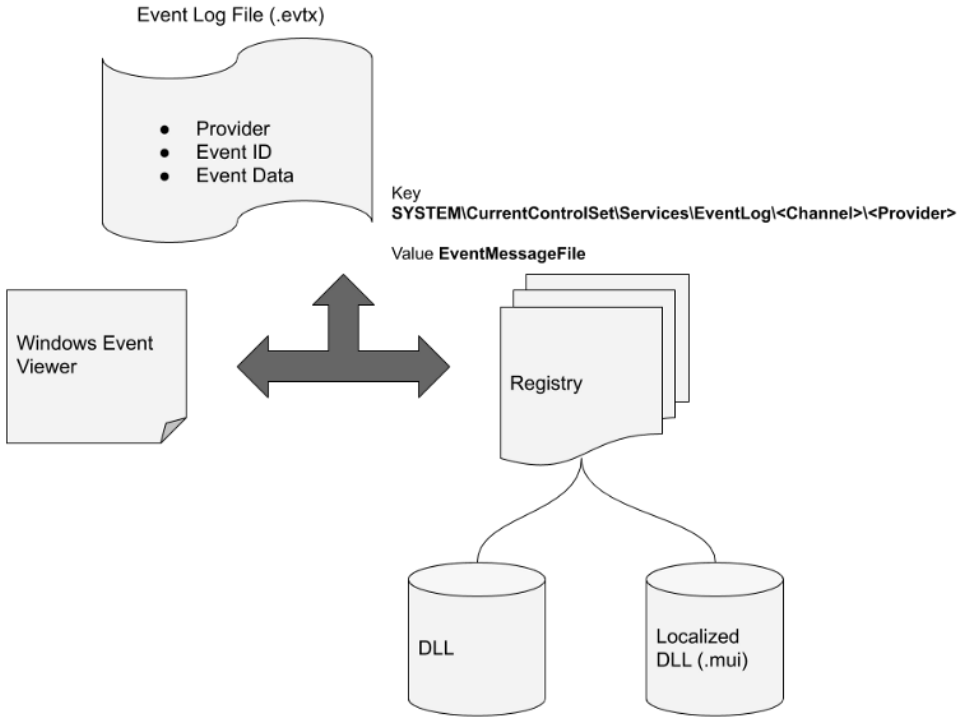
Windows (mindestens ab NT4) verwaltet eine Liste der Ereignisprotokollanbieter in der Windows-Registrierung unter dem Schlüssel: „HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\". Dieser Schlüssel enthält einen Unterschlüssel pro Protokolltyp (z. B. System) und Protokollquelle (z. B. Workstation): „HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\System\". Dieser Unterschlüssel enthält einen Wert mit dem Namen EventMessageFile. Dieser Wert enthält einen oder mehrere Dateinamen, z.B. „% SystemRoot%\System32\netmsg.dll".



Die Vorlagen für Nachrichten werden in „Message-Table Ressource“ Dateien gespeichert, bei denen es sich um ausführbare PE / COFF-Dateien handelt, die einen Ressourcenabschnitt („.rsrc“) enthalten. Eine Ressource im Ressourcenabschnitt der Dateien sollte eine Message-Table Ressource sein, wie im Folgenden unter Nutzung des Ressource Hackers gezeigt.



Diese message-table Ressource enthält eine Liste der Message String Tables Vorlagen mit Bezeichnern, die zumindest für EVT-Dateien mit den Ereignisbezeichnern übereinstimmen. Für .evtx-Dateien kann die Nachrichten-ID durch Kombination der Ereignis-ID und der Qualifier ermittelt werden.



Quelle: Mike Cohen

1.5.2.4 Beispiel Windows XP

Unter Windows XP lautet die entsprechende Ereignismeldungszeichenfolge, wenn die Nachrichtenressource die Datei *C:\Windows\System32\netmsg.dll* ist und die Ereigniskennung 3260 (0x00000cbc) lautet: Dieser Computer wurde erfolgreich mit %1 %2 verbunden.

Hier sind %1 und %2 Platzhalter, die auf die erste und zweite Zeichenfolge im entsprechenden Ereignisprotokoll verweisen. Die tatsächliche Reihenfolge der Zeichenfolgen in der formatierten Zeichenfolge hängt von der Grammatik der Sprache ab, in der die Nachrichtenzeichenfolge generiert wird.

Wenn eine solche Ressourcendatei gelöscht wird, geht die Bedeutung aus dem Log Eintrag verloren. Auch wenn die entsprechende Komponente nicht installiert ist, kann eine solche Nachricht nicht korrekt angezeigt werden. Dies wird durch folgende Ausgabe des Event Viewers deutlich: "The description for Event ID 10016 from source Microsoft-Windows-DistributedCOM cannot be found." In diesem Fall kann eine korrekte Darstellung nur mit der korrekten Ressource Datei erfolgen.

Dazu kann man verschiedene Möglichkeiten nutzen:

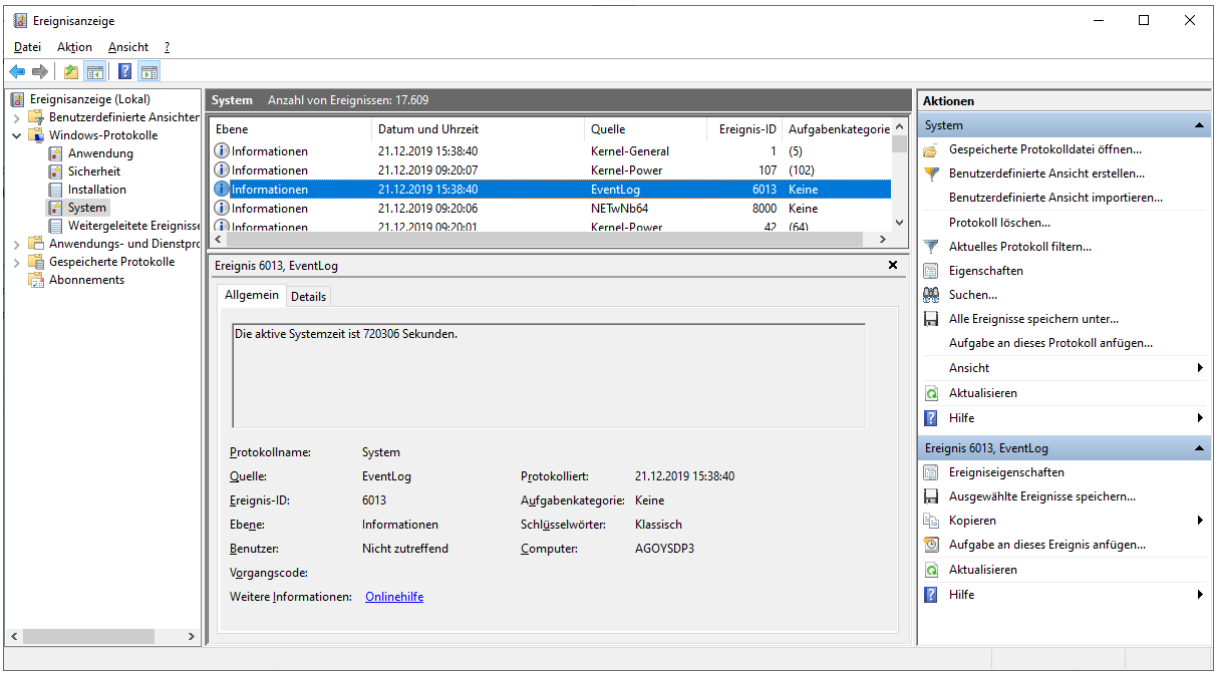
- Untersuchung der Event Logs im Live System
- Virtualisierung des Asservates und Untersuchung des Event Log im virtualisierten System
- Extraktion der Ressourcendateien und Registry Informationen auf das Untersuchungssystem
- Nutzung von 3trd Party Tools mit integrierten Message Table Datenbanken für gängige Softwareanwendungen und Systemdiensten
- Recherche der EventID im Internet für die entsprechende Anwendung

Hinweis: Die EventID der Standard Microsoft Installationen können auf einem Windows Untersuchungssystem in der Regel korrekt dargestellt werden. Hier sollte es keine Probleme mit fehlenden Ressourcen Dateien geben. Sollten Server Betriebssysteme ausgewertet werden, kann dies jedoch bei einzelnen Server Diensten bereits zu fehlenden Log Darstellungen führen.

Die Software zur Einsicht von Log Dateien im Live System findet sich unter: Systemsteuerung\System\Verwaltung\Ereignisanzeige. Diese kann auch genutzt werden, um Event Logs vom untersuchten Asservat darzustellen.

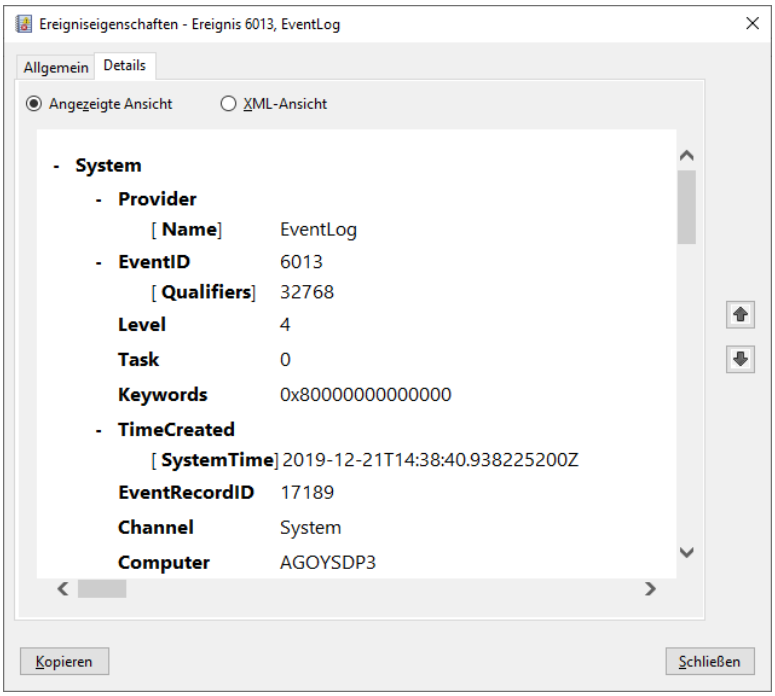
Eine weitere Möglichkeit ist die Nutzung von Plaso/Log2Timeline zur Erstellung von Timelines mit den Standard Events von Microsoft Produkten. Plaso nutzt dazu eine eigene Ressource Table Datenbank. Es gibt noch einige weitere Tools zum Einsehen der Event Logs:

- LogParser
- Event Log Explorer
- LOGAlyze



Darstellung von Events im Windows Event Viewer

Details zu einem Event im Windows Event Viewer



Erweiterte Ansicht zu einem Event im Windows Event Viewer

1.5.3 Windows Logging – Zeit- und Zugriffsanalyse

1.5.3.1 Zeit- und Zugriffsanalysen – Eventlogs

Über die Eintragungen in die Event Log Dateien können Feststellungen unter anderem darüber getroffen werden, ob ein Computer zu einer bestimmten Zeit aktiv war oder nicht.

Es können fundamentale Aussagen über das Starten und Herunterfahren von Computern festgestellt werden. Mit Hilfe der Event Eintragungen zu NTP Diensten können Eintragungen ermittelt werden die beweisen, dass die Uhrzeit zu einem fraglichen Zeitpunkt auf dem aktuellen Stand war.

Die Event Log Eintragungen enthalten zudem Hinweise auf Starts und Beendigungen von Diensten. Dies kann hilfreich sein, um festzustellen, ob bestimmte Malware bestimmte Dienste deaktiviert hat.

Das Event Log beinhaltet unter anderem auch Events zu dessen Löschung, sofern das Event Log manuell zu einem bestimmten Zeitpunkt gelöscht wurde.

1.5.3.2 Last Login und Last Password Change

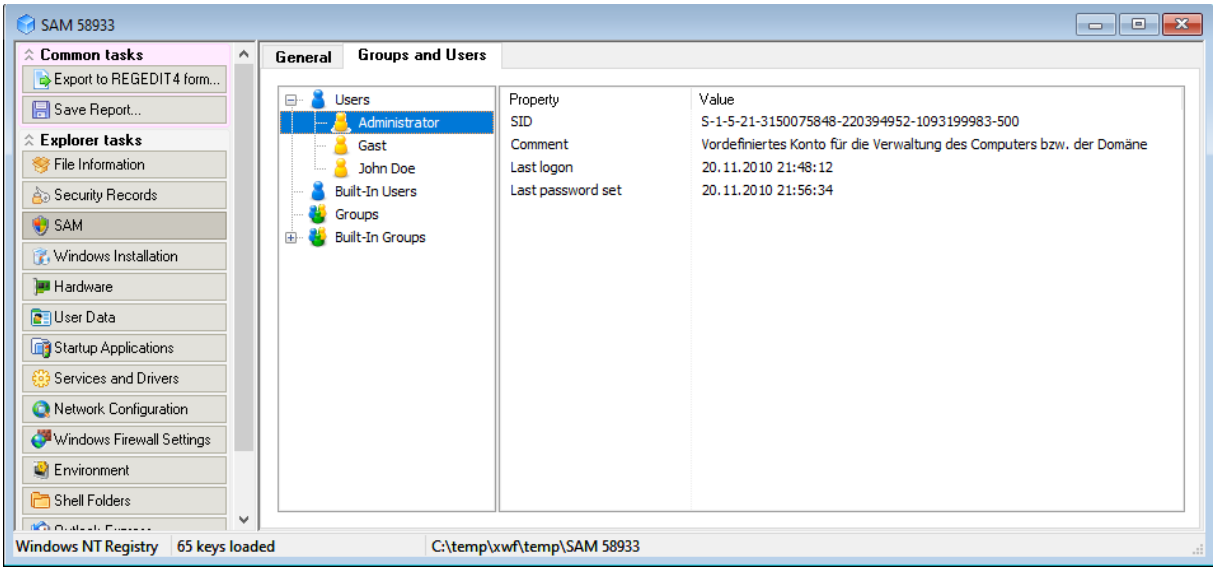
Last Login und Last Password Change Listet die lokalen Konten des Systems und deren zugehörige SID auf, sowie den Zeitpunkt der Passwortänderung.

Speicherort

- C:\windows\system32\config\SAM
  SAM\Domains\Account\Users

Interpretation

- Im Registrierungsschlüssel wird nur die letzte Anmeldezeit und der letzte Zeitpunkt des Passwortwechsel gespeichert



SAM im WRR Registry Viewer angezeigt

1.5.3.3 Success/Fail Logons

Success und Fail Logons ermitteln die Konten, welche für Anmeldeversuche verwendet wurden. Außerdem sind sie für die Verfolgung der Kontonutzung für bekannte kompromittierte Konten.

Speicherort

- Win7/8/10: *%system root%\System32\winevt\logs\Security.evtx*

Interpretation

- Win7/8/10
  - 4624 – Successful Logon
  - 4625 – Failed Logon
  - 4634 | 4647 – Successful Logoff
  - 4648 – Logon using explicit credentials (Runas)
  - 4672 – Account logon with superuser rights (Administrator)
  - 4720 – An account was created

1.5.3.4 Logon Typen

Anmeldeereignisse können sehr genaue Informationen über die Art der Konto Anmeldung in einem System geben. Dazu müssen die gefundenen Daten im Event Log entschlüsselt werden können. Anmeldeereignisse können nicht nur Datum, Uhrzeit, Benutzername, Hostname und Erfolgs- / Fehlerstatus einer Anmeldung mitteilen, sondern auch genau bestimmen, auf welche Weise eine Anmeldung versucht wurde.

Speicherort

- Win7/8/10: *%system root%\System32\winevt\logs\Security.evtx*

Event ID 4624 Eintragungen:

- 2 Logon via console
- 3 Network Logon
- 4 Batch Logon
- 5 Windows Service Logon
- 7 Credentials used to unlock screen
- 8 Network logon sending credentials (cleartext)
- 9 Different credentials used than logged on user
- 10 Remote interactive logon (RDP)
- 11 Cached credentials used to logon
- 12 Cached remote interactive (similar)

1.5.3.5 Remote Desktop Protocol Usage

Remote Desktop Protocol Usage speichert Remote Desktop Protocol Logons im Event Log des Ziel Computers.

Speicherort

- Win7/8/10: *%system root%\System32\winevt\logs\Security.evtx*

Interpretation

- Win7/8/10
  Event ID 4778 – Session Connected/Reconnected
  Event ID 4779 – Session Disconnected
- Event log enthält Hostname und IP-Adresse des Remote Computers, der die Verbindung aufbaut

1.5.3.6 Services/Dienste im Event Log

Durch Analysieren der Protokolle auf verdächtige Dienste, die zum Startzeitpunkt ausgeführt werden, können Hinweise auf Malware festgestellt werden. Überprüfungs- und Schutzdienste werden dabei eventuell um die Zeit eines vermuteten Angriffes gestartet oder gestoppt.

Speicherort

- Win7/8/10: *%system root%\System32\winevt\logs\System.evtx*

Interpretation

- 7034 – Service crashed unexpectedly
- 7035 – Service sent a Start/Stop control
- 7036 – Service started or stopped
- 7040 – Start type changed (Boot | On Request | Disabled)
- 7045 – A service was installed on the system (Win2008R2+)
- 4697 – A service was installed on the system (from Security log)

Eine große Menge von Malware und Würmern in freier Wildbahn nutzt Dienste. Beim Booten gestartete Dienste deuten auf Advanced Persistent Threads hin. Dienste können aufgrund von Angriffen wie Prozess Injection abstürzen.

1.5.3.7 UserAssist

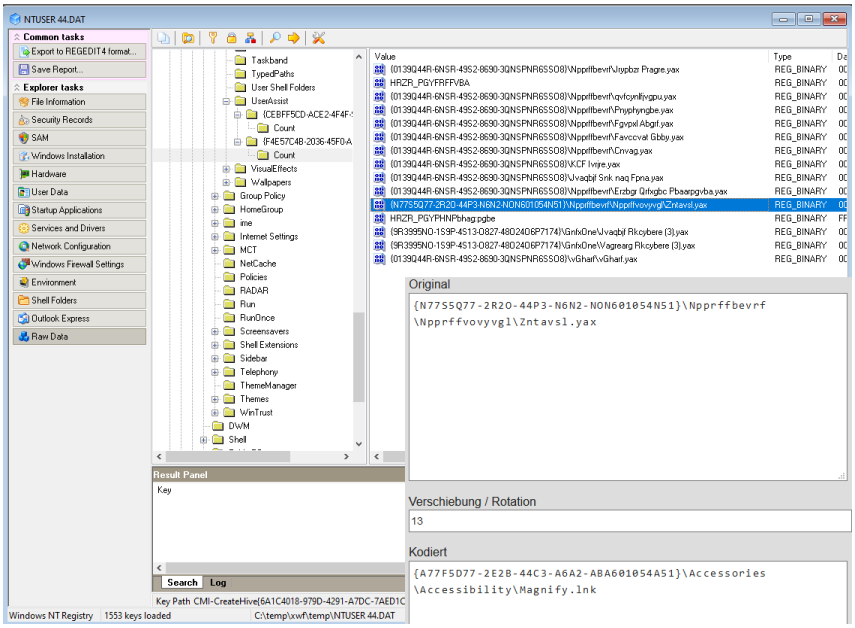
Vom Desktop aus gestartete GUI-basierte Programme werden im Launcher auf einem Windows-System nachverfolgt.

Speicherort

- *NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist*\{GUID}\Count

Interpretation

- Alle Eintragungen sind ROT-13 Encoded
- GUID für XP
  - 75048700 Active Desktop
- GUID für Win7/8/10
  - CEBFF5CD Executable File Execution
  - F4E57C4B Shortcut File Execution



UserAssist in WRR und extern dekodiert

1.5.3.8 Open/Save Most Recent Used

Mit diesem Schlüssel werden im einfachsten Sinne Dateien nachverfolgt, die in einer Windows-Shell-Dialogbox geöffnet oder gespeichert wurden. Dies ist eine große Datenmenge, die nicht nur Webbrowser wie Internet Explorer und Firefox, sondern auch die meisten häufig verwendeten Anwendungen enthält.

Speicherort

- XP: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
- Win7/8/10: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU

Interpretation

- der "*" key – Dieser Subkey enthält die meistgenutzten Dateien einer OpenSaveDialogbox
- .??? (die Extension) – Dieser Subkey enthält die meistgenutzten Dateien einer OpenSaveDialogbox für eine spezifische Extension

1.5.3.9 Last-Visited Most Recent Used

Enthält die Anwendungsdateien (EXE) die zum letzten Öffnen der Dateien im OpenSaveMRU Schlüssel genutzt wurden. Des Weiteren enthält der Eintrag den letzten Dateipfad, der von dieser Anwendung aufgerufen wurde. Beispiel Notepad.exe wurde das letzte Mal gestartet vom Verzeichnis C:\Users\Rob\Desktop.

Speicherort

- XP: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
- Win7/8/10: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

1.5.3.10 Shell Bags

Enthält auf welche Ordner lokal, im Netzwerk und auf Wechselspeichermedien zugegriffen wurde. Enthält damit auch Hinweise auf bereits gelöschte oder überschriebene Verzeichnisse, sowie deren Zugriffszeitpunkt.

Speicherort

Explorer Zugriff:

- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags
- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU

Desktop Zugriff:

- NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU
- NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags

1.5.3.11 Recent Dateien

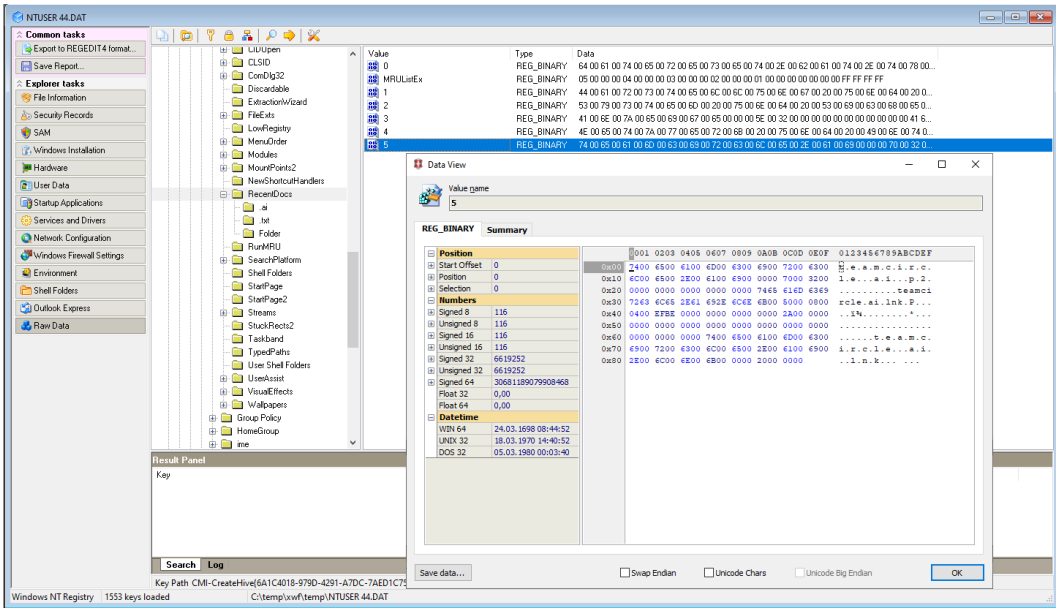
Registrierungsschlüssel, der die zuletzt geöffneten Dateien und Ordner protokolliert und zum Erstellen der Liste der Daten in den Menüs "Zuletzt verwendet" des Startmenüs verwendet wird.

Speicherort

- *NTUSER.DAT*
  NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Interpretation

- RecentDocs - Mit dem Gesamtschlüssel wird die Gesamtreihenfolge der letzten 150 geöffneten Dateien oder Ordner nachverfolgt. Die MRU-Liste verfolgt die zeitliche Reihenfolge, in der die einzelnen Dateien / Ordner geöffnet wurden. Die letzte Eingabe und Änderung dieses Schlüssels sind die Zeit und der Ort, an dem die letzte Datei einer bestimmten Erweiterung geöffnet wurde.
- *.??? - In diesem Unterschlüssel werden die zuletzt geöffneten Dateien mit einer bestimmten Erweiterung gespeichert. Die MRU-Liste verfolgt die zeitliche Reihenfolge, in der die einzelnen Dateien geöffnet wurden. Die letzte Eingabe und Änderungszeit dieses Schlüssels sind die Zeit und der Ort, an dem die letzte Datei einer bestimmten Erweiterung geöffnet wurde.
- Folder - In diesem Unterschlüssel werden die zuletzt geöffneten Ordner gespeichert. Die MRU-Liste verfolgt die zeitliche Reihenfolge, in der die einzelnen Ordner geöffnet wurden. Die letzte Eingabe und Änderungszeit dieses Schlüssels sind die Zeit und der Ort des zuletzt geöffneten Ordners.



WRR Registry Viewer mit Recent Files Eintragungen

1.5.3.12 Shortcut LNK Dateien (Link Dateien)

Von Windows automatisch erstellte Verknüpfungsdateien

- Verlaufsdateien zur Verknüpfung
- Beim Öffnen von lokalen und Remote-Datendateien und -dokumenten wird eine Verknüpfungsdatei (.lnk) erstellt.

Speicherort

- XP:
  C:\%USERPROFILE%\Recent
- Win7/8/10:
  C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\
  C:\%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\

Beachten Sie, dass dies der primäre Speicherort von LNK-Dateien ist. Sie können auch an anderen Orten gefunden werden.

Interpretation

- Datum / Uhrzeit-Datei mit diesem Namen wurde zum ersten Mal geöffnet
  - Erstellungsdatum der Shortcut-Datei (LNK)
- Datum / Uhrzeit-Datei mit diesem Namen wurde zuletzt geöffnet
  - Datum der letzten Änderung der LNK-Datei (Shortcut)
- Daten der LNK-Target-Datei (interne LNK-Dateiinformationen):
  - Änderungs-, Zugriffs- und Erstellungszeiten der Zieldatei
  - Volume-Informationen (Name, Typ, Seriennummer)
  - Informationen zur Netzwerkfreigabe
  - Ursprünglicher Speicherort
  - Name des Systems

Link target information

Target Attributes	A
Target File Size	10040
Show Window	SW_NORMAL
Target Created	23.02.2015 08:34:26 +1
Last Written	23.02.2015 08:34:26 +1
Last Accessed	23.02.2015 08:35:17 +1
ID List	Desktop\N:\Geheime Projekte\ C=23.02.2015 07:35:04 M=23.02.2015 07:35:36 ULTRA GEHEIMER VERTRAG.docx C=23.02.2015 07:34:26 M=23.02.2015 07:34:28 Size=10040
Network share name	\\BERSERKER2\Archiv
DriveLetter	N:
Target path	+
Working Directory	N:\Geheime Projekte
Known Folder Tracking	false
PROPERTYSTORAGE	{46588AE2-4CBC-4338-BBFC-139326986DCE}
Size	0
Host Name	berserker2
Volume ID	{117F8236-FAB7-70BA-9187-DF8DD40CB2F0}
Object ID	{00000902-0000-0000-0400-E81A00000000}

Im Recent Verzeichnis werden auch Dokumente angezeigt, die sich niemals auf der analysierten Festplatte befunden haben! Möglicherweise können dadurch relevante Netzwerk-Shares identifiziert werden. LNK Dateien sind eine sehr ergiebige Datenquelle, um die tatsächliche Nutzung des PCs nachzuvollziehen.

1.5.3.13 Office Files MRU

Ähnlich wie bei den zuletzt geöffneten Dateien (Recent Dateien) werden hiermit die letzten Dateien nachverfolgt, die von jeder MS Office-Anwendung geöffnet wurden. Der letzte Eintrag, der gemäß der MRU hinzugefügt wurde, ist der Zeitpunkt, zu dem die letzte Datei von einer bestimmten MS Office-Anwendung geöffnet wurde.

Speicherort

NTUSER.DAT\Software\Microsoft\Office\VERSION

- *15.0 = Office 365*
- *14.0 = Office 2010*
- *12.0 = Office 2007*
- *11.0 = Office 2003*
- *10.0 = Office XP*

NTUSER.DAT\Software\Microsoft\Office\VERSION\UserMRU\LiveID_####\ FileMRU

1.5.3.14 Prefetch Dateien

Steigern die Leistung eines Systems, indem Codepages häufig verwendeter Anwendungen vorgeladen werden. Der Cache-Manager überwacht alle Dateien und Verzeichnisse, auf die für jede Anwendung oder jeden Prozess verwiesen wird, und ordnet sie einer *.PF-Datei zu. Wird verwendet, um zu wissen, dass eine Anwendung auf einem System ausgeführt wurde.

- Begrenzt auf 128 Dateien unter XP und Win7
- Auf Win8 auf 1024 Dateien beschränkt
- **Format: (exename) - (hash) .pf**
  (Existiert eine *.PF Datei wurde die Anwendung auch ausgeführt!)

Speicherort

- WinXP/7/8/10
  C:\Windows\Prefetch

Interpretation

- Jede *.pf-Datei enthält die letzte Ausführungszeit, die Häufigkeit der Ausführung sowie die vom Programm verwendeten Geräte- und Dateihandles
- Erstmalige Ausführung der Anwendung = Erstellungszeit
- Letzter Zeitpunkt der Ausführung der Anwendung = Änderungszeit

1.5.3.15 Jump Lists

Die Windows 7-Taskleiste (Jump Lists) wurde so gestaltet, dass Benutzer schnell und einfach auf häufig oder kürzlich verwendete Elemente zugreifen können. Diese Funktionalität kann nicht nur aktuelle Mediendateien umfassen. Es kann auch aktuelle Tasks enthalten.

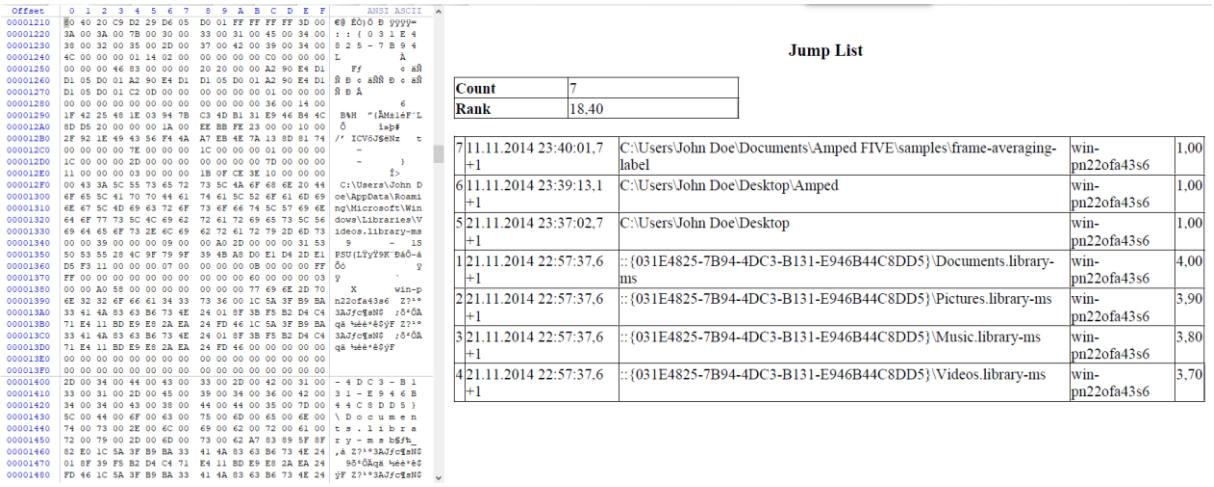
Wenn Sie die AutomaticDestinations öffnen, stellen Sie eine Anzahl an Dateien fest. Den im Ordner AutomaticDestinations gespeicherten Daten wird jeweils eine eindeutige Dateikennung mit der AppID der zugeordneten Anwendung vorangestellt. Jede dieser Dateien ist eine separate LNK-Datei. Sie werden auch in numerischer Reihenfolge vom frühesten (normalerweise 1) bis zum jüngsten (größter ganzzahliger Wert) gespeichert.

Speicherort

- Win7/8/10
  C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Interpretation

- Erstmalige Ausführung der Anwendung.
  Erstellungszeit = Erstes Element, das der AppID-Datei hinzugefügt wurde.
- Letzter Zeitpunkt der Ausführung der Anwendung mit geöffneter Datei.
  Änderungszeit = Zuletzt zur AppID-Datei hinzugefügtes Element.
- Liste der JumpList-IDs -> http://web.archive.org/web/20190427230518/http://www.forensicswiki.org/wiki/List_of_Jump_List_IDs



Jump List

Count	7
Rank	18,40

7	11.11.2014 23:40:01,7 +1	C:\Users\John Doe\Documents\Amped FIVE\samples\frame-averaging-label	win-pn22ofa43s6	1,00
6	11.11.2014 23:39:13,1 +1	C:\Users\John Doe\Desktop\Amped	win-pn22ofa43s6	1,00
5	21.11.2014 23:37:02,7 +1	C:\Users\John Doe\Desktop	win-pn22ofa43s6	1,00
1	21.11.2014 22:57:37,6 +1	::{031E4825-7B94-4DC3-B131-E946B44C8DD5}\Documents.library-ms	win-pn22ofa43s6	4,00
2	21.11.2014 22:57:37,6 +1	::{031E4825-7B94-4DC3-B131-E946B44C8DD5}\Pictures.library-ms	win-pn22ofa43s6	3,90
3	21.11.2014 22:57:37,6 +1	::{031E4825-7B94-4DC3-B131-E946B44C8DD5}\Music.library-ms	win-pn22ofa43s6	3,80
4	21.11.2014 22:57:37,6 +1	::{031E4825-7B94-4DC3-B131-E946B44C8DD5}\Videos.library-ms	win-pn22ofa43s6	3,70

Jump List in X-Ways

1.5.4 Windows Logging – Laufwerkszugriffe

Eine wenig bekannte Tatsache über den IE-Verlauf ist, dass die in den Verlaufsdateien gespeicherten Informationen nicht nur mit dem Browsen im Internet zusammenhängen. Der Verlauf zeichnet auch den lokalen und Remote-Dateizugriff (über Netzwerkfreigaben/UNC Pfade) auf. So können Zugriffshistorien auf Dateien über längere Zeiträume ermittelt werden, auf welche Dateien und Anwendungen zugegriffen wurde. Die Zugriffshistorien werden an verschiedensten Orten gespeichert. Für IE6-7 unter %USERPROFILE%\LocalSettings\History\History.IE5, für IE8-9 unter %USERPROFILE%\AppData\Local\Microsoft\WindowsHistory\History.IE5 und für IE10-11 unter %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat.

Für dessen Interpretation muss einiges beachtet werden. Sie werden in der index.dat als file: ///N:/directory/filename.ext. Dies bedeutet nicht, dass die Datei im Browser geöffnet wurde.

1.5.4.1 Laufwerkszugriffe auf USB-Geräte

Key Identifizierung von USB-Geräten

Angeschlossene USB-Geräte werden in der Registry unter einem bestimmten Schlüssel gespeichert. Die Speicherorte sind folgende: „SYSTEM\CurrentControlSet\Enum\USBSTOR“ und „SYSTEM\CurrentControlSet\Enum\USB“. Mit diesen Einträgen kann der Hersteller, das Produkt und die Version eines an einen Computer angeschlossenen USB-Geräts identifiziert werden. Weiterhin wird ein eindeutiges USB-Gerät identifiziert, das angeschlossen war. Ebenfalls wird die Uhrzeit gespeichert, zu der ein Gerät angeschlossen war. Geräte ohne eine eindeutige Seriennummer haben ein „&“ im zweiten Zeichen der Seriennummer.

First/Last Times von USB-Geräten

Plug and Play Log Dateien für den ersten Anschluss eines USB-Gerätes werden bei Windows XP unter C:\Windows\setupapi.log und unter Windows 7, 8 und 10 unter C:\Windows\inf\setupapi.dev.log gespeichert.

Die First, Last und Removal Zeiten findet man unter \CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties\{83da6326-97a6-4088-9453-a19231573b29}\####.
Die Endung 0064 steht für First Install (Windows 7-), 0066 für Last Connected (Windows 8-) und 0067 für Last Removal (Windows 8-). Hierbei erkennt man die Seriennummer des Gerätes. Außerdem ist die Log File Zeit in Lokalzeit angegeben.

Volume Serial Number

Man kann zusätzlich die Volume-Seriennummer der Dateisystempartition auf dem USB-Stick ermitteln. Bei dieser Volume-Seriennummer handelt es sich nicht um die eindeutige USB-Seriennummer, die in der Gerätefirmware fest codiert ist.

Die Informationen zur Volume-Seriennummer sind unter „SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ENDMgmt“ gespeichert. Für die Interpretation dieser Informationen muss einiges beachtet werden. Die Berechnung erfolgt aus dem Volume Namen und der USB Unique Seriennummer: Hierfür sucht man die letzte Ganzzahl in der Zeile und konvertiert die dezimalen Seriennummern in hexadezimale Seriennummern. Weiterhin enthält die Shortcut-Datei (LNK) die Seriennummer und den Namen des Volumes. Der Registrierungsschlüssel RecentDocs enthält in den meisten Fällen den Namen des Volumes, wenn das USB-Gerät über den Explorer geöffnet wird.

Drive Letter und Volume Name

Man kann die Laufwerksbuchstaben beim letzten Anschluss an den Computer feststellen. Diese Informationen befinden sich unter „SOFTWARE\Microsoft\Windows Portable Devices\Devices“ und unter „SYSTEM\MountedDevices“.

Bezüglich der Interpretation dieser Informationen sollte man wissen, dass man hiermit ein USB-Gerät identifizieren kann, welches zuletzt einem bestimmten Laufwerksbuchstaben zugeordnet wurde. Dies funktioniert jedoch nur für das zuletzt zugeordnete Laufwerk. Weiterhin sind hier keine historischen Aufzeichnungen aller Laufwerksbuchstaben zu finden, die dem Wechseldatenträger zugeordnet waren.

LNK Dateien im Zusammenhang mit externen Geräten

Von allen geöffneten lokalen und remote Datendateien werden Shortcuts Link sogenannte LNK Dateien automatisch im Recent Verzeichnis des Benutzers angelegt. Unter Windows 7, 8, 10 und höher werden diese Informationen unter „%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent“ und unter „%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent“ abgelegt.

An diesen Speicherorten befinden sich Daten der LNK-Target-Datei, welche interne LNK-Dateiinformation enthält. Dazu zählen Änderungs-, Zugriffs- und Erstellungszeiten der Zieldatei, Volume-Informationen (Name, Typ, Seriennummer), Informationen zur Netzwerkfreigabe, der ursprüngliche Speicherort und der Name des Systems.

Für die Interpretation der LNK Dateien im Zusammenhang mit externen USB-Geräten sind die Volume Informationen von größter Bedeutung. Durch Kenntnis der Volume-Seriennummer und dem Volume-Namen können die Daten über die LNK Datei-Analyse und den RECENTDOC-Schlüssel verknüpft und USB-Geräten eindeutig zugeordnet werden.

Im Folgenden wird ein Beispiel in X-Ways dargestellt. Hierbei geht es um das Kopieren von Dateien aus dem Netzlaufwerk auf den USB-Stick:

Name	Beschreibung	Typ	Hash[1] (MD5)
.. = (Stammverzeichnis)	Stammverzeichnis, existier...		
. = Generic USB SD Reader, P1 (6)	Verzeichnis, existierend		
Geheime_zeichnung.drw	Datei, existierend, kopiert	drw	299857EE22D03A3A34BA3EF13BBA62B3
ULTRA GEHEIMER VERTRAG.docx	Datei, existierend, kopiert	docx	92BF9B5D91DEF99F655C1976B073749F
Boot-Sektor	Datei, virtuell (für Untersu...		A7B09B900C4764D2D7645C40C7B55A7C
FAT 1	Datei, virtuell (für Untersu...		FA392474D8EBFD439A390575F7B757CA
FAT 2	Datei, virtuell (für Untersu...		FA392474D8EBFD439A390575F7B757CA
Stammverzeichnis [GB]	Ausschnitt, virtuell (für Un...		1987FC26246FCF1FA83970A8D9403CC7

Inhalt USB Stick sichergestellt beim Beschuldigten

Name	Beschreibung	Typ	Hash[1] (MD5)
.. = Laufwerk N: (2)	Verzeichnis, existierend, b...		
. = Geheime Projekte (2)	Verzeichnis, existierend		
Geheime_zeichnung.drw	Datei, existierend	ascii	299857EE22D03A3A34BA3EF13BBA62B3
ULTRA GEHEIMER VERTRAG.docx	Datei, existierend	docx	92BF9B5D91DEF99F655C1976B073749F

Inhalt Netzlaufwerk N:\ auf Windows Server (Opfer)

Name	Beschreibung	Typ	Hash[1] (MD5)
.. = Windows (4)	Verzeichnis, existierend, b...		
. = Recent (4)	Verzeichnis, existierend, b...		
Geheime Projekte.lnk	Datei, existierend, bereits ...	lnk	015CFD50F62CCFB31B00124ABEFB8755
Geheime_zeichnung.drw.lnk	Datei, existierend, bereits ...	lnk	DE4D26F48DF3439141BB2DA771FF911E
SDCARD (I).lnk	Datei, existierend, bereits ...	lnk	DE9859845BAA83296CC5633A979128F7
ULTRA GEHEIMER VERTRAG.docx.lnk	Datei, existierend, bereits ...	lnk	6FD42A2AE3236A552F4AA45749202987

Inhalt Recent Verzeichnis Windows Client Maschine (Arbeitsplatz Beschuldigter)

Target Attributes	A
Target File Size	10040
Show Window	SW_NORMAL
Target Created	23.02.2015 08:34:26 +1
Last Written	23.02.2015 08:34:26 +1
Last Accessed	23.02.2015 08:35:17 +1
ID List	Desktop\N:\Geheime Projekte\ C=23.02.2015 07:35:04 M=23.02.2015 07:35:36 ULTRA GEHEIMER VERTRAG.docx C=23.02.2015 07:34:26 M=23.02.2015 07:34:28 Size=10040
Network share name	\\BERSERKER2\Archiv
DriveLetter	N:
Target path	+
Working Directory	N:\Geheime Projekte
Known Folder Tracking	false
PROPERTYSTORAGE	{46588AE2-4CBC-4338-BBFC-139326986DCE}
Size	0
Host Name	berserker2
Volume ID	{117F8236-FAB7-70BA-9187-DF8DD40CB2F0}
Object ID	{00000902-0000-0000-0400-E81A00000000}

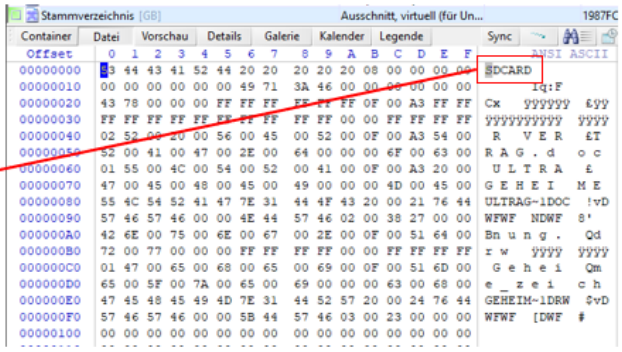
Recent Eintrag Datei: ULTRA GEHEIMER VERTRAG.docx

Target Attributes	A
Target File Size	35
Show Window	SW_NORMAL
Target Created	23.02.2015 08:33:32 +1
Last Written	23.02.2015 08:34:52 +1
Last Accessed	23.02.2015 08:35:29 +1
ID List	Desktop\N:\Geheime Projekte\ C=23.02.2015 07:35:04 M=23.02.2015 07:35:36 Geheime_zeichnung.drw C=23.02.2015 07:33:32 M=23.02.2015 07:34:54 Size=35
Network share name	\\BERSERKER2\Archiv
DriveLetter	N:
Target path	+
Working Directory	N:\Geheime Projekte
Known Folder Tracking	false
PROPERTYSTORAGE	{46588AE2-4CBC-4338-BBFC-139326986DCE}
Size	0
Host Name	berserker2
Volume ID	{117F8236-FAB7-70BA-9187-DF8DD40CB2F0}
Object ID	{00000902-0000-0000-0300-E81A00000000}

Recent Eintrag Datei: Geheime_zeichnung.drw

Target Attributes	(Directory)
Target File Size	0
Show Window	SW_NORMAL
Target Created	01.01.1980 00:00:00 +1
Last Written	01.01.1980 00:00:00 +1
Last Accessed	01.01.1980 00:00:00 +1
ID List	Desktop\I:\
Volume Type	**Removable**
Volume Serial	**0xDE6D7B78**
Volume Name	**SDCARD**
Local Path	**I:**
Known Folder Tracking	false
PROPERTYSTORAGE	{46588AE2-4CBC-4338-BBFC-139326986DCE}
Size	0

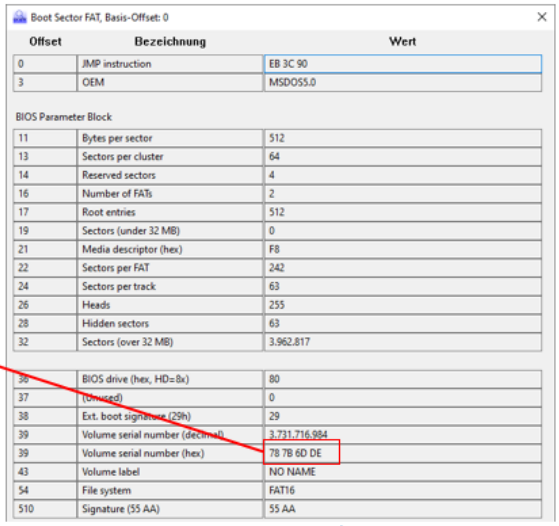
Recent Eintrag Verzeichnis/Gerät: SDCARD



Verzeichniseintrag FAT USB Stick: Root Directory

Target Attributes	(Directory)
Target File Size	0
Show Window	SW_NORMAL
Target Created	01.01.1980 00:00:00 +1
Last Written	01.01.1980 00:00:00 +1
Last Accessed	01.01.1980 00:00:00 +1
ID List	Desktop\I:\
Volume Type	**Removable**
Volume Serial	**0xDE6D7B78**
Volume Name	**SDCARD**
Local Path	**I:**
Known Folder Tracking	false
PROPERTYSTORAGE	{46588AE2-4CBC-4338-BBFC-139326986DCE}
Size	0

Recent Eintrag Gerät: SDCARD



BootSector FAT USB Stick

1.5.5 Zusammenfassung

Sie haben das EVT bzw. das EVTX Log vorgestellt bekommen und wie dieses aufgebaut ist.
Log Dateien bieten grundsätzlich wertvolle Informationen über Aktivitäten auf dem System. Es ist jedoch wichtig den Aufbau der Event Logs zu verstehen, da bei fehlenden Ressourcen Dateien, die Event Eintragungen möglicherweise nicht korrekt angezeigt werden.
Die Account Nutzung und die Recent Dateien geben neben den Event Logs einen Hinweis auf Aktivitäten im Betriebssystem wieder. Hierbei können Eintragungen von Programmstarts ebenso wie genutzte Dateien festgestellt werden. Die dazu notwendigen Informationen befinden sich verteilt zum großen Teil in der Registry aber auch in separaten Dateien mit spezifischem Aufbau.

1.6 Windows Benutzerkonten und Gruppen

1.6.1 Benutzerkonto

1.6.1.1 Windows Benutzerkontenverwaltung SID

Die Benutzerverwaltung auf Windows Betriebssystemen wird mit Hilfe eines Security Identifier, kurz SID realisiert. Die SID ist geeignet um jedes System, jeden Benutzer und jede Gruppe dauerhaft zu identifizieren. An die SID sind die in Access Control Lists festgelegten Zugriffsrechte und Eigentümer gebunden, die auf NTFS Dateisystemen die Benutzerzugriffsverwaltung realisieren. Werden Benutzernamen geändert oder gelöscht, bleiben deren SID unverändert derjenigen Datei oder demjenigen Verzeichnis zugeordnet.

Als Beispiel dient folgende SID: S-1-5-21-7623811015-3361044348-030300820-1013

- S – Kurzzeichen für SID
- 1 – Revisionsnummer
- 5 – Identifier Authority
- 21-76.....0300820 – Domäne oder lokales System
- 1013 – Benutzernummer

Es gibt verschiedene Gruppen von SIDs. 500er Benutzernummern gehören zum System und 1000er Benutzernummern sind für die eigentlichen Benutzer vorgesehen. Die Benutzernummer 500 ist für den Administrator reserviert und die 501 für einen Gast.

1.6.1.2 Benutzerkonten unter Windows

Unter Windows gibt es drei verschiedene Benutzerkontoarten. Die drei Kategorien sind Lokal, Domain und Windows. Die Art des Benutzerkontos bestimmt den Administrator, sprich die Person, welche für die Rechteverwaltung zuständig ist, den Speicherort von Benutzereinstellungen und die Anmeldevoraussetzungen.

1.6.1.3 Lokales Benutzerkonto

Das lokale Benutzerkonto ist aus dem Privat-Computer bekannt. Es wird in der lokalen Security Account Manager (SAM) Datenbank hinterlegt. Weiterhin ist hierfür keine Netzwerkverbindung nötig und das lokale Benutzerkonto wird vom lokalen Administrator Benutzerkonto administriert.

Lokale Standardkonten werden automatisch bei der Installation erstellt. Zu diesen lokalen Standardbenutzerkonten zählen:

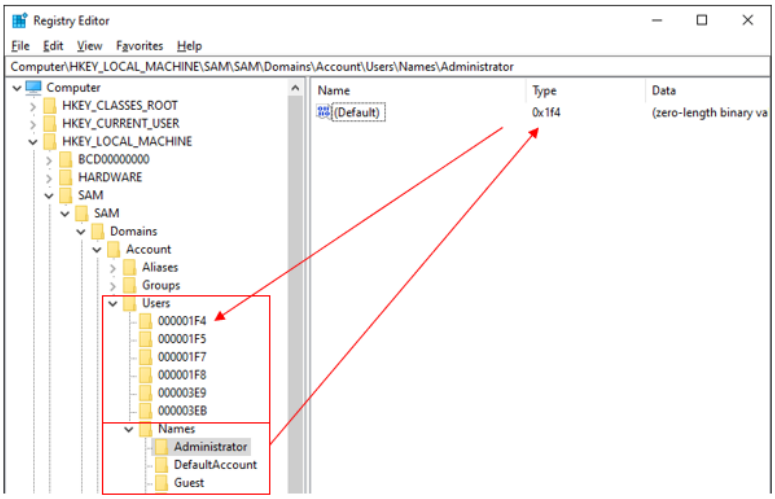
- Administratorkonto (SID S-1-5-Domain-500)
- Gastkonto (SID S-1-5-32-546)

Zu den Lokalen Standardsystemkonten zählen:

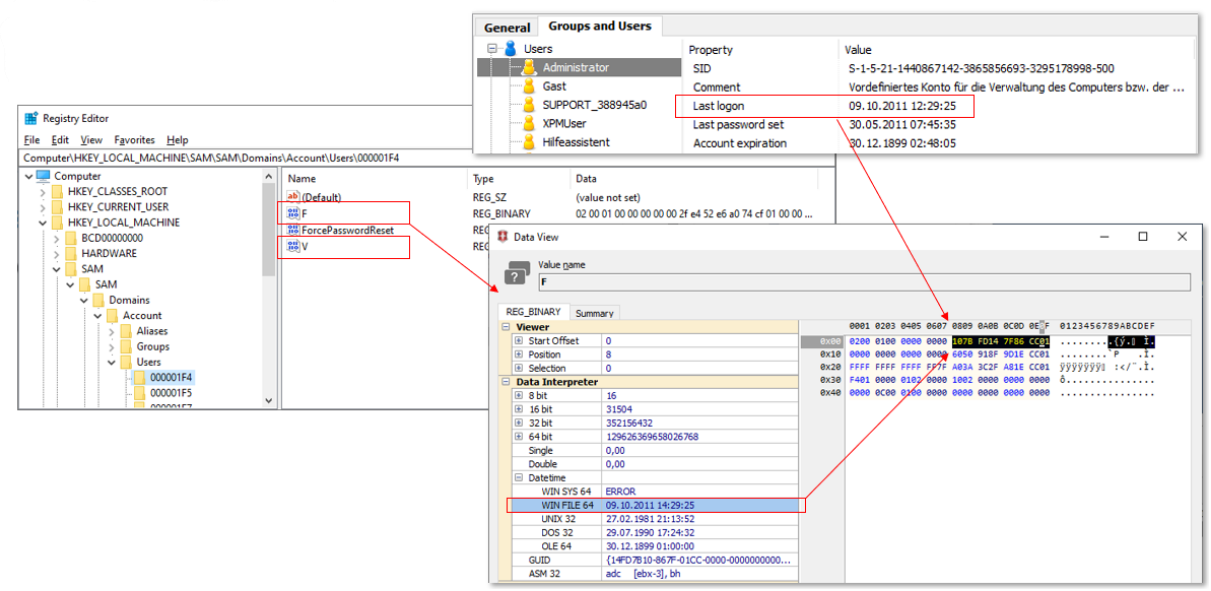
- System (S-1-5-18 LocalSystem)
- Netzwerkdienst (S-1-5-20 NetworkService)
- Lokaler Dienst (S-1-5-19 NT-Autorität)

Forensisch bedeutsame Registry Informationen

Jeder lokale Nutzer hat einen Eintrag in der lokalen SAM Datenbank. Zwei Registry Schlüssel findet man unter „\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users“.



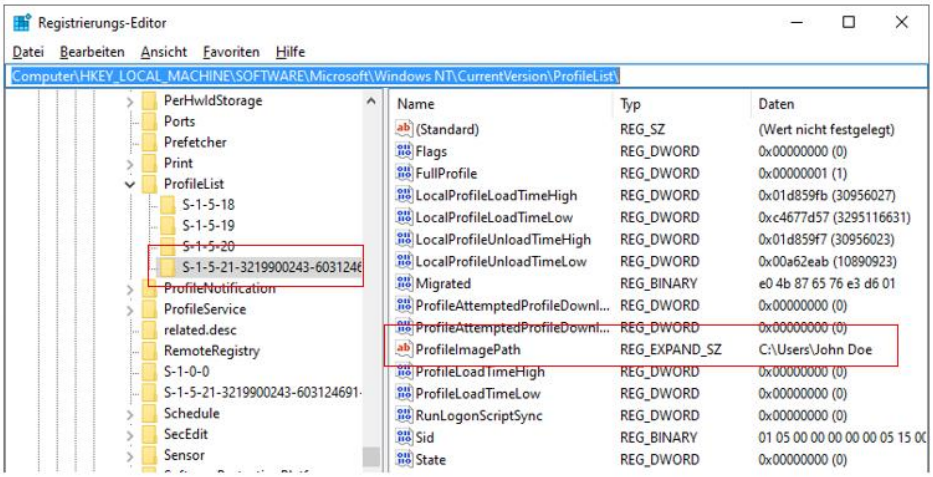
In den Abbildungen werden Users Werte dargestellt:



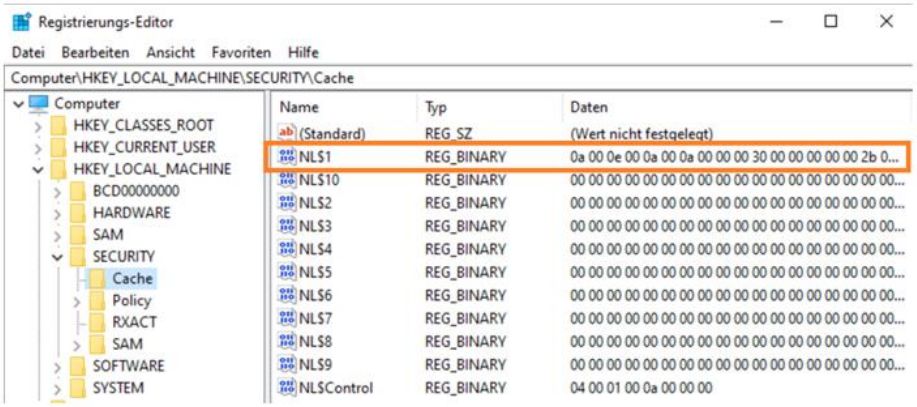
1.6.1.4 Domain Konto

Das Domain-Konto ist in der NTDS.DIT Datenbank des Domaincontrollers hinterlegt. Die Anforderung an die Netzwerkverbindung hängt von der Einstellung auf dem Domaincontroller ab. Administriert wird das Domain-Konto vom Domain-Administrator. Weiterhin befindet sich der Domain-Name unter den Eingabefeldern und wird vor dem Benutzernamen eingegeben, wobei beide Informationen mit „\“ getrennt werden. Ein Beispiel wäre „HSMW\Benutzername“.

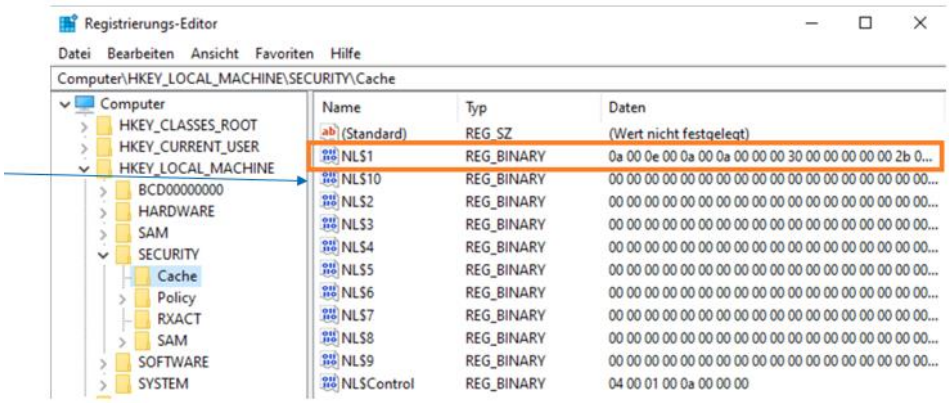
In der lokalen SAM Datenbank ist kein Eintrag vorhanden, aber es gibt einen Referenz Eintrag für Benutzer und Profilordner unter „HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList“.



Cached Credentials werden lokal in der SECUIRITY Registrierung abgespeichert. Diese dienen der lokalen Anmeldung ohne Netzwerk und befinden sich unter „HKEY_LOCAL_MACHINE\SECURITY\Cache“.



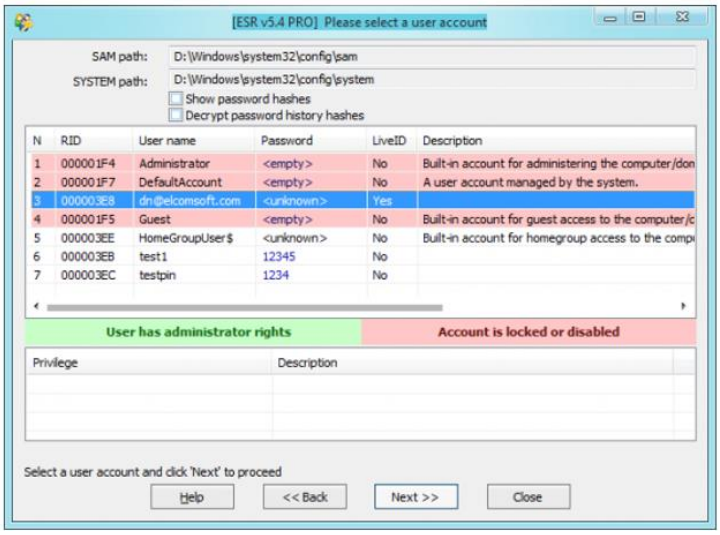
Die Anzahl an maximalen unterschiedlichen Credential, sprich die Anzahl der maximal unterschiedlichen Domänennutzer, wird unter „HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\“ abgelegt. Dort befindet ich ein Eintrag CachedLogonsCount. Dieser hat den Datentyp REG_SZ mit Werten zwischen 0 und 50. Der Standard ist jedoch 10.



1.6.1.5 Windows Account

Der Anmeldung am Windows Account erfolgt über den Microsoft Account Authentication Server. Hierfür wird der Benutzername, welcher die E-Mail-Adresse ist, und das Passwort benötigt. Bei der E-Mail-Adresse kann es sich um die private oder die Microsoft-E-Mail-Adresse handeln. Ehemals war es eine LiveID.

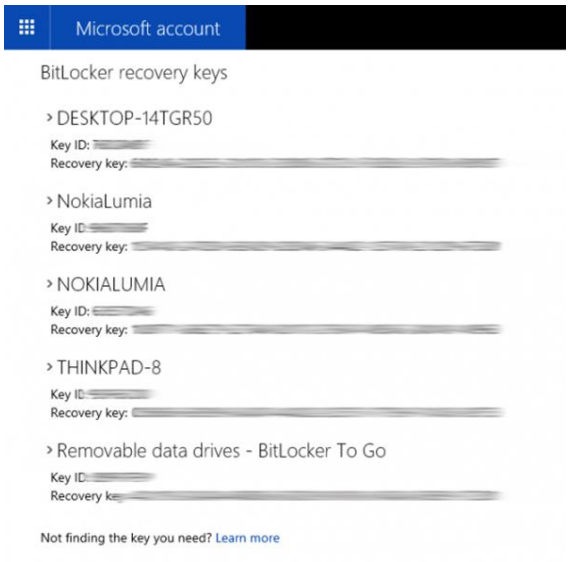
Die Übertragung ist mit SSL gesichert. Ein sogenannter „Remember Login“ speichert den verschlüsselten Wert lokal ab, sodass eine Anmeldung auch ohne Internet möglich ist. Der gespeicherte Wert wird beim Logout gelöscht. Dieser lokale Wert kann extrahiert und „geknackt“ werden:



Der Windows Account ermöglicht auch den Zugriff auf andere Microsoft-Daten dazu zählen:

- OneNote
- Teams
- Bing Search History
- Hotmail und Outlook.com
- OneDrive + OneDrive Backups
- Skype Timeline
- Reset Protection und Find My Device
- (Windows Phone und Windows 10 Mobile Backups)
- Aushebeln der Zwei Faktor Authentifizierung

Weiterhin erstellt Windows automatisch BitLocker-Hinterlegungsschlüssel im Microsoft-Konto des Benutzers. Kennt man das Passwort, kann man diese abrufen.



1.6.2 Gruppen

1.6.2.1 Workgroup

Die Workgroup ist ebenfalls wie das lokale Benutzerkonto aus dem Privat-Computer bekannt. An sich verwaltet sich jeder Computer selbst und kann eigene Ressourcen in Workgroups teilen. Zu diesen Ressourcen gehören beispielsweise angeschlossene Drucker oder Netzwerkordner.

Innerhalb einer Workgroup erfolgt keine zentrale Verwaltung. Ebenfalls gibt es dort keine einheitliche Rechtevergabe. Weiterhin bringen Workgroups einen hohen administrativen Aufwand mit sich.

1.6.2.2 Warum Gruppen?

Gruppen werden eingesetzt, um gleiche Ressourcenzugriffsrechte zu realisieren. Dies bedeutet, dass mehrere Nutzer die gleichen Rechte erhalten. Außerdem lassen sich so die Rechte von Nutzern leichter verwalten und die manuelle Arbeit wird reduziert. Somit sinken der Administrationsaufwand und auch die damit verbundenen Kosten.

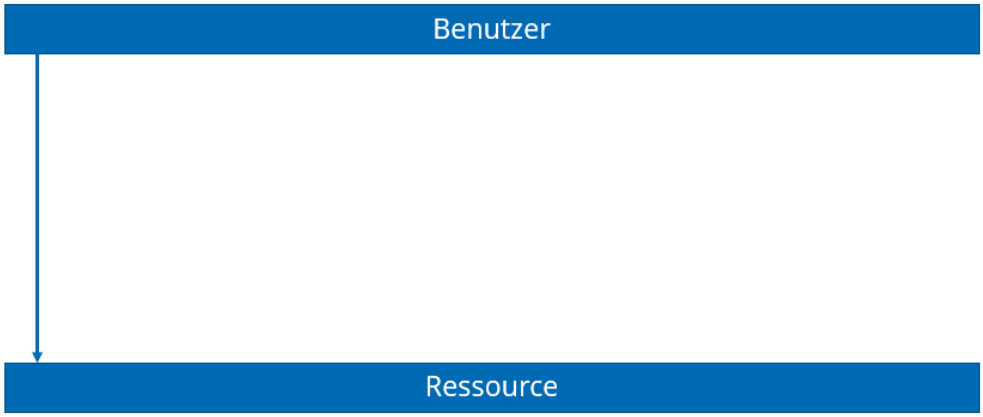
Der Einsatz von Gruppen wird umgesetzt, in dem die Rechteverwaltung sowohl strukturiert als auch vereinheitlicht wird. Weiterhin bekommen Nutzer einen „Rechtesatz“, welcher für eine Gruppe eingestellt ist. Die Arbeitsrolle des jeweiligen Benutzers bestimmt hierbei die Rechte, welche er zugewiesen bekommt.

Die Gruppen beinhalten Ressourcenzugriffsrechte, verschiedene Benutzer und können auch selbst Gruppen enthalten, sodass eine Verschachtelung entsteht. Des Weiteren können Benutzer auch Mitglied in mehreren Gruppen sein.

1.6.2.3 Rechtevergabearten

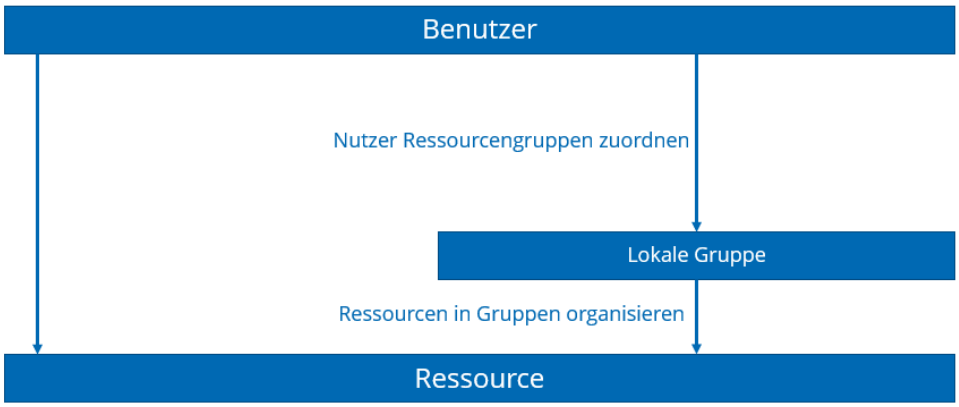
Es gibt verschiedene Arten, auf welche die Rechtevergabe beim Betriebssystem Windows durchgeführt werden kann.

Direkte Rechtevergabe



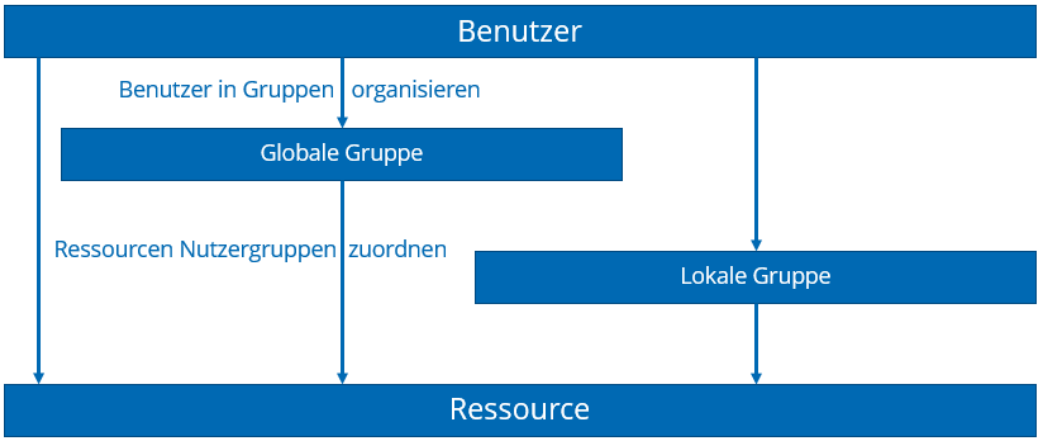
Bei der direkten Rechtevergabe erfolgt die Zuordnung für den Zugriff auf Ressourcen einzeln für jeden Nutzer. Hierbei steigt der administrative Aufwand exponentiell mit der Benutzer- und Ressourcenanzahl. Beispielsweise müssten bei einem neuen Netzwerkshare für einen Vertrieb alle Vertriebsnutzer den Netzwerksharezugriff separat zugeordnet bekommen, was nicht ideal ist. Ebenfalls nicht effizient ist die Situation, wenn es einen neuen Nutzer im Vertrieb gibt. Dieser muss allen Ressourcen hinzugeordnet werden.

Lokale Gruppen



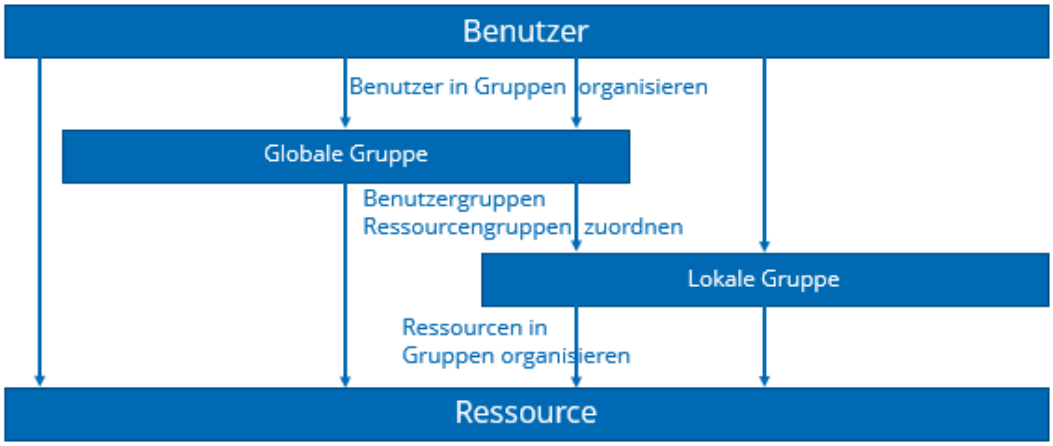
Die Idee ist, dass Ressourcen zu Gruppen zusammengefasst werden. Beispielsweise könnte es eine Druckergruppe, eine Scannergruppe, eine Netzwerksharegruppe oder Ähnliches geben. Die Nutzer werden dann den einzelnen Gruppen hinzugefügt. Denken wir wieder an unsere beiden Szenarien von eben. Ein neuer Netzwerkshare wird für den Vertrieb eingerichtet. Nun würde man eine lokale Netzwerksharegruppe hinzufügen, woraufhin die Nutzer mit Netzwerksharezugriff nun Zugriff auf den neuen Share hätten. Dies wäre effizienter. Jedoch ist das Hinzufügen eines neuen Nutzers in den Vertrieb weiterhin ineffizient, da der Nutzer zu allen lokalen Gruppen hinzugefügt werden muss.

Globale Gruppen



Die Idee hinter den globalen Gruppen ist, dass die Benutzer zu Gruppen zusammengefasst werden. Dabei könnte es sich beispielsweise um Gruppen wie die Administratorgruppe, die Vertriebgruppe oder die Programmierergruppe handeln. Hierbei werden die Ressourcen den Benutzergruppen hinzugefügt. In unserem Szenario Eins würde man einen neuen Netzwerkshare für den Vertrieb einrichten, jedoch wäre dies ineffizient, da der Share allen Benutzergruppen zugeordnet werden muss. Hingegen wäre die Umsetzung des Szenarios Zwei effizient, da hierbei ein neuer Nutzer im Vertrieb lediglich der Vertriebgruppe hinzugefügt werden muss.

Geschachtelte Gruppen



Die Idee von geschachtelten Gruppen ist, dass sowohl Benutzer als auch Ressourcen zu Gruppen zusammengefasst werden. Bei diesen Gruppen könnte es sich beispielsweise um die Programmierergruppe handeln, die in die Druckergruppe, die Netzwerksharegruppe und die Websiteeditgruppe unterteilt ist oder auch die Vertriebsgruppe, die in die Druckergruppe und die Kundendatengruppe unterteilt ist. Beide gewählte Szenarien können mit dieser Art der Gruppierung effizient umgesetzt werden. Für den neuen Netzwerkshare im Vertrieb muss dieser Share nur der Netzwerksharegruppe zugeordnet werden. Der neue Nutzer müsste lediglich zu der Vertriebsgruppe hinzugefügt werden.

Zusammenfassung der Gruppentypen

Zusammenfassend lässt sich festhalten, dass lokale Gruppen Ressourcenrechte zusammenfassen und nur innerhalb einer Domain verfügbar sind. Globale Gruppen hingegen fassen Nutzerrechte zusammen, aber sind ebenfalls nur innerhalb einer Domain. Die universellen Gruppen sind Domainübergreifend und somit keiner Domain zugeordnet.

1.6.3 Lightweight Directory Access Protocol

Das leichtgewichtige Verzeichniszugriffsprotokoll (eng. „Lightweight Directory Access Protocoll“) ist ein Protokoll für die Durchführung von Abfragen und Änderungen in einem verteilten Verzeichnisdienst, ähnlich zu einem Telefonbuch. Dieses Verzeichnis ist wie eine hierarchische Datenbank aufgebaut, sprich es gibt eine Baumstruktur mit Ordnern wie in einem Dateisystem. Das LDAP Protokoll ist im RFC 4532 (IETF) definiert.

Die Aufgabe des LDAP Protokolls ist die zentrale Sammlung und Verwaltung von Benutzerdaten, wobei Rechte und Hardware voneinander getrennt werden. Außerdem bietet dieses Protokoll Flexibilität für den Benutzer und reduziert den administrativen Aufwand für den Administrator. Weiterhin wird mithilfe dieses Protokolls der lesende Zugriff in Bezug auf die Rechtevergabe, die Autorisierung oder ähnliches optimiert.

1.6.3.1 Implementierungen von LDAP

Im Folgenden erfolgt eine Auflistung von Implementierungen von LDAP:

- Active Directory (Microsoft)
- Open Directory (Apple)
- Open LDAP (Linux)
- Apache Directory Studio
- Jxplorer
- FreeIPA
- Samba
- 398 Directory Server (Red Hat)
- OpenDJ
- Zentyal Active Directory
- Oracle Directory Server Enterprise Edition (Oracle)
- eDirectory (Novell)

1.6.3.2 Domainbegriffe Windows

Eine Domain lässt sich mit dem Begriff „Herrschaftsbereich“ beschreiben. Beispielsweise zählt dazu ein physisches Unternehmen oder ein Standort, welche sowohl eine Replikations- als auch eine Sicherheitsgrenze vorweisen. Die Gruppen und Benutzer lassen sich als physische Abteilungen verstehen.

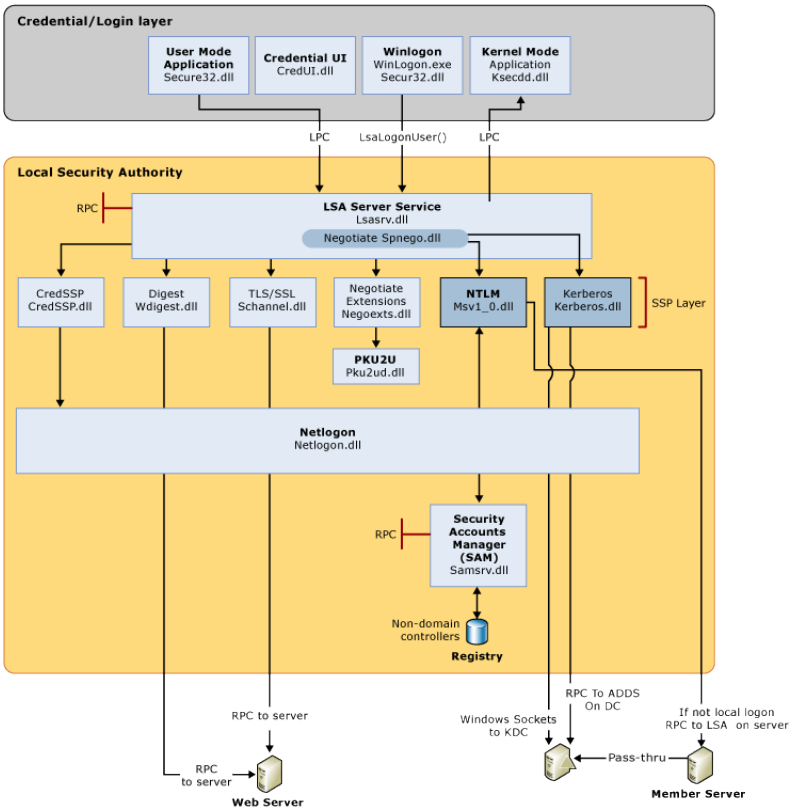
Dabei gibt es Gruppenrichtlinien (Group Policy Object – GPO), welche einen physischen Standort widerspiegeln. Weiterhin kann eine Unterteilung in eine lokale (Domain Local Group – DLG), eine globale (Gobal Group – GG) und eine universelle Gruppe (Universal Group – UG) erfolgen.

Des Weiteren gibt es bei Windows eine Organisationseinheit (Organisation Unit – OU), welche man mit einer physischen Abteilung gleichstellen kann. Die einzelnen Einheiten lassen sich als Baumstruktur darstellen, wobei die Gesamtstruktur durch einen Wald verkörpert wird, was sich mit einem physischen Domaincontroller gleichstellen lässt.

Weiterhin gibt es einen gobalen Katalog. Dieser besteht aus dem ersten Domaincontroller, wobei immer mindestens ein Domaincontroller pro Standort vorliegen muss, einem Datenspeicher für die GPOs und andere Objekte und einer Schnittstelle zu anderen Domains.

1.6.4 Anmeldevorgang

Der Login-Vorgang ist eine interaktive Anmeldung basierend auf Wissen. Dabei unterschiedet man zwischen einer lokalen und einer remote Anmeldung. Weiterhin gibt es verschiedene Anmeldungstypen. Bei der Anmeldung mithilfe einer Smartcard basiert diese auf Wissen und dem Besitz dieser Card. Biometrische Anmeldungen hingegen basieren auf der Verwendung eines biometrischen Merkmals wie dem Fingerabdruck. Ein weiterer Anmeldungstyp ist die Netzwerkanmeldung, welche sich meist automatisieren lässt.



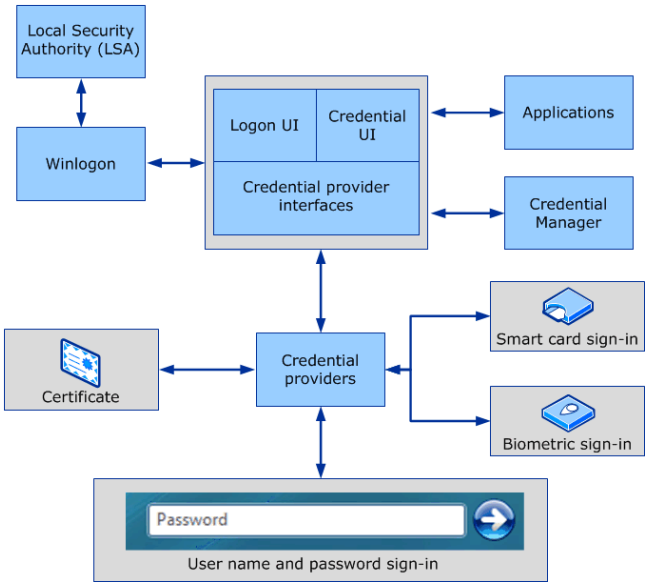
1.6.4.1 Interaktive Anmeldung

Die interaktive Anmeldung erfolgt als physischer Zugriff, falls die Anmeldung lokal durchgeführt wird. Bei einer remote Anmeldung erfolgt diese über den Remote Desktop Service (RDS), wobei das Remote Desktop Protocol (RDP) verwendet wird.

Der Benutzer wird für die interaktive Anmeldung in der lokalen Security Account Manager (SAM) Datenbank hinterlegt und ein Netzwerkzugriff ist nicht erforderlich. Für die eigentliche Anmeldung meldet ich der Benutzer mit seinem Benutzernamen und seinem Passwort an. Falls die Anmeldung erfolgreich war, erhält der Benutzer Zugriff auf lokale Ressourcen und geteilte Netzwerkressourcen. Die Anmeldung des Nutzers in der Domain wird probiert.

1.6.4.2 Anmeldung mit Smartcards

Die Anmeldung mithilfe von Smartcards erfordert den Kerberos Authentifizierungsdienst und kann nur mit dem Domainkonto erfolgen. Weiterhin werden das X.509 (PKCS) Zertifikat auf der Smartcard sowie ein Private/Public Key Paar auf der Smartcard benötigt. Der Security Chip der Smartcard speichert den Private Key, welcher durch den Smartcard Pin freigeschaltet wird. Der Private Key verlässt die Smartcard niemals. Weiterhin signiert die Smartcard verschiedenste Aktionen.



1.6.4.3 Biometrische Anmeldung

Für die biometrische Anmeldung werden biometrische Merkmale verwendet. Häufig nutzt man hierbei den Fingerabdruck, die Iris oder das Gesicht für die Authentifizierung. Bei der Anmeldung wird die aufgenommene Messung des biometrischen Merkmals mit einem bekannten hinterlegten Sample verglichen. Wenn diese hinreichend übereinstimmen, ist die Anmeldung erfolgreich. Wenn einzig eine biometrische Anmeldung erlaubt ist, wird eine Verbindung mit einem AD-Controller benötigt.

1.6.4.4 Netzwerkanmeldung

Die Verwendung der Netzwerkanmeldung ist erst nach einer erfolgreichen Anmeldung am System möglich. Dabei erfolgen eine Benutzer-, eine Dienst- und eine Computerauthentifizierung. Die Netzwerkanmeldung ist meist unsichtbar für den Benutzer, wobei die Anmeldung von Netzwerkdiensten und Prozessen während deren Nutzung geschieht.

Unterstützte Authentifizierungsmethoden sind:

- Kerberos
- Zertifikate mit öffentlichem Schlüssel (PKI)
- Basic Authentication über Secure Socket Layer / Transport Layer Security (SSL / TLS)
- Digest (Username-Hash und Challenge Response)
- NT LAN Manager (NTLM) (nur für Abwärtskompatibilität)

1.6.5 Zusammenfassung

Unter Windows gibt es 3 verschiedene Benutzerkontenarten (lokal, Domain, Windowsnetzwerk). Deren Speicherorte und Administration unterscheiden sich.

Gruppen werden zur vereinfachten Rechteverwaltung verwendet. Windows unterscheidet in 3 Gruppentypten (lokal, global, universell). Die übliche Gruppenverschachtelung ist: A-GG-LG-R oder A-GG-GG-UG-LG-R.

LDAP ist ein Protocol zum Austausch von Verzeichnisdienstinformationen. Active Directory ist Microsoft‘s Implementation von LDAP. Die meistgenutzten Alternativen sind Open Directory von Apple und Open LDAP aus der Linuxwelt.

Es gibt 4 Anmeldevarianten unter Windows. Diese sind: interaktiv, mit Smartcard, biometrisch und Netzwerkanmeldung.

1.7 Windows Sicherheit

1.7.1 Firewall

1.7.1.1 Wiederholung OSI-Modell

Beginnend soll noch einmal der Aufbau des OSI-Modells wiederholt werden. Das OSI-Modell setzt sich aus verschiedenen Schichten zusammen. Die oberste Schicht ist die Anwendungsschicht („Application Layer“), welche für den Informationsaustausch zwischen den Anwendungen verantwortlich ist. Weitere Aufgaben dieser Ebene sind die Teilnehmer Identifikation sowie die Teilnehmer Verifikation und die Durchführung von Sicherheitschecks.

Die darunter liegende Ebene ist die Darstellungsschicht („Presentation Layer“). Sie ist für die Aufbereitung der Daten für die Anwendungsebene verantwortlich, sodass ein einfacher Zugriff ermöglicht wird. Zudem wird hier die Datenformatierung, Kompression und die Übertragungsverschlüsselung realisiert.

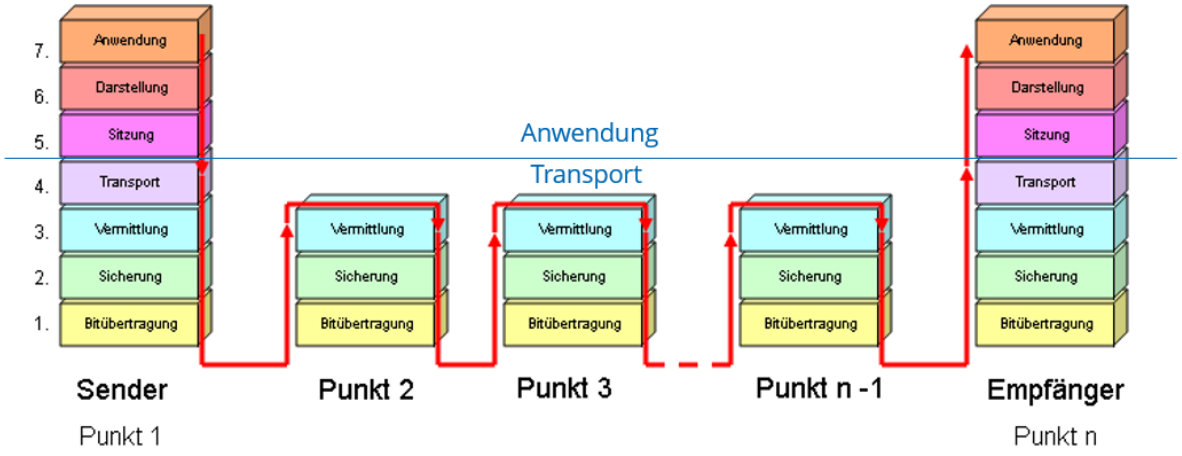
Unter der Darstellungsschicht liegt die Sitzungsebene („Session Layer“). Ihre Aufgaben sind die High-Level Synchronisation zwischen Anwendungen, aber auch die Regelung der Übertragungskommunikation. Damit wird zugeordnet, wer momentan spricht und wer zuhört.

Darauf folgt die Transportschicht („Transport Layer“). In der Transportschicht werden die Daten paketisiert. Außerdem werden ankommende Daten organisiert, sodass ihre richtige Reihenfolge wiederhergestellt ist. Zusätzlich stellt die Transportschicht einen rein logischen Datenstromzugang für die Sitzungsebene bereit.

Die Vermittlungsschicht („Network Layer“) übernimmt die Paketzustellung, sprich das Routing. Auch wird hier die Internetzwerkkommunikation sowie der logische Netzwerkaufbau realisiert.

Unter der Vermittlungsschicht liegt die Sicherungsschicht („Data-Link Layer“). Sie ist für die Datenübertragung innerhalb eines Netzwerks zuständig. Außerdem erreichen die Daten hier den nächsten Knoten auf der Route zum Zielrechner. Auch eine Kollisionserkennung bei der Datenübertragung wird in dieser Schicht durchgeführt.

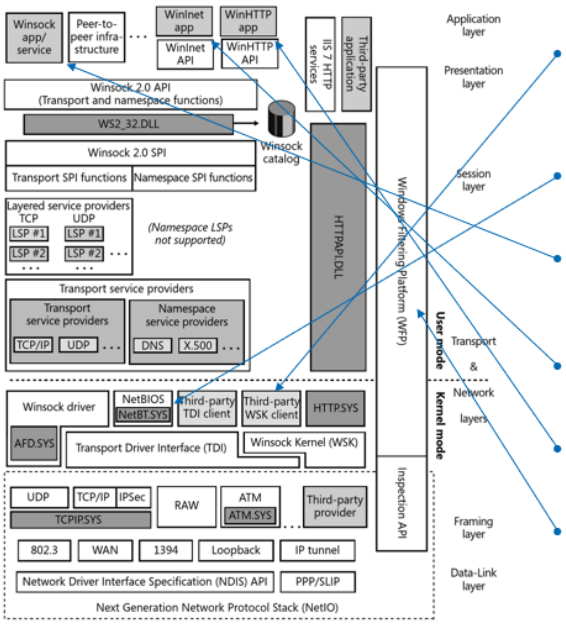
Die unterste Ebene ist die Bitübertragungsschicht („Physical Layer“). In dieser Schicht werden die Bits zum nächsten Kommunikationsgerät über ein bestimmtes Medium übertragen.



Für ein einfacheres Verständnis kann man die einzelnen Aufgaben der Schichten wie folgt ansehen:

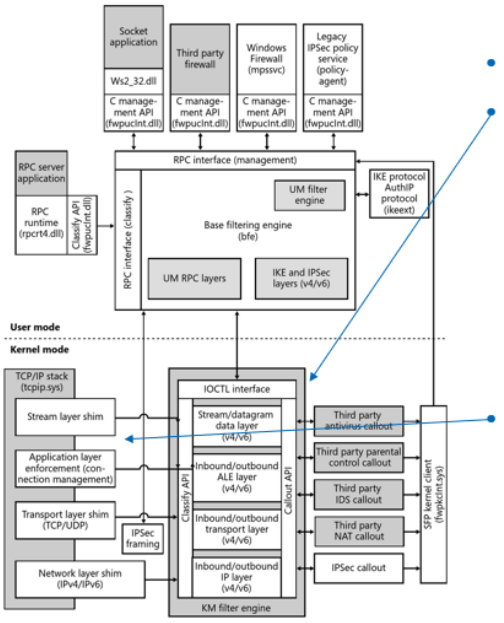
- Application Layer — Nachrichtentext
- Presentation Layer — Sprache, Formatierung von Text und Tabellen, …
- Session Layer — Brieflayout, Formulierungsgrad (formell, informell)
- Transport Layer — Brief in Umschlag verpacken, Frankierung
- Network Layer — Postanschrift
- Data-Link Layer — Verteilungszentrum ordnet Brief Transportmittel zu
- Physical Layer — Postboten, LKWs, Flugzeuge transportieren Brief

1.7.1.2 *Windows Netzwerkkomponenten*

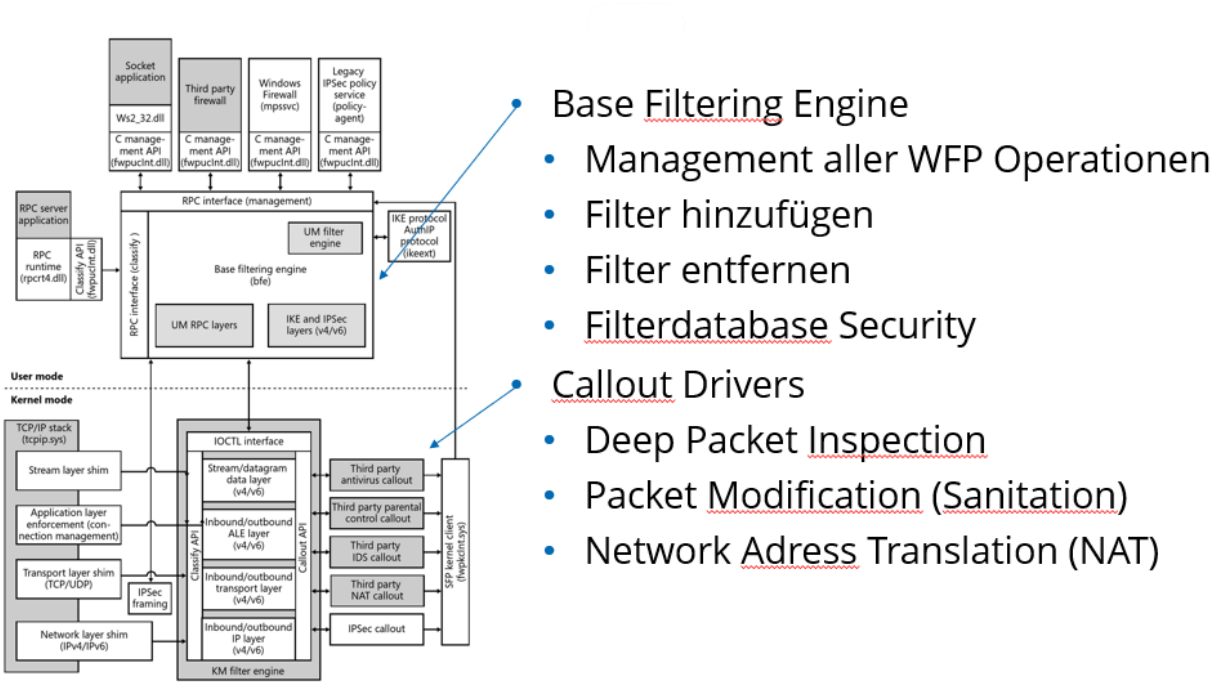


- Windows Sockets
  - Funktionsweise von BSD-Sockets
  - Portierung von BSD/UNIX-Anwendungen
- NetBIOS
  - legacy, Abwährtskompatibilität
- Winsock
  - Client und Server Sockets für Windows-Anwendungen
- WinInet
  - API für FTP und HTTP
- WinHTTP
  - API für HTTP
- Windows Filtering Platform
  - Regeln für Netzwerkverkehr / -zugang

1.7.1.3 *Windows Filtering Platform*



- Filterung auf allen Levels des Network-Stacks
- Filter-Engine
  - User-Mode
    - RPC und IPSec Filter
    - Anwendungsorientiert
  - Kernel-Mode
    - TCP/UDP und IP Filter
    - Transportorientiert
- Shims
  - Normalisierung der Daten für Filter
  - Abfrage an Filter-Engine
  - Aktionsdurchführung (drop, pass, reject)



1.7.1.4 Firewall Actions

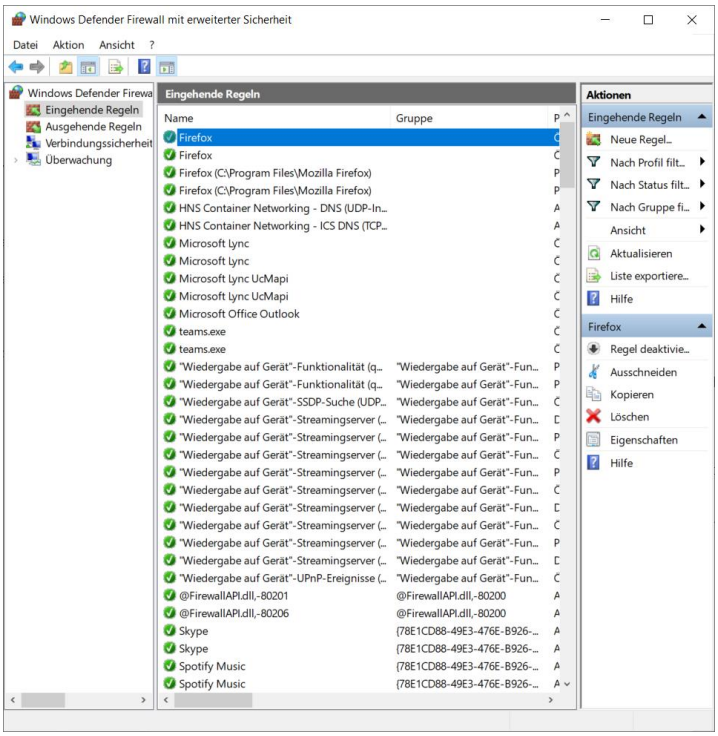
Es gibt verschiedene Aktionen einer Firewall. „Pass“ bedeutet, dass ein Paket normal weitergeleitet wird. „Block/Drop“ hingegen verursacht, dass ein Paket gelöscht wird. Weiterhin gibt es die Aktion „Reject“. Hierbei wird das Paket gelöscht und der Sender wird über das Löschen des Paketes informiert. Außerdem gibt es hier Debug-Informationen für den Netzwerkadministrator. Jedoch bekommt auch der Angreifer Informationen. Beispielsweise weiß er nun, dass eine Firewall vorhanden und aktiv ist. Zusätzlich kann er daraus schließen, dass eine Firewall Regel gegriffen hat und der Administrator eventuell informiert ist.

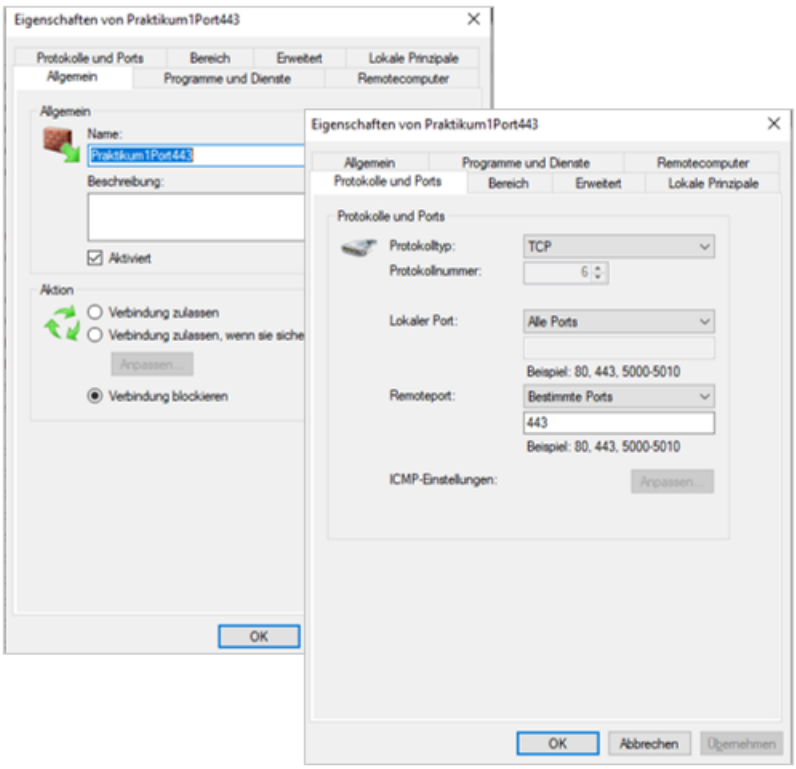
1.7.1.5 Filtermodus

Es gibt zwei verschiedene Filtermodi. Beim Whitelist Modus handelt es sich um eine Liste mit erlaubten Regeln. Alles was nicht auf dieser Liste steht, ist automatisch verboten. Dieser Modus bietet sich für ein sicheres Design an. Er ist anfangs aufwendig einzurichten, aber die Einrichtung wächst mit der Nutzung. Weiterhin ist Whitelisting resistent gegen vergessene Ausnahmen oder Spezialfälle. Ein Beispiel für Whitelisting wäre das Haustürschloss.

Bei dem Blacklist Modus handelt es sich um eine Liste mit verbotenen Regeln. Alles was nicht auf der Liste steht, ist erlaubt. Dieser Modus ist vor allem Anwenderfreundlich, da zunächst alles funktioniert. Die Einrichtung von Blacklisting wächst mit den vorhandenen Angriffswegen. Jedoch muss hier an alle Angriffswege gedacht werden. Ein Beispiel für den Blacklist Modus wären Gesetzestexte.

1.7.1.6 Windows Defender Firewall Regeln



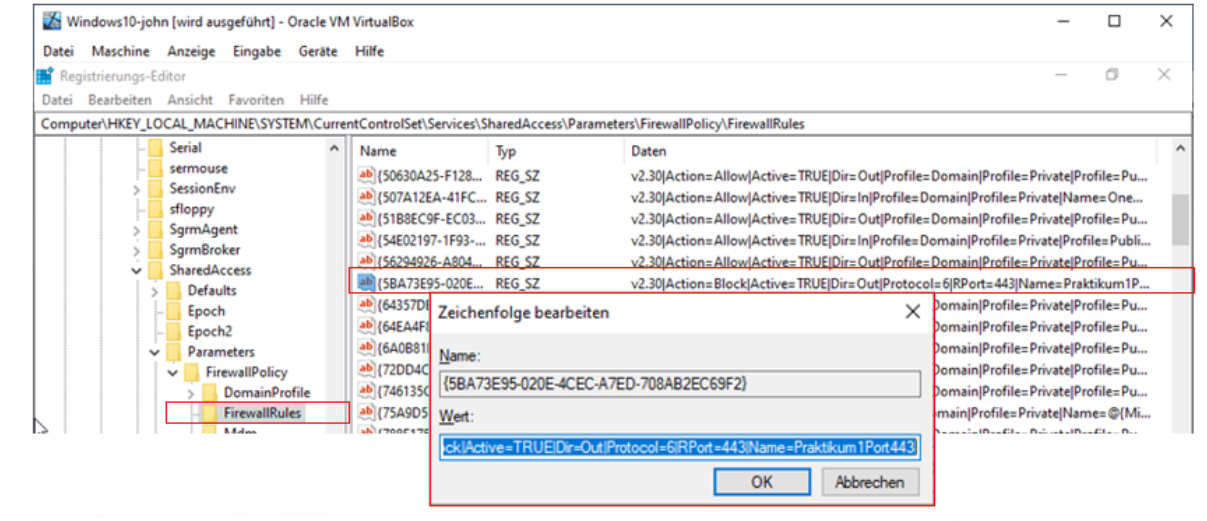


Die Firewall Regeln von Windows Defender basieren auf:

- Ports
  - Eingehend
  - Ausgehend

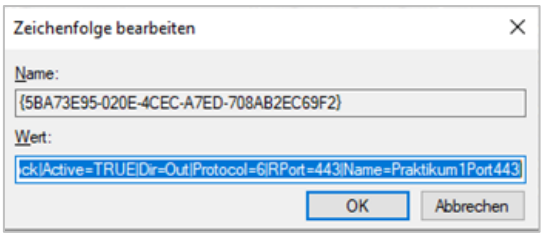
- IP-Adresse
    - Sender
    - Empfänger
- Transportprotokoll
    - TCP
    - UDP
- Richtung
    - eingehend
    - ausgehend
- Anwendung
- Netzwerkumgebung
    - privat (Heimnetzwerk)
    - öffentlich
- Domaine
- Benutzer

Die Firewall Regeln sind in der Registrierung abgelegt und befinden sich unter „HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules“.

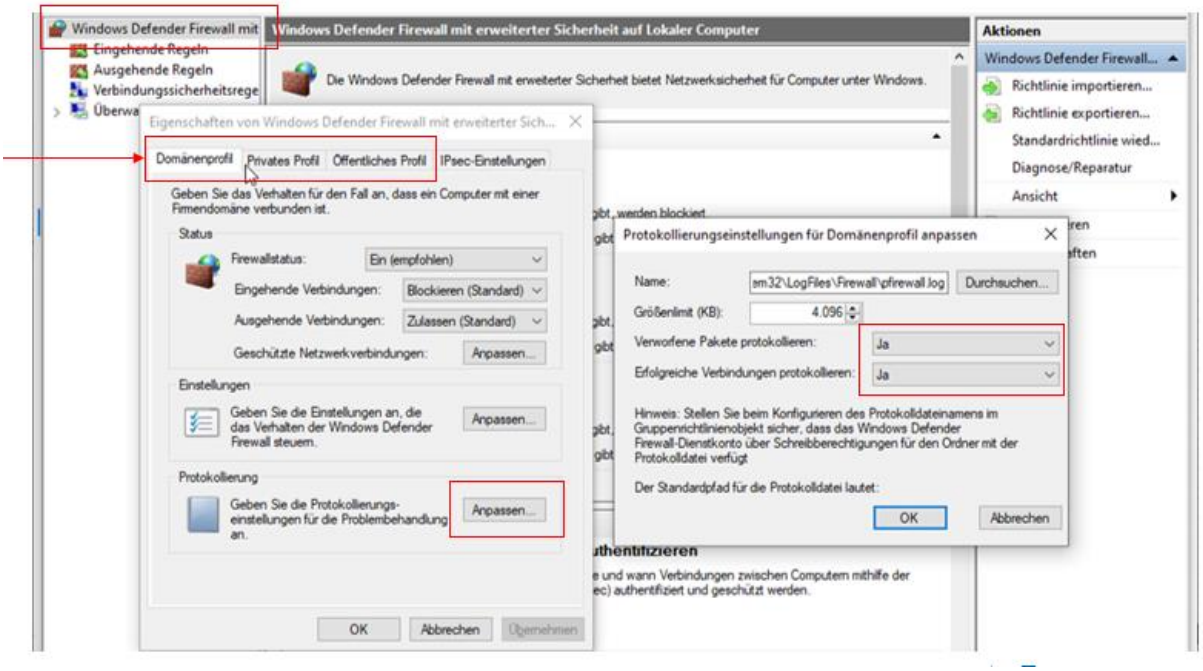


Im Folgenden werden Eintragungen für die Firewall Regeln in der Registrierung aufgelistet:

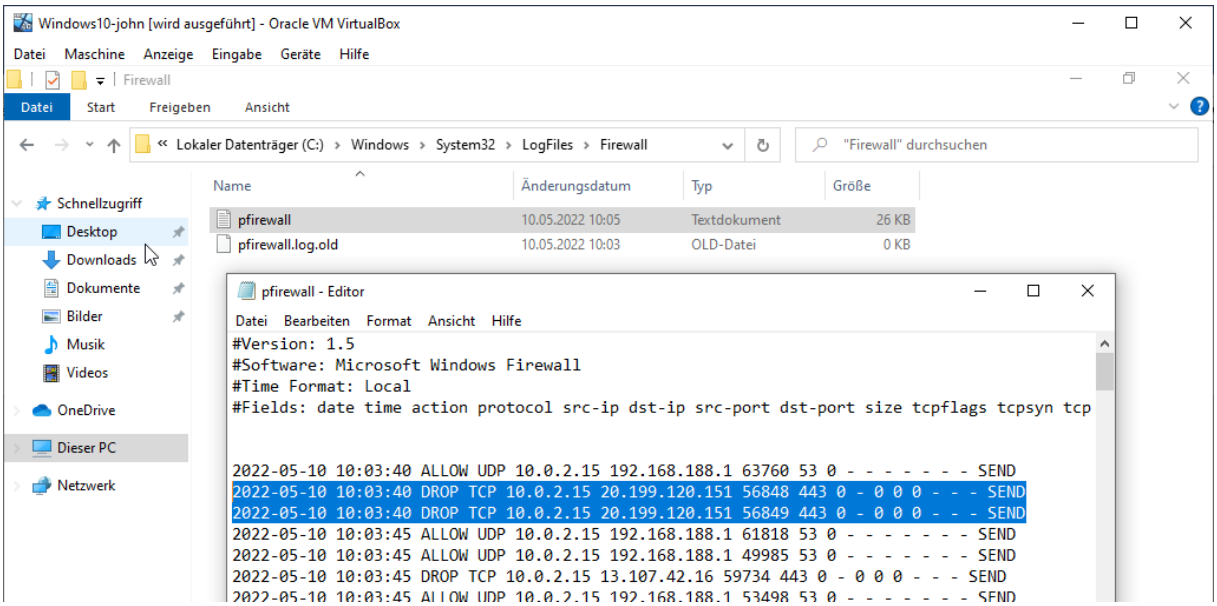
- Protocol:
    - 6 ist TCP
    - 17 ist UDP
    - 1 ist ICMP
- Lport: lokaler Port
- Rport: remote Port
- LA4 oder LA6: lokale IPv4 oder IPv6 Adresse
- RA4 oder RA6: remote IPv4 oder IPv6 Adresse
- App: Applikation für Regel-Match (application-specific rules unabhängig vom Port)
- Name: Regelname
- Profile: Firewall Profil für die Regel gilt (Domain, Private und Public)



Die Firewall Logfiles müssen erst im Standard aktiviert werden. Für alle drei Profile erfolgt hierbei eine separate Aktivierung:



Der Standardpfad ist „%systemroot%\system32\logfiles\firewall\pfirewall.log“:



1.7.2 Netzwerk Zonen

1.7.2.1 Zone Identifier

Mit Windows XP erfolgte die Einführung von SP2 als alternativer NTFS Datenstrom „Zone.Identifier“. Dieser ist NUR auf NTFS Dateisystemen vorhanden. Der Zone.Identifier wird von Webanwendungen generiert und wird angelegt, wenn der Benutzer Dateien aus einer anderen Sicherheitszone im lokalen System speichert.

Es gibt fünf am häufigsten vorkommende Zonen-IDs. 0 ist die lokale Computerzone, die vertrauenswürdigste Zone für Inhalte, die auf dem lokalen Computer vorhanden sind. Die Zone 1 ist die Lokale Intranetzone für Inhalte im Intranet einer Organisation. Zone 2 ist die Zone vertrauenswürdiger Sites für Inhalte auf Websites, die als seriöser oder vertrauenswürdiger gelten als andere Websites im Internet. Die dritte Zone ist die Internetzone für Websites im Internet, die keiner anderen Zone angehören. Schließlich gibt es noch Zone 4, bei welcher es sich um eine Zone für eingeschränkte Sites für Websites handelt, die möglicherweise unsicheren Inhalt enthalten.

Wichtige Registry Keys hierzu sind:

- NTUSER.dat – Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\
- (DisableThumbnailCache = 1)
- NTUSER.dat – Software\Policies\Microsoft\Windows\Explorer\
- (DisableThumbsDBOnNetworkFolders = 1)
- NTUSER.dat – Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\
- (DisableThumbnailCache = 1)
- HKEY Local Machine – Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\
- (DisableThumbnailCache = 1)
- HKEY Local Machine – SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\
- (DisableThumbnailCache = 1)

Im Folgenden werden einige Browser Beispiele für Downloads aufgelistet:

Google Chrome:

```
[ZoneTransfer]
ZoneId=3
ReferrerUrl=http://referringurl.com/
HostUrl=http://referringurl.com/wpcontent/uploads/LOGO_NEW.png
```

Firefox:

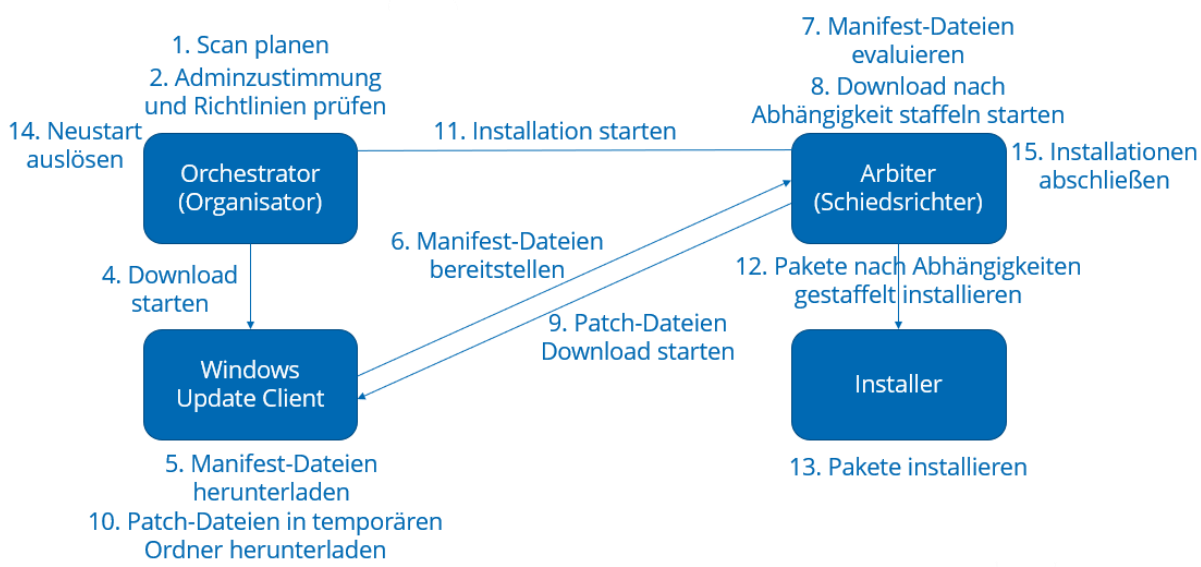
```
[ZoneTransfer]
ZoneId=3
```

Microsoft Edge:

```
[ZoneTransfer]
LastWriterPackageFamilyName=Microsoft.MicrosoftEdge_8wekyb3d8bbwe
ZoneId=3
```

1.7.3 Updates

1.7.3.1 Windows Updateablauf



1.7.3.2 Windows Update-Typen

Bei Windows gibt es verschiedene Update-Typen. Das Feature Update ist ein halbjähriger Release. Dabei werden neue Funktionen im Betriebssystem zur Verfügung gestellt. Cummulative Updates werden alle zwei Wochen durchgeführt. Sie sind für die Fehlerbehebung sowie für Performance- und Sicherheitsupdates verantwortlich. Weiterhin gibt es das Security Update, welches für Sicherheitsupdates zuständig ist. Dieses wird monatlich immer am zweiten Donnerstag des Monats durchgeführt. Bei sehr kritischen Schwachstellen kann das Security Update auch außerplanmäßig durchgeführt werden. Ein weiterer Update-Typ ist das Servicing Stack Update (SSU). Hiermit werden Fehlerpatches für Spezialfälle sowie die Vorbereitung für den eigentlichen Patch behandelt. Das Compartibility and Reliability Update ist für die Kompatibilitätsvorbereitung für Installationen verantwortlich. Weiterhin gibt es das Microcode Update. Hier werden sowohl Patches für CPU-Schwachstellen als auch Patches für Hardwareprobleme durch Microcode geliefert. Der letzte Update-Typ ist das Intelligence Update for Defender Antivirus. Dabei erfolgt ein Update der Liste mit schädlichen Programmen. Außerdem werden die Kennungen von Schadsoftware aktualisiert.

1.7.4 Schutzmechanismen

1.7.4.1 AAA-System

Be dem AAA-System geht es um Authentication (Authentifikation), Authorization (Autorisierung) und Accounting (Protokollierung). Bei der Authentifikation geht es um die Frage „Wer bist du?“. Dabei erfolgt zum einen die Identifizierung („Du bist also Barack Obama?“) und zum anderen der Nachweis des Rechteanfragenden („Beweise mir, dass du Barack Obama bist“).

Die Autorisierung legt fest, was man darf („Das darfst du“). Sie legt fest, worauf zugegriffen werden darf und gewährt diesen Zugriff („Du darfst: drucken, die Datei X öffnen, …“).

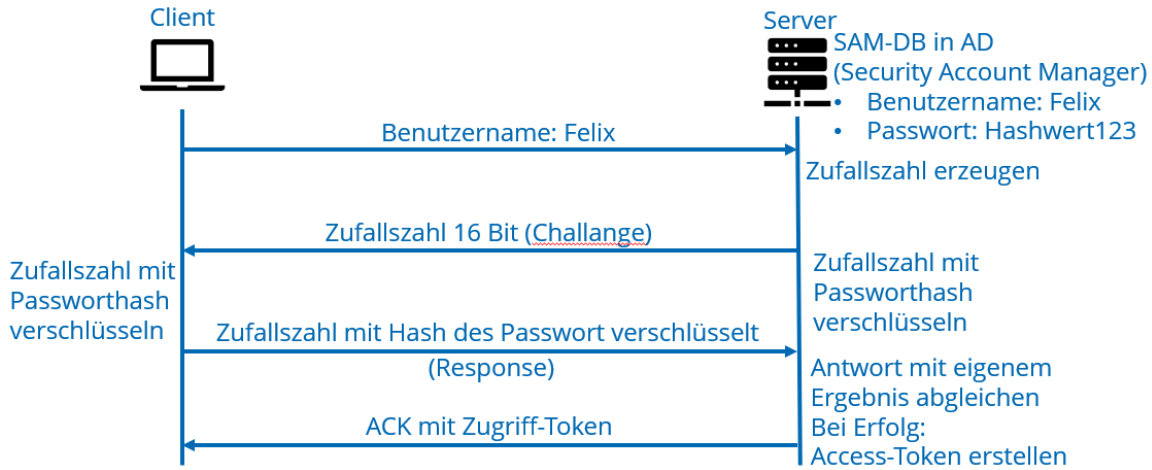
Bei der Protokollierung wird alles dokumentiert („Das wird in den Akten hinterlegt“). Insbesondere werden Zugriffe protokolliert, wobei dokumentiert wird, auf was, wann und wie lang darauf zugegriffen wurde („Person X hat Datei Y um 15:05 Uhr geöffnet“).

1.7.4.2 Authentifizierung unter Windows

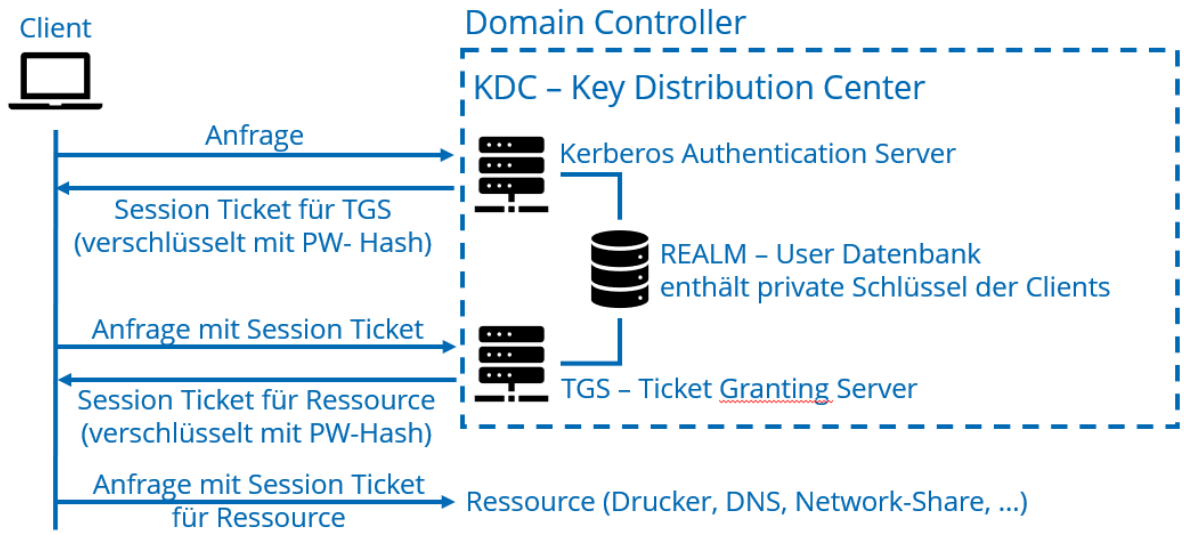
Für die Authentifizierung unter Windows gibt es als privates Geheimnis ein Passwort oder einen PIN, falls das biometrische Merkmal nicht korrekt erkannt wurde. Für die Authentifizierung mithilfe eines biometrischen Merkmals kann entweder eine Gesichts- oder eine Fingerabdruckserkennung eingesetzt werden. Weiterhin ist eine Authentifizierung über ein Besitzeigentum möglich, in diesem Fall eine Keycard.

Für die Authentifizierung unter Windows kann der NT LAN Manager (NTLM) verwendet werden, wobei ein Challenge Response Verfahren angewendet wird. Eine weitere Möglichkeit ist der Authentifizierungsdienst Kerberos, wobei ein gemeinsames Geheimnis für die Authentifizierung genutzt wird.

NT LAN Manager (NTLM)



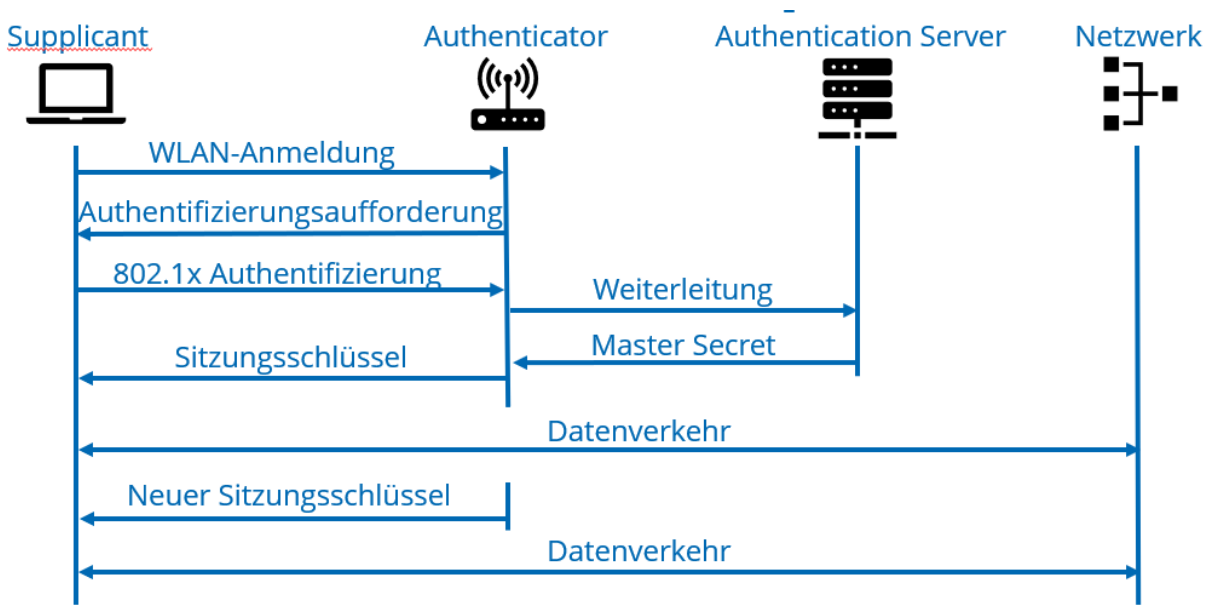
Kerberos



1.7.4.3 EAP und RADIUS

EAP steht für das Extensible Authentication Protocol, welches im Standard IEEE 802.1x definiert ist. Dieses Protokoll ist in der Data-Link-Layer (OSI-Schicht 2) angesiedelt. Die Ziele sind zum einen den Zugang zum Netzwerk nur mit einer durchgeführten Authentifizierung zu gewähren und zum anderen die Protokollierung der Netzwerknutzung. Die Bestandteile sind der Supplicant (Client), der Authenticator (Netzwerkschnittstelle) und der Authentication Server, wobei es sich meistens um einen RADIUS-Server handelt.

EAP und RADIUS (Beispiel WLAN)



1.7.4.4 Windows Passwörter

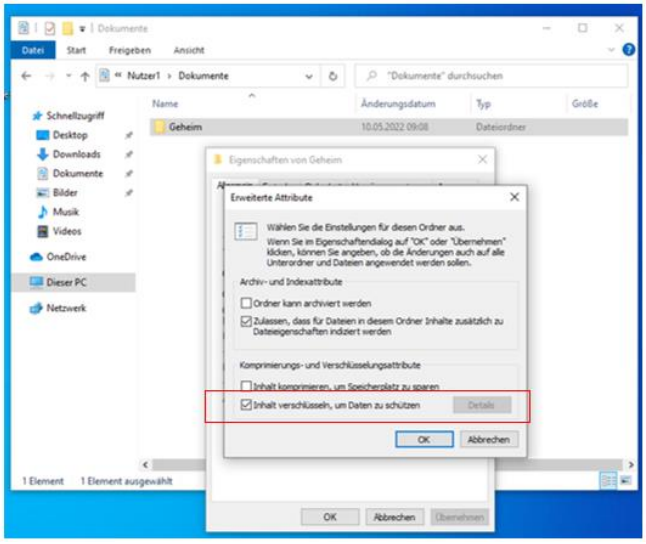
Passwörter unter Windows können aus maximal 127 Zeichen bestehen, wobei die Zeichen aus dem Unicode-Zeichensatz stammen. Sie werden als Hash, jedoch immer ohne Salt, gespeichert. Die Lan Manager-One-Way-Function (LM OWF) bietet eine Abwärtskompatibilität. Hier werden nur die ersten 14 Bytes des Passwortes verwendet und es gibt keine Casae-Sensitivität. Im Gegensatz dazu wird eher die NT One-Way-Funktion (NT OWF) empfohlen, da sie sicherer ist. Hierbei wird ein MD4-Hash angewendet.

1.7.4.5 Windows Passwort umgehen

Um das Passwort bei Windows zu umgehen, kann der PC mit einem Linux-Live-Stick gestartet werden. Die Festplatte wird anschließend unter Linux eingebunden und ein Backup von /Windows/System32/Utilman.exe erstellt. Die Datei /Windows/System32/Ultiman.exe wird dann durch /Windows/System32/cmd.exe überschrieben. Nun wird der PC neu gestartet. Über die erleichterte Bedienung wird CMD mit Systemrechten geöffnet („Uhr“-Symbol in der rechten unteren Ecke). Jetzt gibt man den Befehl „net user USERNAME NEUES_PASSWORT“ ein und kann sich danach mit dem neuen Passwort anmelden.

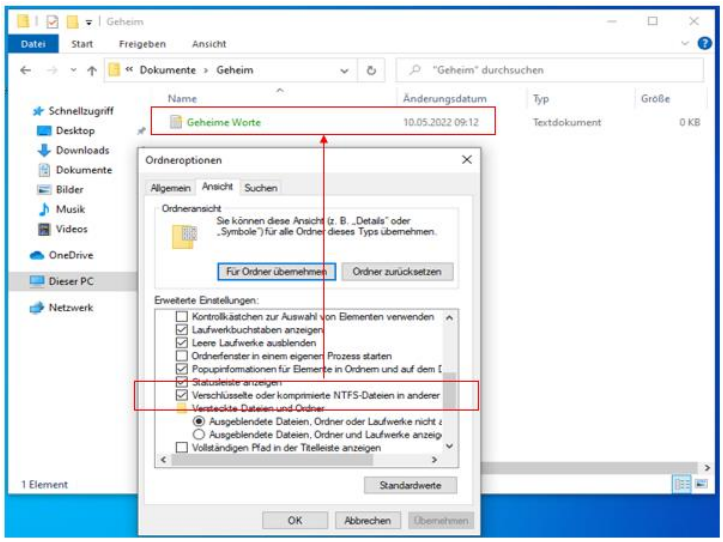
1.7.5 EFS Verschlüsselung

Das Encrypting File System (EFS) kennzeichnet ein System der Dateiverschlüsselung auf NTFS-Datenträgern. Dabei werden die Verschlüsselungsschlüssel an den Benutzer-Account gebunden.



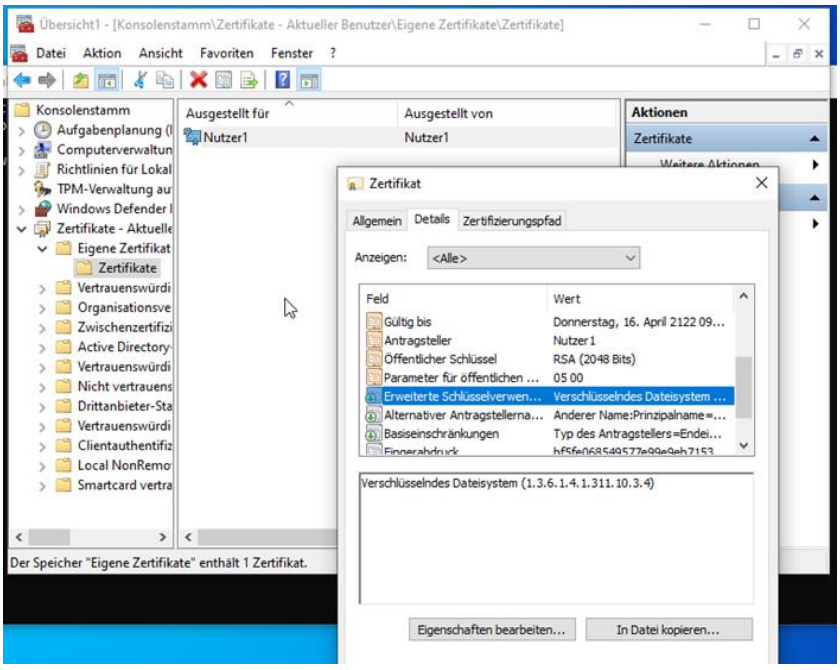
Um eine Datei per EFS zu verschlüsseln, generiert Das System einen zufälligen File Encryption Key (FEK). Die Datei wird anschließend mit dem FEK mittels AES chiffriert. Der FEK wird dann noch mit dem asymmetrischen RSA-Algorithmus unter Benutzung des öffentlichen Schlüssels des Benutzers (SAM) verschlüsselt. Zuletzt wird der RSA-FEK mit der Datei zusammen abgespeichert. Um die Datei zu lesen, muss der FEK mit dem geheimen Schlüssel des Benutzers entschlüsselt werden. Anschließend kann damit der Klartext der verschlüsselten Datei wiederhergestellt werden.

Um EFS verschlüsselte Daten während einer forensischen Untersuchung zu finden, wählt man „Ansicht > Optionen“, dann nutzt man das Register „Ansicht“ und markiert „Verschlüsselte oder komprimierte NTFS-Dateien in anderer Farbe anzeigen“.



Um die EFS verschlüsselten Daten in einer forensischen Untersuchung einzusehen, muss man sich mit der Benutzerkennung am Rechner mit den verschlüsselten Daten anmelden. Dies bedingt, dass man das Passwort des Benutzers kennt. Ist das Passwort unbekannt, muss es zuerst geknackt werden. Hat na sich erfolgreich angemeldet, kann man den EFS Schlüssel vom Benutzer als Zertifikat exportieren und an der forensischen Untersuchungsmaschine importieren. Nun kann man die EFS verschlüsselten Dateien öffnen.

Zertifikat mit dem EFS Schlüssel exportieren:



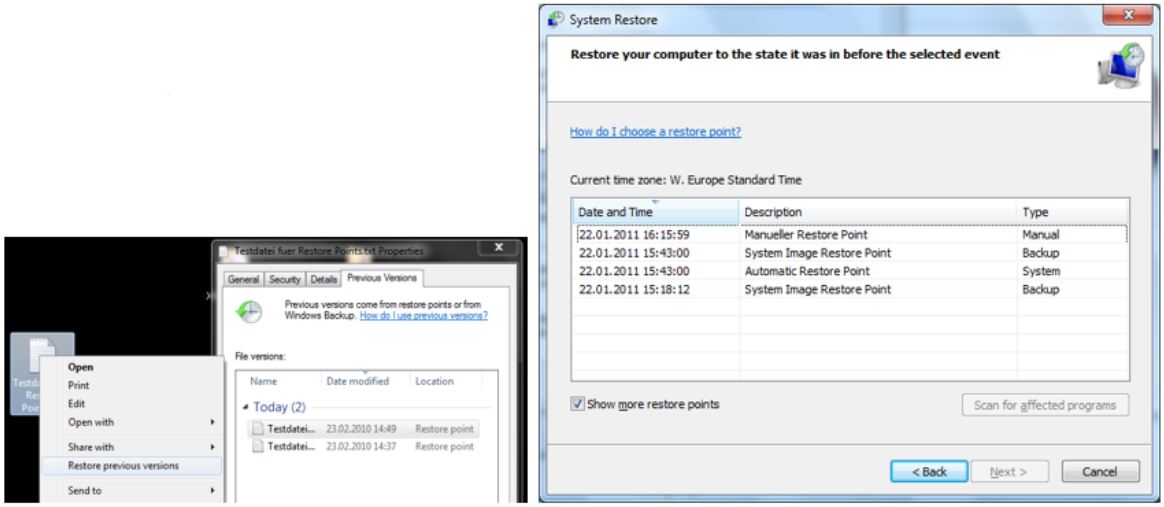
Wichtig: Die Nutzung von Boot CD zum zurücksetzen des PW des Benutzers funktioniert in einem solchen Fall nicht, da beim Löschen der Benutzerkennwörter auch die Möglichkeit der Dechiffrierung der EFS Dateien verloren geht, da der FEK mit dem Passwort des Benutzers verschlüsselt wird.

Wahlweise kann man auch eine Virtualisierung des Asservates in Erwägung ziehen und die EFS verschlüsselten Daten nach Anmeldung am System mit der entsprechenden Benutzerkennung exportieren und damit für eine Untersuchung erlangen.

1.7.6 VSS – Volume Shadow Copy Service

Seit Windows 2003 gibt es den sogenannten „Volume Shadow Copy Service“ (VSS). Dies ist ein Hintergrunddienst, der mehrere Versionen von Dateien vorhält. Seit Windows 7 ist er standardmäßig aktiviert. Die gesicherten Daten werden im Verzeichnis „System Volume Information“ abgelegt. Diese Schattenkopien ersetzen die „RestorePoints“-Funktionalität aus Windows-Versionen vor Vista. Weiterhin dienen Schattenkopien als einheitliche Datenquelle für zwei Funktionen. Zum einen dienen sie als RestorePoints, sprich Wiederherstellungspunkte, und zum anderen dienen sie als PreviousVersions, sprich vorherige Versionen.

Die gespeicherten vorherigen Versionen von Dateien können an eine beliebige Stelle kopiert werden („copy“) oder wiederhergestellt werden, womit sie die aktuelle Fassung ersetzen („Restore“).

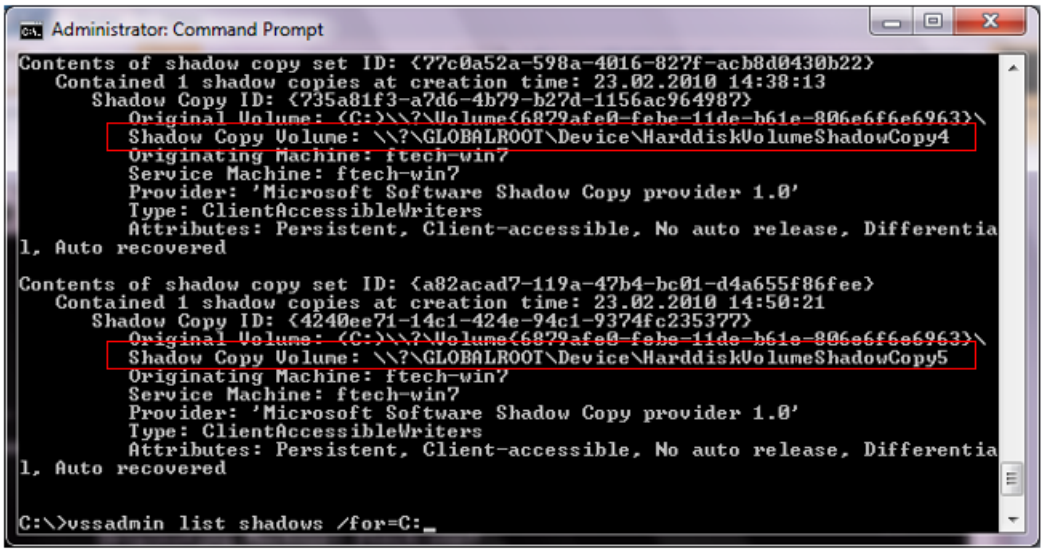


Unter Windows 7 und höher werden zu mehreren Ereignissen Schattenkopien erstellt. Sie können manuell erstellt werden, alle sieben Tage automatisch, vor einem Windows-Update oder der Installation eines unsignierten Treibers oder bei einer Anwendung, die eine Sicherung über die Windows-API anfordert. Die Daten aus den Schattenkopien werden standardmäßig entfernt, wenn mehr als 5% des Speichers bei einer Partition, welche größer als 64GB ist, oder mehr als 3% des Speichers bei einer Partition, die kleiner als 64GB ist, belegt sind.

Schattenkopien bleiben erhalten, selbst wenn die zugehörigen Quelldateien gelöscht, gewiped oder verschlüsselt werden. Weiterhin können frühere Versionen von Dateien aus Schattenkopien wiederhergestellt werden. Daher sind Schattenkopien ein wichtiges Element im Rahmen der Analyse gelöschter Dateien.

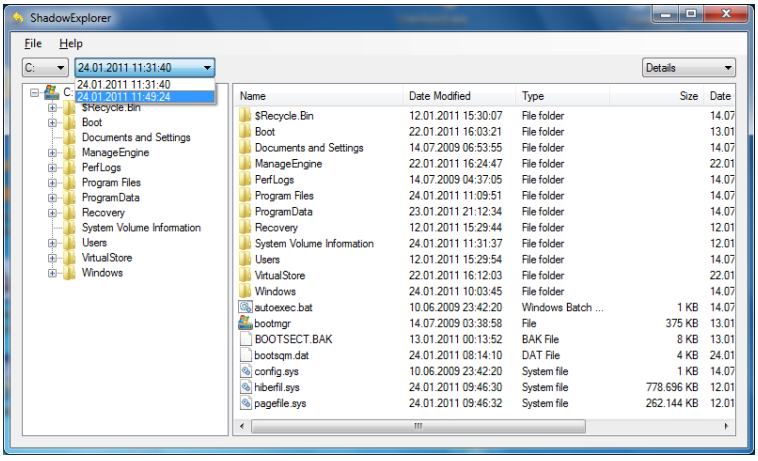
Wichtig für das Verständnis der Funktionsweise ist das sog. „Copy-on-Write“-Konzept: Änderungen in eine Schattenkopie werden nur dann geschrieben, wenn die Originaldatei geändert wurde. Daher funktioniert die Erstellung eines kompletten RestorePoints auch so schnell! Es wird pro Schattenkopie nur die jeweils letzte Änderung an einer Datei gespeichert. Als Konsequenz daraus wird also nicht jede Änderung gesichert, sondern nur falls zwischenzeitlich eine neue Schattenkopie angelegt wurde.

In der Kommandozeile kann mit vssadmin list shadows /for=C: die Schattenkopien von Laufwerk C:\ aufgelistet werden. Hierbei kann der Shadow Copy Volume Identifier herausgelesen werden.



Anhand des Shadow Copy Volume Identifiers kann auf eine Schattenkopie live zugegriffen werden: „mklink/d c:\vss-test \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4\“. Der Befehl erstellt einen Link auf die Schattenkopie.In „c:\vss-test“ befindet sich dann die Ordneransicht zum Zeitpunkt der Erstellung der Schattenkopie.

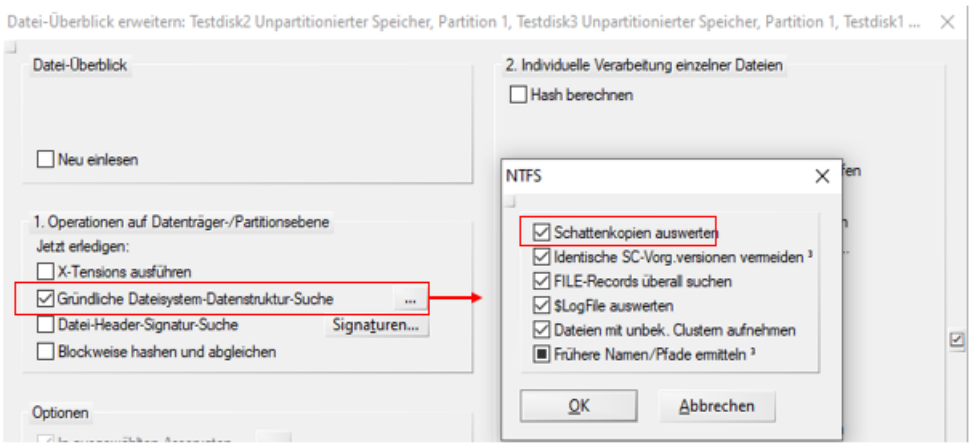
Alternativ kann hierzu auch das kostenfreie Tool „ShadowExplorer“ genutzt werden:



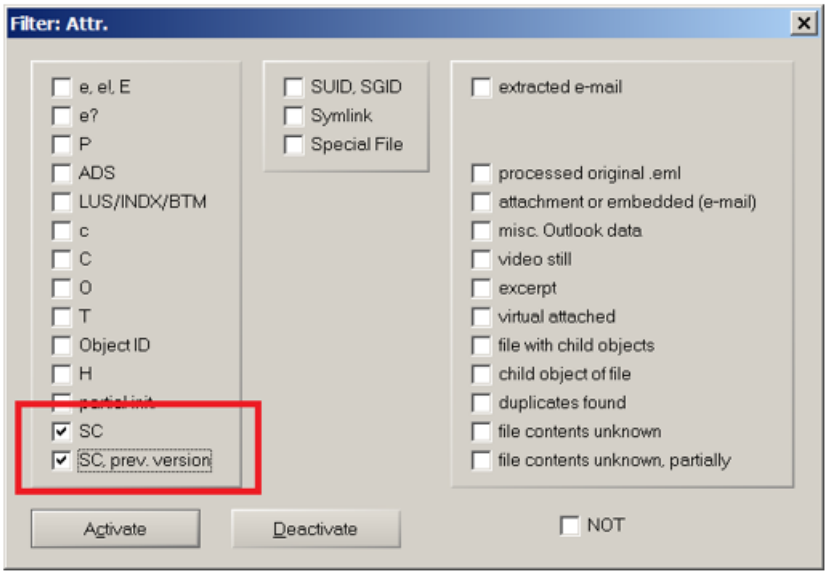
Der Shadow Copy Volume Identifier kann auch als Quelle für eine Image-Erstellung genutzt werden: „dd if=\\.\HarddiskVolumeShadowCopy4 of=d:\shadowrawkopie4.dd –localwrt“. Hierbei wird ein Image auf dem Laufwerk D:\ des Rechners in der Datei shadowrawkopie4.dd erstellt. Das Image stellt die Sicht auf den Datenträger zum Zeitpunkt der Erstellung der Schattenkopie dar. Dieses Image kann dann als logischer Datenträger in Forensik-Tools importiert und näher analysiert werden.

Das Image einer Shadow Copy hat dieselbe Größe wie die Quellpartition. Durch die potentiell hohe Anzahl von Shadow Copies ergeben sich damit sehr große Datenmengen, die auszuwerten sind. Gegebenenfalls sind hier Einschränkungen auf Basis des vermuteten Tatzeitraumes möglich. Außerdem können durch die Bildung von Hashsets und einem entsprechenden Abgleich die bereits aus anderen Schattenkopien bekannten Dateiversionen ausgeblendet werden.

X-Ways kann dazu verwendet werden, die Volumenschattenkopien zu untersuchen. Unter dem Punkt „Spezialist“, kann man „Dateiüberblick erweitern“ wählen. Dort wählt man die Option „gründliche Dateisystem-Datenstruktur-Suche“ aktivieren. Die Aufbereitung von Schattenkopien kann zusätzlich zu anderen Optionen wie der Aufbereitung von MFT-Record-Datensätzen, INDEX-Puffern und $LogFiles durchgeführt werden.



Weiterhin kann man im Verzeichnisbrowser Dateien auflisten, die aus „Schattenkopien“ extrahiert wurden. Mithilfe der Attributspalte filtert man nach „SC“ (Dateien in Volumenschattenkopien) und „SC vorherige Version“ (frühere Version von „SC“). Solche früheren Versionen von „SC“ bezeichnen Dateien, die dem Volume-Snapshot bereits vor der Dateisystemdatenstruktur-Suche bekannt waren.



Kombiniert man dies mit anderen Filteroptionen (wie Typ oder Datum), erhält man so konkrete geänderte Dateien zu entsprechenden Zeitstempeln. Z. B.: "Zeige mir alle Dateien einer Schattenkopie an, bei denen es sich um eine Bilddatei mit einem Änderungsdatum zwischen Datum X und Y handelt."

1.7.7 Zusammenfassung

Das OSI-Modell strukturiert die Netzwerkkommunikation in verschiedene Ebenen mit entsprechenden Aufgabengebieten. Windows implementiert diese Ebenen in ihren Windows-Networkstack. Dieses ist auf Grund von Abwährtskompatibilität sehr komplex.

Zugriffsüberwachung übernimmt unter Windows die Windows Filtering Plattform. Diese integriert die Windows Firewall und die Antivirussoftware Windows Defender.

Der Windows Updateprozess teilt sich in Orchestrator, Windows Update Client, Arbiter und Installer auf.

Das AAA-Konzept gliedert sich in Authentification, Authorization und Accounting auf. Hierzu wurden verschiedene Authentifizierungsverfahren detaillierter betrachtet

1.8 Windows Netzwerke

1.8.1 OSI-Modell

Beginnend soll noch einmal der Aufbau des OSI-Modells wiederholt werden. Das OSI-Modell setzt sich aus verschiedenen Schichten zusammen. Die oberste Schicht ist die Anwendungsschicht („Application Layer“), welche für den Informationsaustausch zwischen den Anwendungen verantwortlich ist. Weitere Aufgaben dieser Ebene sind die Teilnehmer Identifikation sowie die Teilnehmer Verifikation und die Durchführung von Sicherheitschecks.

Die darunter liegende Ebene ist die Darstellungsschicht („Presentation Layer“). Sie ist für die Aufbereitung der Daten für die Anwendungsebene verantwortlich, sodass ein einfacher Zugriff ermöglicht wird. Zudem wird hier die Datenformatierung, Kompression und die Übertragungsverschlüsselung realisiert.

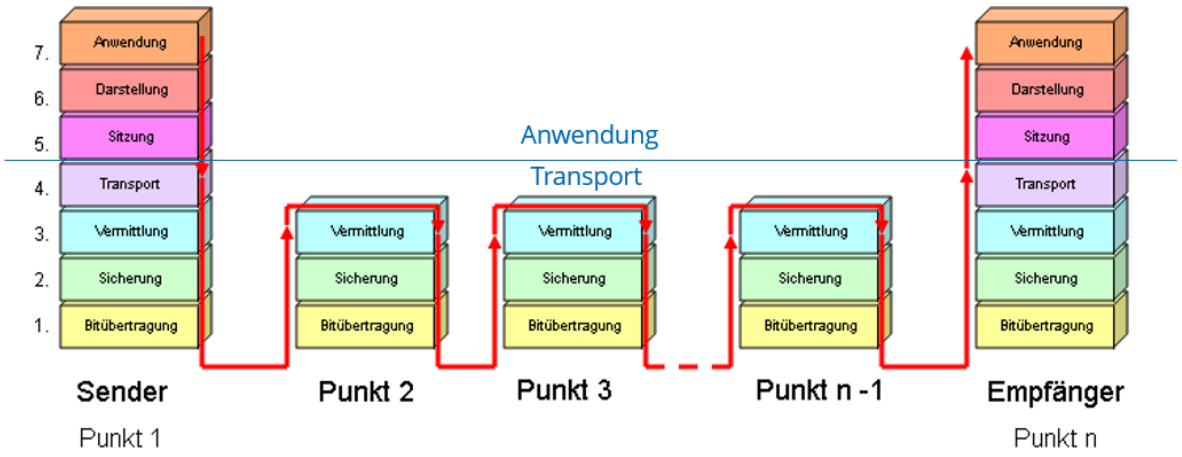
Unter der Darstellungsschicht liegt die Sitzungsebene („Session Layer“). Ihre Aufgaben sind die High-Level Synchronisation zwischen Anwendungen, aber auch die Regelung der Übertragungskommunikation. Damit wird zugeordnet, wer momentan spricht und wer zuhört.

Darauf folgt die Transportschicht („Transport Layer“). In der Transportschicht werden die Daten paketisiert. Außerdem werden ankommende Daten organisiert, sodass ihre richtige Reihenfolge wiederhergestellt ist. Zusätzlich stellt die Transportschicht einen rein logischen Datenstromzugang für die Sitzungsebene bereit.

Die Vermittlungsschicht („Network Layer“) übernimmt die Paketzustellung, sprich das Routing. Auch wird hier die Internetzwerkkommunikation sowie der logische Netzwerkaufbau realisiert.

Unter der Vermittlungsschicht liegt die Sicherungsschicht („Data-Link Layer“). Sie ist für die Datenübertragung innerhalb eines Netzwerks zuständig. Außerdem erreichen die Daten hier den nächsten Knoten auf der Route zum Zielrechner. Auch eine Kollisionserkennung bei der Datenübertragung wird in dieser Schicht durchgeführt.

Die unterste Ebene ist die Bitübertragungsschicht („Physical Layer“). In dieser Schicht werden die Bits zum nächsten Kommunikationsgerät über ein bestimmtes Medium übertragen.



1.8.2 Netzwerke unter Windows

1.8.2.1 Übersicht – Wichtige Begrifflichkeiten

Heimnetzgruppen

Das Ziel von Heimnetzgruppen ist es, eigene Ressourcen in einer Netzwerkgruppe teilen zu können. Hiermit ist eine dezentrale Verwaltung von Ressourcen wie Dateien (Bilder, Musik, ..) oder Druckern möglich. Heimnetzgruppen sind nur für Windows 7, 8 und 8.1 anwendbar, wobei auch ein Passwortschutz der Gruppe möglich ist. Nur Bestimmte können zu einer bestehenden Gruppe beitreten. Dies ist nur für Windows 7 Starter, Windows 7 Home Basic und Windows RT 8.1 möglich. In Windows 10 ersetzt die Share-Funktion die Heimnetzgruppe.

Netzwerkprofile

Bei dem Netzwerkprofil kann man zwischen öffentlich und privat auswählen. Das öffentliche Netzwerkprofil ist für öffentliche Netze wie beispielsweise das Hotel WLAN gedacht. Bei dieser Einstellung ist man im Netzwerk nicht sichtbar (Explorer-Auflistung unter Netzwerk). Weiterhin sind die Dateifreigabe und Drucker gesperrt.

Das private Netzwerkprofil hingegen ist für private Netze wie das Heimnetzwerk gedacht. Hiermit ist man im Netzwerk sichtbar, sprich man wird in der Explorer-Auflistung unter Netzwerk geführt. Zudem sind die Dateifreigabe (Einstellung bei Datei oder Ordner) und Drucker (Einstellung bei Drucker) erlaubt.

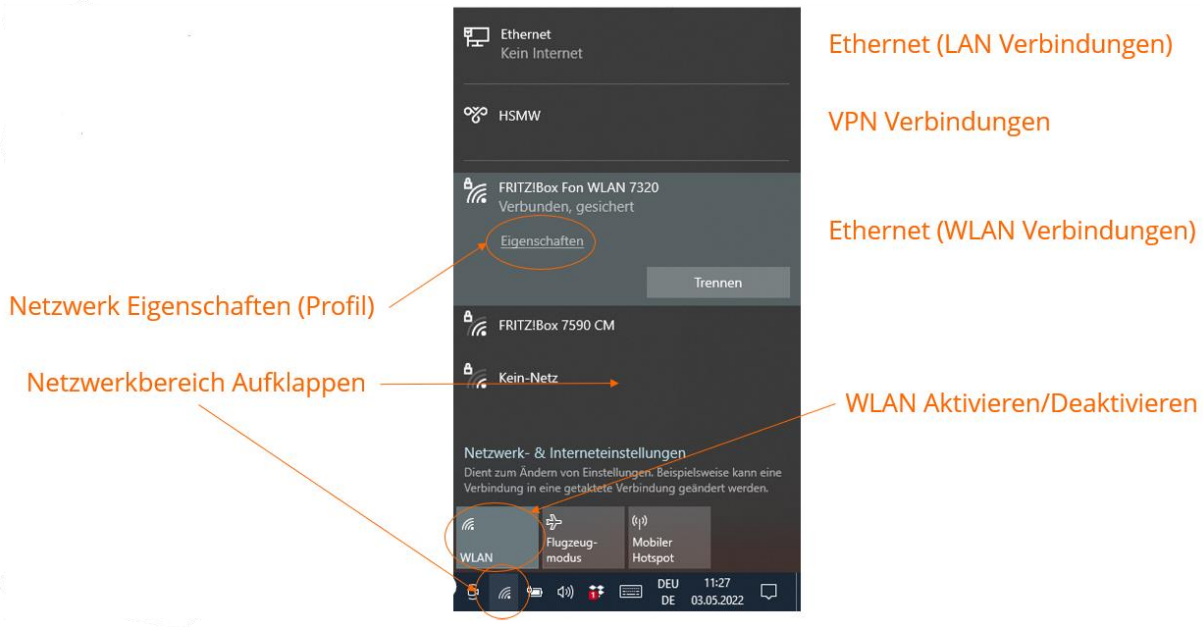
Aktuellen Status auslesen

Um den aktuellen Status auslesen zu können gibt es verschiedene Möglichkeiten für die Informationsgewinnung. Man kann hierfür die graphische Oberfläche nutzen, mit CMD-Befehlen oder aber auch mit PowerShell-Befehlen arbeiten.

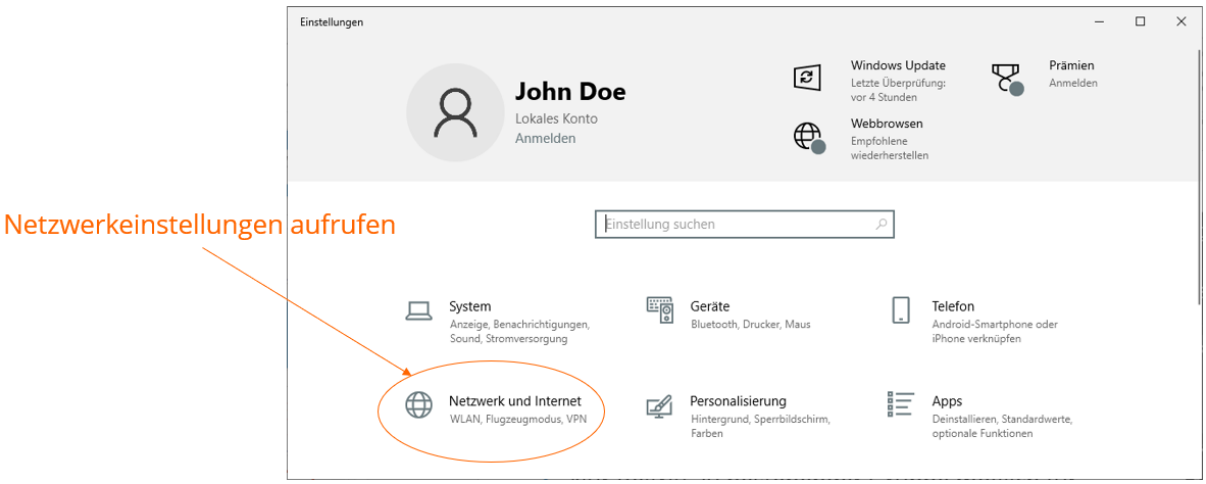
1.8.2.2 Graphische Oberfläche

Windows Netzwerk Übersicht

Um Netzwerke in Windows aufzurufen, wählt man in der Taskleiste das Netzwerk-Symbol.

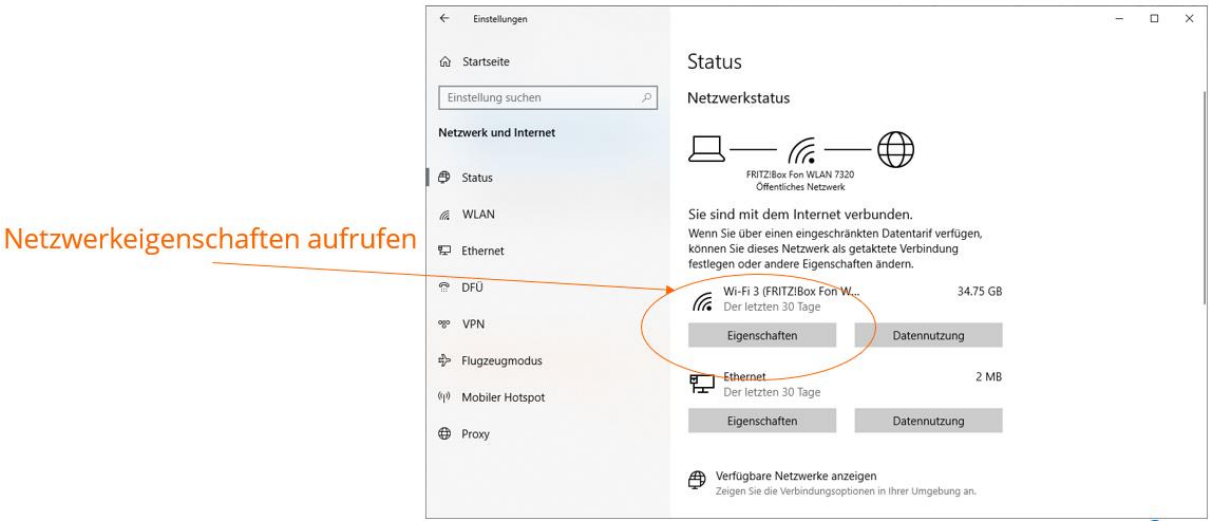


Um Netzwerke in Windows einzurichten, wählt man mit der rechten Maustaste den Startbutton und wählt im sich öffnenden Menü den Punkt „Einstellungen“.



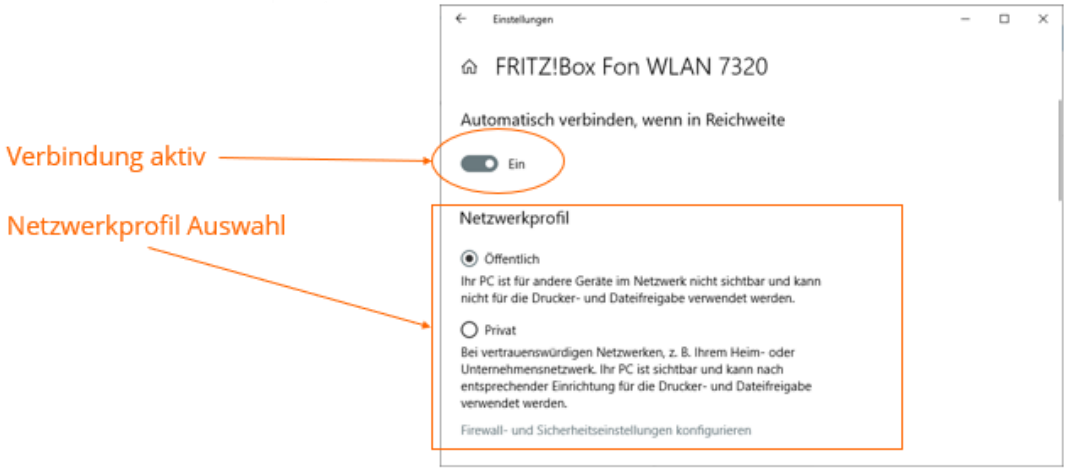
Netzwerkeinstellungen

In den Netzwerkeinstellung erfolgt eine Auflistung des Netzwerkstatus, sprich der Verbindungen.



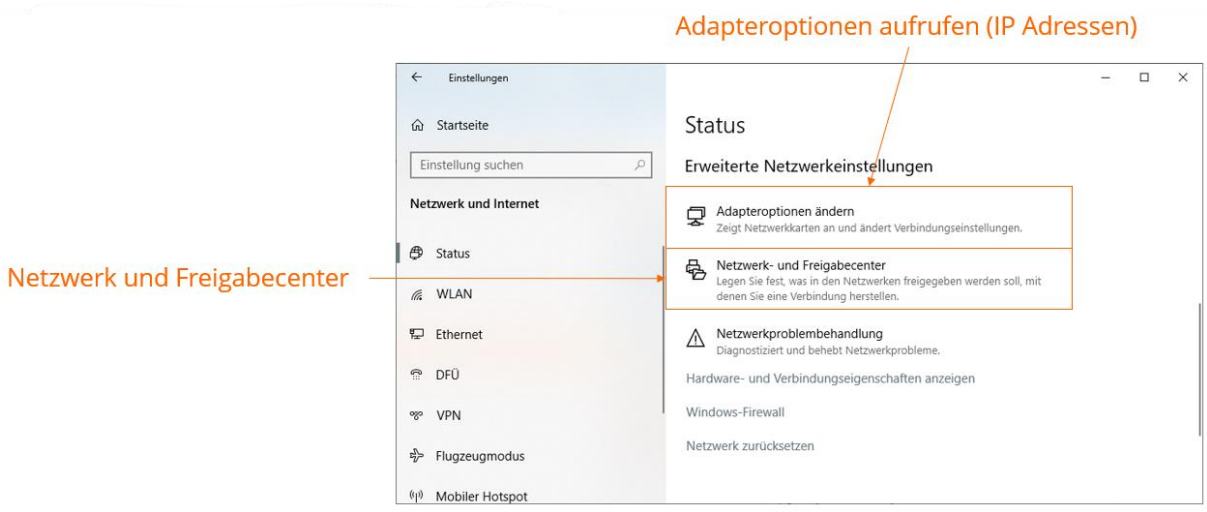
Netzwerkprofil

Das Netzwerkprofil zeigt Profileinstellungen an.



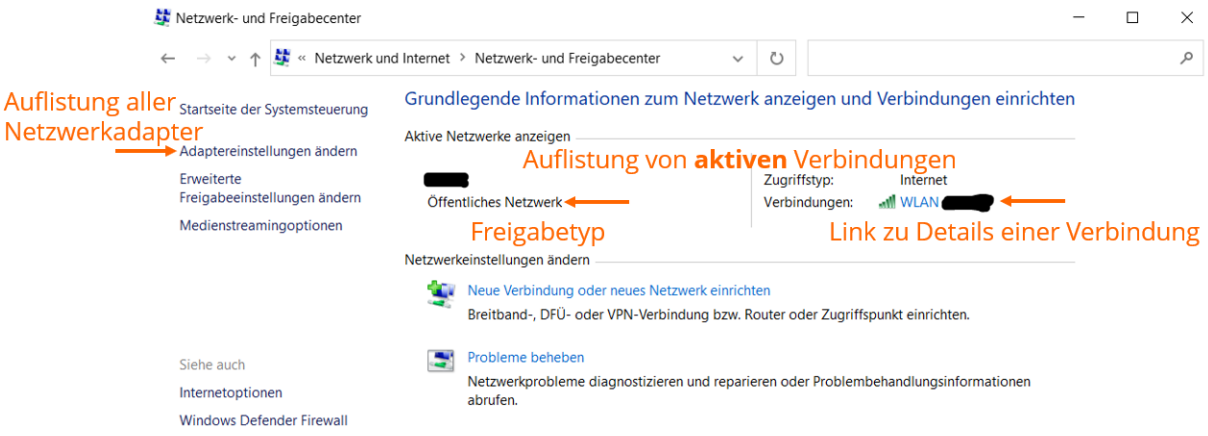
Erweiterte Netzwerkeinstellungen

Die erweiterten Netzwerkeinstellungen geben erweiterte Statusinformationen an.



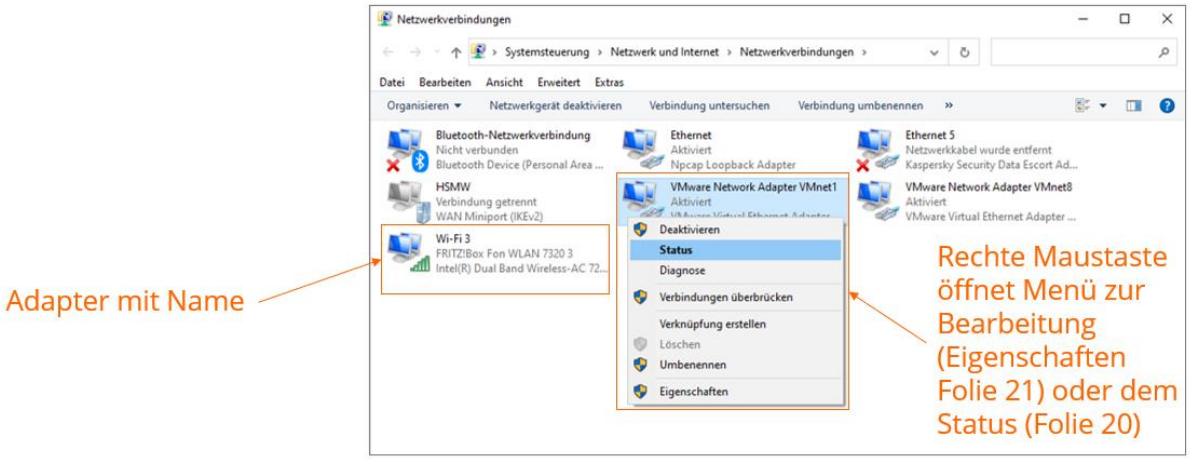
Netzwerk und Freigabecenter

Für genauere Informationen wie die Auflistung der Netzwerkadapter oder die Auflistung von aktiven Verbindungen, kann man im Netzwerk und Freigabecenter schauen.



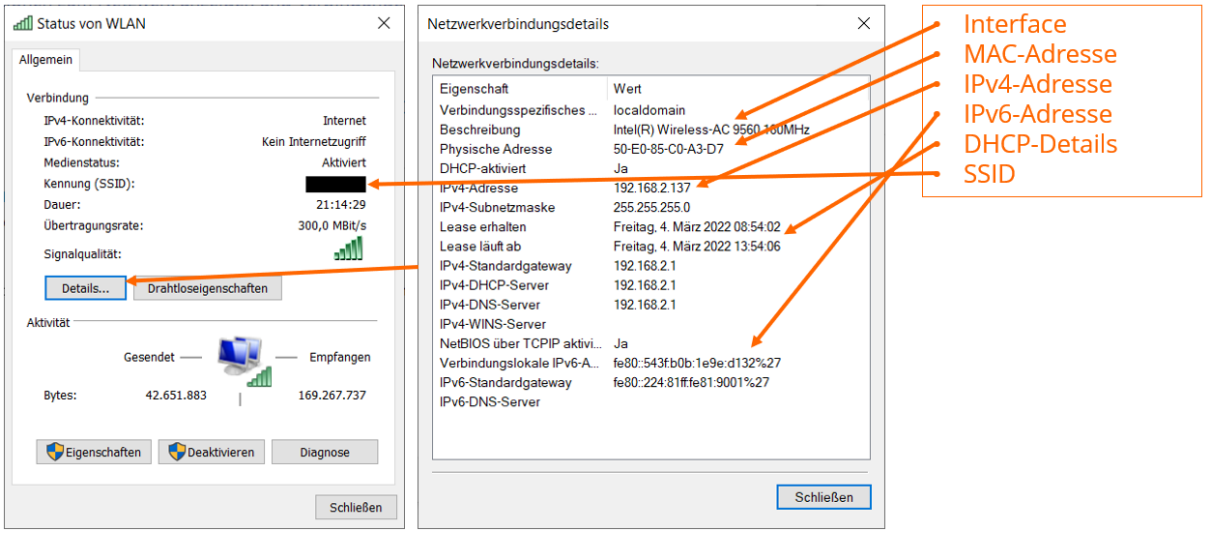
Adapteroptionen

Die Adapteroptionen geben eine Übersicht über alle Netzwerkadapter (Hardware und virtuell).

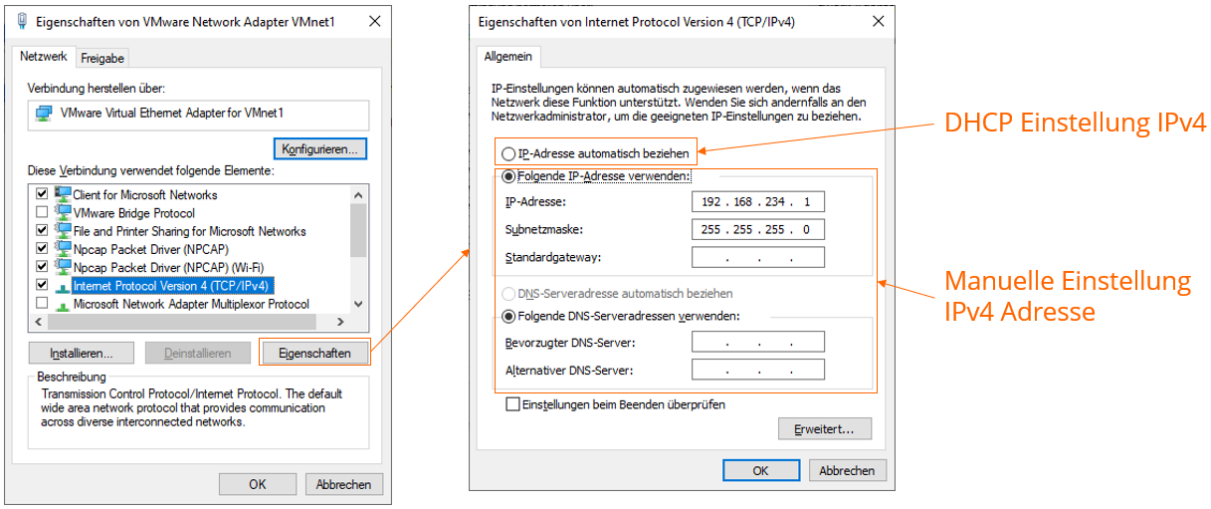


Verbindungsdetails

Weiterhin kann man über den Status vom WAN näheres zu den Netzwerkverbindungen ablesen.



Verbindungseinrichtung



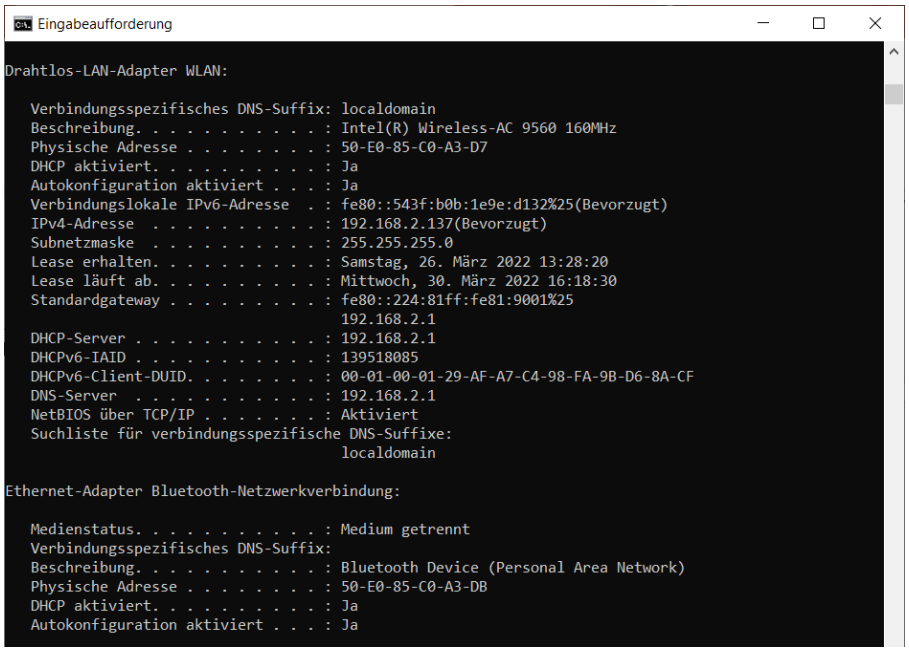
1.8.2.3 CMD-Befehle

Im Folgenden gibt es eine Auflistung von wichtigen CMD-Befehlen:

- ipconfig
  - Network interfaces anzeigen
- getmac
  - MAC-Adressen von interfaces anzeigen
- netstat
  - Ports & offene TCP-Verbindungen
- systeminfo
  - Zusammenfassung des Systems (Hardware & OS)
- ping
  - Senden von ICMP-Requsts
- tracert
  - Route mit TTL ermitteln
- pathping
  - Kombination von ping und tracert
- arp
  - ARP-Tabelle auswerten
- nslookup
  - DNS-Tabelle auswerten

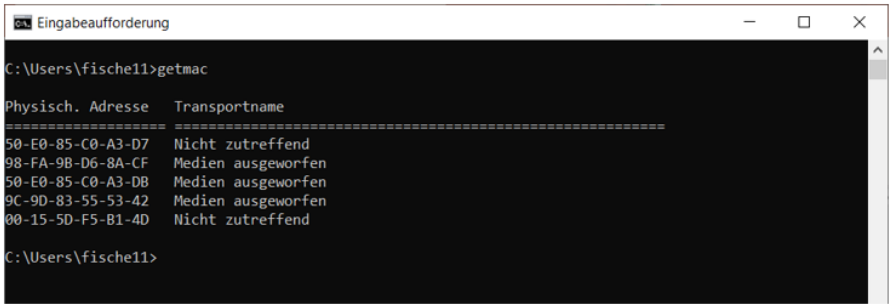
ipconfig

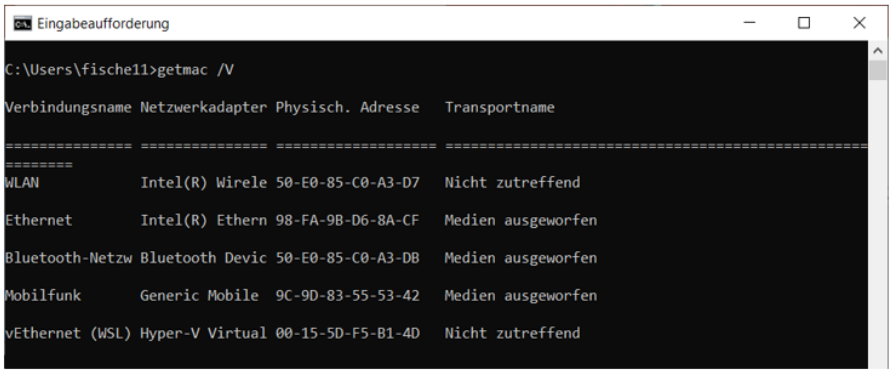
Mittels ipconfig lassen sich Network interfaces anzeigen. Weiterhin werden vorhandene Anschlüsse (sowohl physikalisch als auch logisch), die IP-Adresse (v4 und v6), die Subnetzmaske, die MAC-Adresse und die DHCP-Konfiguration aufgelistet. Zusätzlich wird der DNS-Speicher ausgelesen.



getmac

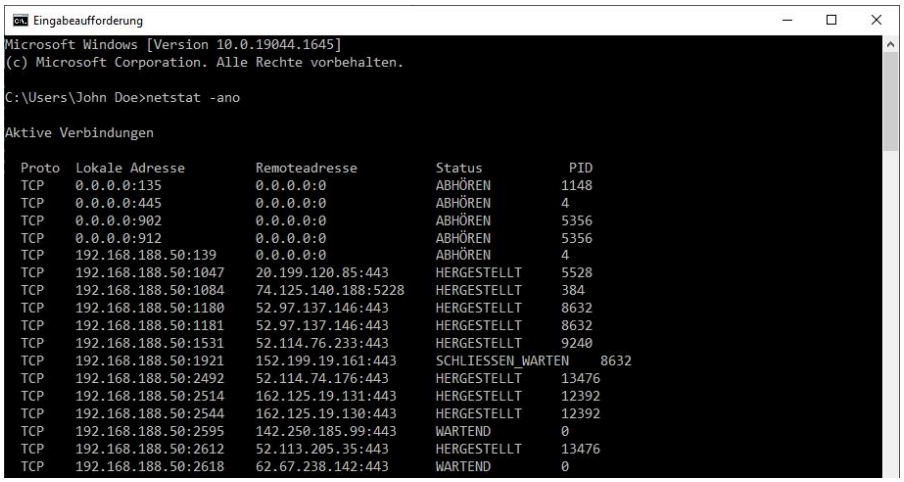
Der Befehl getmac zeigt Interfaces an und listet MAC-Adressen auf.



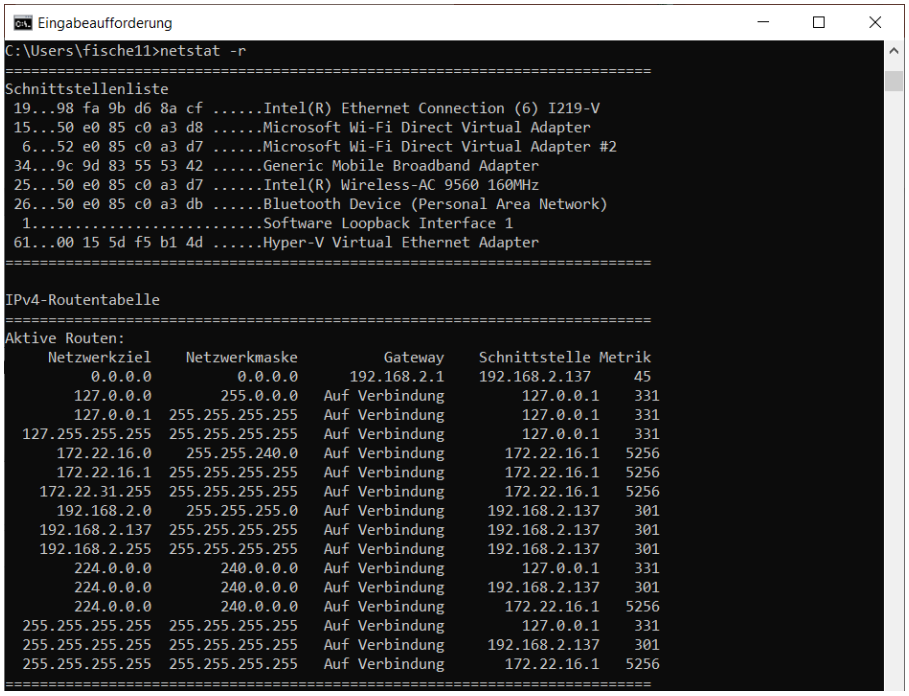


netstat

netstat listet aktive TCP-Verbindungen auf und zeigt offene TCP-Ports an.

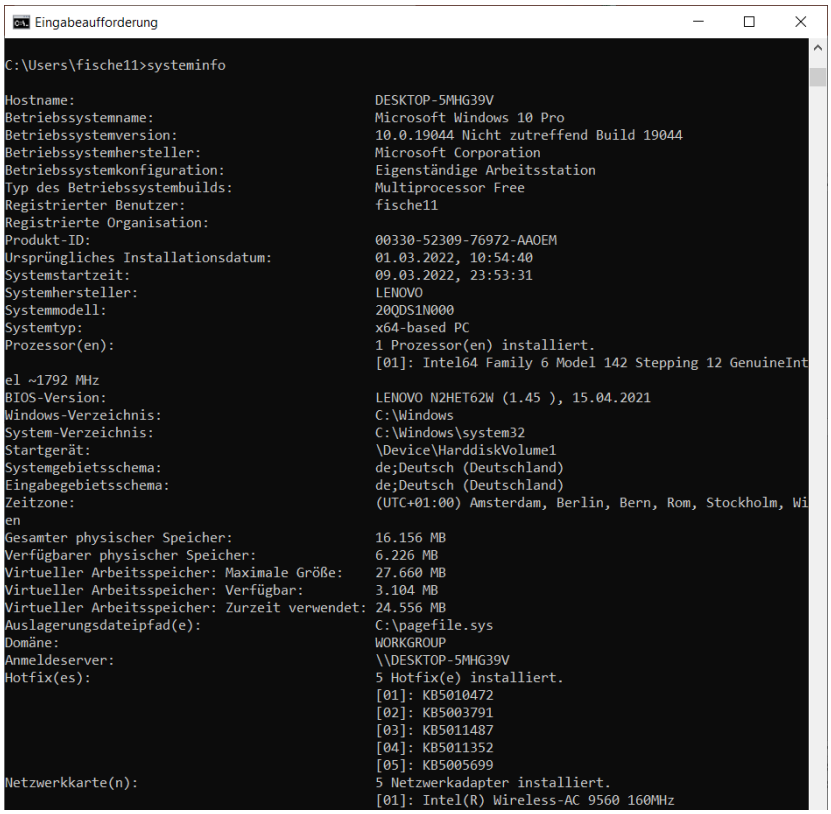


Außerdem listet netstat Routing-Tabellen auf und kann Statistiken zu den einzelnen Protokollen anzeigen.



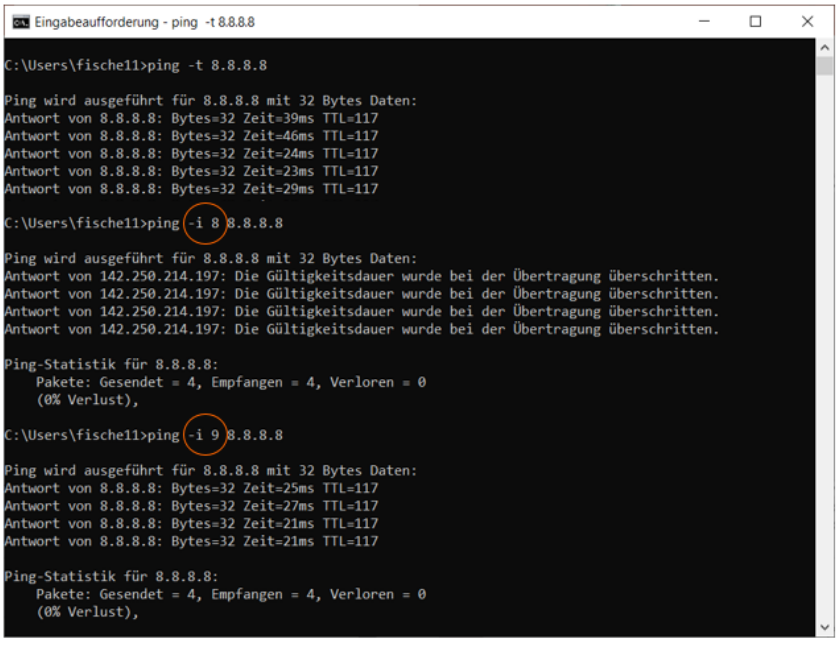
systeminfo

Der Befehl systeminfo gibt Informationen über das System, sprich den Computer aus. Dazu gehören die OS-Version, der Hostname, der Prozessor, die BIOS-Version, der Arbeitsspeicher, der Domainname und Netzwerkadapter mit IPs.



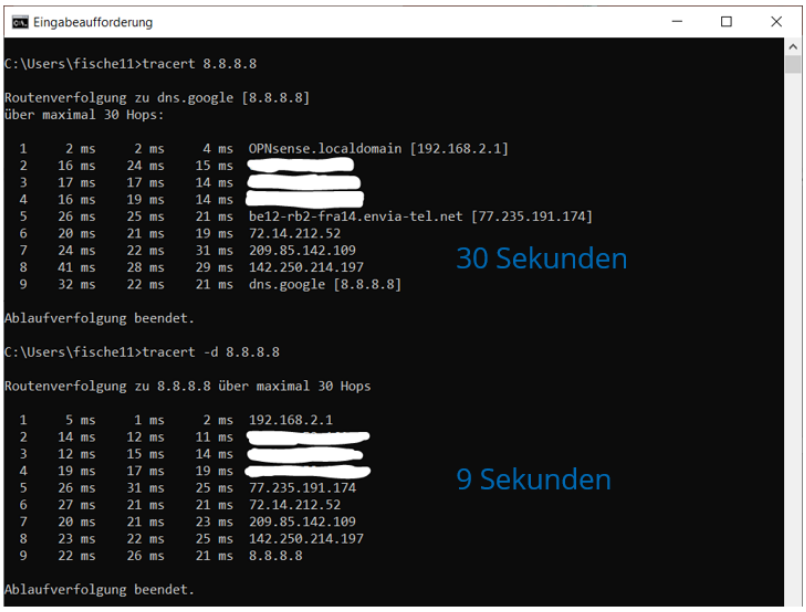
ping

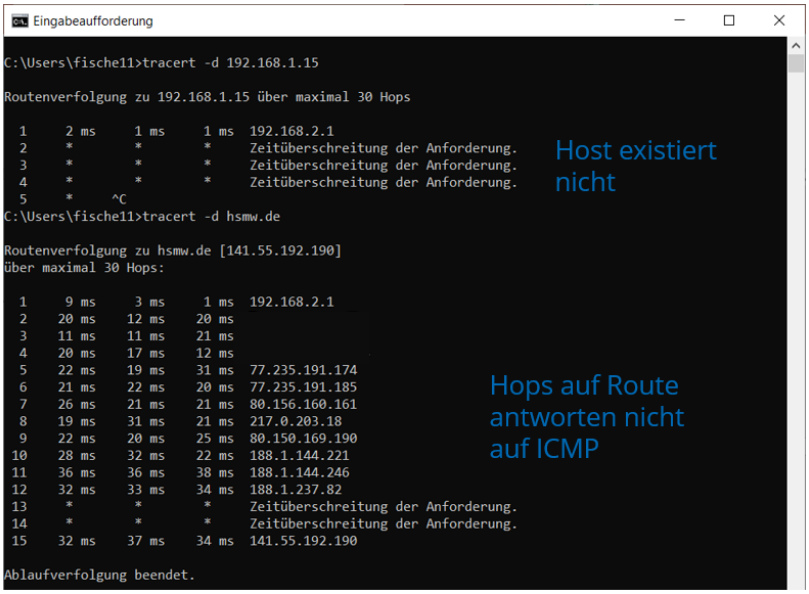
Der ping-Befehl prüft die Erreichbarkeit einer IP-Adresse. Die Standard TTL (Time To Live) beträgt 64. Weiterhin können mit dem ping-Befehl Hops auf der Route zum Ziel ermittelt und ICMP-Errors angezeigt werden.



tracert

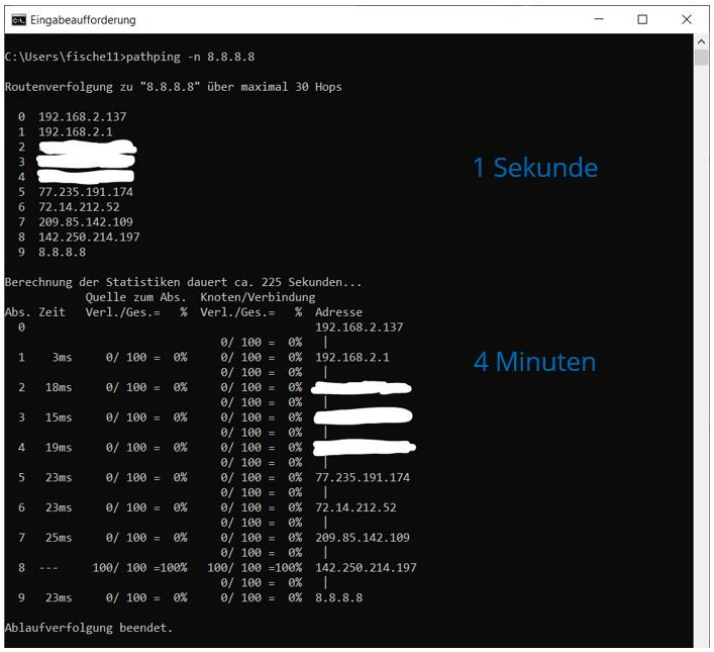
Der tracert-Befehl ermittelt die Hops zum Ziel, was meistens der Route zum Ziel entspricht. Jedoch benötigt die Namensauflösung viel Zeit.



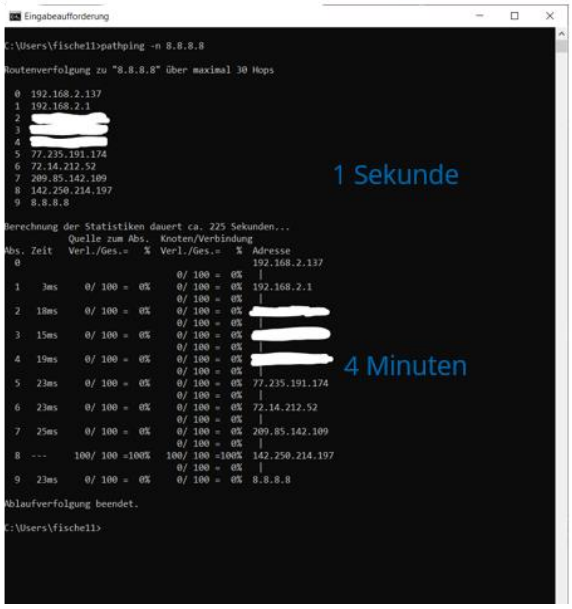


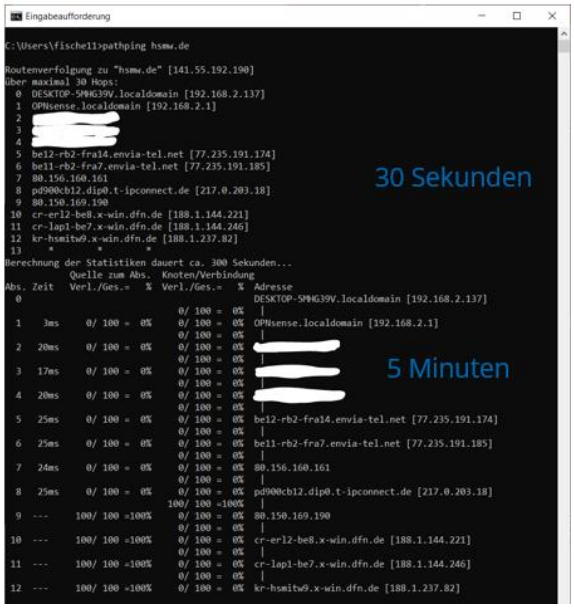
pathping

pathping liefert eine detailliertere Auflistung als tracert. Hierbei wird die eigene IP-Adresse mit angezeigt. Weiterhin wird der Path schneller angezeigt, dafür ist die Statistik langsamer, aber auch ausführlicher. pathping adressiert Hops direkt, wodurch Probleme im Netzwerk leichter identifizierbar sind.



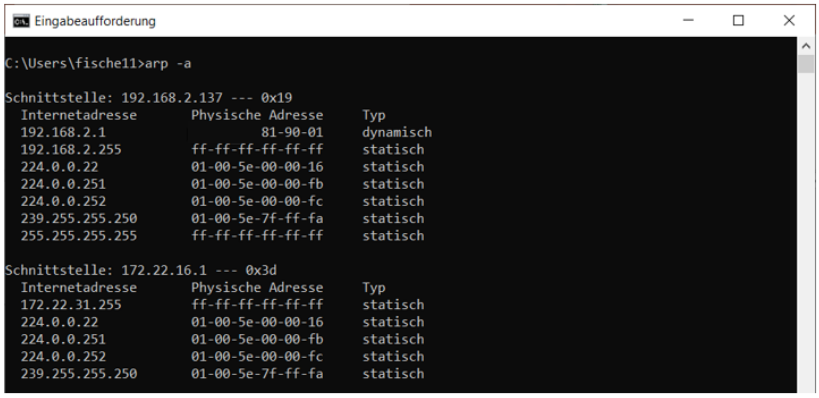
-n

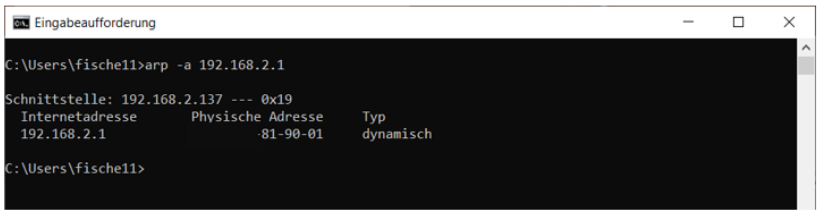




arp

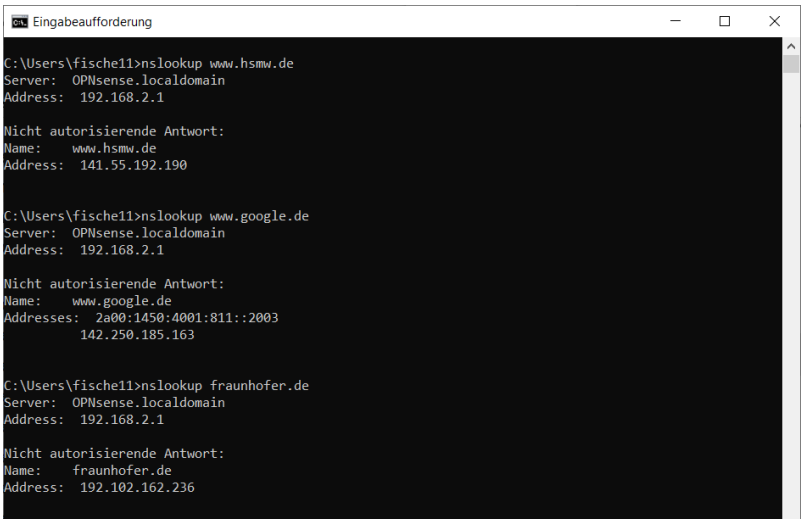
Der arp-Befehl zeigt die ARP-Tabelle an. Weiterhin werden Kommunikationspartner, Teilnehmer des Netzwerkes und die Hersteller von den Netzwerkkarten (Vendor Lookup) angezeigt.

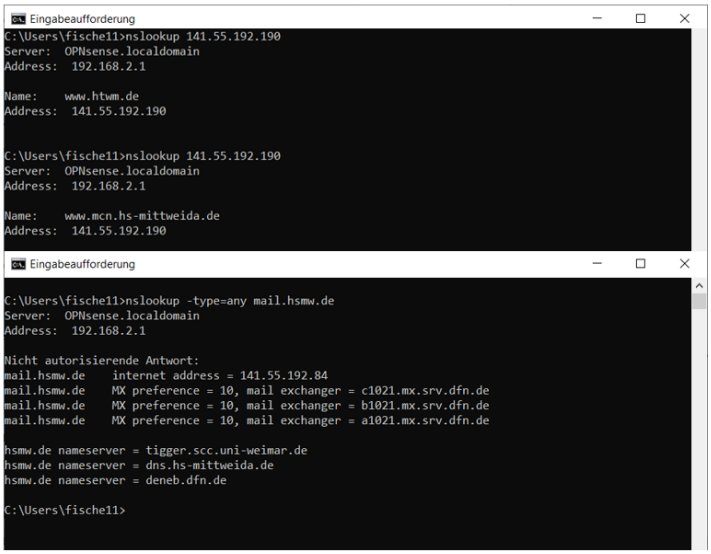




nslookup

nslookup ist für die Auflösung der DNS-Adresse zuständig. Zudem wird die IP-Adresse in DNS aufgelöst. Achtung: mehrere DNS-Adressen können die gleiche IP zeigen und mehrere IP-Adressen können für eine DNS-Adresse hinterlegt werden (Anycast).





Reverse Lookup

-type=any

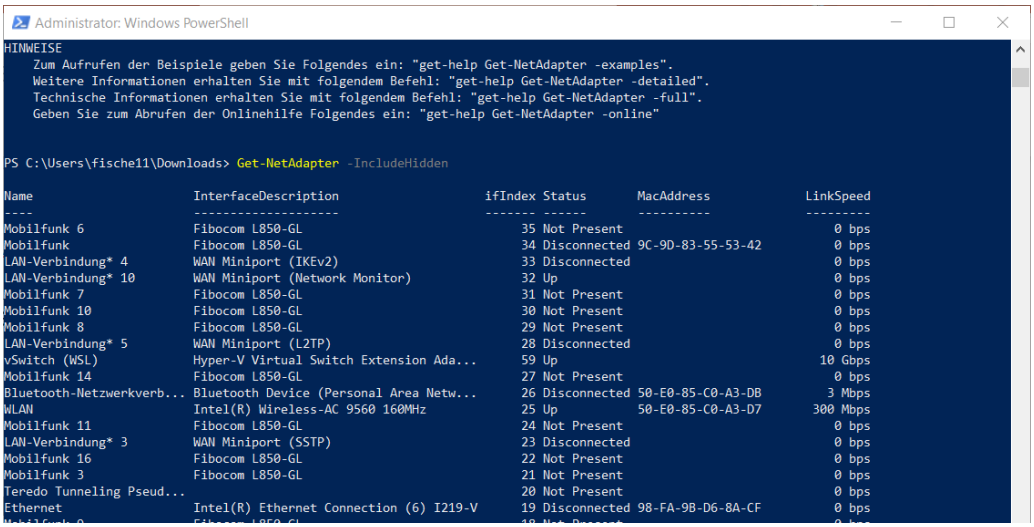
1.8.2.4 PowerShell-Befehle

Folgende PowerShell-Befehle können Informationen zum Netzwerk liefern:

- Get-NetAdapter
  - Netzwerkadapter auflisten
- Get-NetAdapterAdvancedProperty
  - Einstellungen zu Netzwerkadaptern anzeigen
- Get-NetAdapterHardwareInfo
  - Hardware zu Netzwerkadaptern auflisten
- Get-NetAdapterPowerManagement
  - Energieverbraucheinstellungen zu Netzwerkadaptern anzeigen
- Get-NetAdapterStatistics
  - Sende- & Empfangsstatistik von Netzwerkadaptern
- Get-NetIPAddress
  - Informationen zu IP-Adresse
- Get-NetNeighbor
  - Auflistung bekannter Netzwerkteilnehmer in angeschlossenen Netzwerken
- Get-NetRoute
  - Auflistung der Routingtabelle
- Get-NetTCPConnection
  - Auflistung aller TCP-Ports & TCP-Verbindungen
- Get-NetUDPEndpoint
  - Auflistung aller UDP-Ports

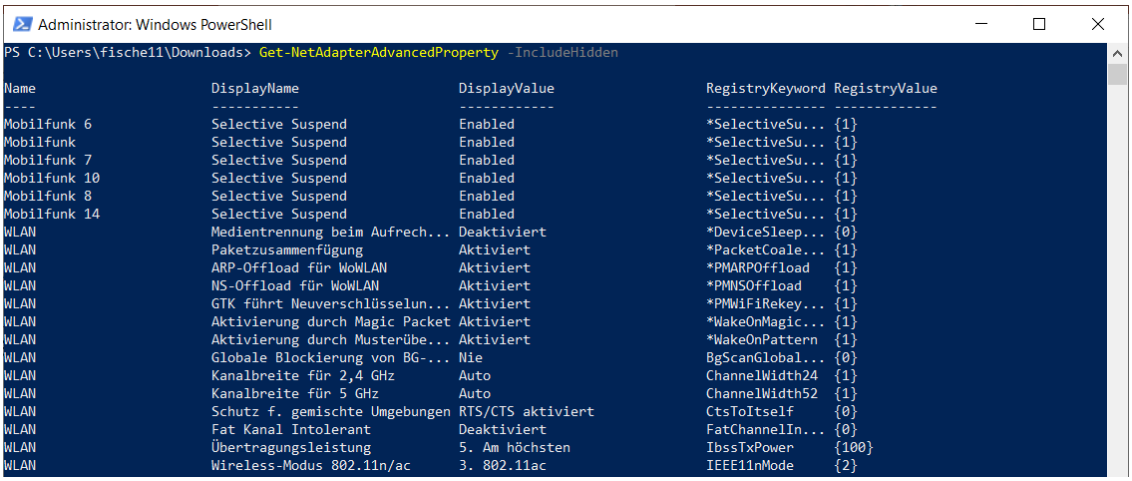
Get-NetAdapter

Mit dem Befehl Get-NetAdapter werden die Netzwerkadapter aufgelistet. Hierbei werden Informationen wie der Name, das Interface, der Interface Index, der Status, die MAC-Adresse und die Verbindungsgeschwindigkeit mit ausgegeben.



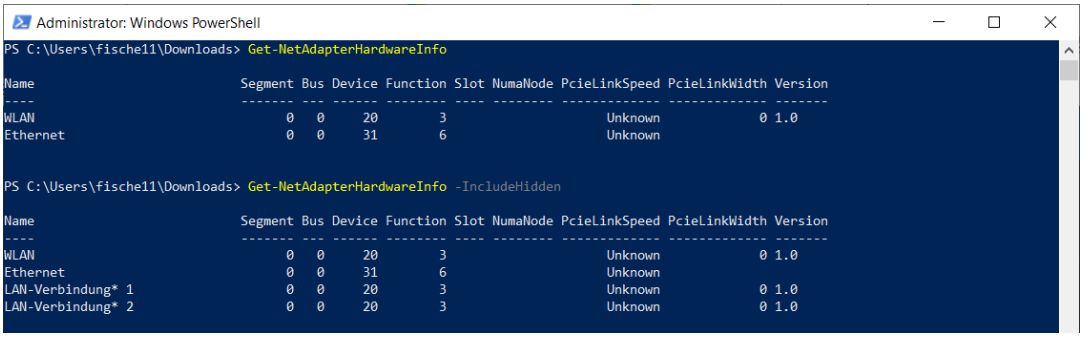
Get-NetAdapterAdvancedProperty

Mit Get-NetAdapterAdvancedProperty werden die Eigenschaften von Netzwerkadaptern angezeigt. Hierzu zählen das Interface, die Eigenschaft, der Wert, das Registry-Keyword und das Registry-Value.



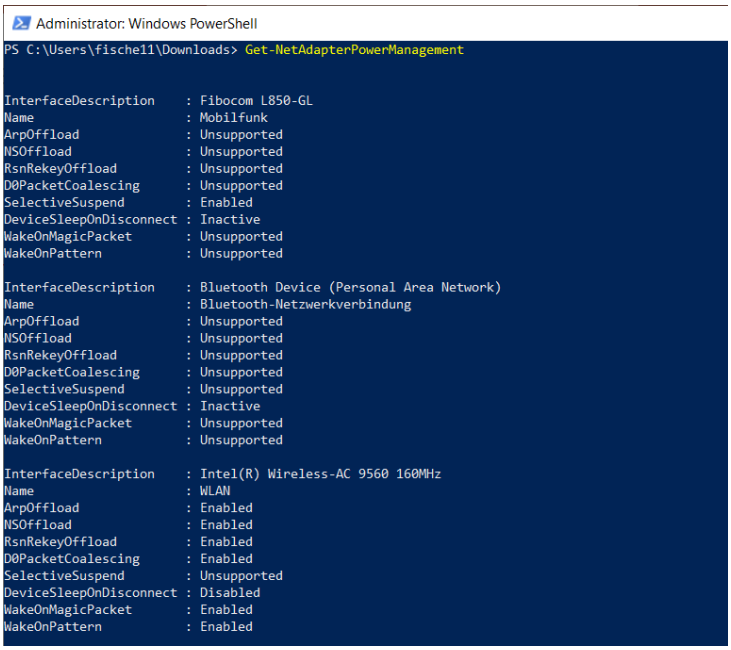
Get-NetAdapterHardwareInfo

Der Befehl Get-NetAdapterHardwareInfo listet die Netzwerkhardware und die physikalischen Interfaces auf.



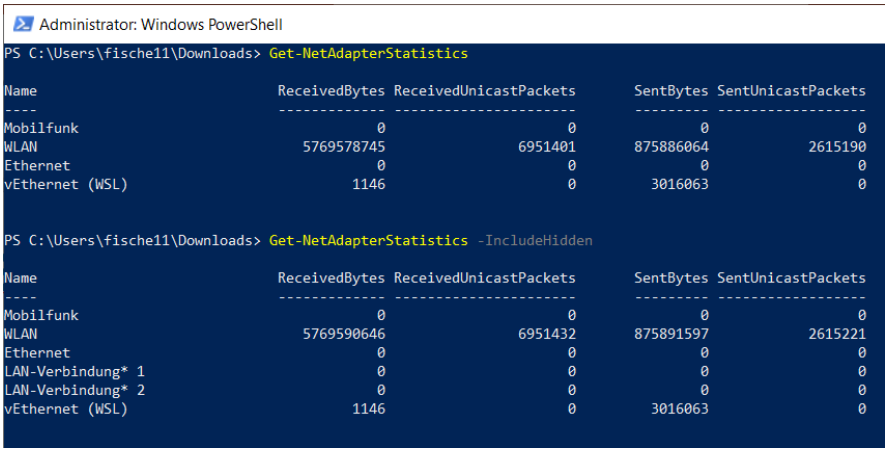
Get-NetAdapterPowerManagement

Mit Get-NetAdapterPowerManagement werden Strom Management Features aufegelistet. Weiter werden physikalische und logische Interfaces wie beispielsweise Hyper-V angezeigt.



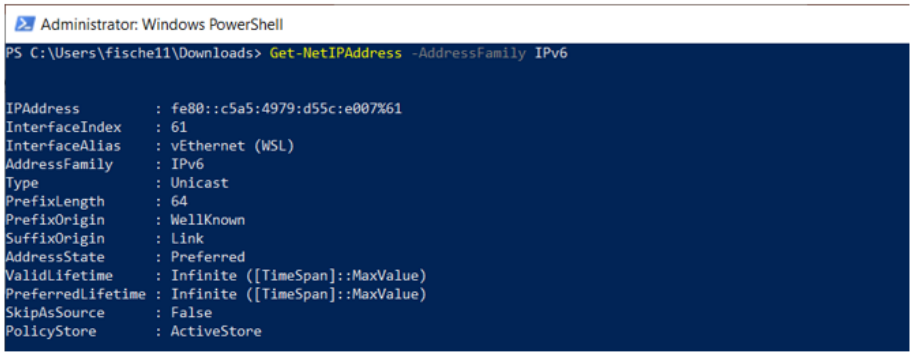
Get-NetAdapterStatistics

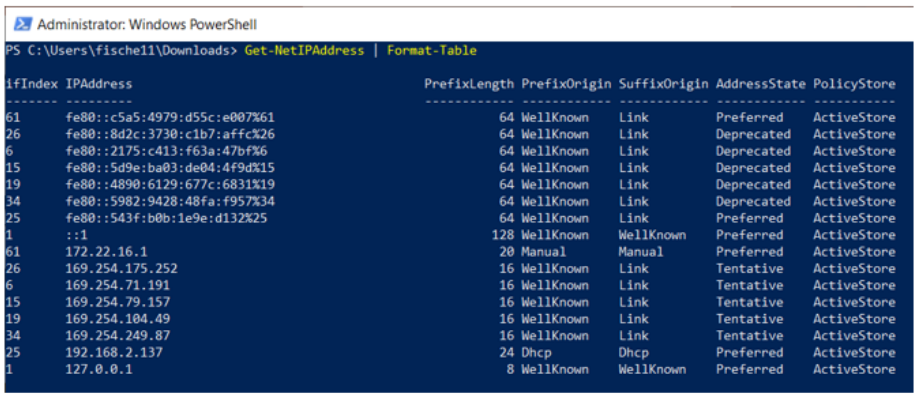
Der Befehl Get-NetAdapterStatistics listet Netzwerkadapter auf. Weitere angezeigte Informationen sind die Bytes, welche direkt oder als unicast gesendet wurden sowie die direkt oder unicast empfangenen Bytes.



Get-NetIPAddress

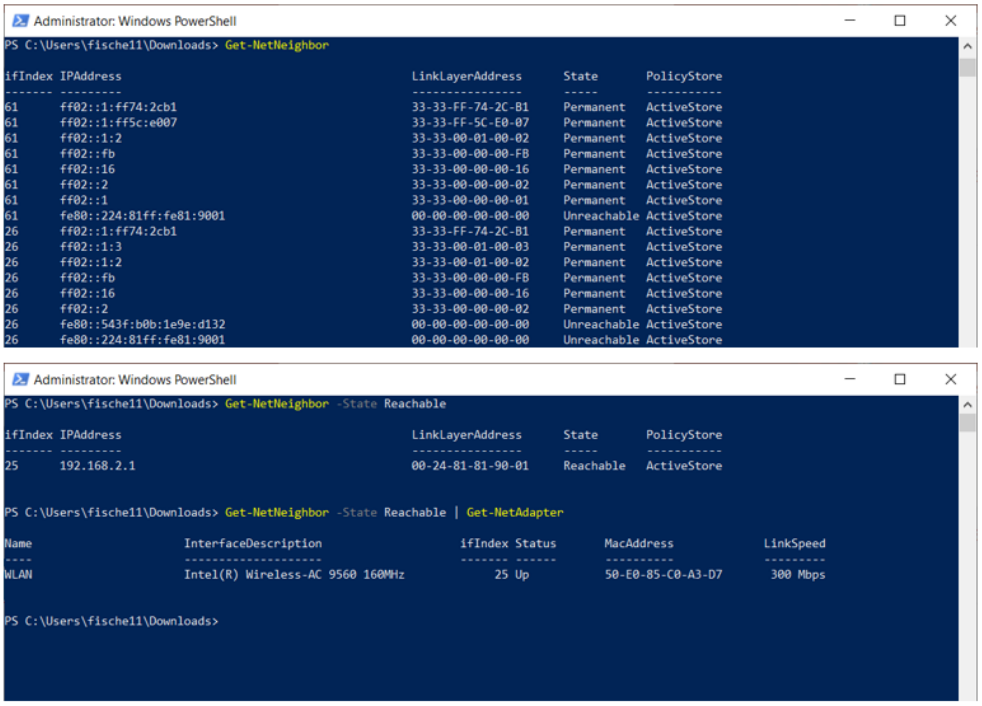
Dieser Befehl zeigt IPv4 und IPv6 Adressen an. Weiterhin wird der Zuordnungstyp ausgegebene, sprich ob es sich um Wellknown (IP-Standard), Link (self-assigned), DHCP (DHCP-Server), RouterAdvertisement (IPv6) oder Other handelt.





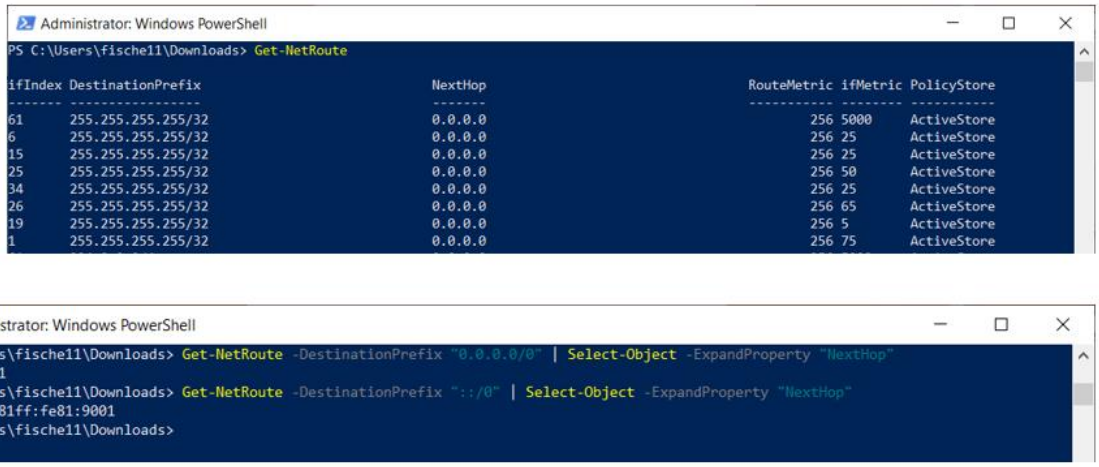
Get-NetNeighbour

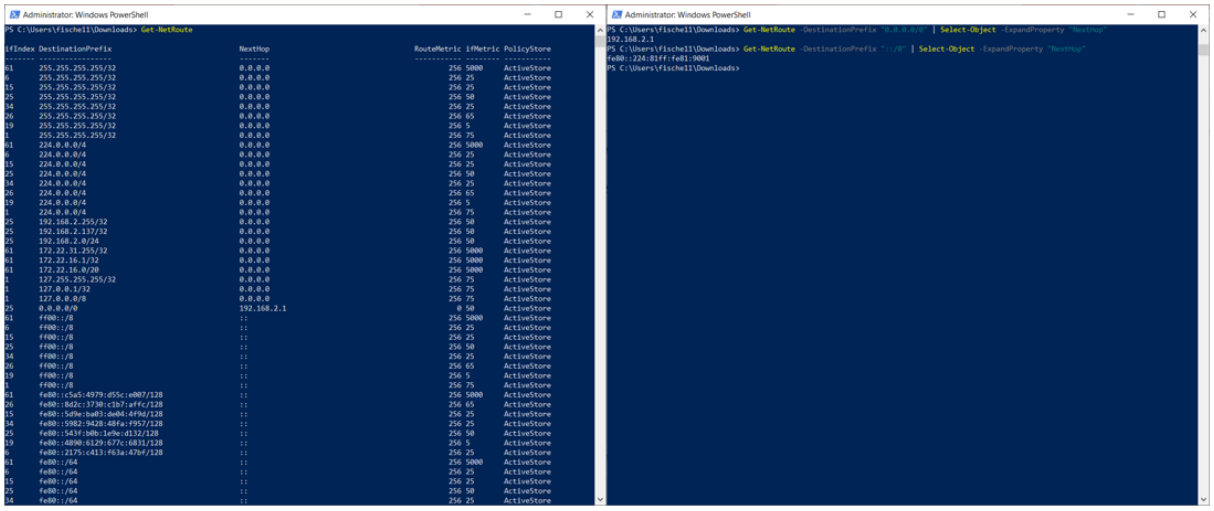
Der Befehl Get-NetNeighbour listet bekannte Nachbarn im Netzwerk auf, sprich Geräte, die sich im gleichen Subnetz befinden. Zusätzlich werden die IP- und die MAC-Adresse ausgegeben.



Get-NetRoute

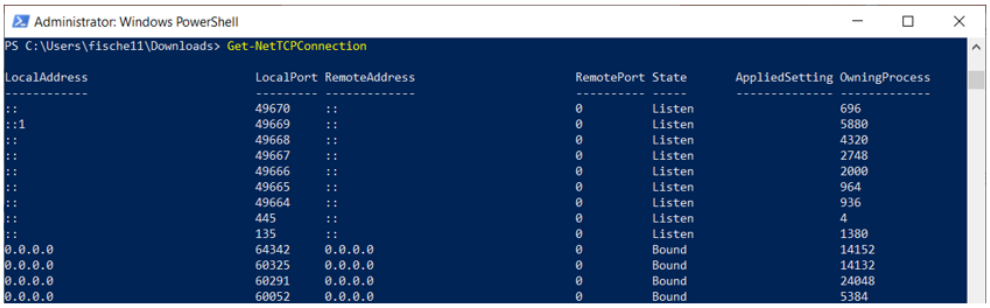
Get-NetRoute liest Routing-Tabellen aus und gibt Informationen zu den Routen von IPv4 und IPv6 Adressen aus. Weiterhin werden Routing Metriken angezeigt.

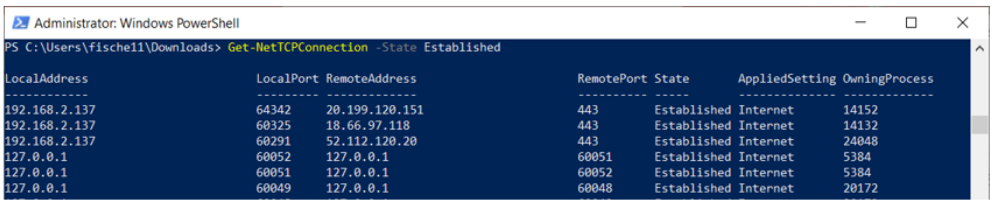




Get-NetTCPConnection

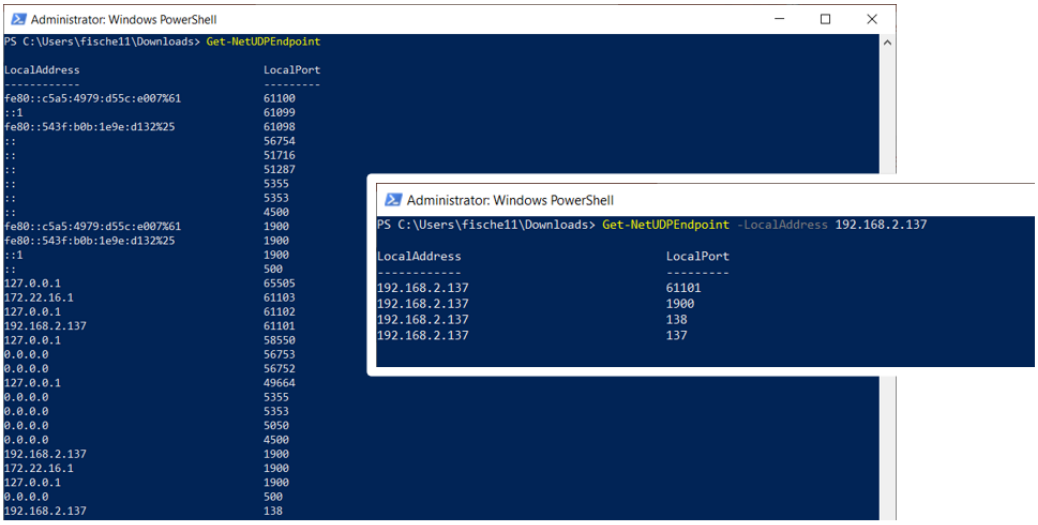
Get-NetTCPConnection listet TCP-Ports auf. Dazu werden Infos zu Listening-Ports, aktiven Verbindungen und Port-Mapping ausgegeben.





Get-NetUDPEndpoint

Der Befehl Get-NetUDPEndpoint listet lokale und remote UDP-Ports auf. Weiterhin wird noch die IP-Adresse mit ausgegeben.



1.8.3 Zusammenfassung

Sie kennen nun die Funktion Heimnetzgruppe, sowie die Teilen-Funktion unter Windows 10.

Es wurde das ISO-Modell kurz wiederholt und auf die Schichten 1-3 genauer eingegangen. Dabei wurde eine Protokollübersicht präsentiert und wichtige Protokolle für einen Windows-Client hervorgehoben.

Abschließend wurden Ihnen die verschiedenen Möglichkeiten vorgestellt, Netzwerkkonfigurationen unter Windows auszulesen. Dabei wurden 3 Wege offengelegt. Diese lauten: graphisch, mit CMD-Befehlen und mit PowerShell-Befehlen.

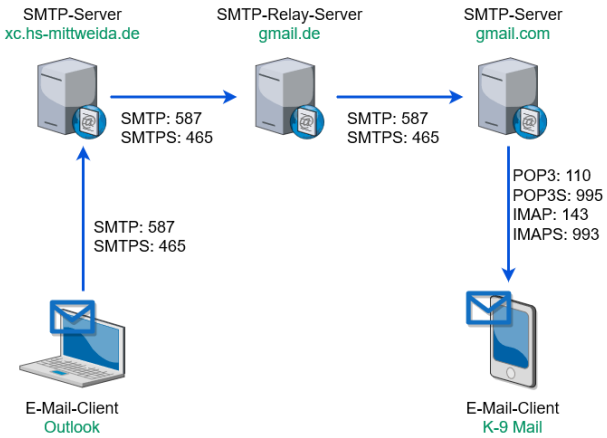
Auf die wichtigsten Befehle und deren Einsatzmöglichkeiten wurde detailliert eingegangen.

1.9 Cloudanwendungen

Die Cloud wird für die Synchronisation von Client-Daten über einen Server verwendet. Weiterhin ist es möglich, die Daten auf entfernten Servern zu speichern und diese auch für andere Nutzer freizugeben (Share). Bei Cloudmodellen erfolgt eine geteilte Ressourcennutzung einer zentralen Ressource, wobei die Nutzer auf einen gemeinsam genutzten Pool von Ressourcen zugreifen können. Die zentralen Ressourcen befinden sich in den Rechenzentren des Cloud Providers. Ein weiteres Merkmal von Cloudanwendungen ist die Möglichkeit der Abrechnung anhand der Nutzungsdauer und -menge.

1.9.1 E-Mail

Es gibt drei verschiedene E-Mail-Protokolle. Dazu gehören SMTP, POP3 und IMAP.



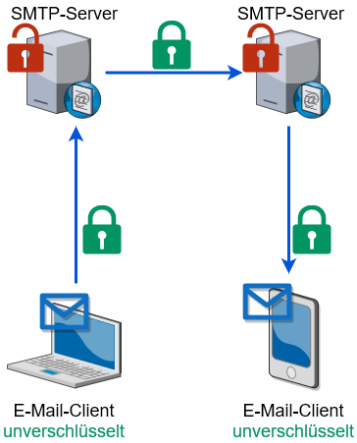
SMTP steht für Simple Mail Transport Protocol. Die erste Version ist im RFC 821 definiert, welcher 1982 erstellt wurde. Mittlerweile ist die aktuelle Version RFC 5321 von 2008. SMTP wird für das Versenden von E-Mails genutzt. Hierbei erfolgt das Versenden vom Client zum Server. Zwischen einzelnen Servern erfolgt eine Weiterleitung (Relay), währenddessen Server auch E-Mails filtern können. Die Standardports für SMTP sind 587 für die unverschlüsselte Version und 465 für die TLS-verschlüsselte Variante SMTPS.

POP3 steht für Post Office Protocol Version 3. Die erste Version ist im RFC 918 definiert, welcher 1984 erstellt wurde. Mittlerweile ist die aktuelle Version RFC 1939 von 1996. POP3 ist für das Auflisten, Löschen und Abholen von E-Mails am Server zuständig. Hier werden keine Ordnerstrukturen beachtet. Weiterhin wird durch einen Mailabruf die Mail auf dem Server gelöscht. Bei POP3 ist keine Synchronisation mit anderen Clients möglich. Die Standardports für POP3 sind 110 für die unverschlüsselte Version und 995 für die TLS-verschlüsselte Variante POP3S.

IMAP steht für Internet Message Access Protocol, welches früher als Interactive Mail Access Protocol bezeichnet wurde. Der aktuelle RFC ist der 9051er, welcher 2021 erstellt wurde. IMAP ist für das Abrufen der E-Mails vom Server zuständig, wobei das Suchen und Sortieren direkt auf dem Server stattfindet. Moderne Clients haben jedoch die Möglichkeit, im lokalen Cache zu suchen. Der Server hält alle E-Mails und der Client greift nur auf den Server zu. Bei der Verwendung von IMAP werden die Clients synchronisiert. Die Standardports für IMAP sind 143 für die unverschlüsselte Version und 993 für die TLS-verschlüsselte Variante IMAPS.

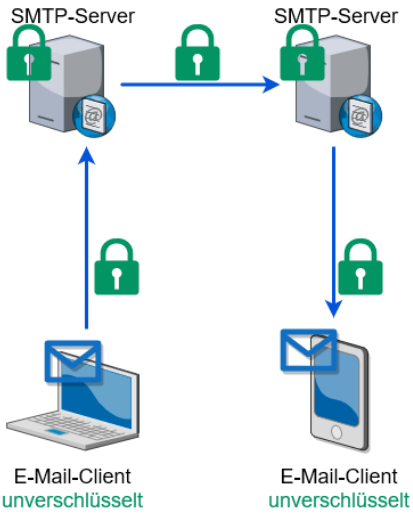
1.9.1.1 Transportverschlüsselung

Bei der Transportverschlüsselung geht es um die Verschlüsselung der Transportwege. Dabei werden Client-Server-, Server-Server- und Server-Client-Verbindungen verschlüsselt. TLS (Transport Layer Security) ist als Protokoll in HTTPS (Webclient), POP3S, IMAPS und SMTPS vorhanden.



1.9.1.2 Ende-zu-Ende-Verschlüsselung

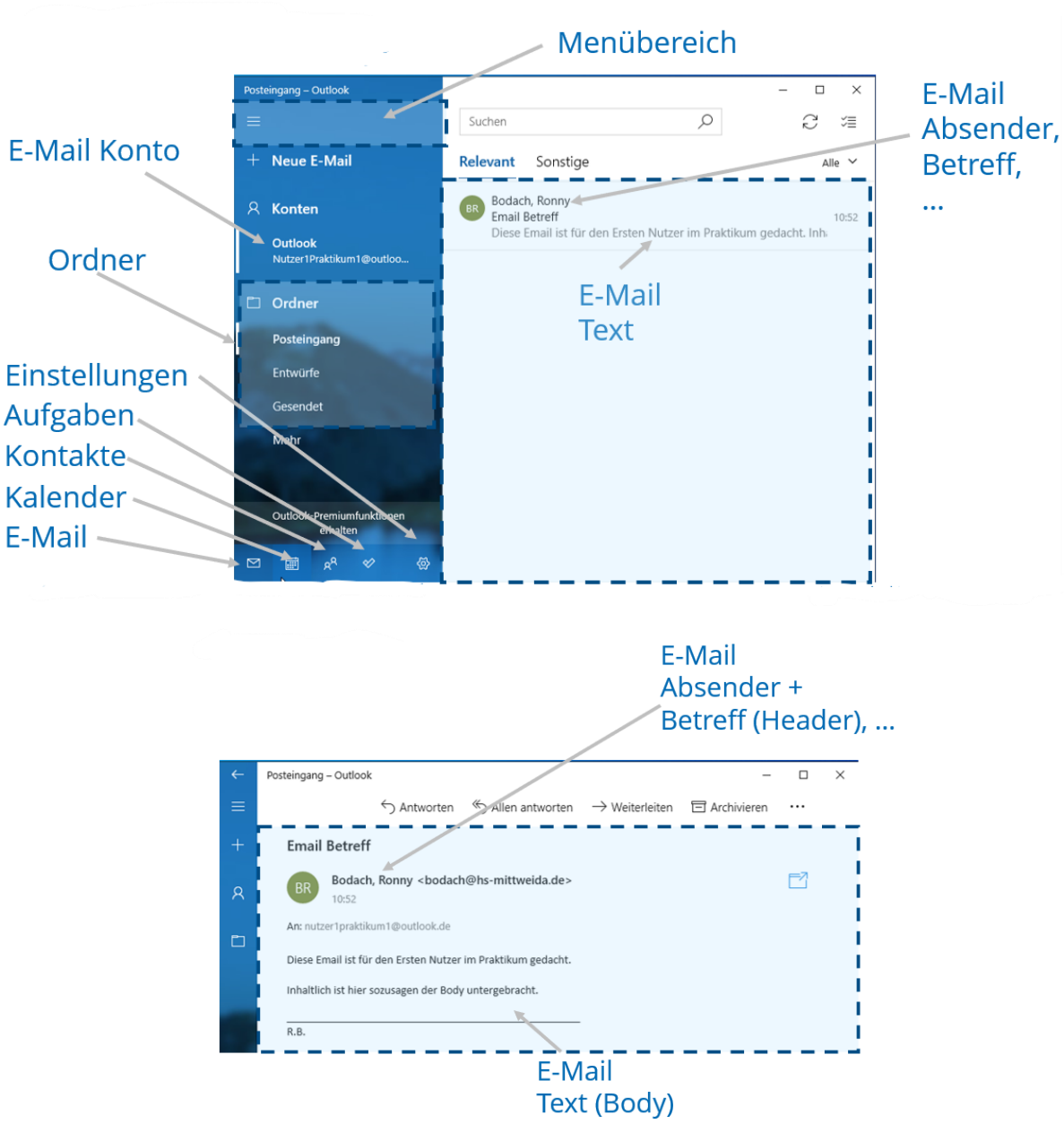
Das Ziel der Ende-zu-Ende-Verschlüsselung ist, dass die Nachricht unverschlüsselt beim Sender und Empfänger vorliegt, der gesamte Transport jedoch verschlüsselt erfolgt. Der Absender ist hierbei kryptographisch verifiziert und die Nachricht wird während des Transports nicht verändert.



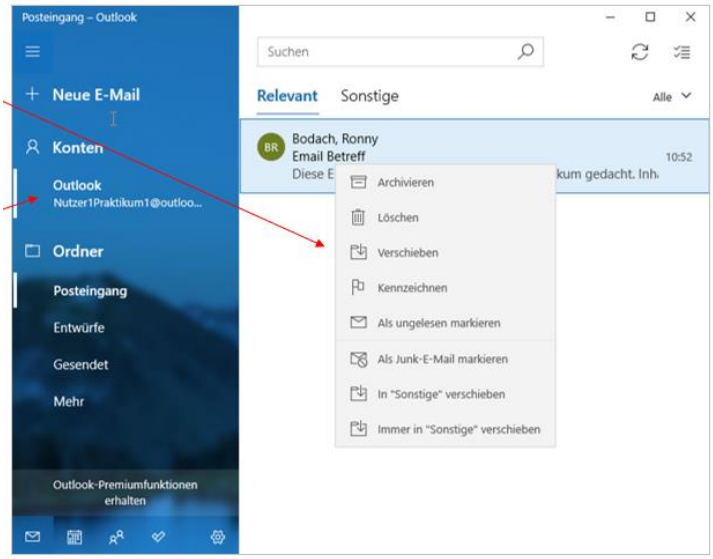
Für die Ende-zu-Ende-Verschlüsselung gibt es zum einen S/MIME oder OpenPGP. S/MIME steht für Secure/Multipurpose Internet Mail Extensions, welches in den RFCs 3369, 3370, 3850 und 3851 definiert ist. Es basiert auf PKCS#7, was im RFC 2315 definiert und zertifikatsbasiert ist. Bei S/MIME signiert eine zentrale Autorität die public keys, wobei dieser zentralen Autorität vertraut wird.

OpenPGP steht für Open Pretty Good Privacy und ist im RFC 4880 definiert. Es ist ein Dezentrales System mit Web of Trust. Der Public Key wird auf einem Key-Server veröffentlicht. Diese Public Keys können von Nutzern signiert werden, wobei diese Signierung öffentlich einsehbar ist.

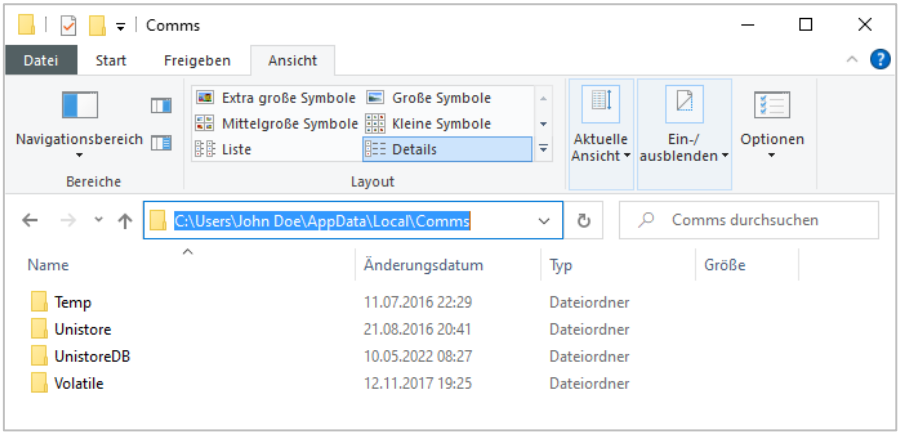
1.9.1.3 MS Mail App



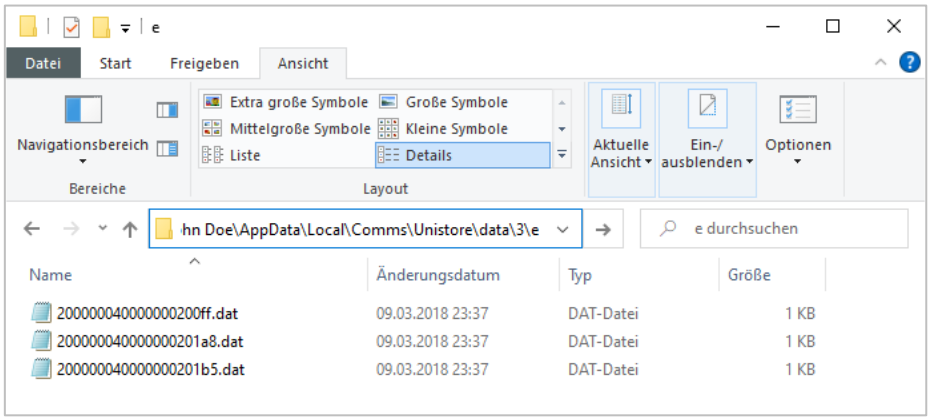
Die E-Mails der Mail App lassen sich nicht mehr exportieren. Außerdem sind sie nicht mehr als *.eml Dateien gespeichert. Die Mail App ist in der Lage, Multiple Accounts zu verwalten. Weiterhin können Benutzer andere E-Mail Provider wie Gmail zur Microsoft-Mail-App hinzufügen.



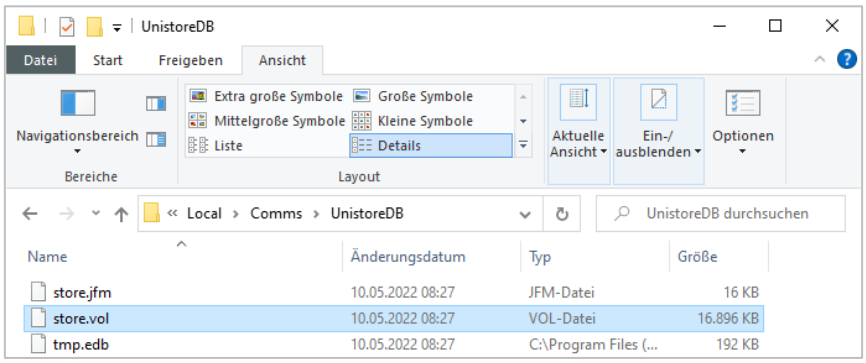
Die Inhalte der Mail-App sind unter „\Users\Username\AppData\Local\Comms“ gespeichert. Dabei gibt es fünf Unterverzeichnisse: Temp, Unistore, UnistoreDB, UserDataTempFiles und Volatile.



Die Inhalte der Unterverzeichnisse bestehen aus dem Data Verzeichnis. Das Data Verzeichnis besteht aus den Unterverzeichnissen 2, 3, 7, etc.. Diese Unterverzeichnisse bestehen wiederum aus Verzeichnissen b, c, d, e. Diese enthalten *.dat Dateien sowie temporäre Dateien, wozu der HTML Body (3, 5), Attachments (7) und Kontaktbilder (2) zählen.

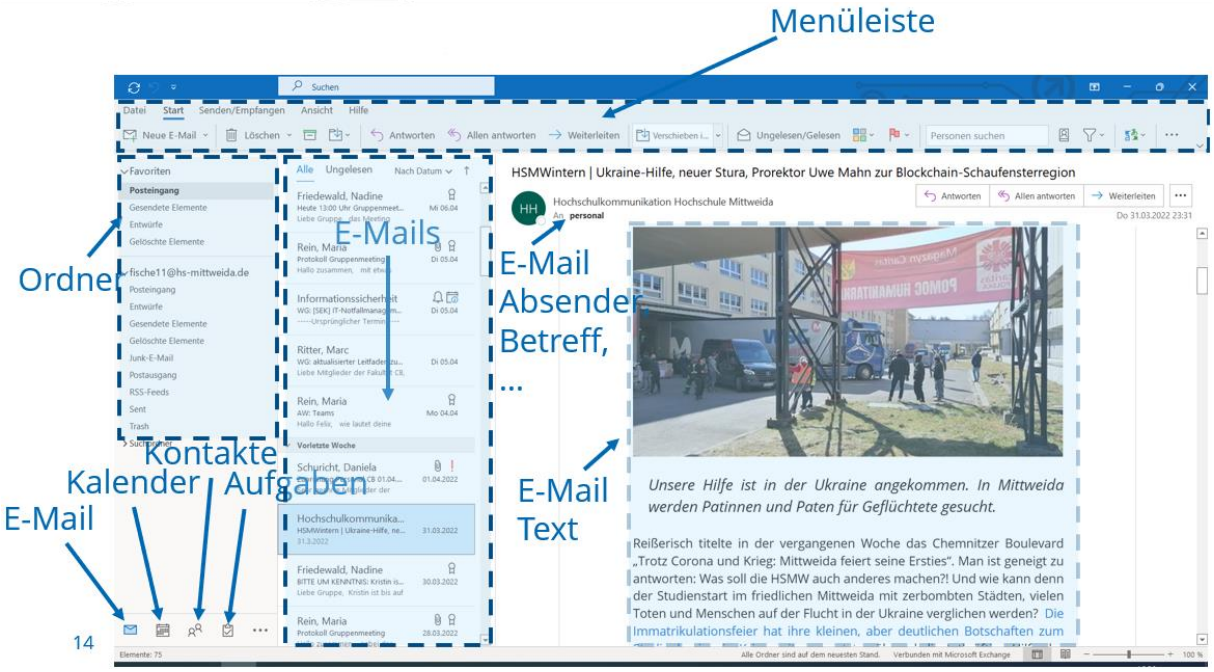


Die EDB Datenbank, welche Headerinformationen und die Verlinkung der Body Nachrichten und Attachments erhält, ist unter „AppData\Local\Comms\UnistoreDB\store.vol“ abgelegt. Diese Datei ist im laufenden Betreib gesperrt.



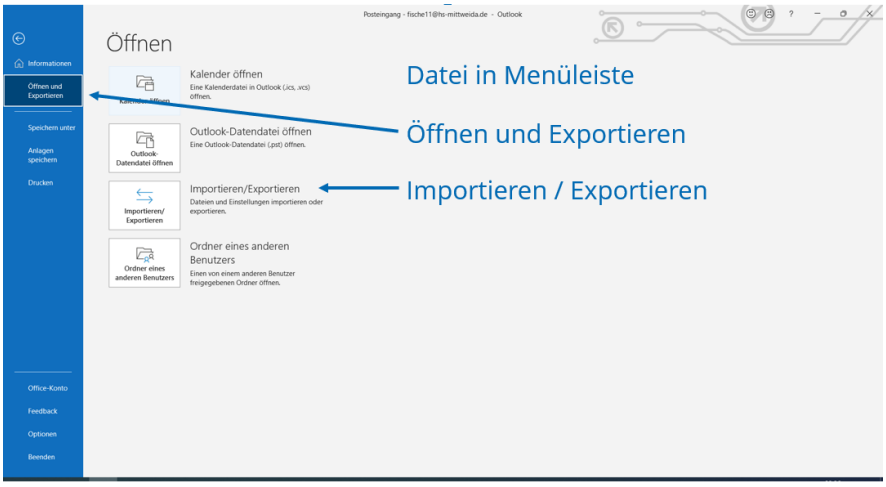
1.9.1.4 MS Outlook

Die Abbildung zeigt die verschiedenen Elemente der Oberfläche von MS Outlook.

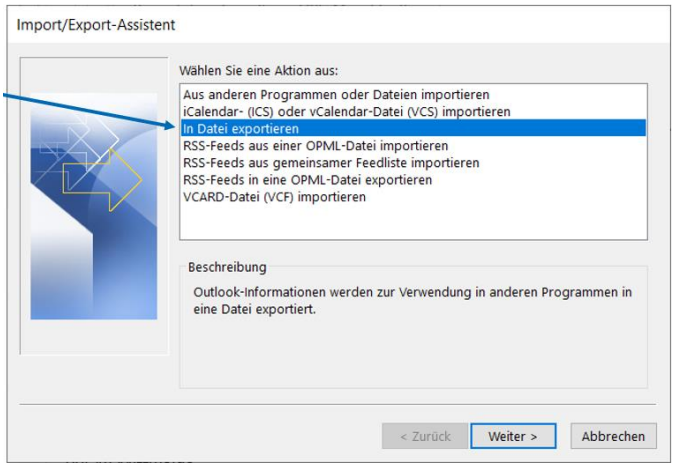


Outlook E-Mails exportieren

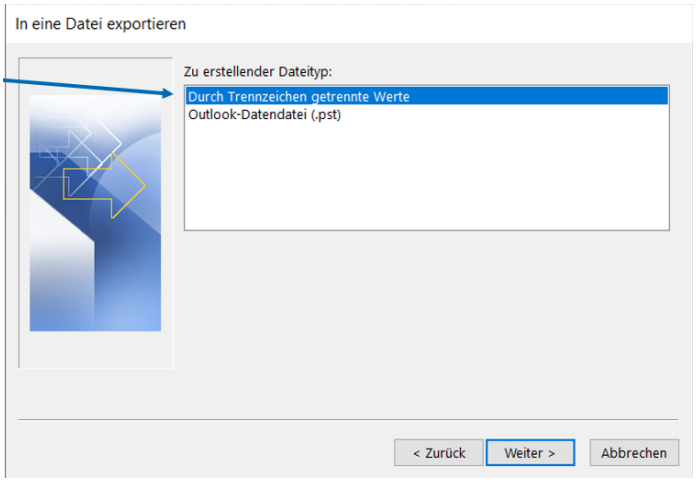
Um in Outlook E-Mails exportieren zu können wählt man in der Menüleiste den Reiter „Datei“. Dort wählt man den Punkt „Öffnen und Exportieren“ und geht anschließend auf „Importieren/Exportieren“.



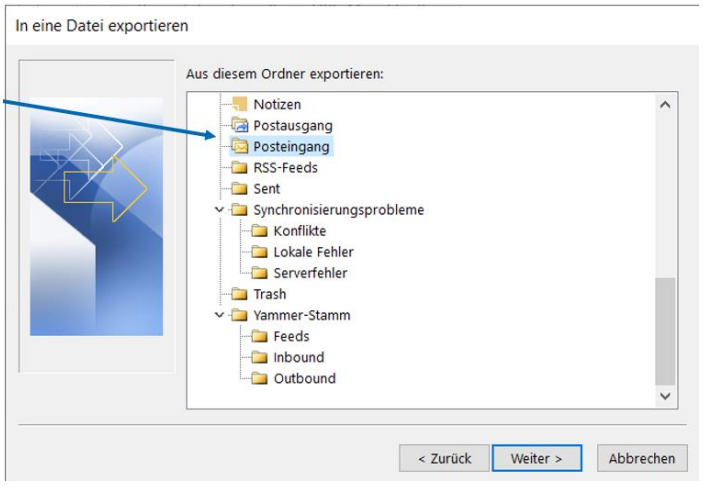
Es öffnet sich ein Import/Export-Assistent, in welchem man „in Datei exportieren“ wählt, um die E-Mails in eine Datei zu exportieren.



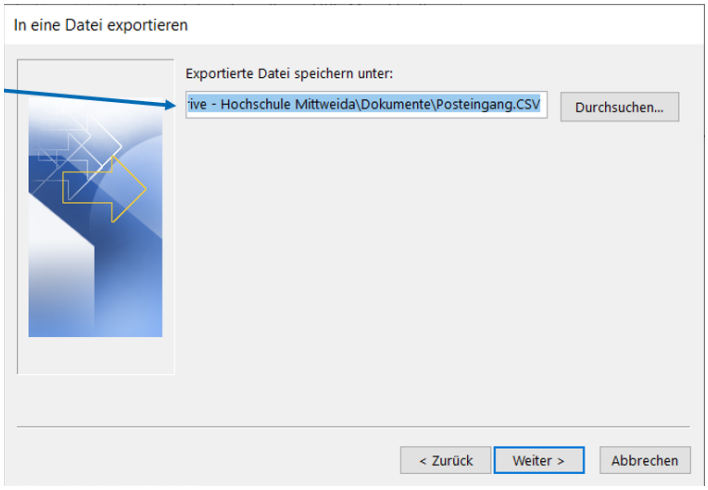
Daraufhin öffnet sich ein weiteres Fenster, in welchem man den zu erstellenden Dateityp wählen kann. Wenn man „Durch Trennzeichen getrennte Werte“ wählt, wird die E-Mail als CSV-Datei exportiert, wobei sie im Klartext vorliegt und mit eigenen Skripten oder Programmen ausgewertet werden kann. Wählt man „Outlook-Datendatei (.pst)“, wird die E-Mail als PST Datei exportiert. Dabei handelt es sich um ein proprietäres Dateiformat von MS und die E-Mail liegt als Binärdatei vor, wobei eine Kompression erfolgt und dadurch ein geringerer Speicherplatzbedarf nötig ist. In diesem Fall wird der Export als CSV Datei ausgewählt.



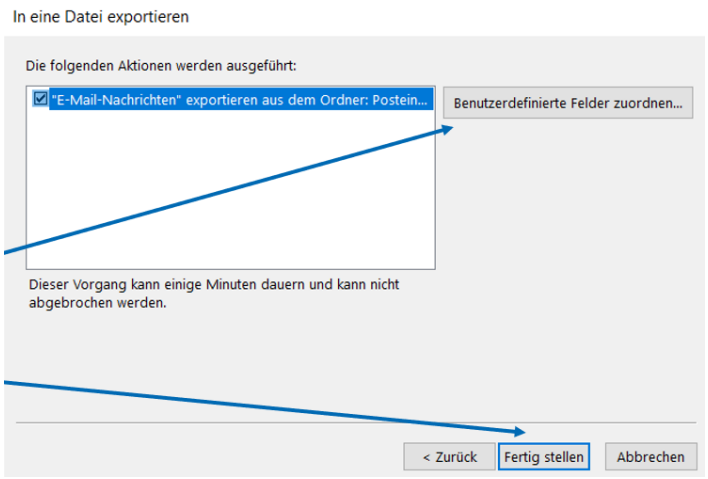
Anschließend wählt man den Ordner aus, aus welchem die E-Mails exportiert werden sollen.



Daraufhin legt man den Speicherort fest, wo die exportierte Datei abgelegt werden soll.

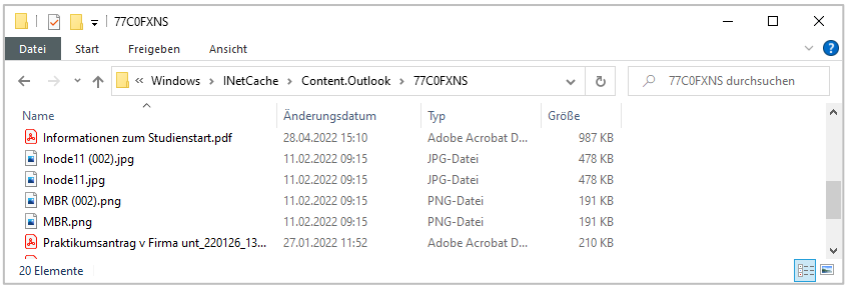


Im letzten Fenster werden die auszuführenden Aktionen angezeigt. Über den Button „Benutzerdefinierte Felder zuordnen..“ lässt sich der CSV-Header umbenennen. Über den Button „Fertig stellen“ wird der Export durchgeführt.



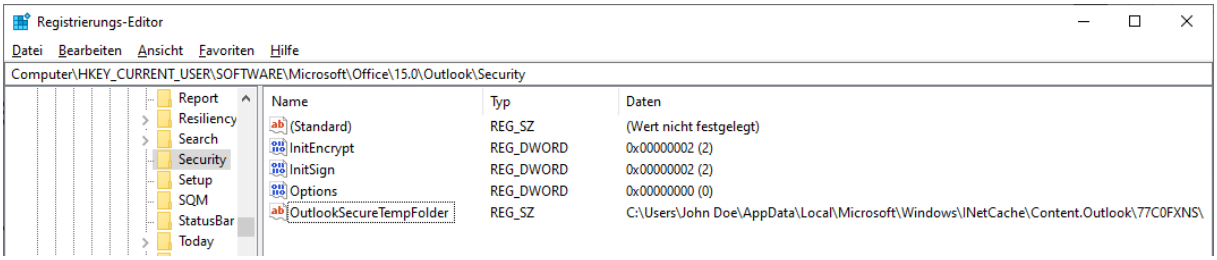
Outlook E-Mails Attachments

Dateianhänge die als sicher gelten, legt Outlook temporär ab. Als Standard wird hierfür der OLK Ordner unter dem Pfad „\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\[KENNUNG]\“ abgelegt. Hier können geöffnete oder bereits wieder gelöschte Attachments festgestellt werden.



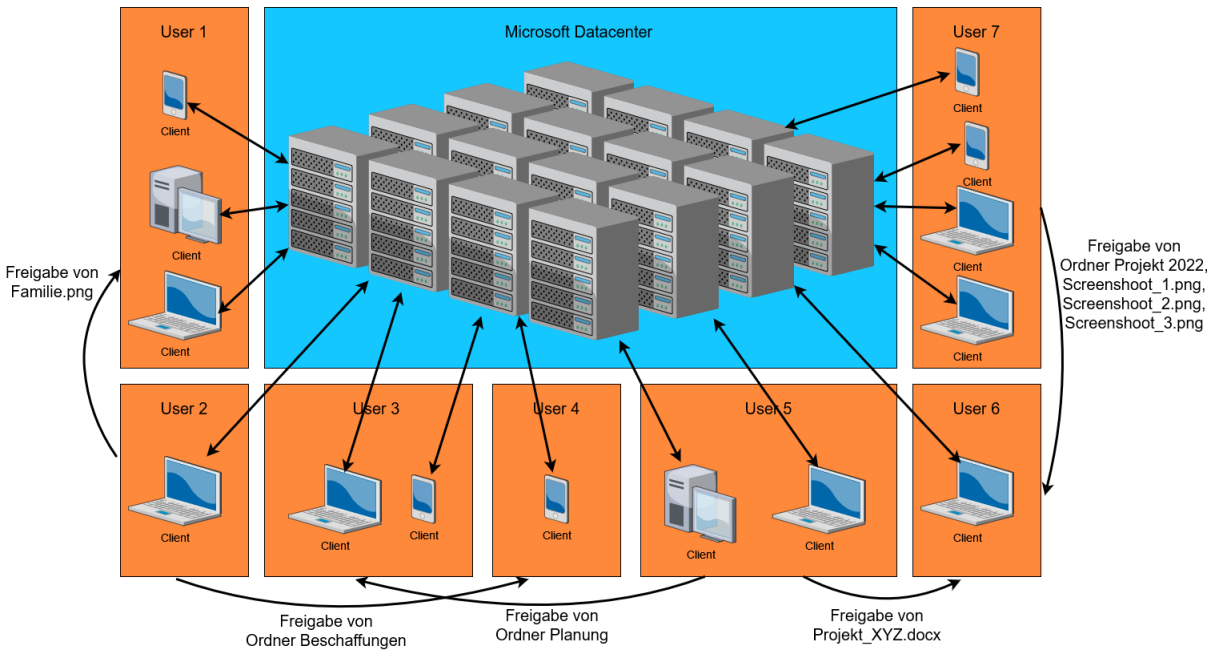
Der OLK wird in der Windows Registry als „HKEY_CURRENT_USER\Software\Microsoft\Office\ {OUTLOOKVERSION}\Outlook\Security“ abgelegt. {OUTLOOKVERSION} stellt die Versionsnummer von Outlook dar:

- 12.0 = Outlook 2007
- 14.0 = Outlook 2010
- 15.0 = Outlook 2013
- 16.0 = 365
- etc.



1.9.2 OneDrive

Bei OneDrive handelt es sich um ein Cloud Storage Anbieter. Cloud Storage funktioniert, in dem lokale Ordner für die Cloud-Synchronisation festgelegt werden. Die entsprechenden Daten werden dann mit den Servern synchronisiert. Andere Clients landen die Daten vom Server. Die Freigabe für die Daten oder die Ordner kann an andere Nutzer erteilt werden. Dann laden die Clients der anderen Nutzer die freigegebenen Daten vom Server.



1.9.2.1 OneDrive Symbologie

Beruflicher Account, Privater Account

Nicht angemeldet

Synchronisierung Fehlgeschlagen

Synchronisierung Warnung

Synchronisierung Angehalten

Synchronisierung in Progress

Synchronisierung blockiert durch blockiertes Konto

Synchronisierung verhindert (z.B. durch Admin)

Lokal gespeichert, von Cloud synchronisiert

Datei wurde als „immer auf diesem Gerät speichern“ markiert

Datei nur online gespeichert

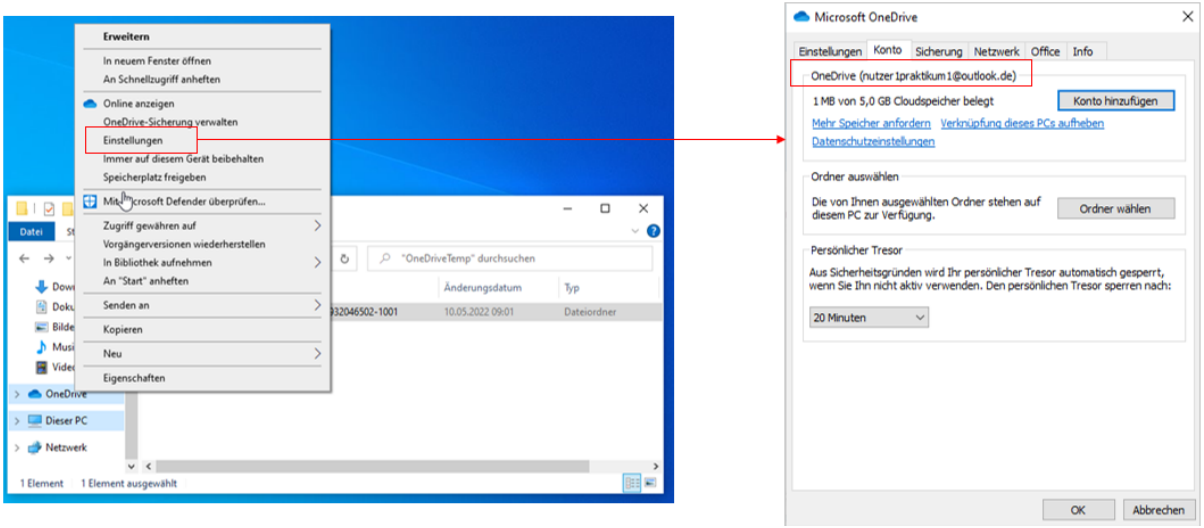
Datei für andere Nutzer freigegeben

Datei wurde von anderem Nutzer freigegeben

Synchronisierung der Datei / Ordner nicht erlaubt

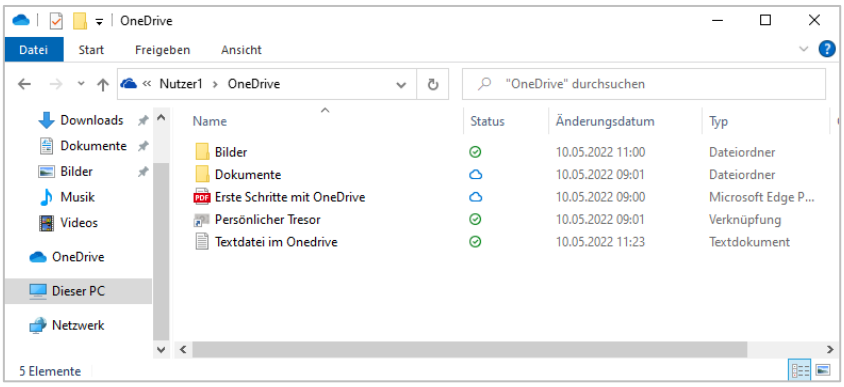
1.9.2.2 OneDrive App

In den Einstellungen wird das Konto angezeigt:



1.9.2.3 Standard-Speicherorte

Standardmäßig erfolgt die Speicherung unter Windows im Ordner C:\Users\<Benutzer>\OneDrive-<OneDrive-Name>. In diesem Ordner werden die synchronisierten Ordner aufgelistet. Standardmäßig befinden sich dort Bilder, der Desktop, Dokumente und Microsoft Teams-Chatdateien.



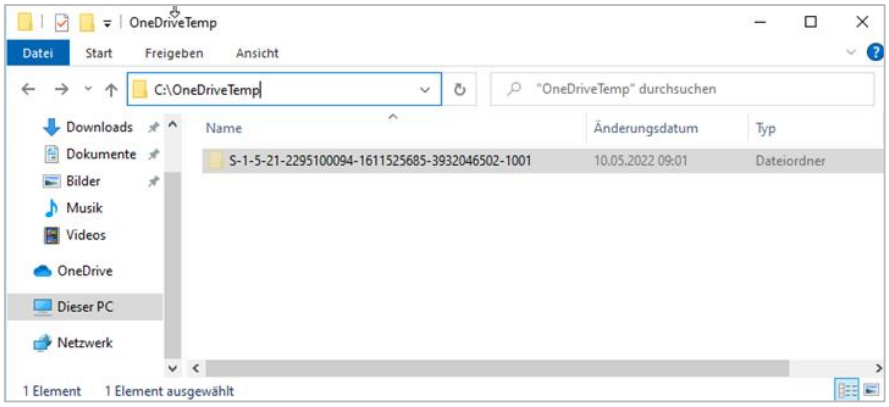
Log Dateien befinden sich im Ordner „\Users\<USERNAME>\AppData\Local\Microsoft\OneDrive\logs“. Dieser hat die Unterverzeichnisse Common und Personal. Der Ordner Personal enthält die Datei SyncEngine.odl, welche logs der Synchronisation wie synchronisierte Dateien und Datei-Hashes enthält, die Datei Trace.ETL, welche die Log Dateien TraceCurrent.ETL und TraceArchive.ETL zur Ablaufverfolgung enthält, und die Datei SyncDiagnostics.txt, welche eine Logdatei mit aktuellen Synchronisationsinhalten ist. Die Log Dateien sind nur mit Zusatzsoftware lesbar:

Timeline View | **Artifact View** | Reporting

OneDrive (Win Apps) Items — OneDrive MountPoin

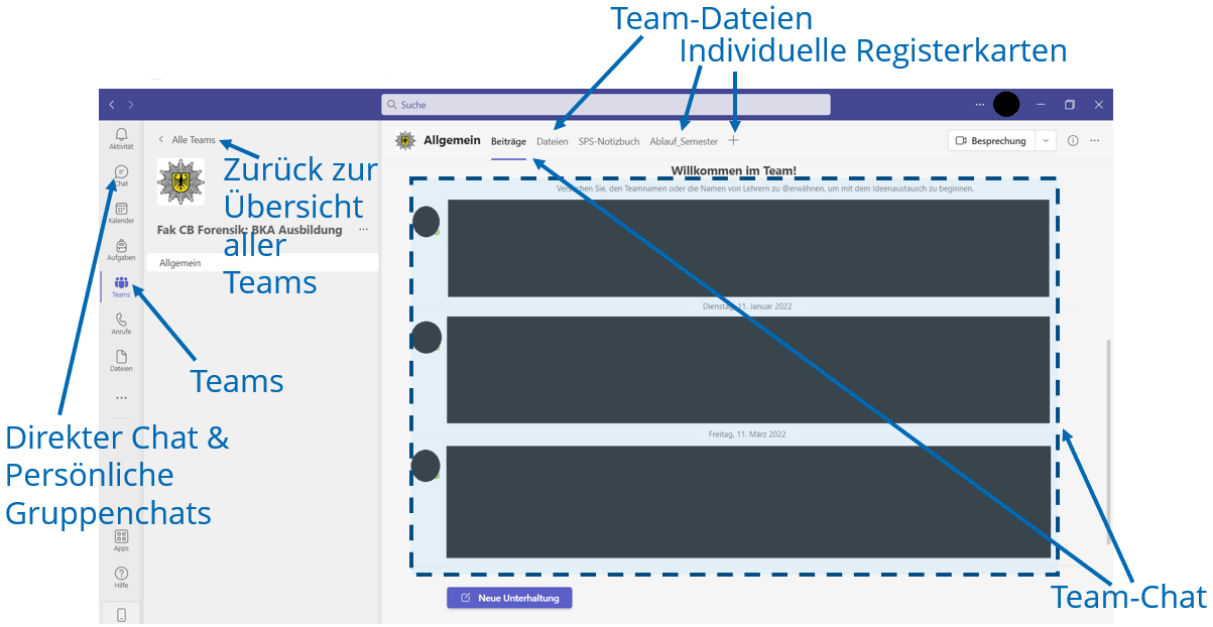
Time (UTC)	Time Description	#Last Modification on Drive	#Name	#Extension	#Item Icon Type	#Owner Name	#Is Offline	#Creation Date	#Taken Date
<Timeless Entry>	<Timeless Entry>	2017-03-20 00:09:49 GMT+03:00	<Value not available>	<Value not ...	NonEmptyDocumen...	Sena Dagistanli	No	2017-03-20 00:09:...	<Value not av...
03/19/2017 21:09:49	Item last modifi...	2017-03-20 00:09:49 GMT+03:00	Belgeler	<Value not ...	NonEmptyDocumen...	Sena Dagistanli	No	2017-03-20 00:09:...	<Value not av...
03/19/2017 21:09:49	Item last modifi...	2017-03-20 00:09:49 GMT+03:00	Resimler	<Value not ...	NonEmptyAlbum	Sena Dagistanli	No	2017-03-20 00:09:...	<Value not av...
03/19/2017 21:09:49	Item last modifi...	2017-03-20 00:09:49 GMT+03:00	<Value not available>	<Value not ...	<Value not available>	Sena Dagistanli	No	<Value not availab...	<Value not av...
03/19/2017 21:09:50	Item last modifi...	2017-03-20 00:09:50 GMT+03:00	E-posta ekleri	<Value not ...	NonEmptyDocumen...	Sena Dagistanli	No	2017-03-20 00:09:...	<Value not av...
03/19/2017 21:09:50	Item last modifi...	2017-03-20 00:09:50 GMT+03:00	OneDrive'ı kullanmaya başlama	.pdf	Pdf	Sena Dagistanli	Yes	2017-03-20 00:09:...	<Value not av...
03/19/2017 21:20:49	Item last modifi...	2018-08-01 16:35:45 GMT+03:00	Sena Resume-6	.docx	Docx	Sena Dagistanli	No	2017-03-20 00:20:...	<Value not av...
03/19/2017 21:28:23	Item last modifi...	2018-08-01 17:10:06 GMT+03:00	testsharingfrom Sena To Kabile	.docx	Docx	Sena Dagistanli	No	2017-03-20 00:28:...	<Value not av...
05/23/2018 20:35:46	Item last modifi...	2018-05-23 23:35:46 GMT+03:00	Ekran Görüntüleri	<Value not ...	NonEmptyAlbum	Sena Dagistanli	No	2018-05-23 23:35:...	<Value not av...
07/11/2018 12:36:04	Item last modifi...	2018-07-11 15:36:04 GMT+03:00	INNA - Nirvana Official Music Video	.mp3	Audio	Sena Dagistanli	No	2018-08-01 17:22:...	<Value not av...
08/02/2018 08:46:34	Item last modifi...	2018-08-02 11:46:34 GMT+03:00	Shared	.txt	Txt	Sena Dagistanli	No	2018-08-02 11:46:...	<Value not av...
08/16/2018 12:00:07	Item last modifi...	2018-08-16 15:00:44 GMT+03:00	Document	.docx	Docx	Sena Dagistanli	No	2018-08-16 15:00:...	<Value not av...
08/16/2018 12:04:18	Item last modifi...	2018-08-16 15:04:41 GMT+03:00	sample excel shared by sena to kabile	.xlsx	Xlsx	Sena Dagistanli	No	2018-08-16 15:04:...	<Value not av...
08/16/2018 12:11:30	Item last modifi...	2018-08-16 15:11:30 GMT+03:00	SHARED NOTE FROM SENA TO KABILE	<Value not ...	Notebook	Sena Dagistanli	No	2018-08-16 15:11:...	<Value not av...
08/16/2018 12:11:31	Item last modifi...	2018-08-16 15:12:03 GMT+03:00	<Value not available>	.onetoc2	Onetoc2	Sena Dagistanli	No	2018-08-16 15:11:...	<Value not av...
08/16/2018 12:11:33	Item last modifi...	2018-08-16 15:11:49 GMT+03:00	Quick Notes	.one	One	Sena Dagistanli	No	2018-08-16 15:11:...	<Value not av...
08/16/2018 12:11:52	Item last modifi...	2018-08-16 16:57:15 GMT+03:00	SEC2	.one	One	Sena Dagistanli	No	2018-08-16 15:11:...	<Value not av...
09/05/2018 12:54:58	Item last modifi...	2018-09-05 15:54:58 GMT+03:00	samplefordeleted	.txt	Txt	Sena Dagistanli	No	2018-09-05 15:54:...	<Value not av...
09/05/2018 13:07:15	Item last modifi...	2018-09-05 16:07:24 GMT+03:00	CCapture (2)	.mp4	Video	Sena Dagistanli	No	2018-09-05 16:07:...	2018-09-05 1...
09/05/2018 13:07:50	Item last modifi...	2018-09-05 16:07:50 GMT+03:00	CCapture (3)	.jpg	Photo	Sena Dagistanli	No	2018-09-05 16:07:...	2018-09-05 1...

Weiterhin gibt es einen temporär Ordner mit der Benutzer SID auf dem Laufwerk C:\:



1.9.3 Microsoft Teams

Microsoft Teams ist ein Tool für kollaboratives Arbeiten. Dateien können hier parallel bearbeitet werden und dessen Synchronisation erfolgt über die Microsoft-Cloud. Ebenfalls sind in Teams ein Chat und die Möglichkeit für Video-Konferenzen integriert. Das Team ist eine Gruppe von Nutzern, welche über den Chat kommunizieren können und eine gemeinsame Dateienfreigabe sowie einen gemeinsamen Kalender haben. Die folgende Abbildung zeigt den Aufbau der Microsoft Teams Anwendung.



Die Dateien von Microsoft Teams sind auf den Microsoft Servern in der Cloud hinterlegt. Wenn eine Datei bearbeitet wird, wird eine temporäre Datei angelegt. Das lokale Speichern von Dateien gilt als Download, sodass die heruntergeladenen Dateien standardmäßig im Download-Ordner zu finden sind. Dateien, welche im Chat geteilt werden, befinden sich im Ordner C:\Users\<Benutzer>\OneDrive-<OneDrive-Name>\Microsoft Teams-Chatdateien.

1.9.4 Andere Cloud-Software

1.9.4.1 Amazon Chime

Amazon Chime ist ein Konferenztool, wobei alle Funktionen im Browser nutzbar sind. Die Dateisynchronisation erfolgt über den Amazon S3-Cloud-Storage. Hierbei handelt es sich nicht um eine Office Suite.

1.9.4.2 Google Workspace

Google Workspace ist proprietär und hat Funktionen wie E-Mail (GMail), Kalender, Textdokumente (Google Docs), Tabellen (Google Sheets), Präsentationen (Google Slides), Cloud Speicher (Google Drive) und Video-Konferenzen (Google Meet) integriert. Alle Anwendungen sind über den Webbrowser bedienbar.

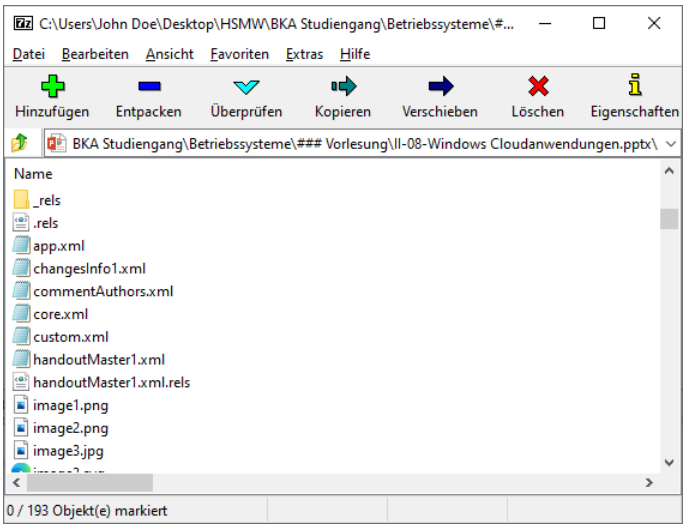
1.9.4.3 Nextcloud

Nextcloud hat Funktionen wie den Kalender, E-Mail (externer E-Mail-Server), Textdokumente (Libre Writer), Tabellen (Libre Calc), Präsentationen (Libre Impress), Cloud Storage und Video-Konferenzen (Nextcloud-Talk) integriert. Auch hier sind alle Funktionen über den Webbrowser bedienbar. Nextcloud ist eine Open Source Software und privates Hosting auf der eigenen Hardware ist möglich.

1.9.5 Microsoft Office Suite

Die Microsoft Office Suite setzt sich aus mehreren Anwendungen zusammen. Dazu gehören Microsoft Word (Textdokumente), Microsoft Power Point (Präsentationen) und Microsoft Excel (Tabellenkalkulation). Weitere Anwendungen der Microsoft Office Suite sind Microsoft Outlook (E-Mail-Client), Microsoft OneNote (Notizen), Microsoft OneDrive (Cloud-Speicher), Microsoft Teams (Team Kommunikation und Organisation) und Microsoft Access (Datenbankzugriff).

Microsoft Office Dateiformate wie *.doc**x** sind gepackte Dateien. Das Speicherformat ist somit eine ZIP-Datei. Die Dateien können mit einem ZIP-Programm entpackt werden. Bilder werden hier ohne Vorverarbeitung (Skalierung, etc.) hinterlegt und Texte und Templates sind zum Teil in XML enthalten.



Für ein schnelleres Arbeiten kann man Vorlagen verwenden. Formatvorlagen für Texte werden in Word bereitgestellt. In Power Point gibt es Masterfolien als Vorlage für Präsentationfolien. Überschriften lassen sich mit einer entsprechenden Formatvorlage direkt formatieren. Weiterhin kann man das Inhaltsverzeichnis automatisch generieren und die Farben global über das Design ändern.

Im Folgenden werden einige Tastenkürzel vorgestellt:

- Strg + c = Kopieren
- Strg + v = Einfügen
- Strg + x = Ausschneiden
- Strg + t = nur Text beim Einfügen (Formatierung wird nicht übernommen)
- Strg + Umschalt + c = Format kopieren
- Strg + Umschalt + v = Format einfügen

1.9.6 Zusammenfassung

Sie kennen nun die Übertragungsprotokolle von E-Mail. Dazu gehören SMTP, POP3 und IMAP. Für E-Mail haben Sie viele Server- und Client-Software vorgestellt bekommen. Für Microsoft Outlook wurde sich insbesondere der Designaufbau und die Exportmöglichkeit angeschaut.

Sie haben einen Überblick über die Cloud-Anwendungen OneDrive, Teams und die Microsoft Office Suite erhalten. Dazu sollte ihnen das generelle Aufgabengebiet der Anwendungen bekannt sein.

Darüber hinaus wurden einige Alternativen zu Microsoft Anwendungen vorgestellt.

1.10 Windows Virtualisierung

1.10.1 Wiederholung Virtualisierung

Bei der Virtualisierung wird eine zusätzliche Abstraktionsebene zwischen Hard- und Software gezogen, um Hard- und Software voneinander zu trennen. Das Ziel der Virtualisierung ist eine bessere Auslastung der Hardware. Dabei bringt die Einsparung von Ressourcen gleichzeitig auch eine Einsparung der Kosten mit sich. Die Abstraktion dient der vereinfachten Wartung, vor allem in Netzwerklaufwerken. Weiterhin gibt es mit der Virtualisierung die Möglichkeit, verschiedene Betriebssysteme auf der gleichen Hardware aufzusetzen. Die Gastsysteme sind untereinander sowie auch vom Hostsystem abgekapselt, was ein wichtiger Sicherheitsaspekt ist. Ein weiterer Vorteil der Virtualisierung ist die Ausfallsicherheit, da virtuelle Maschinen bei Problemen on the fly auf ein anderes System migriert werden können (Livemigrierung). Ebenfalls ist durch die Virtualisierung eine Emulation systemferner Hardware wie ARM, PowerPC oder Game Boy möglich.

1.10.1.1 Virtualisierungsbereiche

Es gibt verschiedene Bereiche, welche virtualisiert werden können. Es gibt die Möglichkeit der Hardwarevirtualisierung. Diese wird in Mainframe-Computern (LPAR) eingesetzt und mithilfe einer Emulation durchgeführt. Ein Vertreter hierfür ist Java-Virtual-Machine.

Die Speichervirtualisierung wird als Storage Attached Network (SAN) umgesetzt. Ein Vertreter hierfür ist der Linux Logical Volume Manager (LLVM).

Die Netzwerkvirtualiserung wird mithilfe von VLANs oder dem Software Defined Network oder VPN umgesetzt.

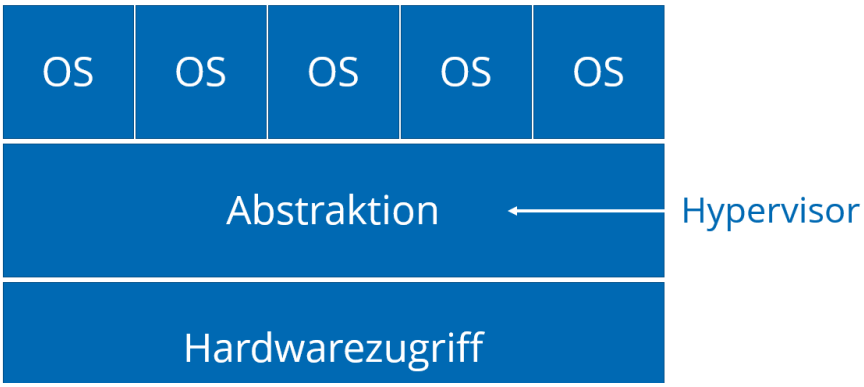
Eine weitere bedeutende Form der Virtualisierung ist die Systemvirtualisierung, wobei ein gesamtes System virtualisiert wird. Hierfür wird ein Hypervisor (KVM, VMWare, Hyper-V, Virtual Box) eingesetzt, welcher die Aufteilung der physischen Hardware auf die Gastsysteme durchführt.

Weiterhin gibt es die Betriebssystemvirtualisierung, wofür Container wie Docker, Jail, Zone oder LXC eingesetzt werden.

Die Desktopvirtualisierung kann über Critix VirtualDesktop, VMware Horizon oder X2Go durchgeführt werden.

Die letzte Variante ist die Softwarevirtualisierung. Diese kann mit Honey-Pod, Windows-XP-Modus, Wine (unter Linux) oder portable Software realisiert werden.

1.10.1.2 Grundlegender Aufbau

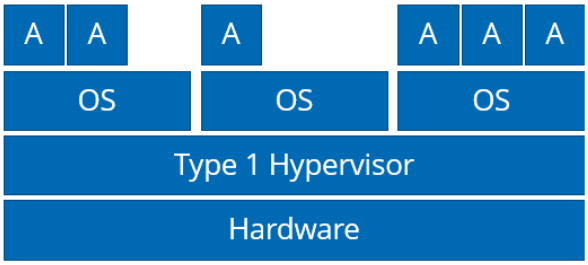


1.10.1.3 Hypervisor Aufgaben

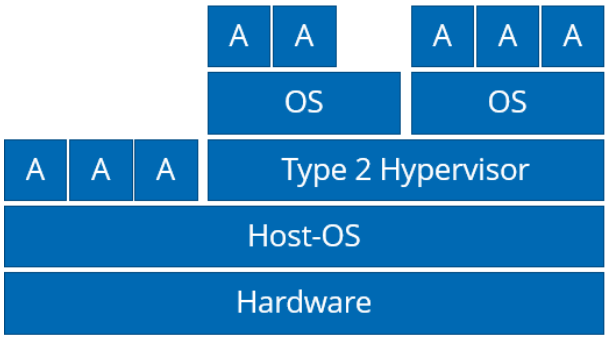
Der Hypervisor abstrahiert die physische Hardware und stellt sie als virtuelle Ressourcen bereit. Weiterhin teilt er den Gastsystemen diese Ressourcen zu. Bei den Ressourcen handelt es sich um den Prozessor, den Arbeitsspeicher, die Laufwerke (Diskette, CD, DVD, HDD, SSD), die Netzwerke (Zugriff extern, Internes Netzwerk zwischen VMs), die Grafikkarte und I/O-Geräte (USB, Audio, ..). Eine weitere Aufgabe des Hypervisors ist die Verwaltung von Rechten.

1.10.1.4 Hypervisor Typen

Es gibt zwei Typen von Hypervisoren. Der Hypervisor Typ 1, auch nativ oder bare-metal genannt, läuft direkt auf der Hardware, weshalb kein zusätzliches Host Betriebssystem benötigt wird. Der Hypervisor besitzt hierbei einen Treiber für die Hardware und ist sehr performant.



Der zweite Typ ist der hosted Hypervisor. Dieser läuft als Anwendung unter einem Host Betriebssystem. In diesem Fall nutzt der Hypervisor die Treiber des Host-OS.



1.10.1.5 Hypervisor Kommunikationsmodelle

Eine Möglichkeit ist die Vollvirtualisierung. In diesem Fall weiß das Gastbetriebssystem nichts von der Virtualisierung. Ein Vorteil ist, dass die Gastbetriebssysteme nicht angepasst werden müssen.

Bei der Paravirtualisierung kennt das Gastbetriebssystem hingegen den Hypervisor. Mit sogenannten Hypercalls kann das Gast-OS mit dem Hypervisor statt mit der Hardware kommunizieren. Hierfür sind jedoch Anpassungen des Gast-OS nötig. Eine weitere Möglichkeit ist die Betriebssystem-Virtualisierung. In diesem Fall nutzt das Gast-OS die Infrastruktur (den Kernel) vom Host Betriebssystem. Hierbei erzeugt der Art „Hypervisor“ einen geringeren Overhead und ist nur für die Rechteverwaltung zuständig. Diese Variante wird daher eher selten als Hypervisor bezeichnet.

1.10.1.6 Hypervisor Software

Im Folgenden werden verschiedene Softwareanwendungen aufgezählt, mit welchen sich die beiden Hypervisor Typen realisieren lassen.

Typ 1

- Hyper-V
- VMware ESXi
- Citrix XenServer
- z/VM

Typ 2

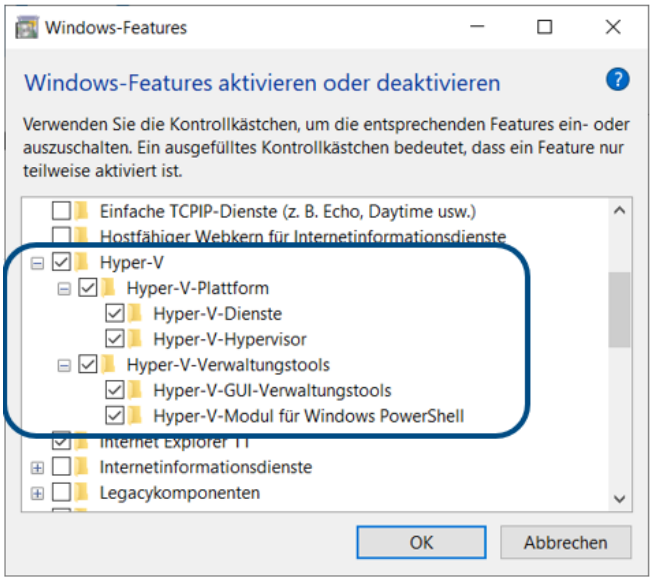
- Hyper-V
- Docker, LXC, OpenVZ, Linux VServer
- VirtualBox
- Proxmox VE
- KVM
- QEMU
- VMware Fusion
- WSL, WoW, Virtual DOS Machine

1.10.2 Microsoft Hyper-V

Für die Verwendung von Microsoft Hyper-V sind einige Voraussetzungen nötig. Es wird eine 64-Bit CPU benötigt. Ebenfalls ist eine Hardware-Assisted Virtualization wie AMD-V und Intel-VT nötig. Eine weitere Voraussetzung ist Hardware-enabled data execution prevention (DEP) mit XD-bit Intel (Execution Disabled) und NX-bit AMD (no Execution). Als letzte Voraussetzung wird eine gültige Lizenz benötigt, welche Teilweise schon im Betriebssystem enthalten ist.

1.10.2.1 Installation

Für die Installation müssen in den Windows-Features die Hyper-V Features aktiviert werden. Anschließend erfolgt ein Neustart des PCs. Im Startmenü wählt man Windows Verwaltungsprogramme und dann Hyper-V-Schnellerstellung. Falls der Hyper-V nicht im Startmenü angezeigt wird, so fehlt https://www.microsoft.com/en-us/download/details.aspx?id=45520 (WindowsTH-KB2693643-x64). Nach der Installation erfolgt ein erneuter Neustart.



1.10.2.2 VM Komponenten

Zu den Komponenten der VM zählen die Konfigurationsdatei und die Virtual Hard Disk. Die Konfigurationsdatei ist im XML-Format und enthält Hardwaredetails wie Informationen zu den CPU-Kernen, dem RAM, dem HDD-Speicherplatz oder Ähnlichem. Weiterhin werden dort VM-Einstellungen festgelegt. Hierzu zählen beispielsweise die Rechte für den Netzwerk- oder I/O-Zugriff.

Die Virtual Hard Disk besitzt eine feste Größe, falls die Dateiendung .vhd ist. Die Größe ist dynamisch und wird somit beim Schreiben immer größer, wenn die Dateiendung .vhdx lautet. Die Virtual Hard Disk speichert Daten der VM.

1.10.2.3 Netzwerkanschlüsse

	External	Internal	Private
Host-externes Netzwerk	Ja	Nein	Nein
Host System	Ja	Ja	Nein
Andere VMs	Ja	ja	Ja

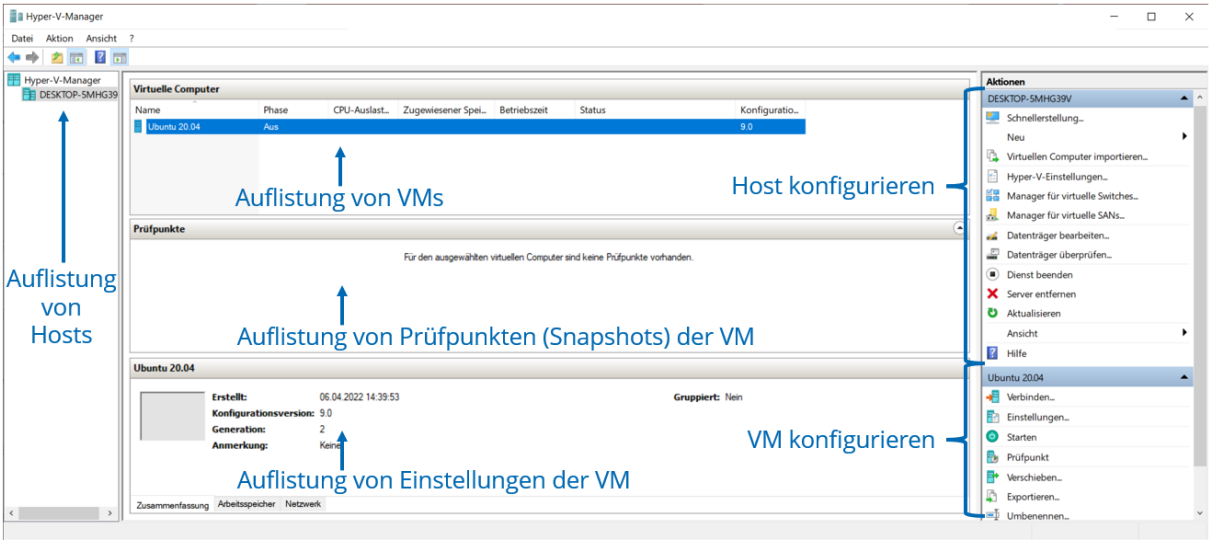
1.10.2.4 Interaktion mit VMs

Die Hyper-V-Schnellerstellung (Hyper-V Quick Create) ist für das Erstellen von VMs aus Vorlagen von Microsoft verantwortlich (Stand 06.04.2022). Hierfür kann man manuell ein ISO auswählen oder es stehen verschiedene Vorlagen zur Verfügung:

- Ubuntu 18.04 LTS
- Ubuntu 19.10
- Ubuntu 20.04
- Windows-11-Entwicklungsumgebung

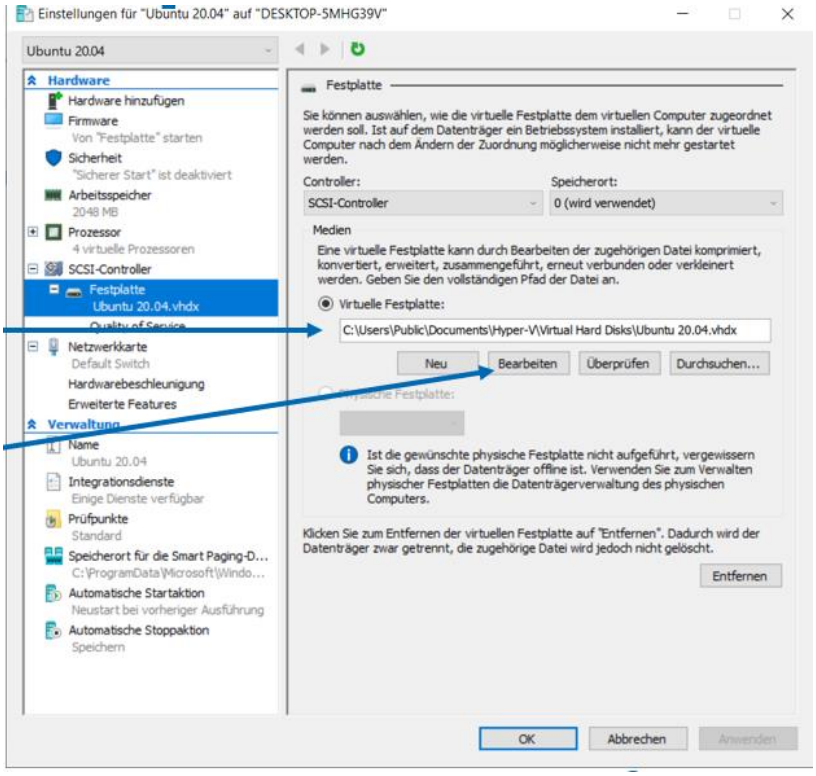
Der Hyper-V Manager ist für die Verwaltung von VMs zuständig. Dabei handelt es sich um das Erstellen, das Löschen, das Verändern und das Starten und Stoppen von virtuellen Maschinen.

1.10.2.5 Hyper-V Manager



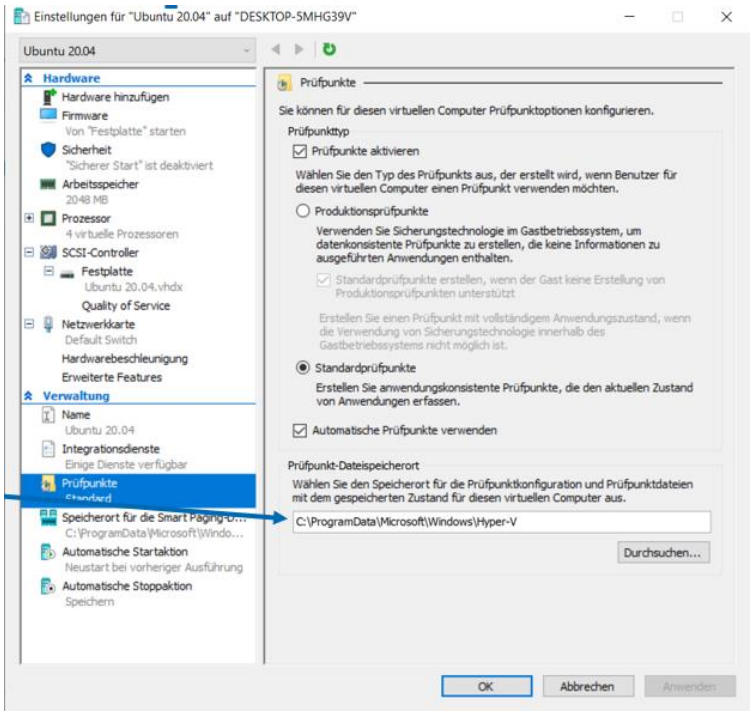
1.10.2.6 Hyper-V Festplatte Speicherorte

Standardmäßig wird die Festplatte unter C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks gespeichert. Jedoch ist dieser Speicherort für jede Festplatte änderbar. In der Konfiguration kann man den Speicherort angeben. Über den Button „Bearbeiten“ kann die Festplatte zusätzlich komprimiert werden.



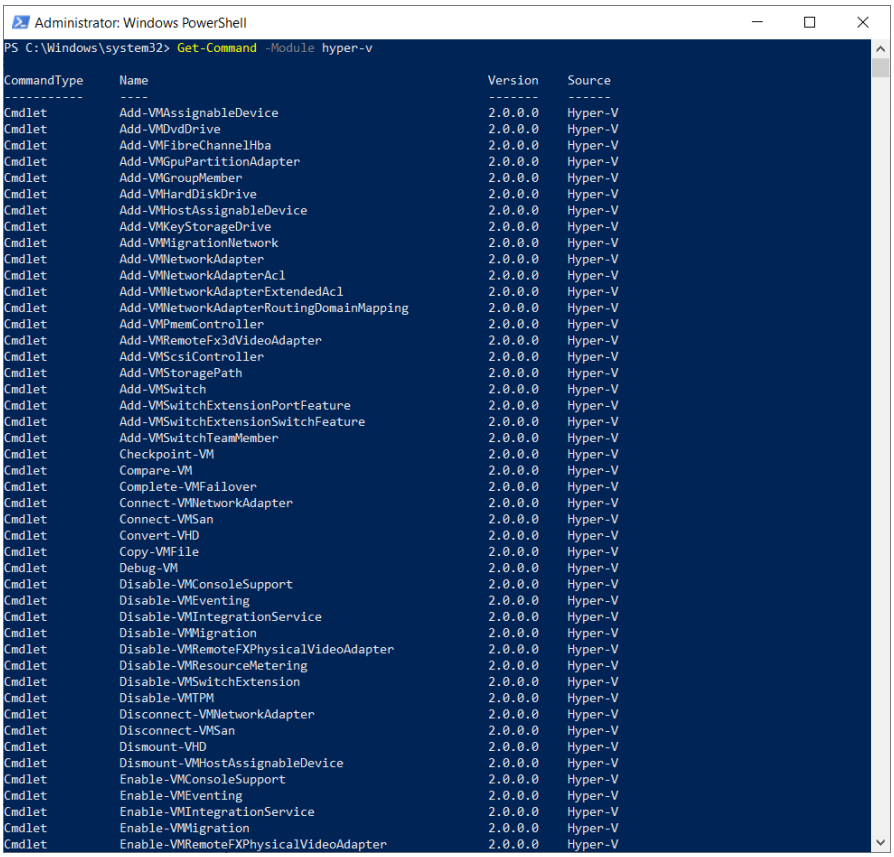
1.10.2.7 Hyper-V Prüfpunkte Speicherorte

Die Prüfpunkte für die Speicherorte sind Snap-Shots. Diese zeigen da Abbild zu einem bestimmten Zeitpunkt und sind somit eine Art „Foto“ einer VM. Diese befinden sich standardmäßig unter „C:\ProgramData\Microsoft\Windows\Hyper-V“. Auch dieser Speicherort ist für jede VM änderbar und ist in der Konfiguration anpassbar.



1.10.2.8 Hyper-V mit PowerShell

Der Befehl Get-Command -Module hyper-v bietet eine Übersicht über alle PowerShell-Befehle. Da Hyper-V Administratorrechte benötigt, werden auch für die PowerShell Administratorrechte benötigt.



1.10.2.9 Wichtige PowerShell-Befehle

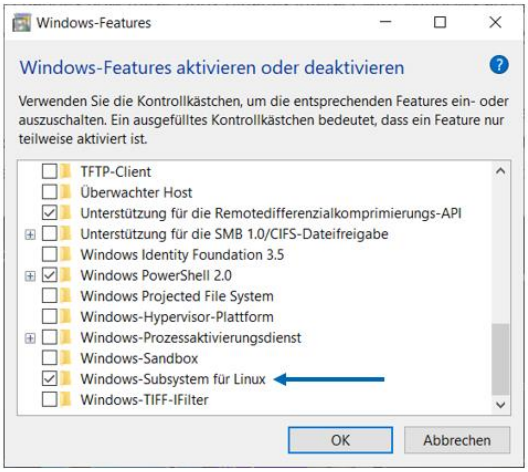
Im Folgenden werden wichtige PowerShell-Befehle aufgelistet:

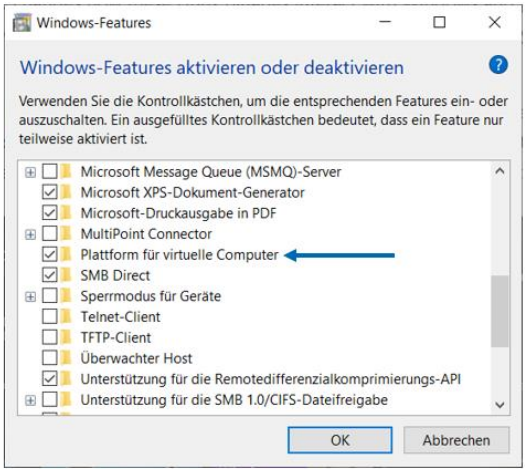
- Get-VMHostCluster
  - Hyper-V-Cluster auflisten
- Get-VMHost
  - Hyper-V-Hosts auflisten
- Get-VM
  - VMs auflisten
- Get-VMHardDiskDrive
  - Festplatten mit Speicherort auflisten
- Mount-VHD
  - Virtuelle Festplatte einbinden
- Get-VMNetworkAdapter
  - Netzwerkanschlüsse mit MAC-Adresse auflisten
- Get-VMNetworkAdapterVlan
  - VLAN von NetzwerkAdaptern auflisten

- Get-VMSnapshot
    - Prüfpunkte einer VM auflisten
- Export-VM
    - VM exportieren
- Import-VM
    - VM importieren

1.10.3 Windows Subsystem for Linux

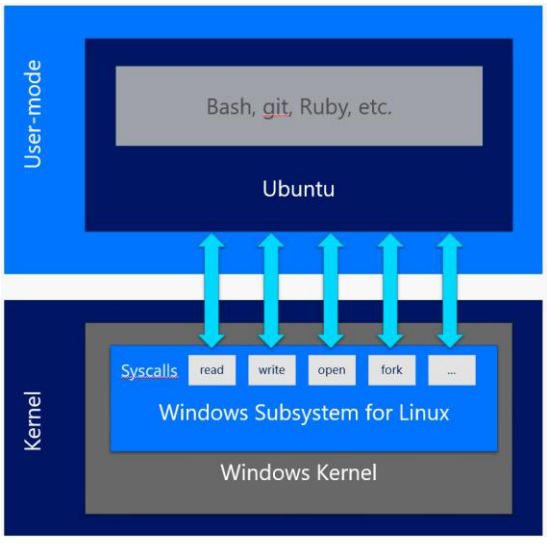
Die Voraussetzung für Windows Subsystem for Linux ist Windows 10 oder höher. Weiterhin müssen die entsprechenden Systemfeatures aktiviert werden.





1.10.3.1 Aufbau

Mithilfe des LXSS-Manager Service werden die Linux-Befehle erkannt. Die Ausführung wird an das Subsystem übergeben, wobei das Linux-Subsystem einen Windows-Kernel nutzt. Dieser wurde durch eine Linux-Kernel-API erweitert. Das Linux-Subsystem kann auch eine Windows-API nutzen. Weiterhin ist ein Windows Filesystem im Linux-Subsystem gemountet.



1.10.3.2 Ist WSL eine VM?

WSL ist keine VM, sondern es ist eher mit Docker vergleichbar. WSL nutzt einen Windows-Kernel wohingegen WSL2 einen Linux-Kernel verwendet. Ebenfalls erfolgt keine Virtualisierung der Hardware.

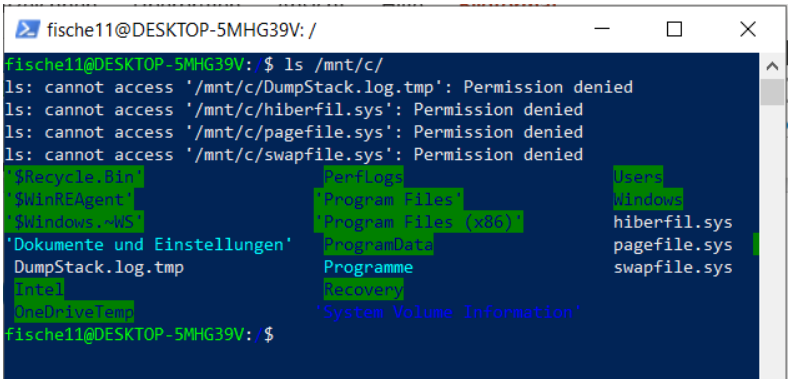
1.10.3.3 WSL1 vs. WSL2

WSL1 bzw. WSL ist das erste Linux Subsystem. Linux-Kernel Aufrufe werden hierbei in Windows-Kernel Aufrufe übersetzt, woraus eine schlechte Performance resultiert. Es kann als „Beta-Version“ angesehen werden.

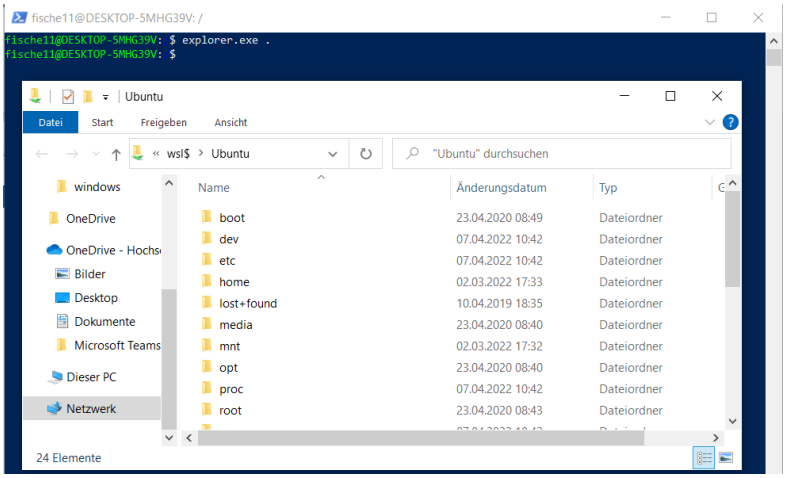
WSL2 hat eine deutliche Performanceverbesserung insbesondere in Bezug auf die Read/Write-I/O. Es bietet eine vollständige Kompatibilität, da alle Kernel-Funktionen enthalten sind. Weiterhin enthält es einen echten Linux-Kernel in einer kleinen VM und bietet Schnittstellen zu anderen Programmen, wie beispielsweise die Windows Docker-GUI.

1.10.3.4 Dateieinbindung

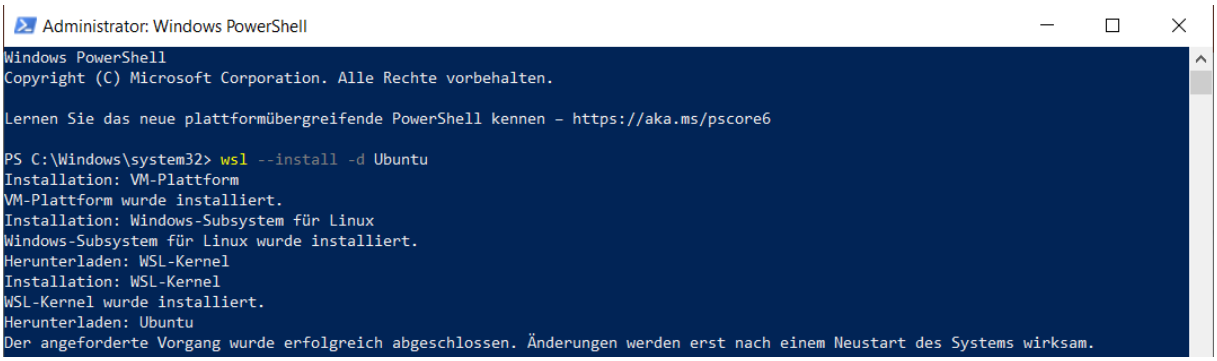
Windows Dateien werden in WSL unter /mnt/<Laufwerk-Buchstabe>/ eingebunden.



WSL-Distro Dateien werden in Windows unter „\\wsl$\<DistroName>“ gespeichert. Das Öffnen wird in WSL-Distro mit dem Befehl explorer.exe durchgeführt.



1.10.3.5 Installation



1.10.3.6 Unterstützte Distributionen

Alle Distributionen werden unterstützt und können als .tar-Datei importiert werden. Über den Microsoft Store sind direkt die Distributionen Ubuntu, Kali, Debian und SUSE verfügbar.

1.10.3.7 Wichtige PowerShell-Befehle

Im Folgenden werden einige wichtige PowerShell-Befehle aufgelistet:

- wsl --list --online
  - Auflisten aller Distros im Microsoft-Repository
- wsl --list
  - Auflisten aller installierten Distros
- wsl --list --verbose
  - Auflisten der Zustände aller installierten Distros
- wsl --distribution <d> --user <u>
  - Einloggen als User u in Distro d
- wsl --install --distribution <d>
  - Distro installieren
- wsl --export <d> <f>
  - Distro d in Datei f exportieren
- wsl --import <d> <i> <f>
  - Distro d aus Datei f importieren
- wsl --terminate <d>
  - Distro Beendung erzwingen
- wsl --shutdown
  - Alle Distros und WSL-VM ausschalten

1.10.4 Zusammenfassung

Sie kennen nun die unterschiedlichen Ebenen der Virtualisierung. Darüber hinaus sind die zweit Hypervisor-Typen Ihnen nun bekannt.

Heute erhielten Sie einen Einblick in die Funktionsweise von Hyper-V und können diesen bedienen. Es ist Ihnen damit möglich VMs einzurichten. Außerdem haben Sie nun Kenntnis über die möglichen Netzwerkkommunikationsebenen zwischen VMs, Host und externen Geräten.

Ihnen ist nun der Begriff Windows Subsystem for Linux bekannt und sie können Linux-Subsysteme installieren. Sie kennen darüber hinaus den Unterschied zwischen Subsystem und VM.

Heute haben Sie außerdem gelernt, wie Sie Subsysteme und VMs mittels PowerShell cmdlets erstellen, sichern und steuern.