



Angewandte Computer- und Biowissenschaften



**HOCHSCHULE
MITTWEIDA**
University of Applied Sciences

Betriebssysteme

Systemeinrichtungen und Systemadministration

Autor: Tim Wetterau, B.Sc.

Stand: 16.05.2024



Bundeskriminalamt

Agenda

1. Installation
2. Bootprozess
3. Systemverwaltung
4. Konsolen
5. Geräte unter Windows
6. Dienste und Systemprozesse

Installation

Systemvoraussetzung Windows 10

- 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

Installationsmöglichkeiten

Manuelle Installation

- Update von Windows 7, 8, 8.1
- Wiederherstellung mittels Wiederherstellungspartition
- Installationsmedium
 - USB-Stick
 - DVD

private Nutzung
oder
Kleinunternehmen

Automatisierte Installation

- PXE-Boot (Installation über Intranet)
 - bevorzugt im Businessbereich zu verwenden
 - Falls nicht vorhanden wenden Sie sich an Ihren Admin

Behörde
oder
Großunternehmen

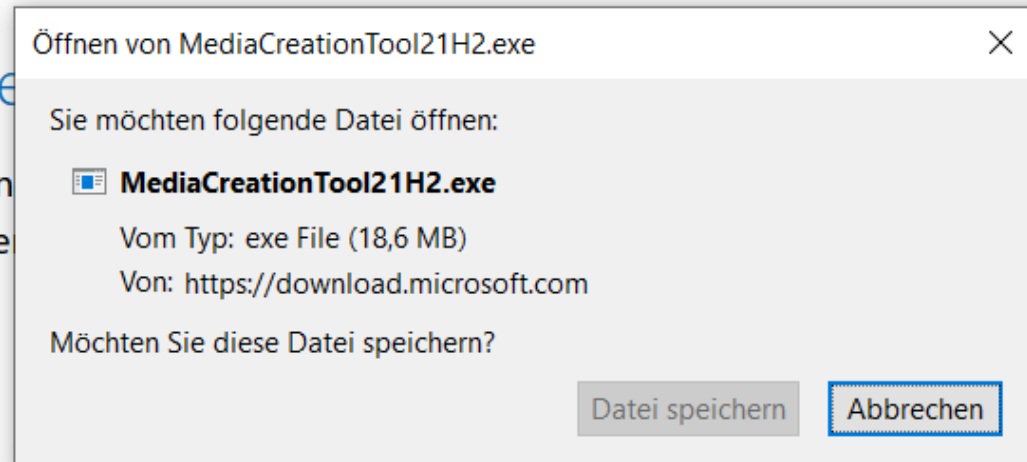
Installationsmedium (USB-Stick)

MediaCreationTool von Microsoft herunterladen und ausführen

Sie möchten Windows 10 auf Ihre

Zunächst benötigen Sie eine Lizenz zur Installation
Creation Tool herunterladen und ausführen. Weiter
zur Verwendung dieses Tools.


Tool jetzt herunterladen



Download: <https://www.microsoft.com/de-de/software-download/windows10>

Installationsmedium (USB-Stick)

- „Installationsmedium für einen anderen PC erstellen“ auswählen

 Windows 10 Setup



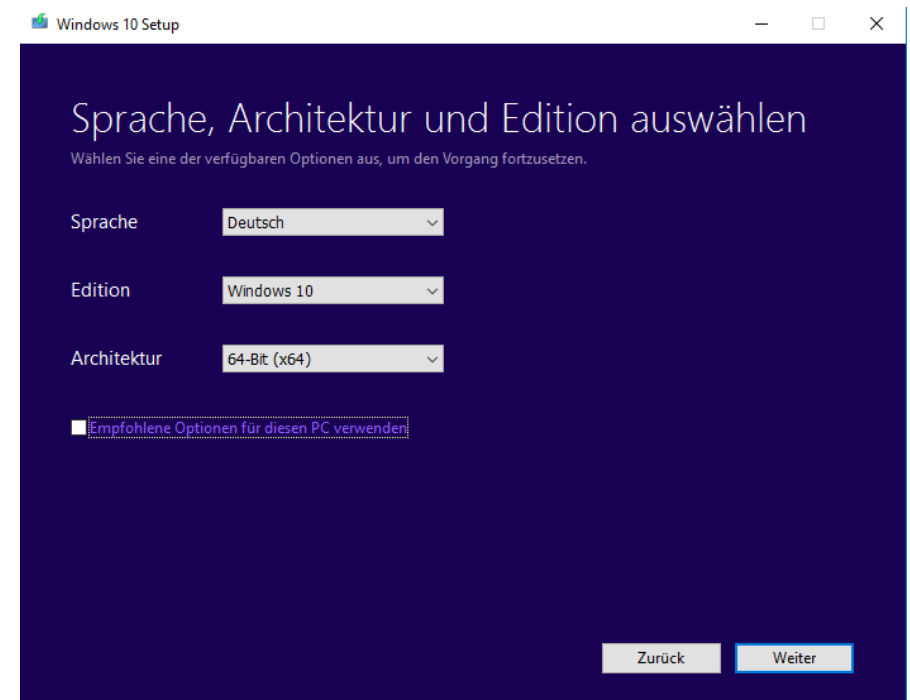
Wie möchten Sie vorgehen?

- Jetzt Upgrade für diesen PC ausführen
- Installationsmedien (USB-Speicherstick, DVD oder ISO-Datei) für einen anderen PC erst

- Windows Variante auswählen
- USB-Speicherstick auswählen
(USB-Stick mit mindestens 8GB erforderlich)

Installationsmedium (USB-Stick)

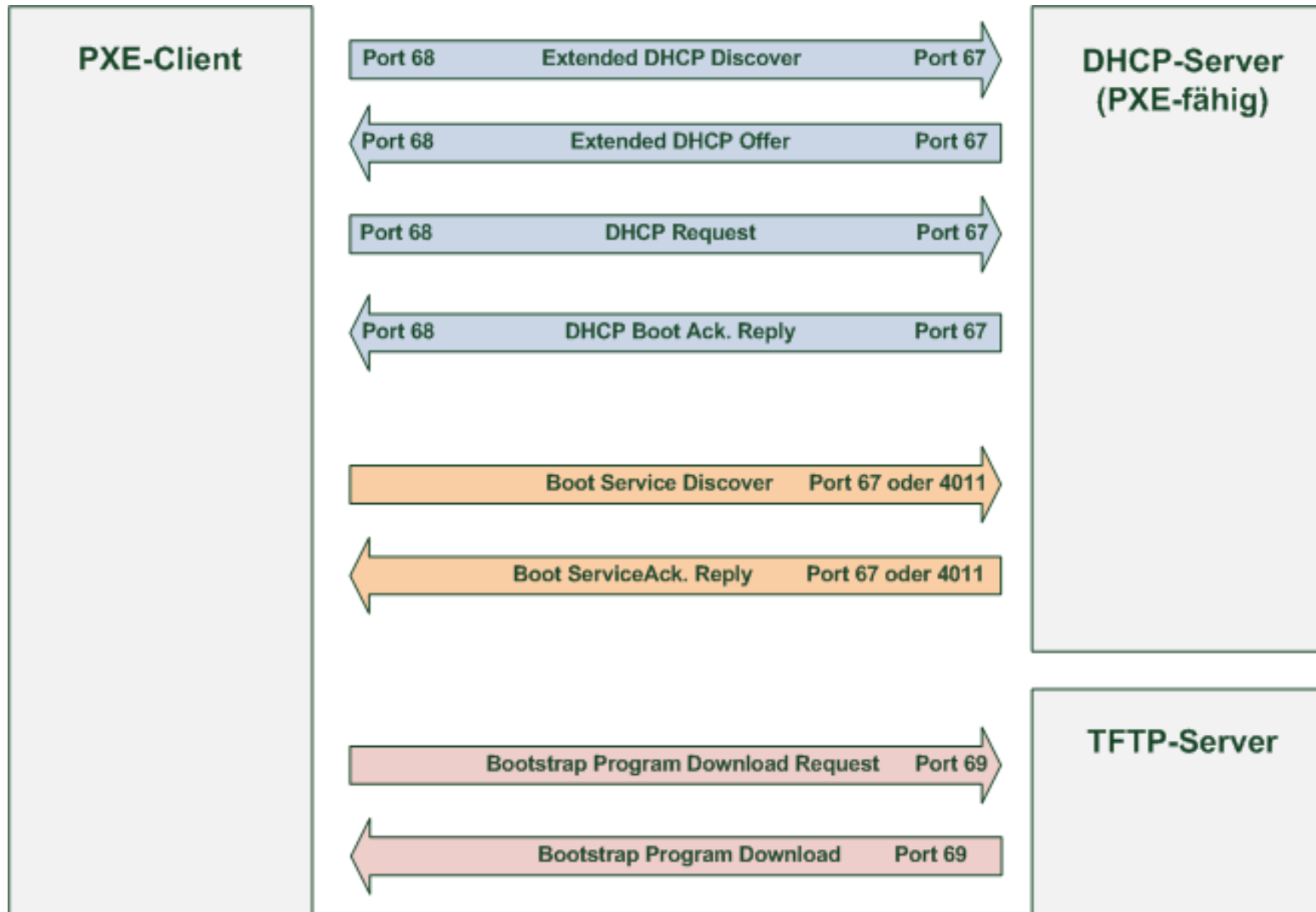
- USB-Stick am Ziel-PC anschließen
- vom USB-Stick aus booten
 - beim booten BIOS aufrufen (F12, F8 oder Entf-Taste)
- USB-Stick als Bootoption auswählen
- Installationsanweisungen folgen



Installation über PXE

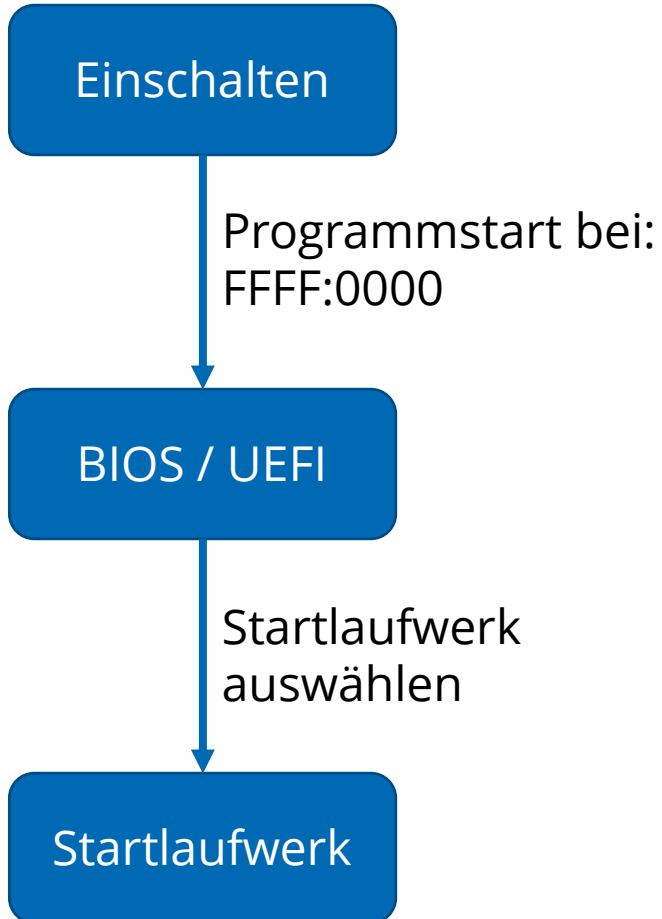
- Automatisierte Zero Touch Installation
 - Windows-Installation & Konfiguration
 - Installation übers Intranet
 - Anwendungen werden mit installiert
-
- Arbeitsplatz wird vordefiniert bereitgestellt
 - Automatisierung reduziert Arbeitslast für Nutzer und Admin

Installation über PXE



Bootvorgang

Startprozess Computer



Einschalten:

- PWR_SW-Pins werden kurzgeschlossen
- Hardware mit Strom versorgt

BIOS:

- Kalt- / Warmstart (in Adresse 0000:0472 = Wert 1234 ?)
- Systemdiagnose (Power on Self Test = POST)
- Zugriff auf Startlaufwerk (HDD, SSD, USB, DVD)

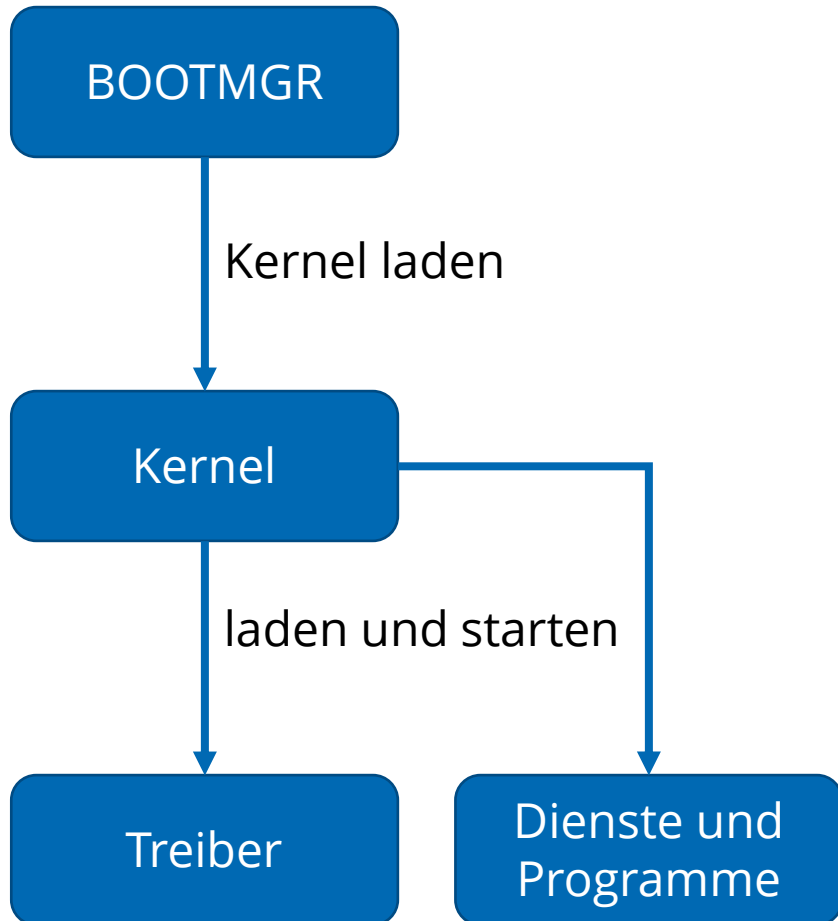
UEFI:

- Boot Manager direkt laden
- Übergabe an Boot Manager

Startlaufwerk:

- Master Boot Record (MBR) ausführen
- Partitionstabelle auswerten
- Primäre Partition laden
- Übergabe an Boot Manager (NTLDR / BOOTMGR / grub2)

Windows NT Bootprozess



Boot Manager:

- Boot-Konfiguration laden (Boot Configuration Data)
- Core Device Driver laden (Hal.dll)
- Kernel laden (winload.exe / winload.efi)
- Registry laden

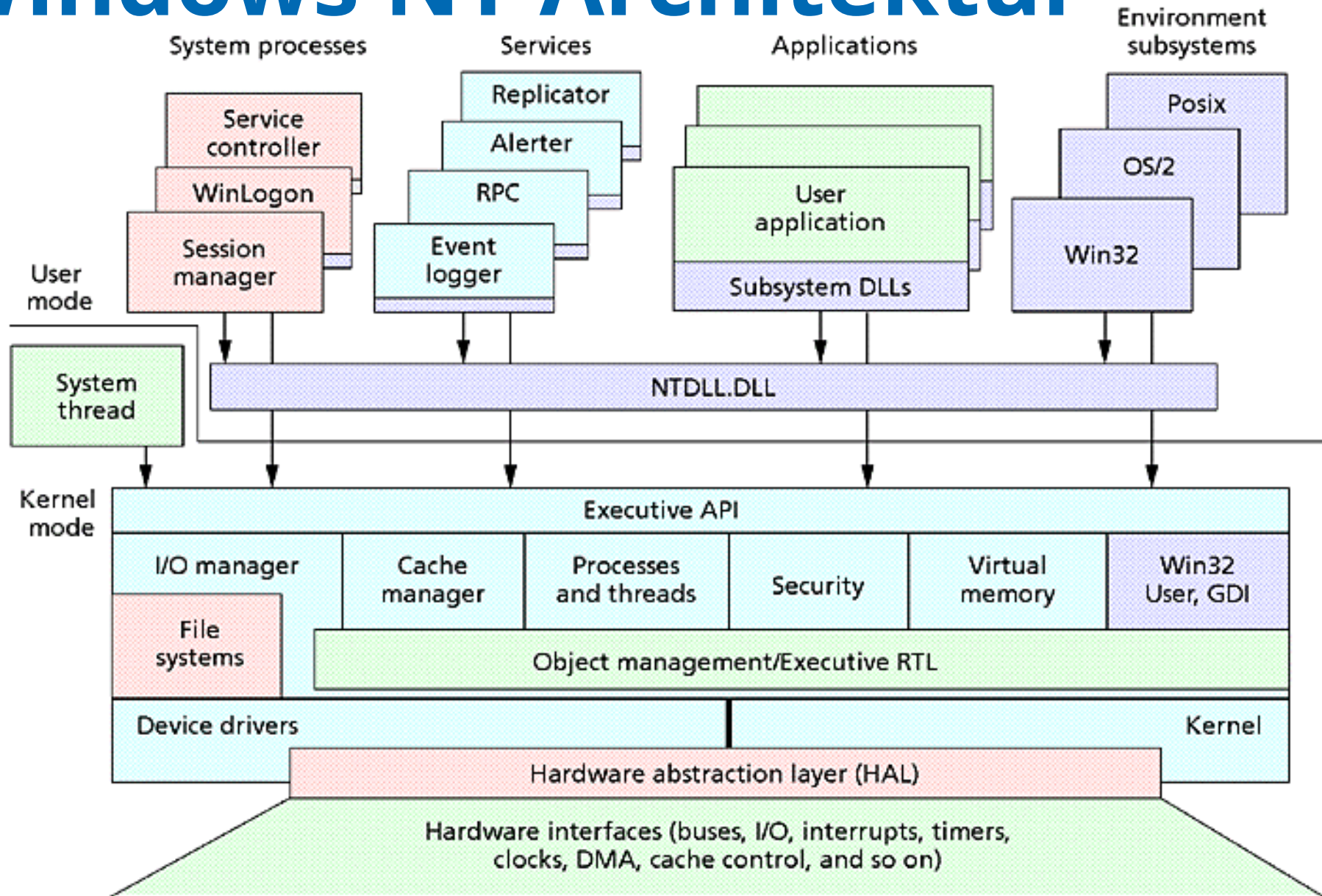
Kernel:

- ntoskrnl.exe
- Hardwareabstraktion
- Memory Management

Treiber und Programme:

- Zusätzliche Treiber laden (Sound, Grafik, Eingabe, ...)
- Dienste und Anwendungen starten (Windows Services, Subsysteme, Explorer, GUI, ...)

Windows NT Architektur



Systemverwaltung

Systemsteuerung

Einstellungen des Computers anpassen

Anzeige: Kategorie ▾



System und Sicherheit

Status des Computers überprüfen
Sicherungskopien von Dateien mit dem Dateiversionsverlauf speichern
Sichern und Wiederherstellen (Windows 7)



Netzwerk und Internet

Netzwerkstatus und -aufgaben anzeigen



Hardware und Sound

Geräte und Drucker anzeigen
Gerät hinzufügen
Häufig verwendete Mobilitätseinstellungen ändern



Programme

Programm deinstallieren



Benutzerkonten

Kontotyp ändern



Darstellung und Anpassung



Zeit und Region


Datums-, Uhrzeit- oder Zahlenformat ändern



Erleichterte Bedienung

Einstellungen empfehlen lassen
Visuelle Darstellung des Bildschirms optimieren

Netzwerkcenter

 Netzwerk- und Freigabecenter

← → ▾ ↑  > Systemsteuerung > Netzwerk und Internet > Netzwerk- und Freigabecenter ▾ ↻ System

Startseite der Systemsteuerung

Adaptereinstellungen ändern



Erweiterte
Freigabeeinstellungen ändern

Medienstreamingoptionen

Grundlegende Informationen zum Netzwerk anzeigen und Verbindungen einrichten

Aktive Netzwerke anzeigen


Öffentliches Netzwerk

Zugriffstyp: Internet
Verbindungen:  WLAN  ←

Netzwerkeinstellungen ändern



[Neue Verbindung oder neues Netzwerk einrichten](#)

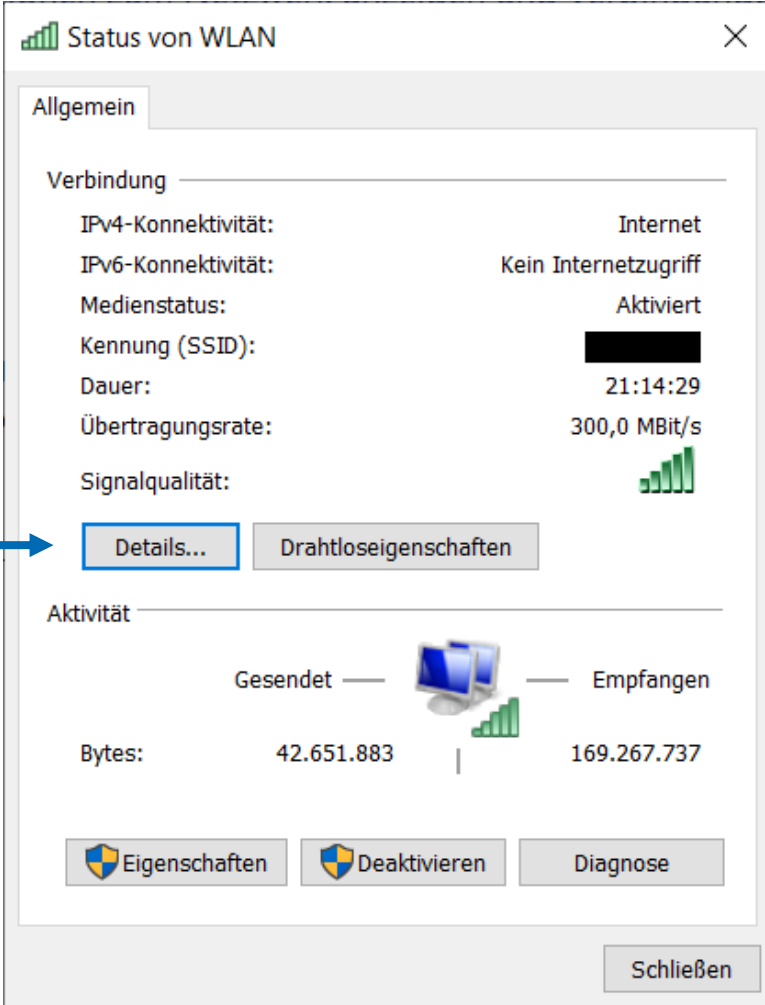
Breitband-, DFÜ- oder VPN-Verbindung bzw. Router oder Zugriffspunkt einrichten.



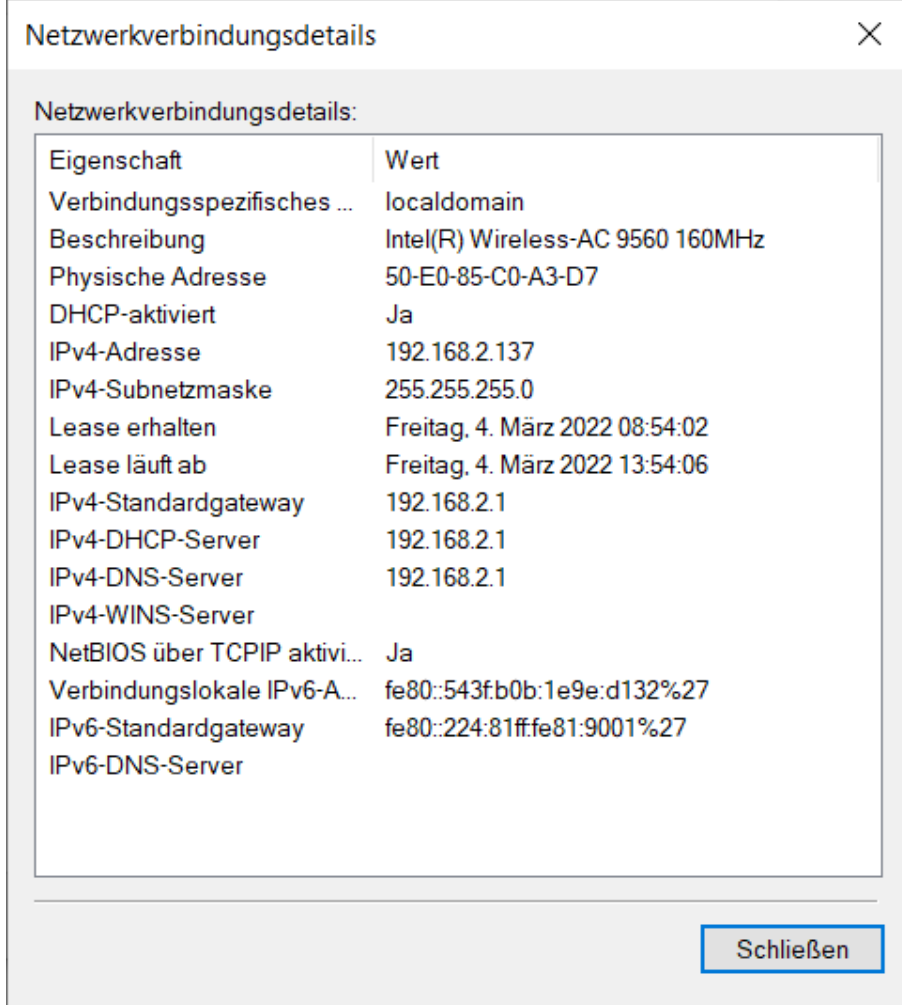
[Probleme beheben](#)

Netzwerkprobleme diagnostizieren und reparieren oder Problembehandlungsinformationen abrufen.

Verbindungsdetails



The screenshot shows the 'Status von WLAN' window. The 'Allgemein' tab is selected. Under 'Verbindung', the following information is displayed: IPv4-Konnektivität: Internet; IPv6-Konnektivität: Kein Internetzugriff; Medienstatus: Aktiviert; Kennung (SSID): [redacted]; Dauer: 21:14:29; Übertragungsrage: 300,0 MBit/s; Signalqualität: [signal strength icon]. Below this, there are two buttons: 'Details...' (highlighted with a blue arrow) and 'Drahtloseigenschaften'. Under 'Aktivität', there is a graph showing data transfer. The 'Gesendet' (Sent) value is 42.651.883 bytes and the 'Empfangen' (Received) value is 169.267.737 bytes. At the bottom, there are buttons for 'Eigenschaften', 'Deaktivieren', 'Diagnose', and 'Schließen'.



The screenshot shows the 'Netzwerkverbindungsdetails' window. It displays a list of network properties and their values:

Eigenschaft	Wert
Verbindungsspezifisches ...	localdomain
Beschreibung	Intel(R) Wireless-AC 9560 160MHz
Physische Adresse	50-E0-85-C0-A3-D7
DHCP-aktiviert	Ja
IPv4-Adresse	192.168.2.137
IPv4-Subnetzmaske	255.255.255.0
Lease erhalten	Freitag, 4. März 2022 08:54:02
Lease läuft ab	Freitag, 4. März 2022 13:54:06
IPv4-Standardgateway	192.168.2.1
IPv4-DHCP-Server	192.168.2.1
IPv4-DNS-Server	192.168.2.1
IPv4-WINS-Server	
NetBIOS über TCP/IP aktivi...	Ja
Verbindungslokale IPv6-A...	fe80::543f:b0b:1e9e:d132%27
IPv6-Standardgateway	fe80::224:81ff:fe81:9001%27
IPv6-DNS-Server	

At the bottom right, there is a 'Schließen' button.

Programme deinstallieren

Programm deinstallieren oder ändern

Wählen Sie ein Programm aus der Liste aus, und klicken Sie auf "Deinstallieren", "Ändern" oder "Reparieren", um es zu deinstallieren.

Organisieren ▾ Deinstallieren ☰ ▾ ?

Name	Herausgeber	Installiert am	Größe	Version
Microsoft 365 Apps for Enterprise - de-de	Microsoft Corporation	01.03.2022		16.0.14729.20322
Microsoft Edge	Microsoft Corporation	02.03.2022		98.0.1108.62
Microsoft Edge WebView2-Laufzeit	Microsoft Corporation	01.03.2022		98.0.1108.62
Microsoft OneDrive	Microsoft Corporation	03.03.2022	200 MB	22.022.0130.0001
Microsoft Teams	Microsoft Corporation	02.03.2022	118 MB	1.5.00.4689
Microsoft Update Health Tools	Microsoft Corporation	01.03.2022	1,05 MB	3.65.0.0
Microsoft Visual C++ 2015-2019 Redistributable (x64)...	Microsoft Corporation	01.03.2022	23,1 MB	14.24.28127.4
Mozilla Firefox (x64 de)	Mozilla	01.03.2022	404 MB	97.0.1
Mozilla Maintenance Service	Mozilla	01.03.2022	533 KB	91.6.1
Mozilla Thunderbird (x64 de)	Mozilla	01.03.2022	233 MB	91.6.1
Teams Machine-Wide Installer	Microsoft Corporation	01.03.2022	118 MB	1.4.0.22976
Windows Subsystem for Linux Update	Microsoft Corporation	02.03.2022	67,4 MB	5.10.16

Mozilla Produktversion: 91.6.1 Supportlink: <https://www.mozilla.or...> Größe: 233 MB
Hilfelinke: <https://www.thunderbi...> Updateinformation: <https://www.thunderbi...> Kommentare: Mozilla Thunderbird 91.6.1 (x64 de)

Konsolen

CMD (Windows Eingabeaufforderung)

- Historische Windows-Shell von OS/2
- DOS-Befehle
- Skripting möglich (Batch-Dateien mit .bat oder .cmd)
- Unterstützte Befehle:
 - assoc, call, cd, color, copy, date, del, endlocal, for, format, ftype, goto, help, if, mkdir, popd, pushd, prompt, set, setlocal, shift, start, ...
 - „help“-Befehl für genaue Erläuterung
- Eingeschränkt erweiterbar

→ Grundlegende Befehle für Dateisystemverwaltung, Programmausführung und Systemadministrationsaufgaben

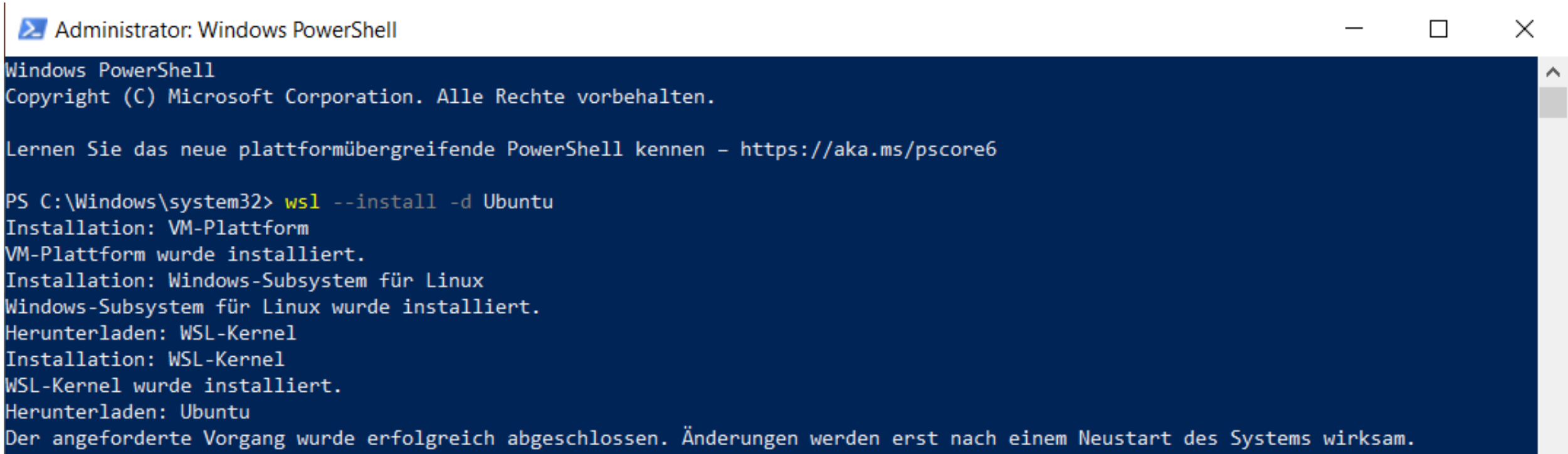
PowerShell

- seit Windows 7 vorinstalliert
- Leistungsfähigere und fortschrittlichere Kommandozeilenumgebung
- Basiert auf .NET-Framework
- Shell für Skripte (.ps1-Dateien)
 - Skripting mit Cmdlets = vordefinierte Befehle
 - Z.B. „get-help“-Befehl für detaillierten Hilfetext
 - Objektorientiertes Skripting mit .NET-Objekten

→ Komplexe Aufgaben der Systemadministration, Verwaltung des Windowssystems oder -domain

Bash (Bourne-again-Shell)

- Nutzung über WSL (Windows Subsystem for Linux)
- Installation mittels PowerShell:



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

Lernen Sie das neue plattformübergreifende PowerShell kennen – https://aka.ms/pscore6

PS C:\Windows\system32> wsl --install -d Ubuntu
Installation: VM-Plattform
VM-Plattform wurde installiert.
Installation: Windows-Subsystem für Linux
Windows-Subsystem für Linux wurde installiert.
Herunterladen: WSL-Kernel
Installation: WSL-Kernel
WSL-Kernel wurde installiert.
Herunterladen: Ubuntu
Der angeforderte Vorgang wurde erfolgreich abgeschlossen. Änderungen werden erst nach einem Neustart des Systems wirksam.
```

Bash

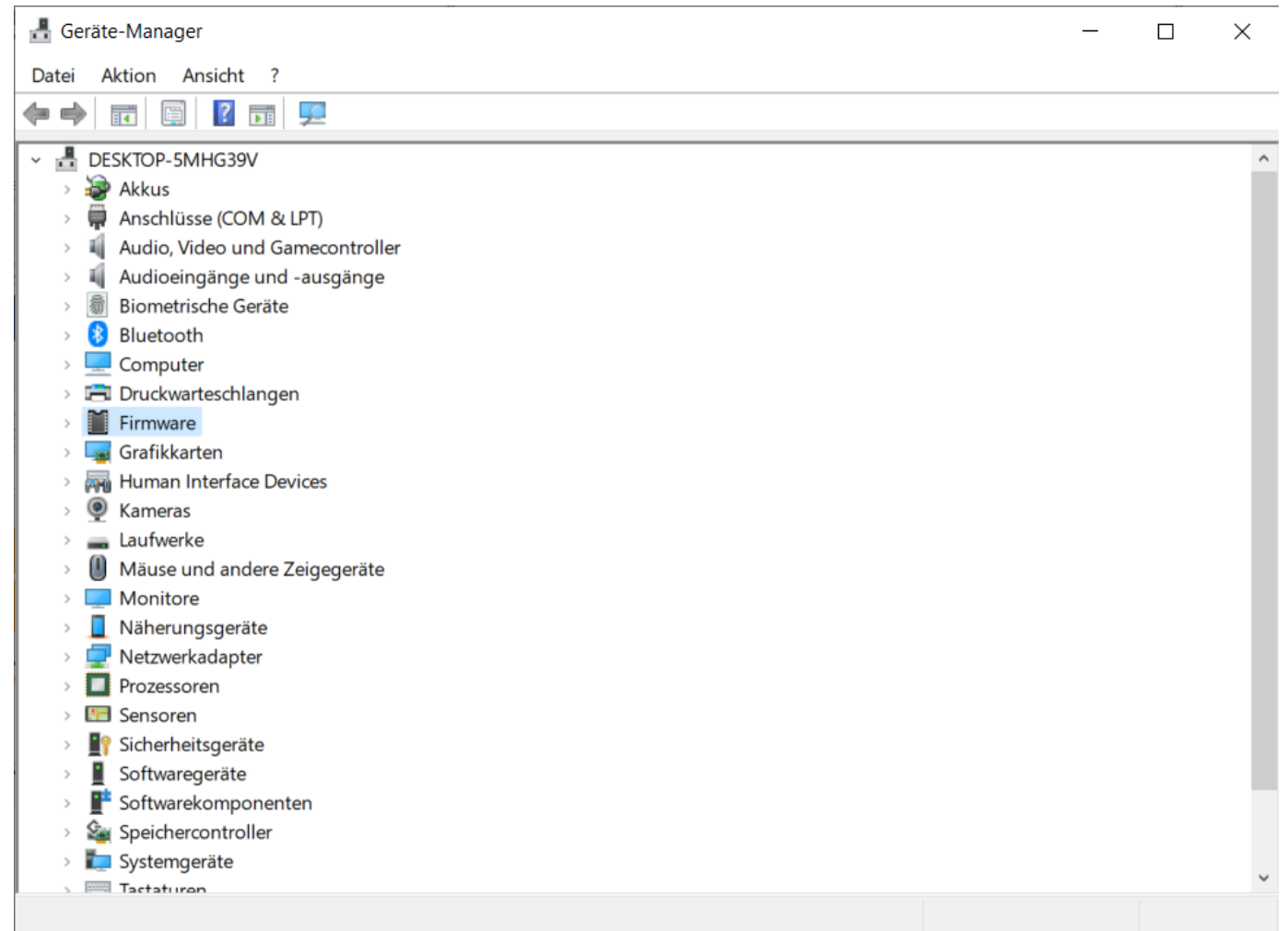
- Mächtige Shell aus der Unix-Welt
- Skriptfähig
- IEEE POSIX P1003.2/ISO 9945.2 Shell and Tools standard conform
- Quelloffen unter GPL-Lizenz
- Umfangreich dokumentiert
- Viele Beispiele online verfügbar

→ Näheres dazu in der Linux Vorlesung

Geräte unter Windows

Gerätemanager

- Auflistung aktuell angeschlossener Geräte
- Auflistung von bisher angeschlossenen Geräten
- Verwaltung von Gerätetreiber
 - Deaktivierung
 - Neuinstallation
 - Update



Laufwerke

- **Physisches Laufwerk**

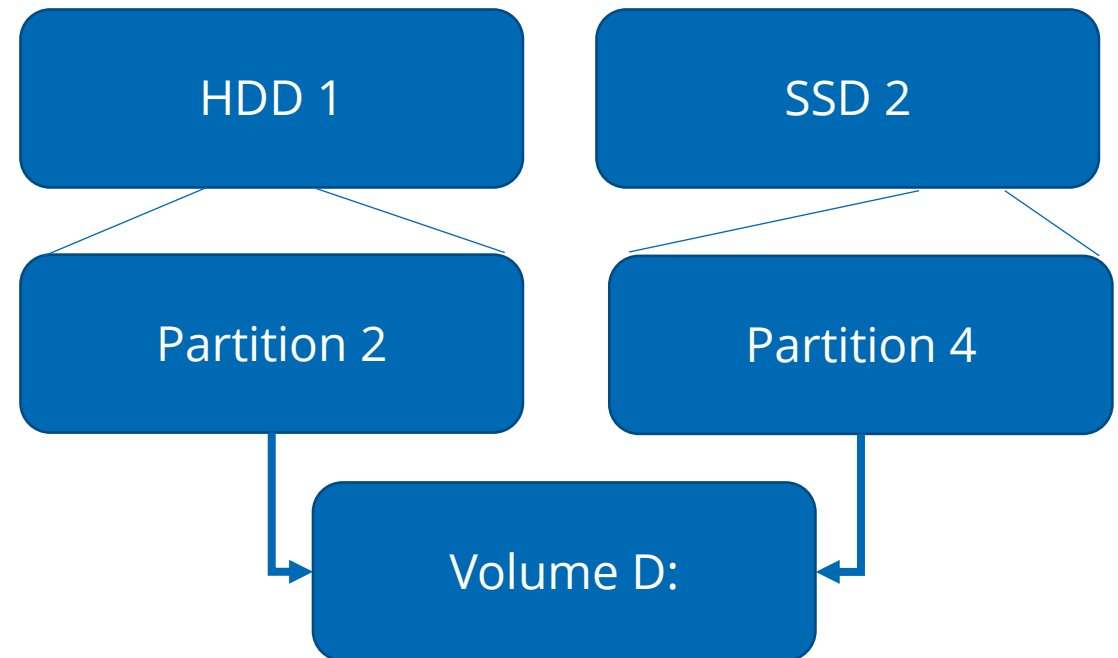
- Hard Disk Drive (HDD)
- Solid State Drive (SSD)
- Digital Video Disk (DVD)
- USB-Stick

- **Logisches Laufwerk**

- Partition
- RAID
- Netzwerklaufwerk

- **Volume**

- Zusammenfassung eines oder mehrerer logischer Laufwerke
- im Dateieexplorer sichtbar



Datenträgerverwaltung

- Auflistung von Datenträgern, logischen Laufwerken und Volumes
- Verwalten von Datenträgern
 - Partitionieren
- Verwalten von Volumes
 - Formatieren
 - Erstellen von RAID-Volumes
 - Laufwerksbuchstaben festlegen
- **Forensische Informationen:**
 - Erstmaliges Einhängen in das System
 - Angeschlossener Bus
 - Treiberdetails

Datenträgerverwaltung

The screenshot shows the Windows Disk Management console. At the top, a table lists the system volumes:

Volume	Layout	Typ	Dateisystem	Status	Kapazität	Freier S...	% frei
(C:)	Einfach	Basis	NTFS (BitLo...	Fehlerfrei ...	476,31 GB	427,23 GB	90 %
(Datenträger 0 Par...	Einfach	Basis		Fehlerfrei ...	100 MB	100 MB	100 %
(Datenträger 0 Par...	Einfach	Basis		Fehlerfrei ...	525 MB	525 MB	100 %

A blue bracket labeled "Auflistung von Volumes" spans the table. Below, the "Datenträger 0" section shows a physical disk with three partitions:

- 100 MB Fehlerfrei (EFI-Systempartition)
- (C:) 476,31 GB NTFS (BitLocker-verschlüsselt) Fehlerfrei (Startpartition, Auslagerungsdatei, Absturzabbild, Basisdatenpartition)
- 525 MB Fehlerfrei (Wiederherstellungspartition)

Blue arrows point from the labels "Partition", "eingebundene Partition als Volume C:", and "Partition" below to their respective partitions in the disk layout. A blue bracket labeled "Physisches Laufwerk" encompasses the entire disk layout area.

Legend: ■ Nicht zugeordnet ■ Primäre Partition

Automatische Laufwerksbuchstaben

- A: und B: Diskettenlaufwerke
- C: Systemfestplatte
- D:, E:, ...
 - weitere Festplatten
 - interne Laufwerke (CD, DVD, Blue-Ray, ...)
 - externe Datenträger (USB-Stick, DVD, ...)
- ... , X:, Y:, Z:
 - Netzwerklaufwerke

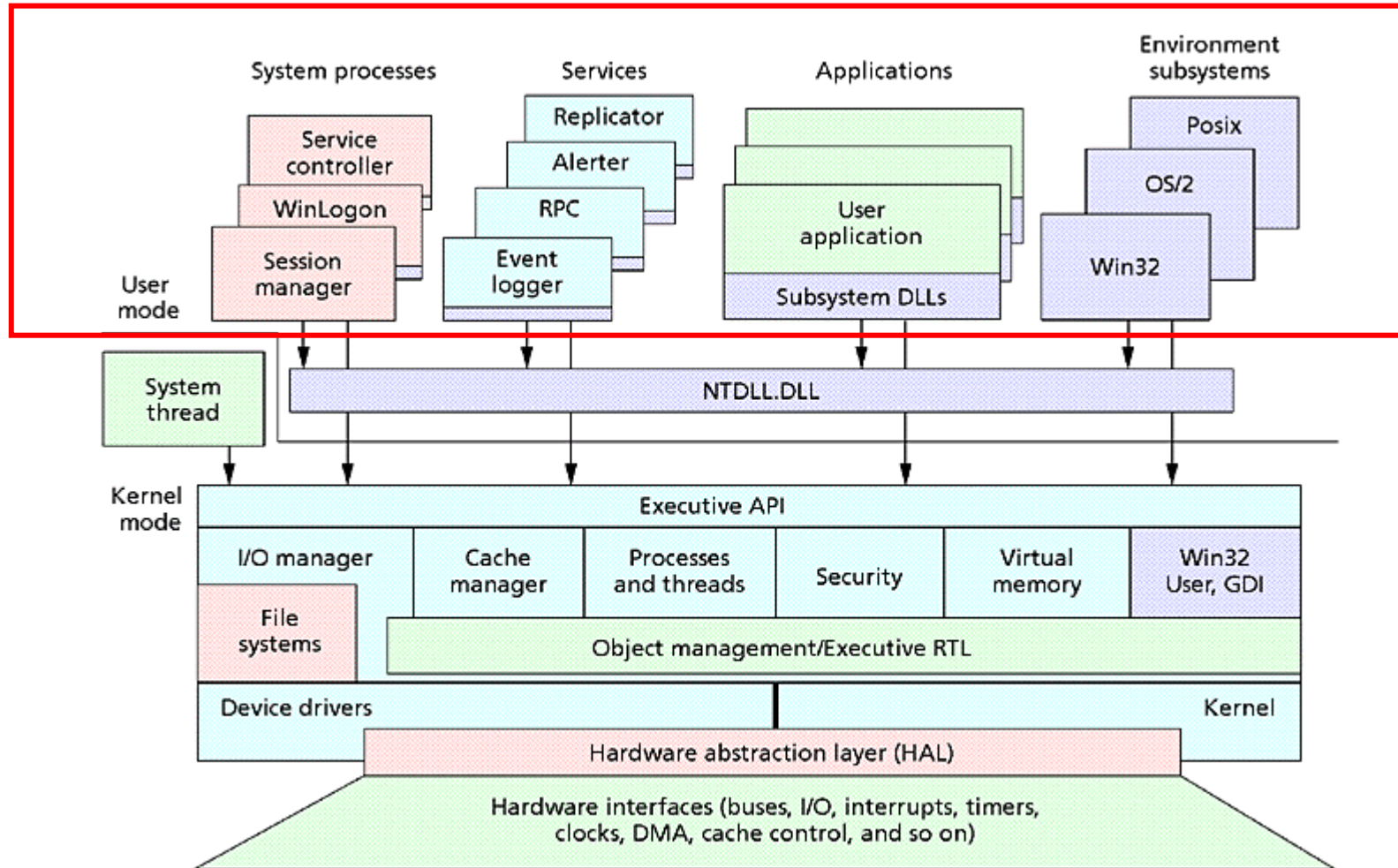
→Jederzeit individuell änderbar:
→diskpart
→Sel vol <voln>
→assign letter=<LWB>

Dienste und Systemprozesse

Programmbezeichnungen

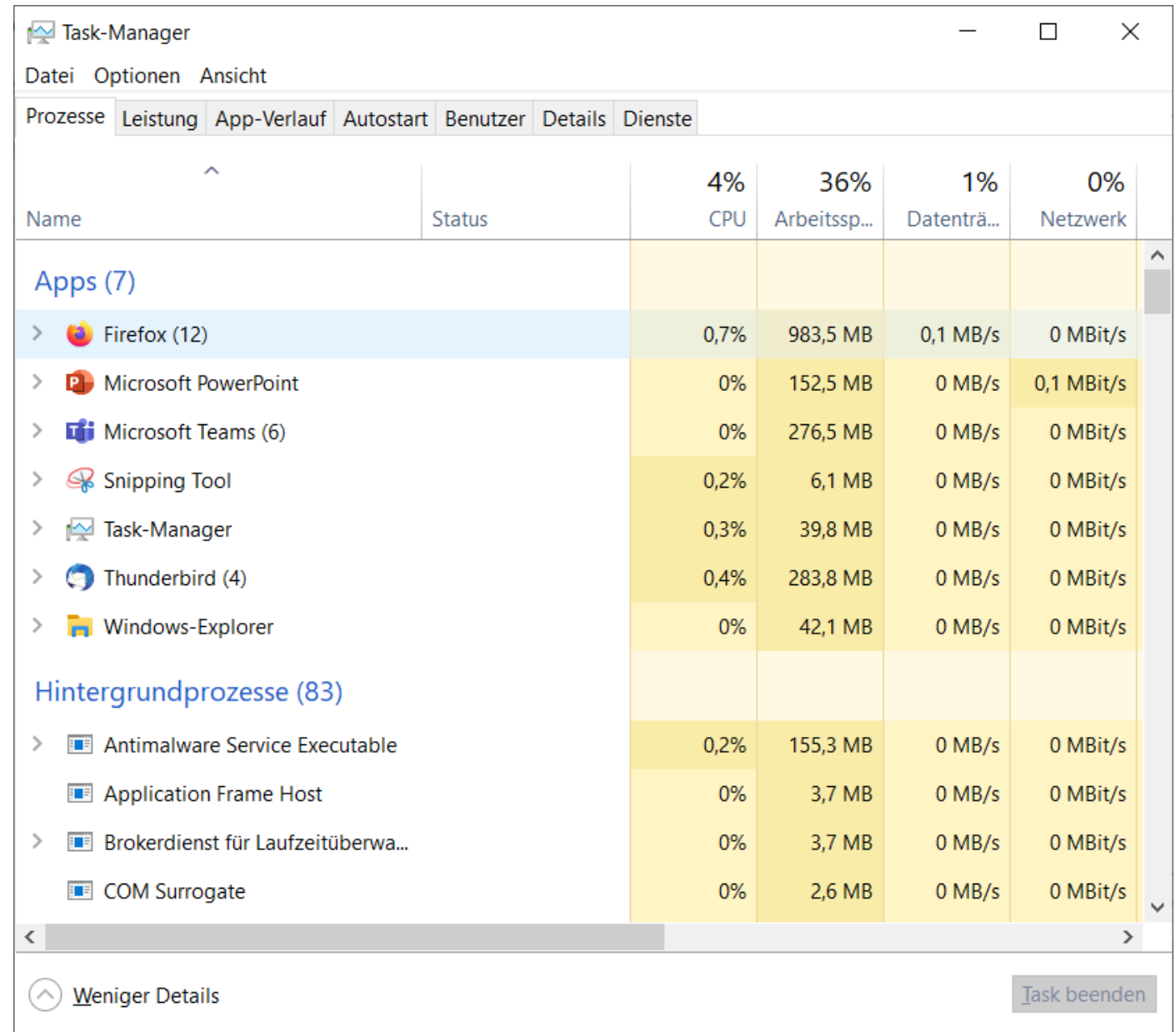
- **Dienste**
 - Anwendung ohne Graphische Oberfläche (GUI)
 - geeignet für periodische und zeitaufwendige Aufgaben
- **Systemprozesse**
 - Funktionalität des Betriebssystems
 - Bereitstellung der Infrastruktur für Anwendungen
 - Schnittstelle zwischen Nutzer und Betriebssystem
- **Anwendungen / Application**
 - Programm für Endnutzer
 - Meistens mit Graphischer Oberfläche

Programmbezeichnungen



Taskmanager

- Prozesse auflisten
- Programmbeendigung erzwingen
- Systemauslastung anzeigen
- Autostartprogramme festlegen
- Eingeloggte Benutzer anzeigen
- Aufrufbar über Tastenkombi strg + shift + esc

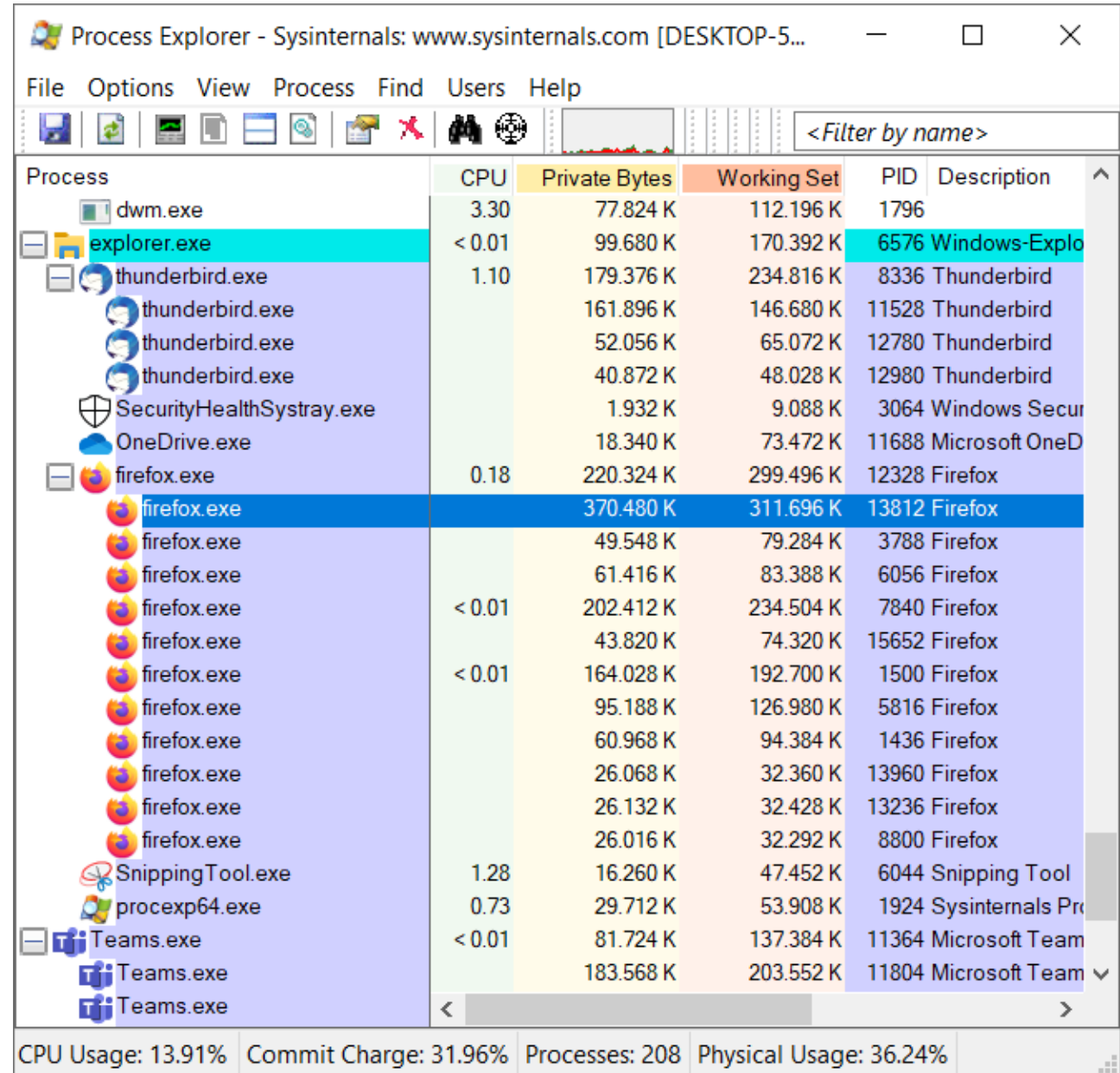


The screenshot shows the Windows Task Manager window with the 'Leistung' (Performance) tab selected. The window title is 'Task-Manager' and it has standard Windows window controls. Below the title bar, there are menu options: 'Datei', 'Optionen', and 'Ansicht'. The main area is divided into tabs: 'Prozesse', 'Leistung', 'App-Verlauf', 'Autostart', 'Benutzer', 'Details', and 'Dienste'. The 'Leistung' tab is active, showing system performance metrics: CPU at 4%, Arbeitsspeicher (Memory) at 36%, Datenträger (Storage) at 1%, and Netzwerk (Network) at 0%. Below these metrics is a table of running processes, categorized into 'Apps (7)' and 'Hintergrundprozesse (83)'. The 'Apps' section is expanded, showing details for Firefox (12), Microsoft PowerPoint, Microsoft Teams (6), Snipping Tool, Task-Manager, Thunderbird (4), and Windows-Explorer. The 'Hintergrundprozesse' section is partially visible, showing Antimalware Service Executable, Application Frame Host, Brokerdienst für Laufzeitüberwa..., and COM Surrogate. At the bottom of the window, there is a 'Weniger Details' button and a 'Task beenden' button.

Name	Status	4% CPU	36% Arbeitssp...	1% Datenträ...	0% Netzwerk
Apps (7)					
> Firefox (12)		0,7%	983,5 MB	0,1 MB/s	0 MBit/s
> Microsoft PowerPoint		0%	152,5 MB	0 MB/s	0,1 MBit/s
> Microsoft Teams (6)		0%	276,5 MB	0 MB/s	0 MBit/s
> Snipping Tool		0,2%	6,1 MB	0 MB/s	0 MBit/s
> Task-Manager		0,3%	39,8 MB	0 MB/s	0 MBit/s
> Thunderbird (4)		0,4%	283,8 MB	0 MB/s	0 MBit/s
> Windows-Explorer		0%	42,1 MB	0 MB/s	0 MBit/s
Hintergrundprozesse (83)					
> Antimalware Service Executable		0,2%	155,3 MB	0 MB/s	0 MBit/s
Application Frame Host		0%	3,7 MB	0 MB/s	0 MBit/s
> Brokerdienst für Laufzeitüberwa...		0%	3,7 MB	0 MB/s	0 MBit/s
COM Surrogate		0%	2,6 MB	0 MB/s	0 MBit/s

Process Explorer

- Kostenlos von Microsoft über Sysinternals Suite
 - Mehr Details über Prozesse
 - Hierarchische Prozessstruktur
 - RAM Memory Dump
 - Integrierte Virusüberprüfung über Virustotal
- <https://learn.microsoft.com/de-de/sysinternals/downloads/process-explorer>



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-5...]

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description
dwm.exe	3.30	77.824 K	112.196 K	1796	
explorer.exe	< 0.01	99.680 K	170.392 K	6576	Windows-Explo
thunderbird.exe	1.10	179.376 K	234.816 K	8336	Thunderbird
thunderbird.exe		161.896 K	146.680 K	11528	Thunderbird
thunderbird.exe		52.056 K	65.072 K	12780	Thunderbird
thunderbird.exe		40.872 K	48.028 K	12980	Thunderbird
SecurityHealthSystray.exe		1.932 K	9.088 K	3064	Windows Secur
OneDrive.exe		18.340 K	73.472 K	11688	Microsoft OneD
firefox.exe	0.18	220.324 K	299.496 K	12328	Firefox
firefox.exe		370.480 K	311.696 K	13812	Firefox
firefox.exe		49.548 K	79.284 K	3788	Firefox
firefox.exe		61.416 K	83.388 K	6056	Firefox
firefox.exe	< 0.01	202.412 K	234.504 K	7840	Firefox
firefox.exe		43.820 K	74.320 K	15652	Firefox
firefox.exe	< 0.01	164.028 K	192.700 K	1500	Firefox
firefox.exe		95.188 K	126.980 K	5816	Firefox
firefox.exe		60.968 K	94.384 K	1436	Firefox
firefox.exe		26.068 K	32.360 K	13960	Firefox
firefox.exe		26.132 K	32.428 K	13236	Firefox
firefox.exe		26.016 K	32.292 K	8800	Firefox
SnippingTool.exe	1.28	16.260 K	47.452 K	6044	Snipping Tool
procxp64.exe	0.73	29.712 K	53.908 K	1924	Sysinternals Pro
Teams.exe	< 0.01	81.724 K	137.384 K	11364	Microsoft Team
Teams.exe		183.568 K	203.552 K	11804	Microsoft Team
Teams.exe					

CPU Usage: 13.91% Commit Charge: 31.96% Processes: 208 Physical Usage: 36.24%

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

Vielen Dank



**HOCHSCHULE
MITTWEIDA**
University of Applied Sciences

Tim Wetterau B.Sc.

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Angewandte Computer- und Biowissenschaften

T +49 (0) 3727 58-1752
@ wetterau@hs-mittweida.de
www.cb.hs-mittweida.de

Haus 8 | Richard-Stücklen Bau | Raum 8-303
Am Schwanenteich 6b | 09648 Mittweida

hs-mittweida.de