



Betriebssysteme

Praktikum 4

In diesem Praktikum lernen Sie die Nutzung des VSS (Volume Shadow Copy Service) und das Mounten von Volumen-Schattenkopien kennen. Zudem extrahieren Sie Dateien aus dem VSS. Zum Schluss widmen Sie sich der Untersuchung von Recent-Einträgen wie bspw. LNK-Dateien und der Nutzung der Windows Defender Firewall.

Inhalte des Praktikums:

- Firewall konfigurieren und lesen
- Recent + LNK-Dateianalyse
- USB-Datenträger
- VSS-Nutzen um Dateisperren zu Umgehen

LÖSUNG

Vorbereitung

Nutzen Sie bitte für die weitere Bearbeitung die in PR1 erstellte Windows VM oder die OVA aus PR2.

Zusätzlich finden Sie hier die für das Praktikum 4 zu nutzende ISO-Datei **PR4.iso**:

<https://download.hs-mittweida.de/intranet/R:/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum/Windows/PR4.iso>

und eine zweite VMDK-Datei mit zusätzlichen Daten:

<https://download.hs-mittweida.de/intranet/R:/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum/Windows/Windows10-BS-Praktikum-extern-USB.vmdk>

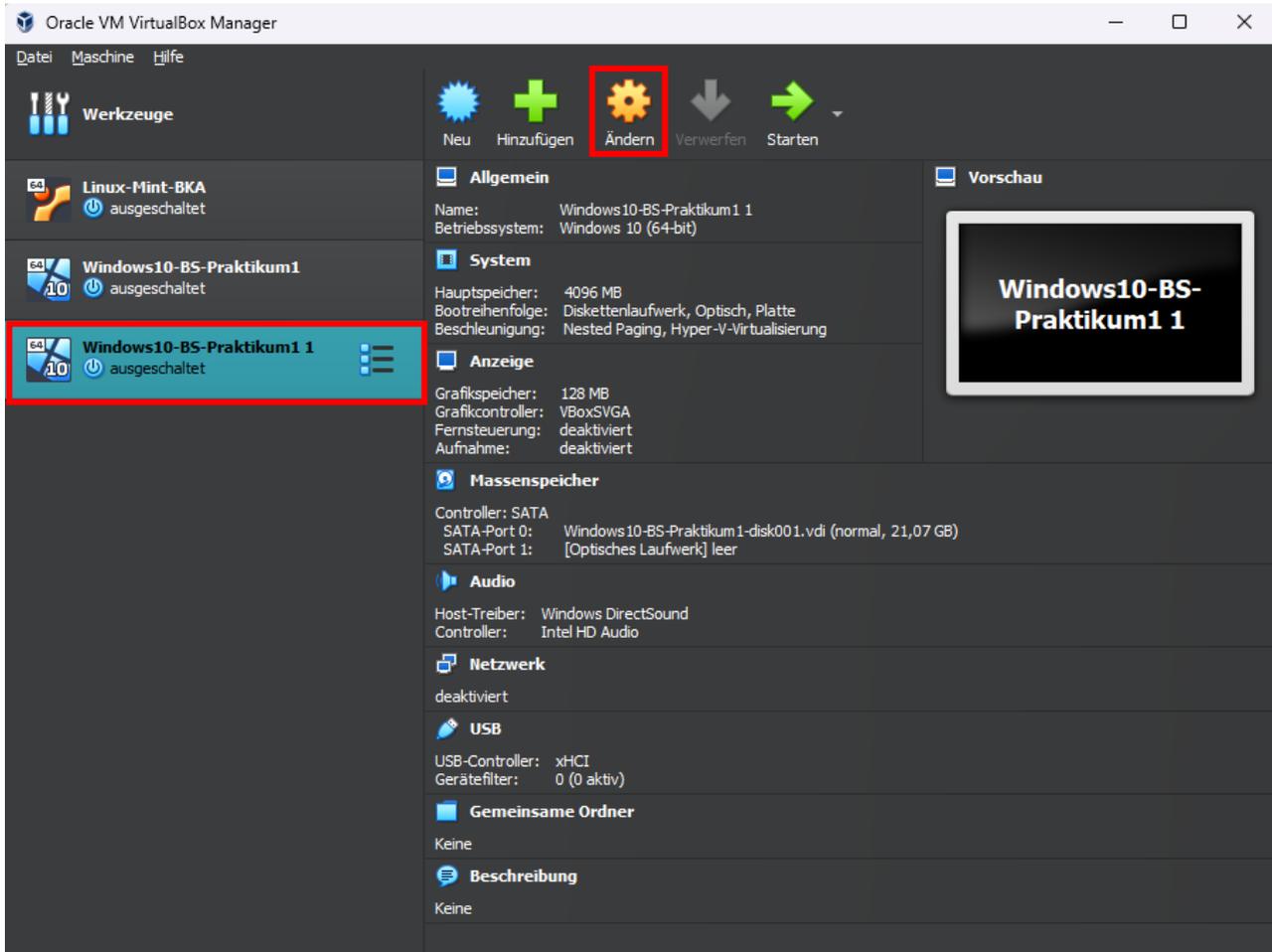
Allgemeine Hinweise

Kopieren Sie bitte die ISO Datei **PR4.iso (786MB)** und die **VMDK-Datei (448KB)** auf ihre lokale Festplatte in ein separates Verzeichnis, auf das Sie Zugriff haben, bestenfalls in das VM-Verzeichnis von Praktikum1.

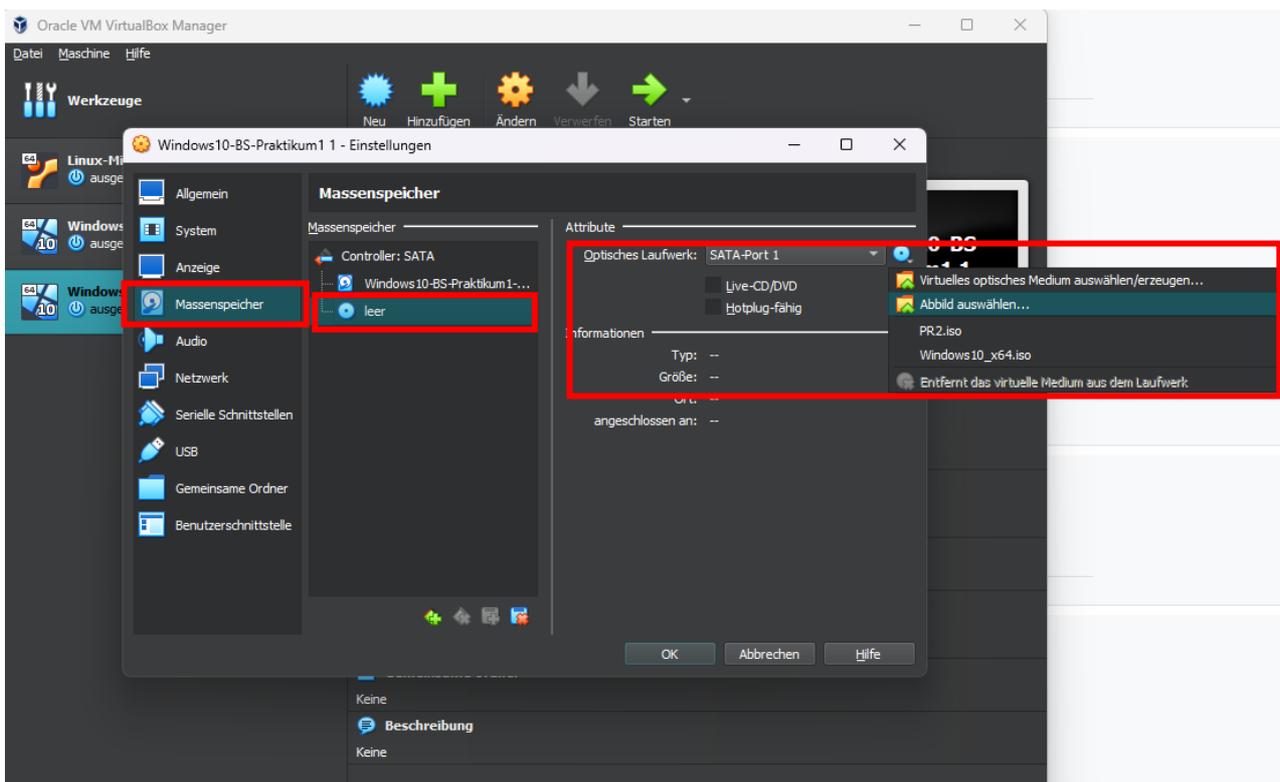
Einbindung der PR4.iso und VMDK-Datei

Öffnen Sie Virtualbox.

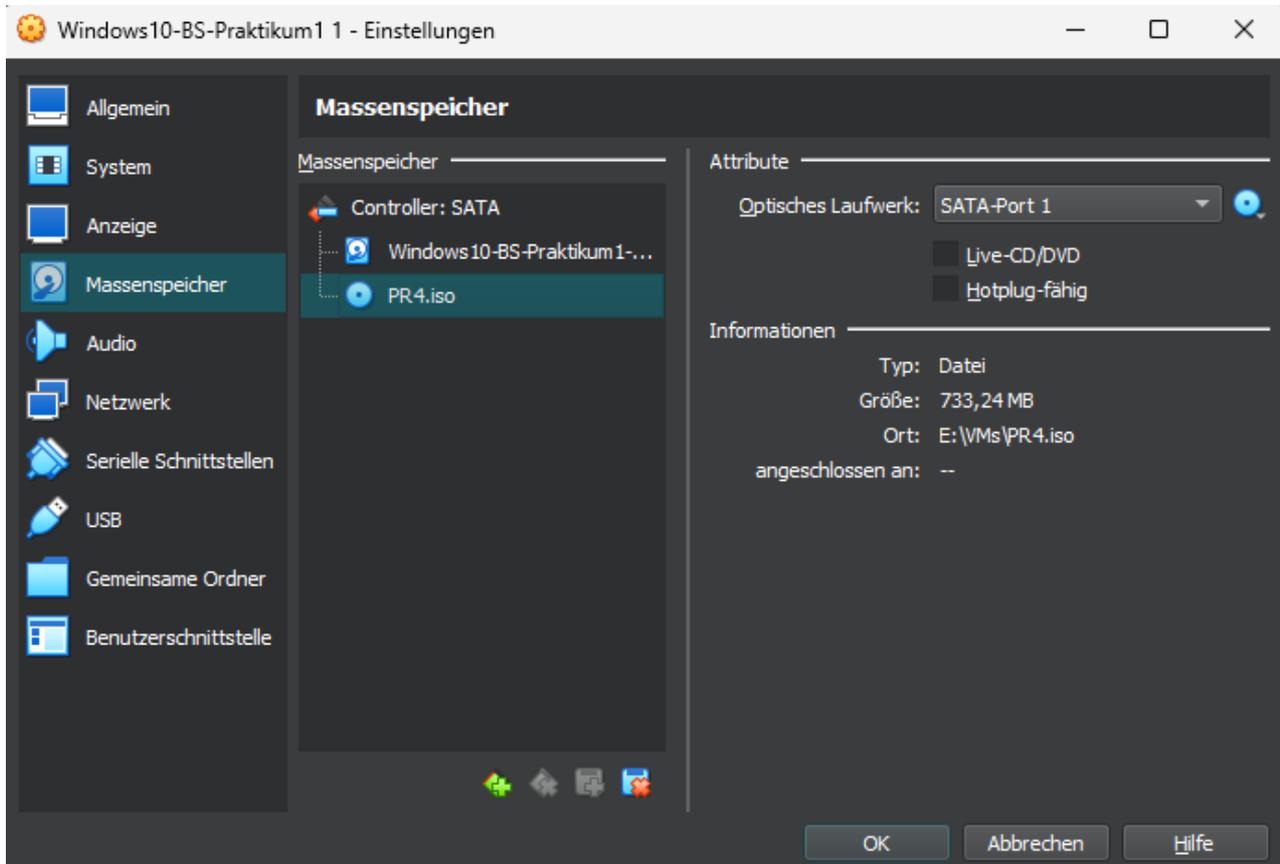
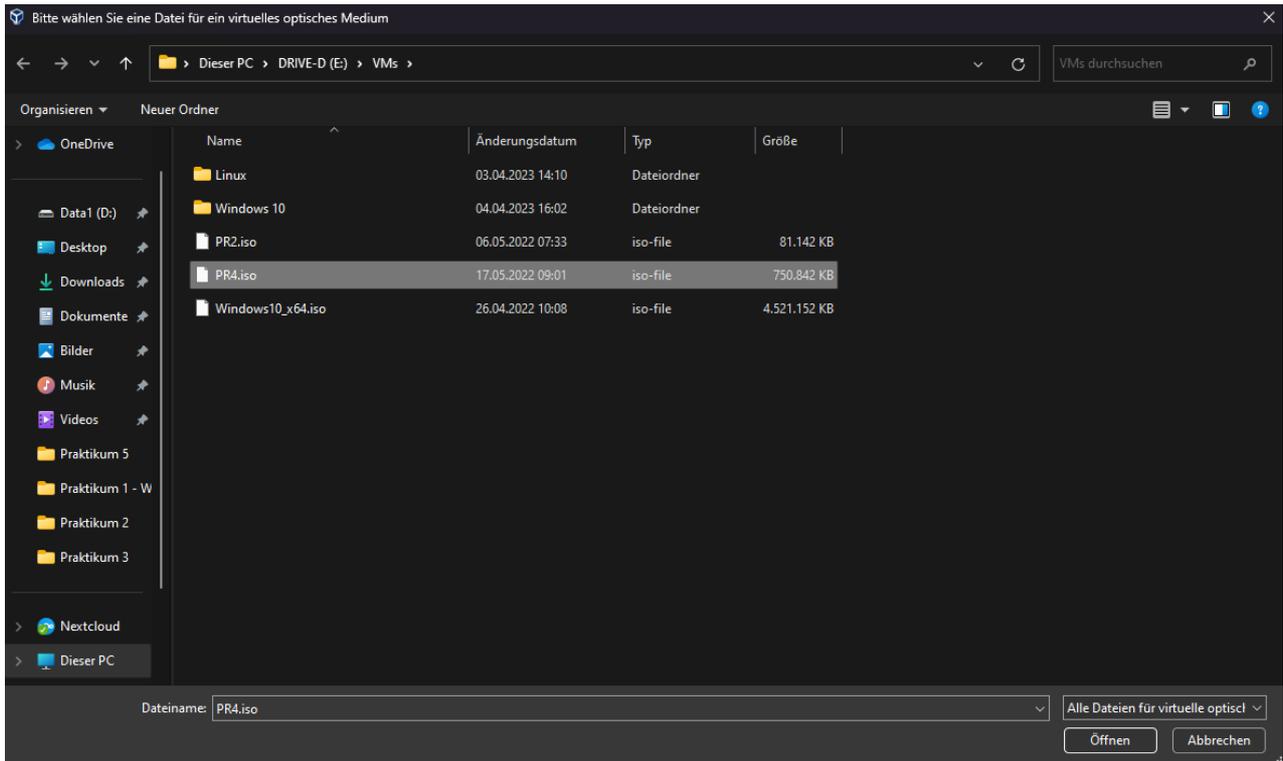
Wählen Sie die im Praktikum 1 angelegte VM aus oder importieren Sie zuerst die OVA-Datei wählen dann die VM des Praktikum 1 aus. Gehen Sie auf **Ändern** (nicht Doppelklicken auf die VM, das würde diese Starten).



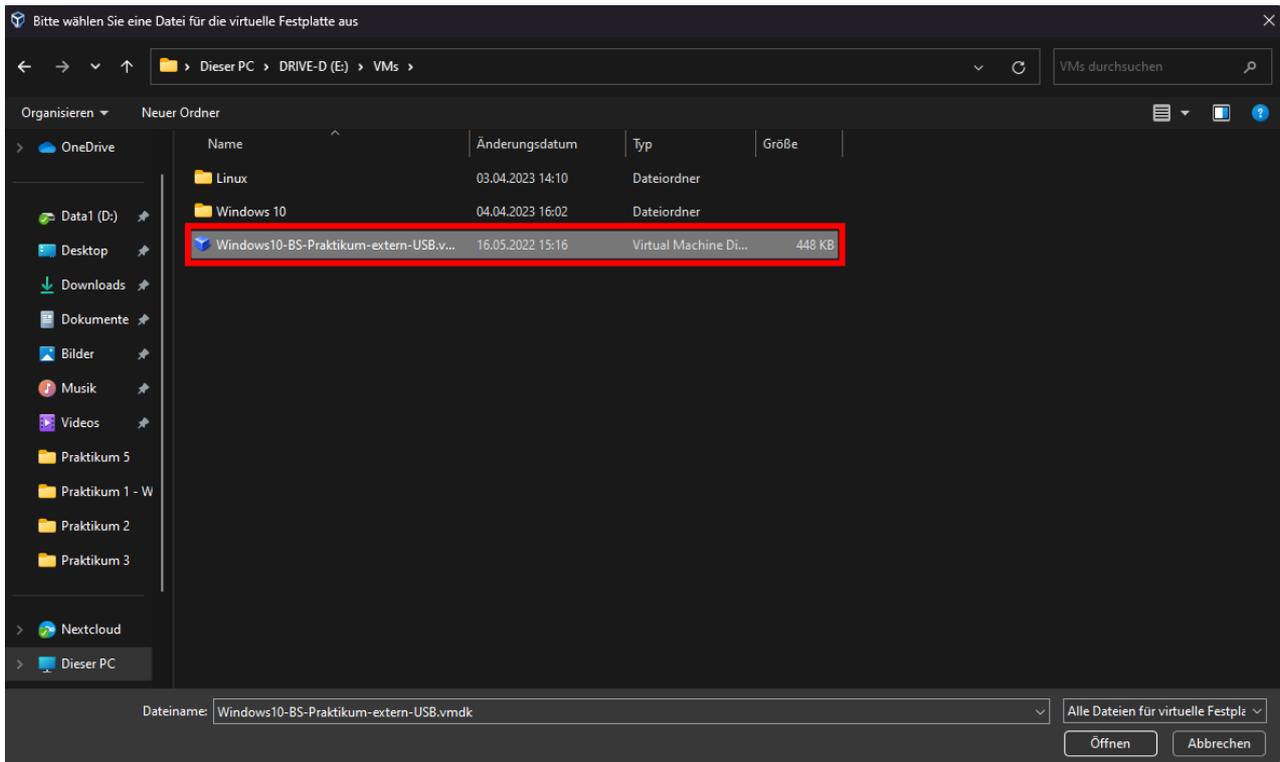
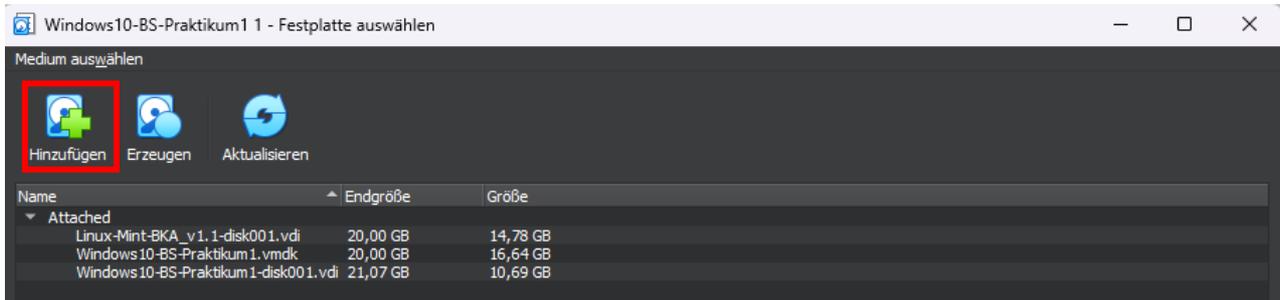
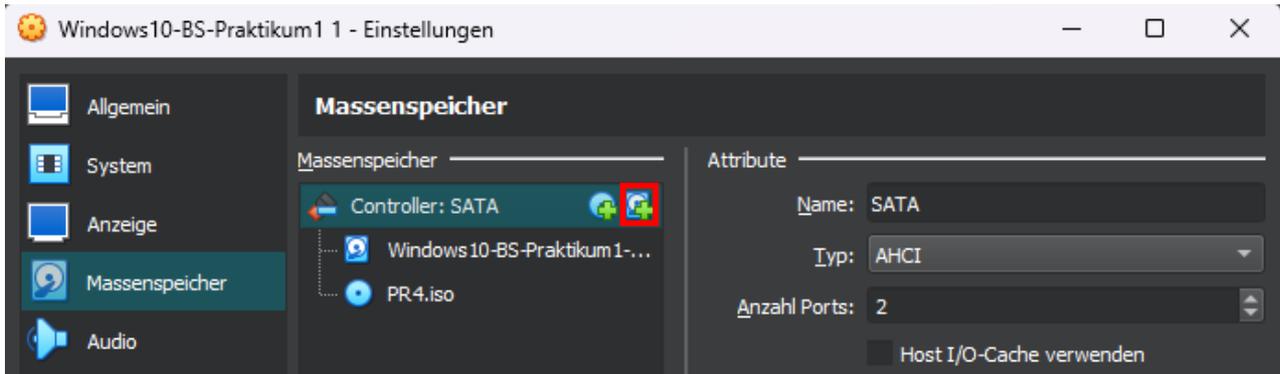
➤ Wählen Sie den Massenspeicher aus

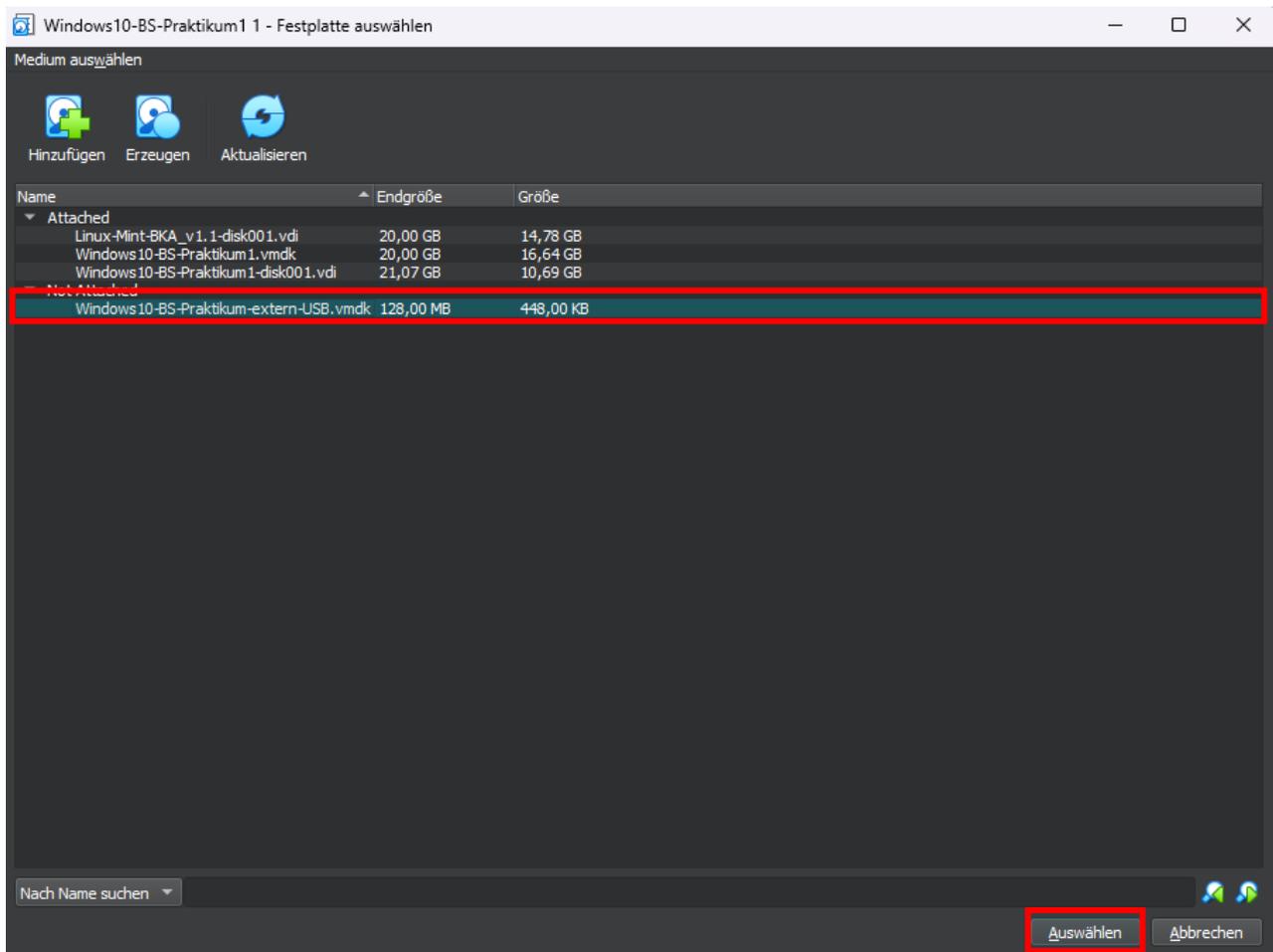


- Binden Sie bei der CD die heruntergeladene Abbilddatei **PR4.iso** ein

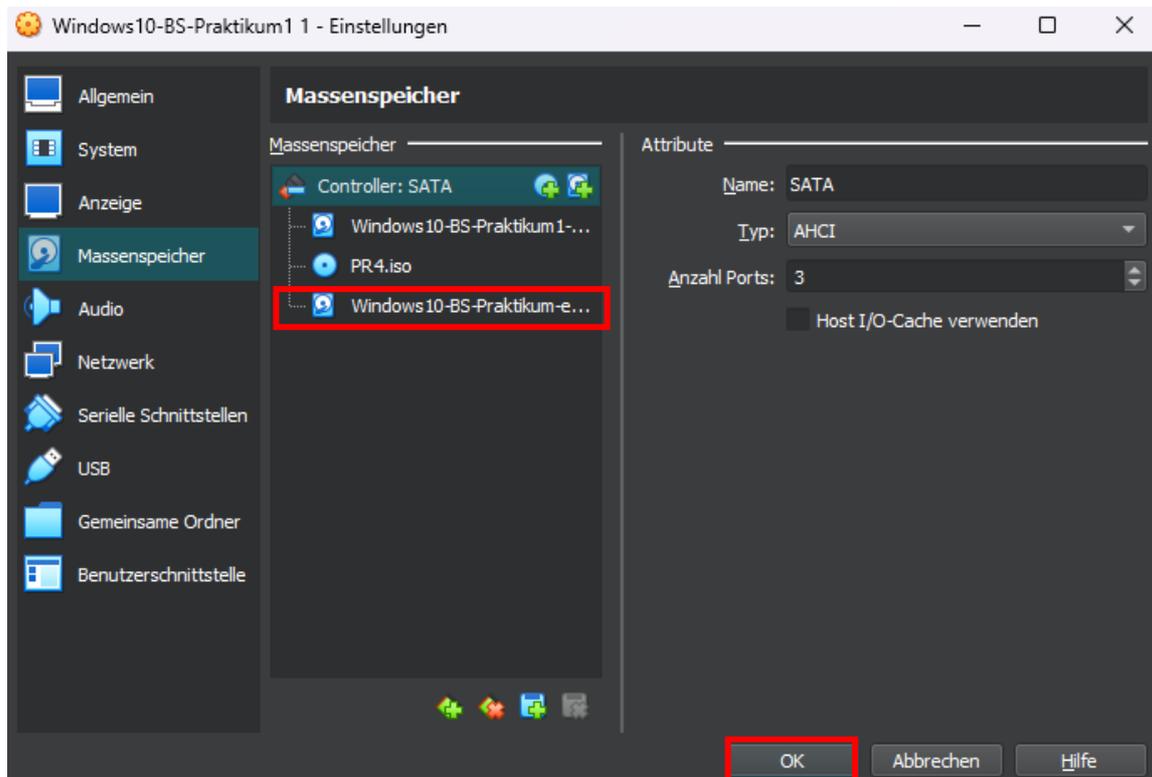


- Fügen Sie die VMDK-Datei ...extern-USB.vmdk als Massenspeicher zur VM hinzu



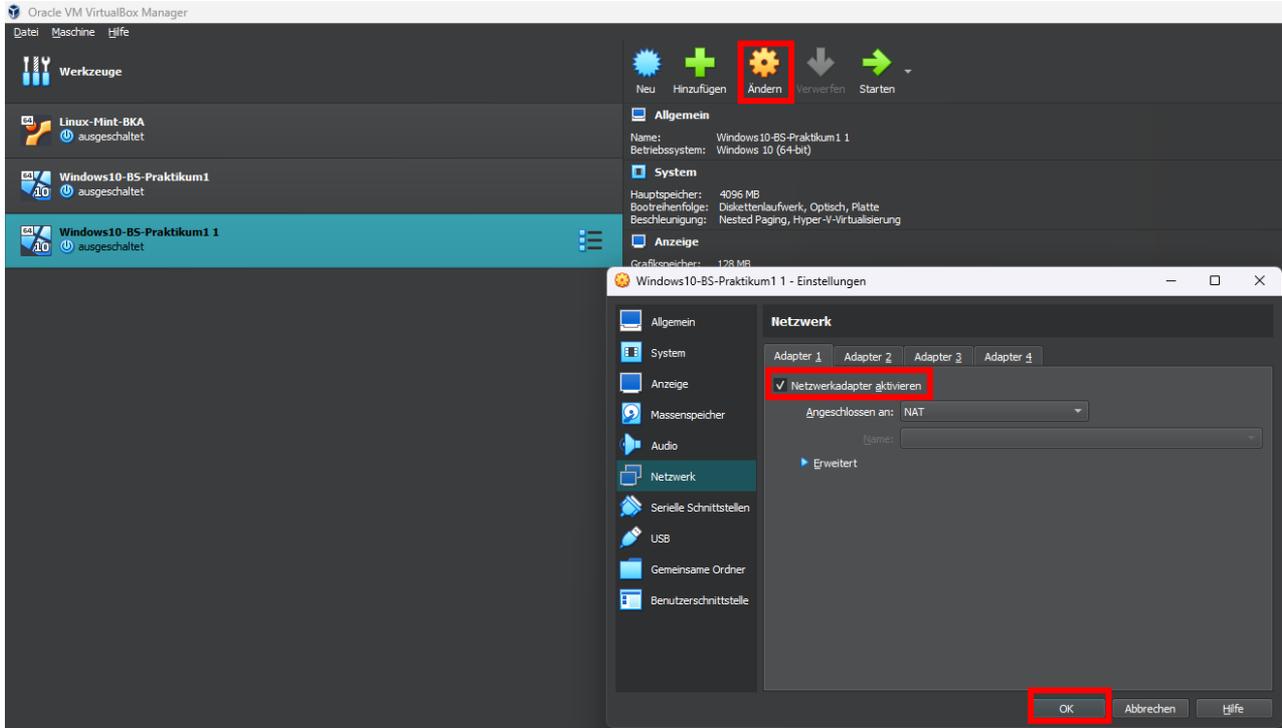


- Bestätigen Sie die Änderungen mit OK

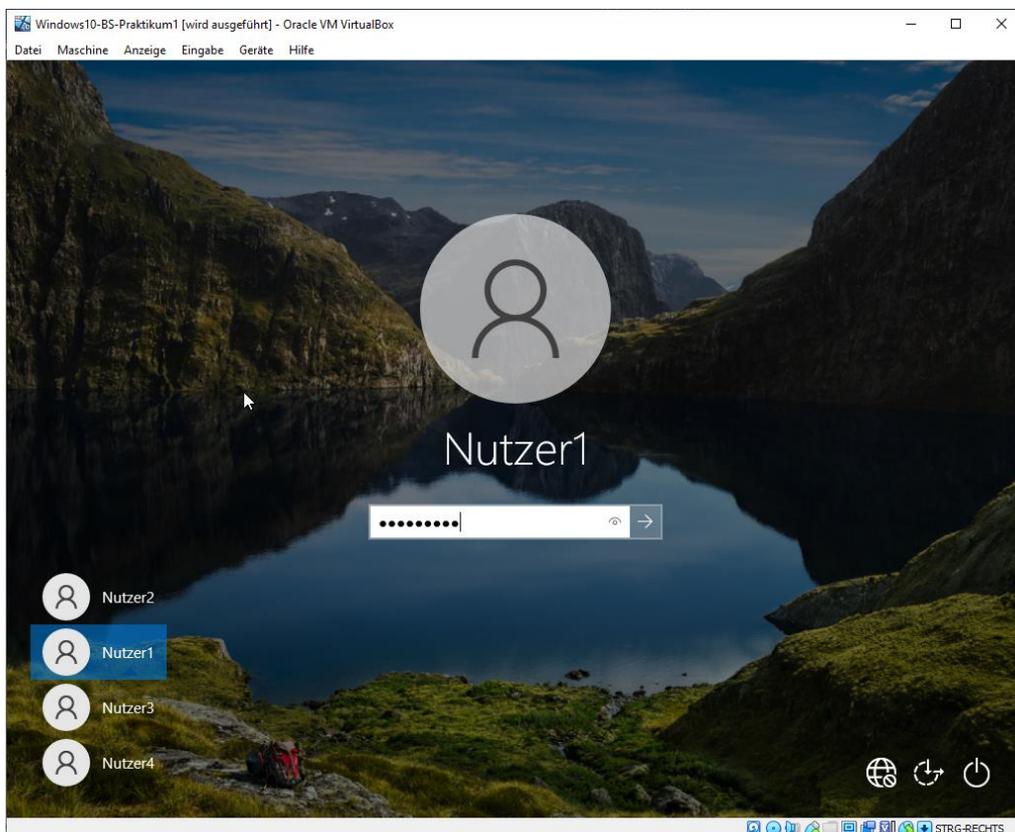


Die Firewall Einstellungen

Gehen Sie erneut auf **Ändern** (nicht Doppelklicken auf die VM, das würde diese Starten). Überprüfen Sie nun, ob der Netzwerkadapter aktiviert ist. Wenn nicht, setzen Sie bitte den Haken bei „**Netzwerkadapter aktivieren**“.

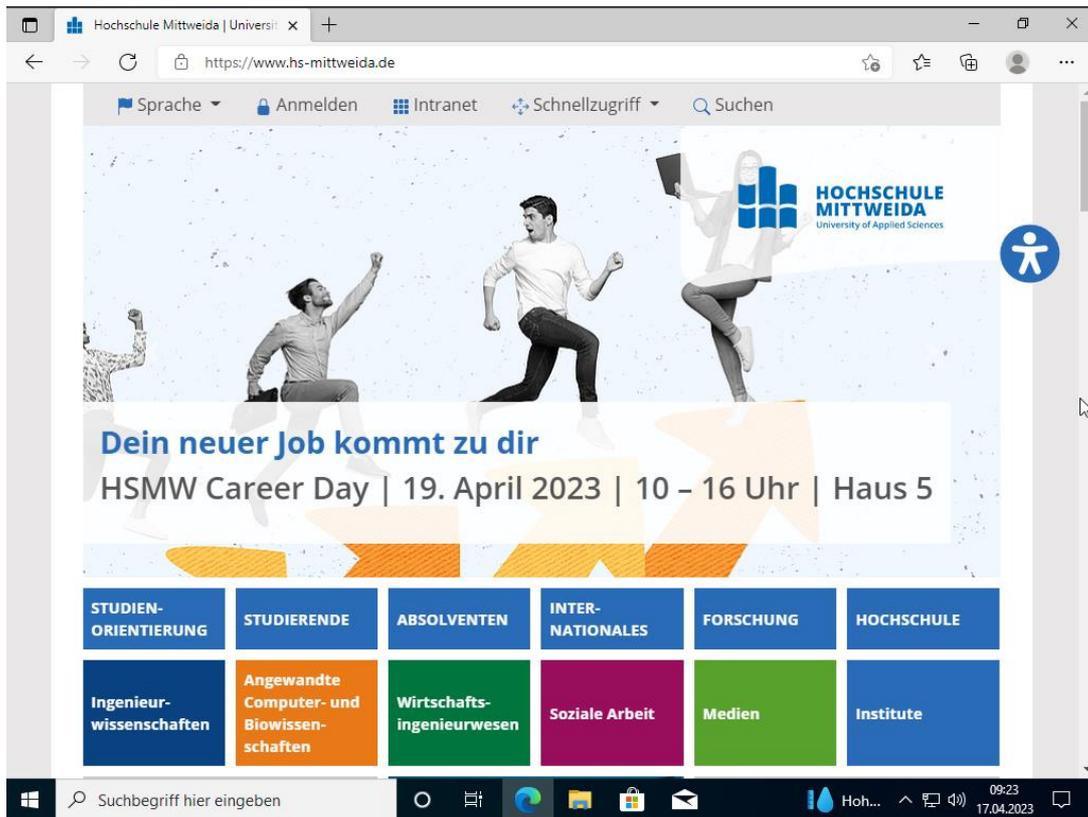


Starten Sie jetzt die VM und loggen sich als **Nutzer1** mit **Kennwort1** ein.

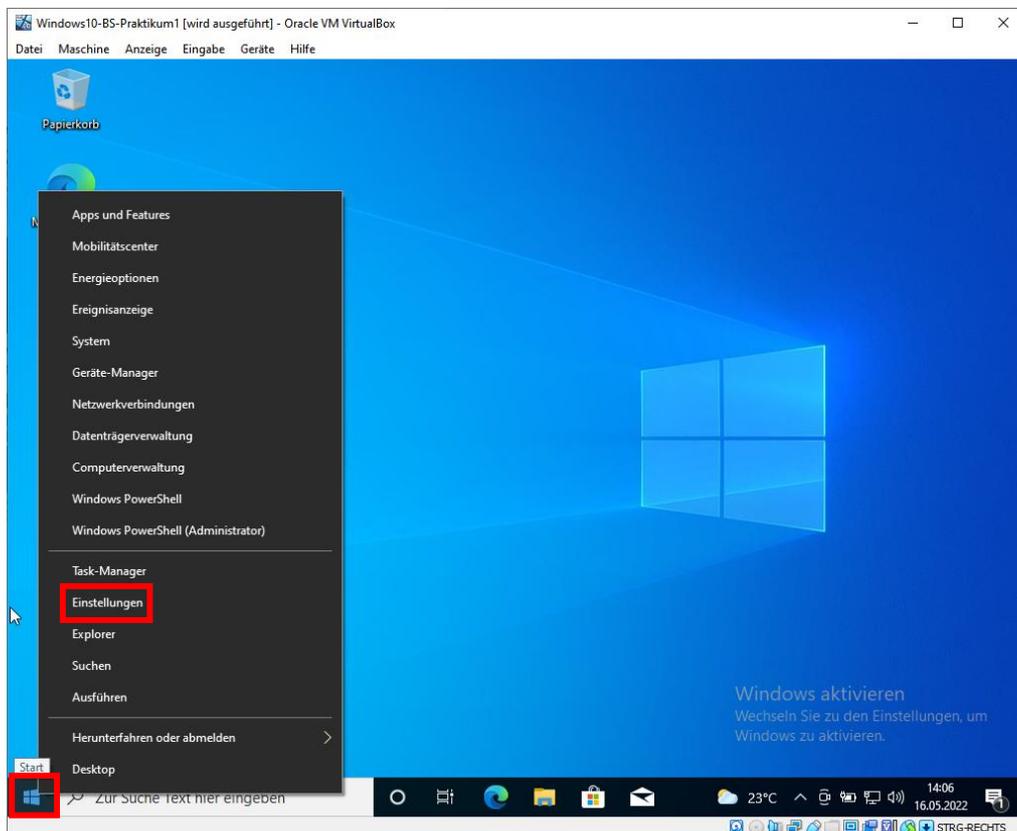


Öffnen Sie im Schritt 2 den **MS Edge** als Browser und bestätigen Sie die kommenden Dialoge.

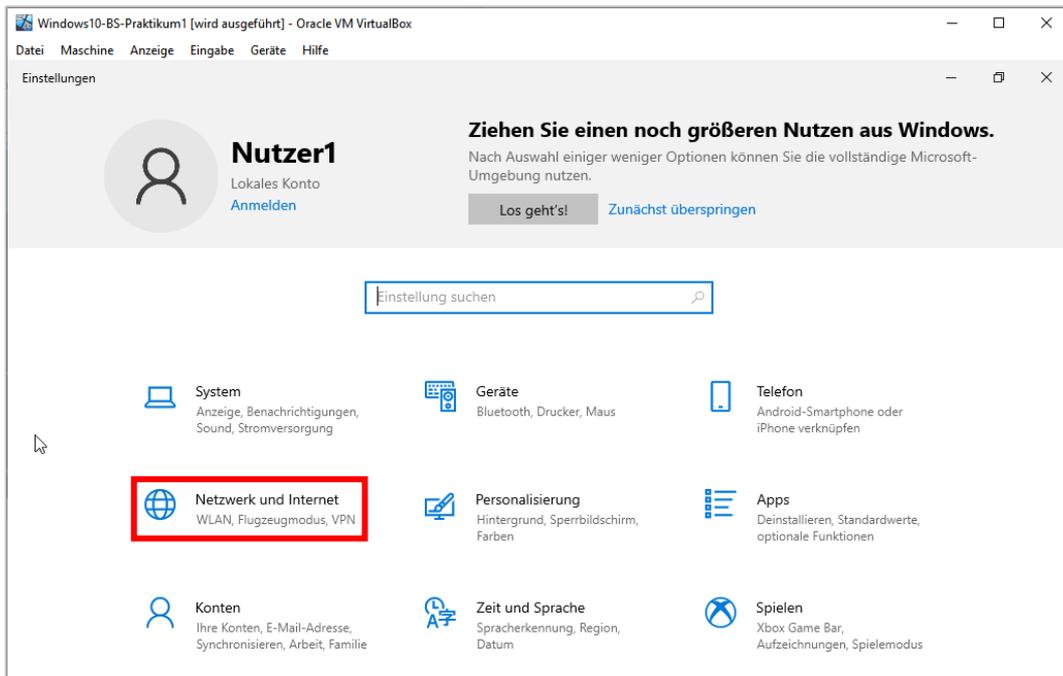
Navigieren Sie zur Webseite www.hs-mittweida.de.



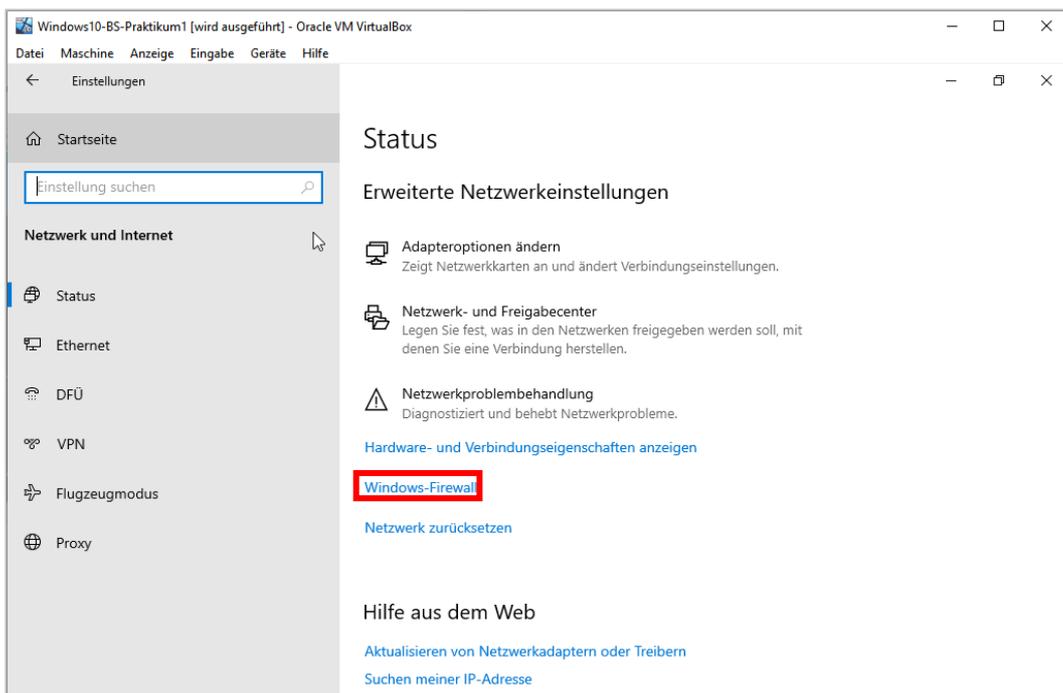
Rufen Sie die Einstellungen mit rechter Maustaste auf den Windows Start Button auf.



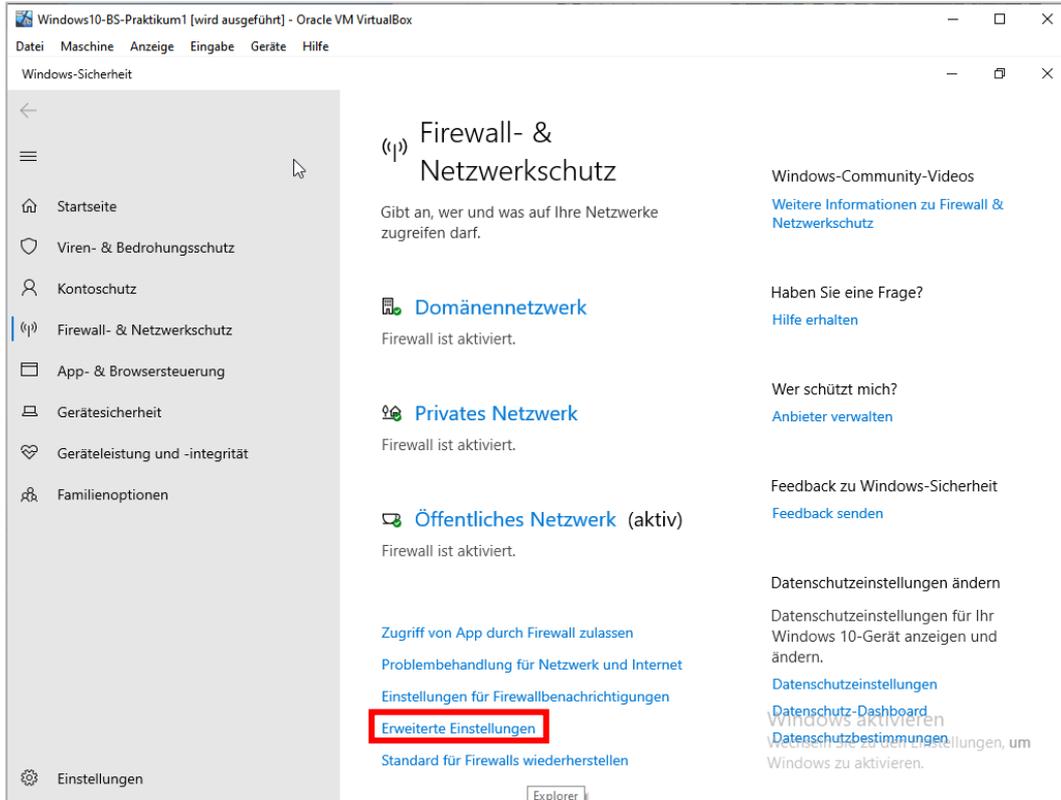
➤ Wählen Sie in den Einstellungen Netzwerk aus



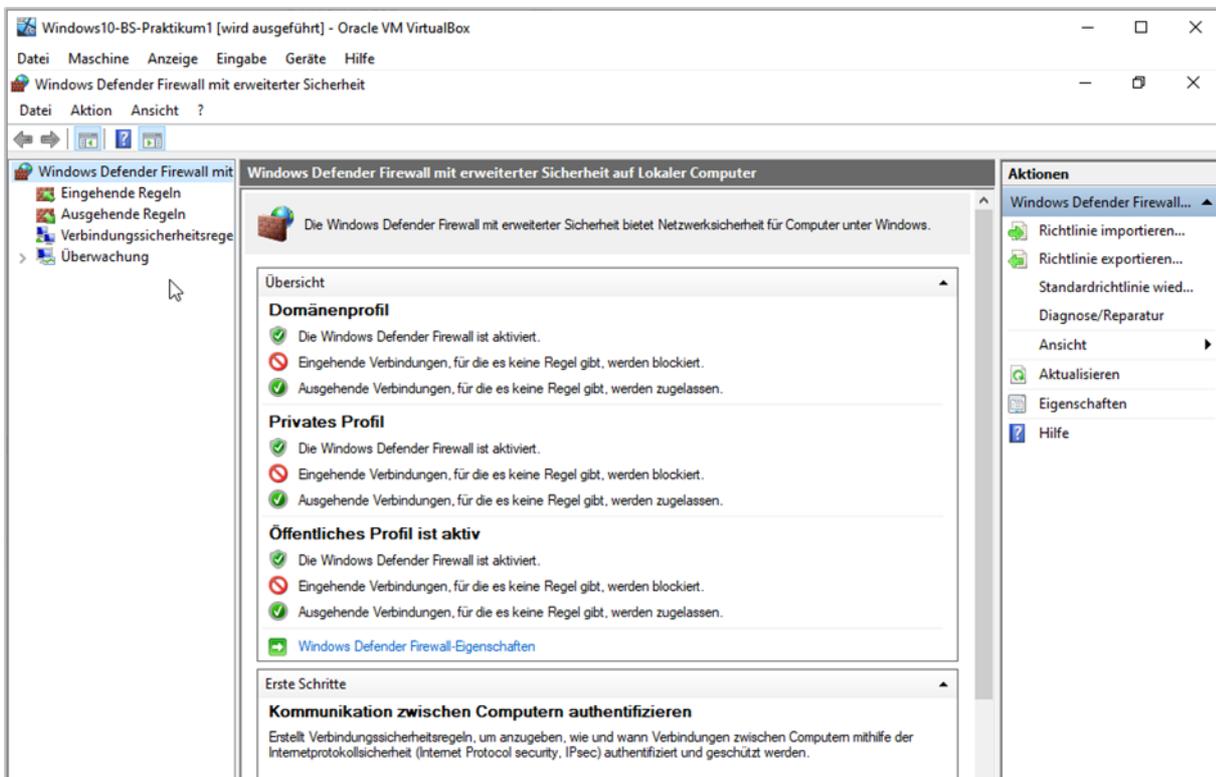
➤ Öffnen Sie die Windows Firewall



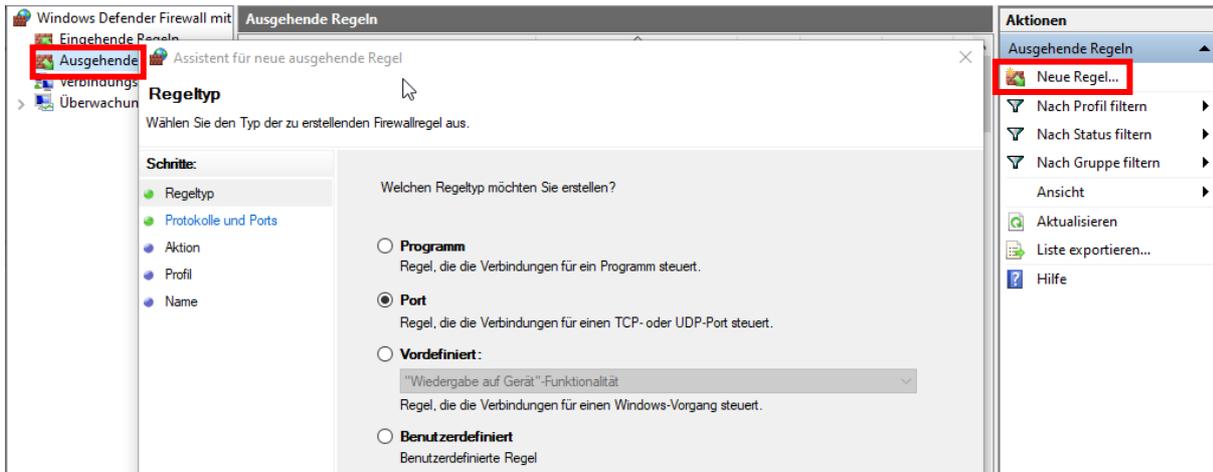
➤ Wählen Sie hier Erweiterte Einstellungen



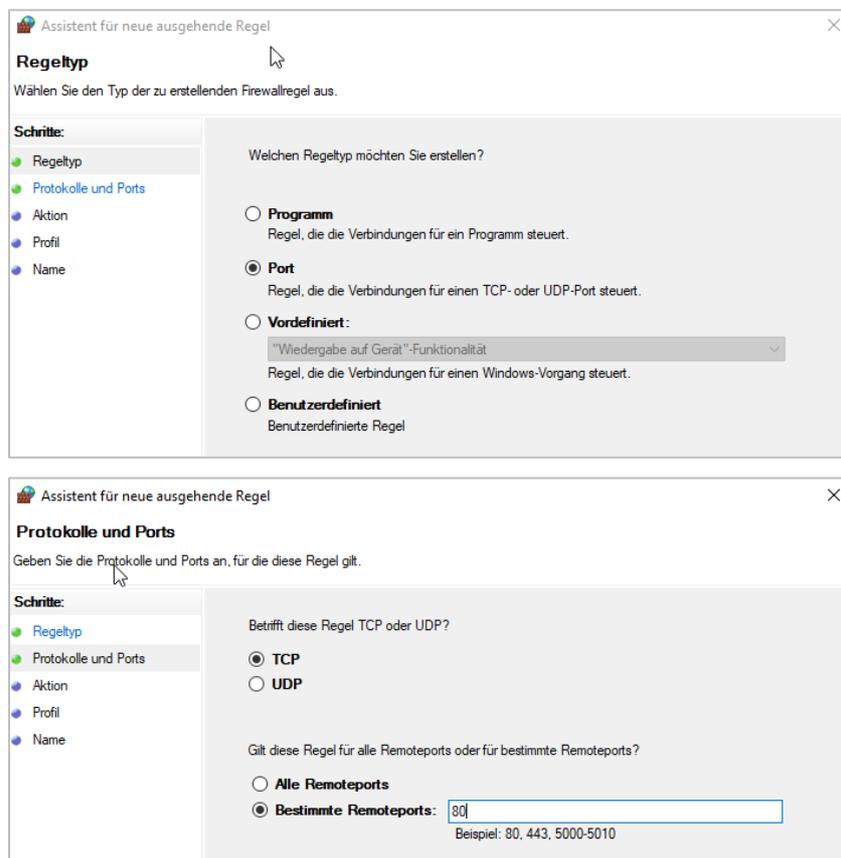
- Achtung es gibt beim Aufrufen einen Bug in der Ansicht
- Erweiterte Einstellungen sind im Hintergrund – Alt+TAB zum Hervorholen wählen



➤ Gehen Sie auf Ausgehende Regeln und Wählen mit dem Seiten-Menü **Neue Regel**



➤ In der Neuen Regel wählen Sie bitte Port aus und tragen dann Port 80 ein



➤ Wählen Sie **Verbindung blockieren** und tragen dies **für alle Profile** ein

Assistent für neue ausgehende Regel

Aktion

Legen Sie die Aktion fest, die ausgeführt werden soll, wenn eine Verbindung die in der Regel angegebenen Bedingungen erfüllt.

Schritte:

- Regeltyp
- Protokolle und Ports
- Aktion
- Profil
- Name

Welche Aktion soll durchgeführt werden, wenn eine Verbindung die angegebenen Bedingungen erfüllt?

Verbindung zulassen
Dies umfasst sowohl mit IPsec geschützte als auch nicht mit IPsec geschützte Verbindungen.

Verbindung zulassen, wenn sie sicher ist
Dies umfasst nur mithilfe von IPsec authentifizierte Verbindungen. Die Verbindungen werden mit den Einstellungen in den IPsec-Eigenschaften und -regeln im Knoten "Verbindungssicherheitsregel" gesichert.

Anpassen...

Verbindung blockieren

Assistent für neue ausgehende Regel

Profil

Geben Sie die Profile an, für die diese Regel zutrifft.

Schritte:

- Regeltyp
- Protokolle und Ports
- Aktion
- Profil
- Name

Wann wird diese Regel angewendet?

Domäne
Wird angewendet, wenn ein Computer mit der Firmendomäne verbunden ist.

Privat
Wird angewendet, wenn ein Computer mit einem privaten Netzwerk (z.B. zu Hause oder am Arbeitsplatz) verbunden ist.

Öffentlich
Wird angewendet, wenn ein Computer mit einem öffentlichen Netzwerk verbunden ist.

➤ Benennen Sie diese Regel mit **Praktikum4**

Assistent für neue ausgehende Regel

Name

Geben Sie den Namen und die Beschreibung dieser Regel an.

Schritte:

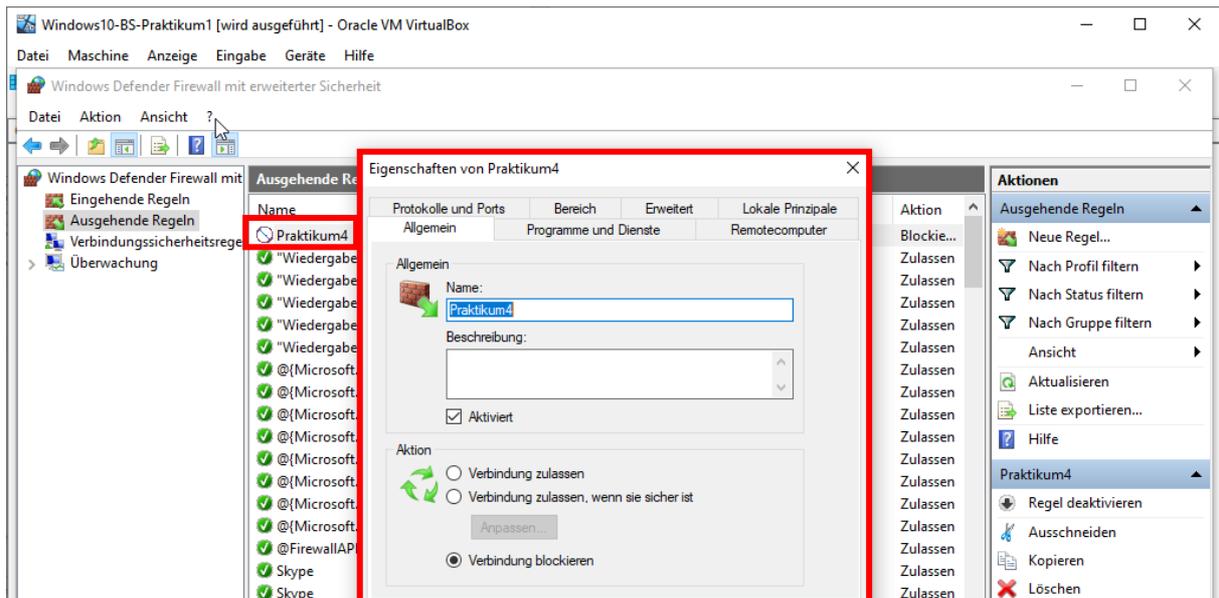
- Regeltyp
- Protokolle und Ports
- Aktion
- Profil
- Name

Name:
Praktikum4

Beschreibung (optional):

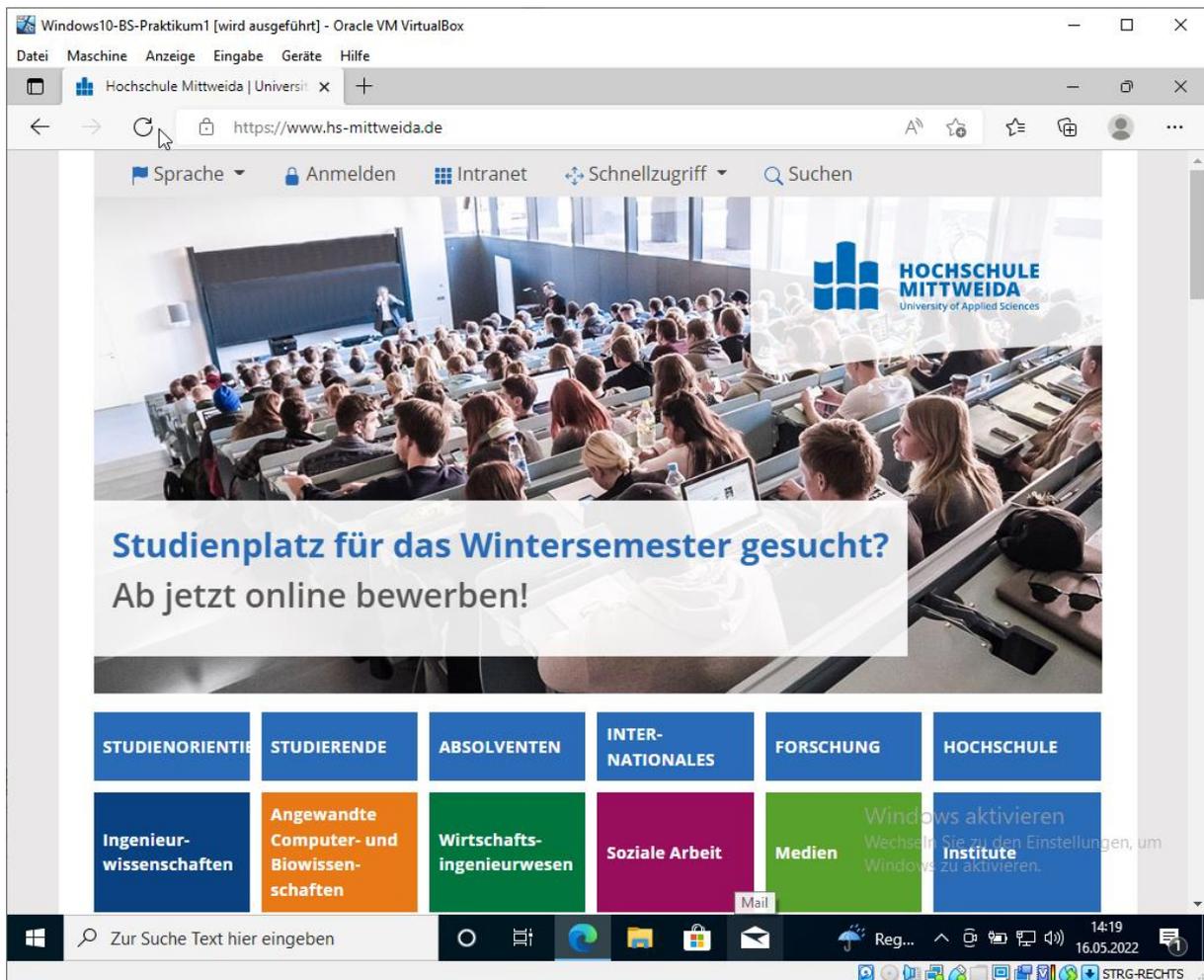
< Zurück **Fertig stellen** Abbrechen

- Überprüfen Sie die so erstellte Regel



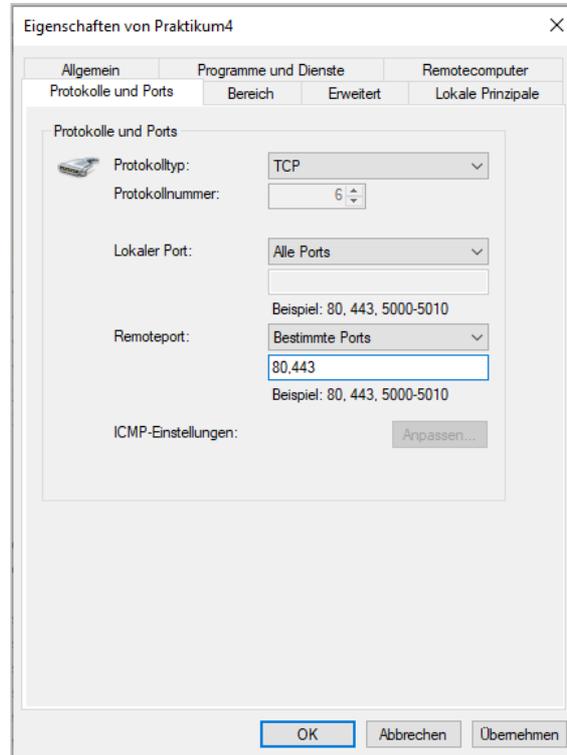
- Hat alles funktioniert?

Rufen Sie im MS Edge Browser die Webseite www.hs-mittweida.de erneut auf.

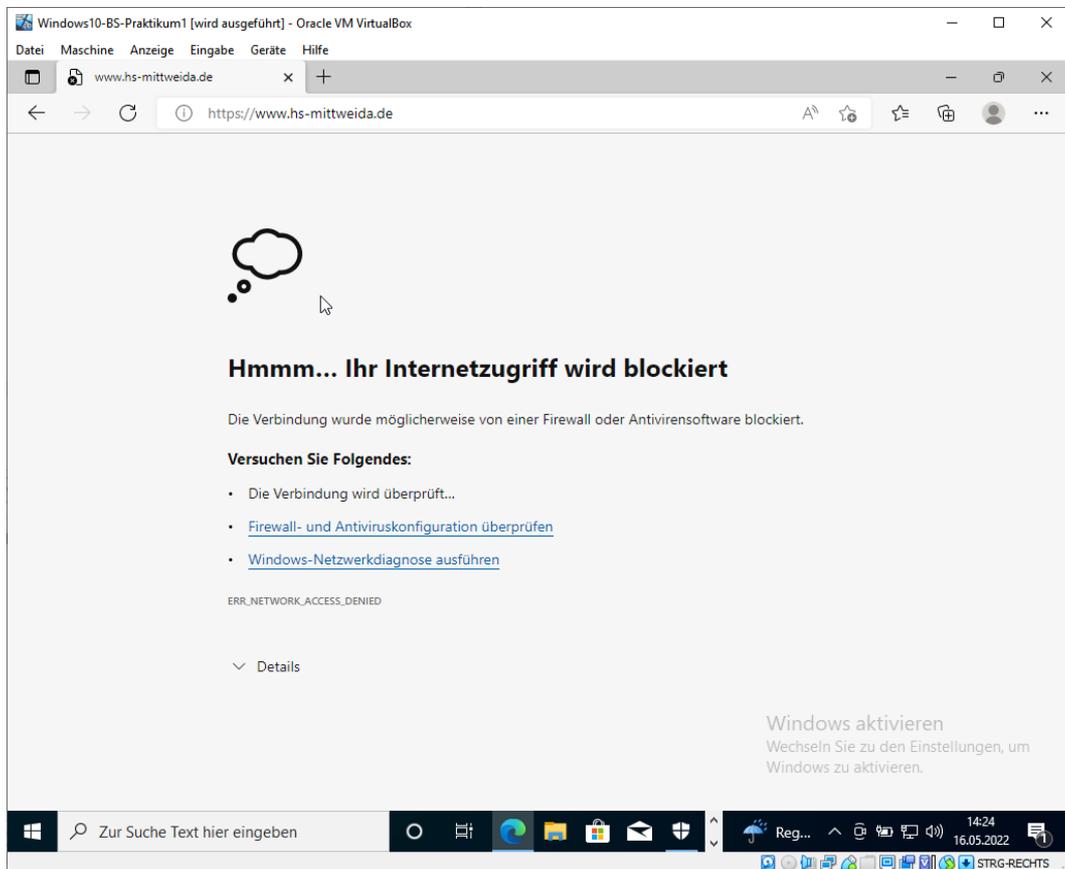


Warum ist der Abruf möglich?

- Gefiltert wird nur http auf Port 80!
- Es fehlt noch der Filter von HTTPS auf Port 443. Fügen Sie diesen **in allen drei Profilen** hinzu

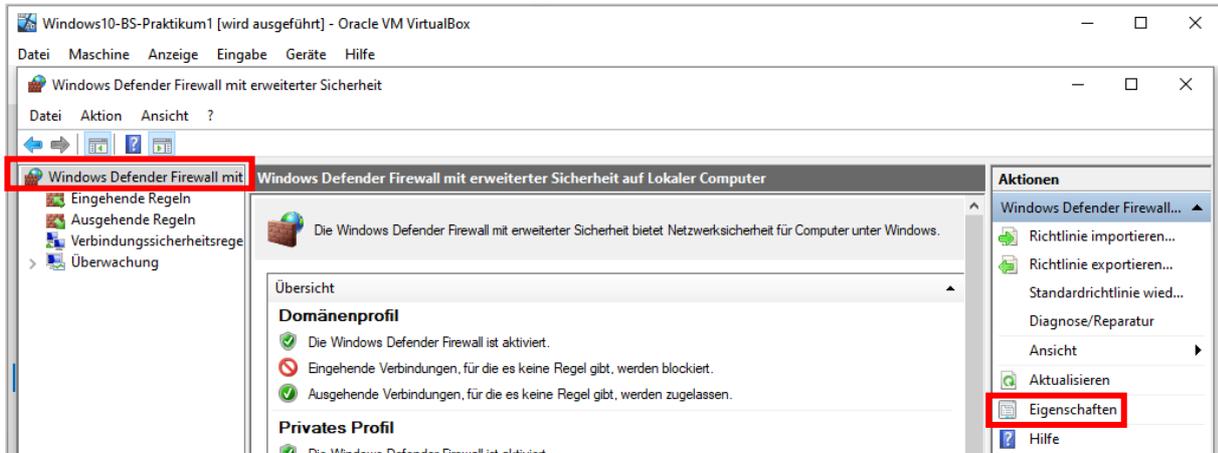


- Nun sollte der Zugriff auf die Webseite blockiert sein

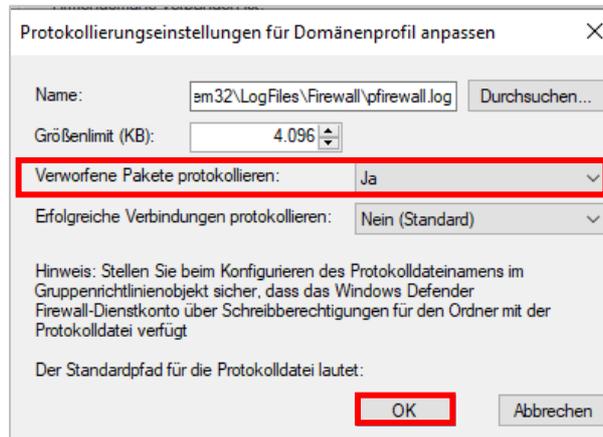
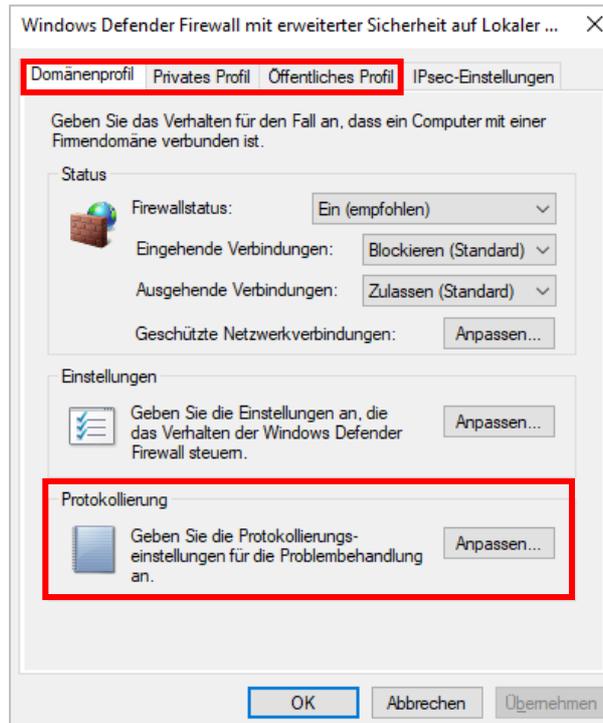


Firewall-Log Dateien einrichten und prüfen

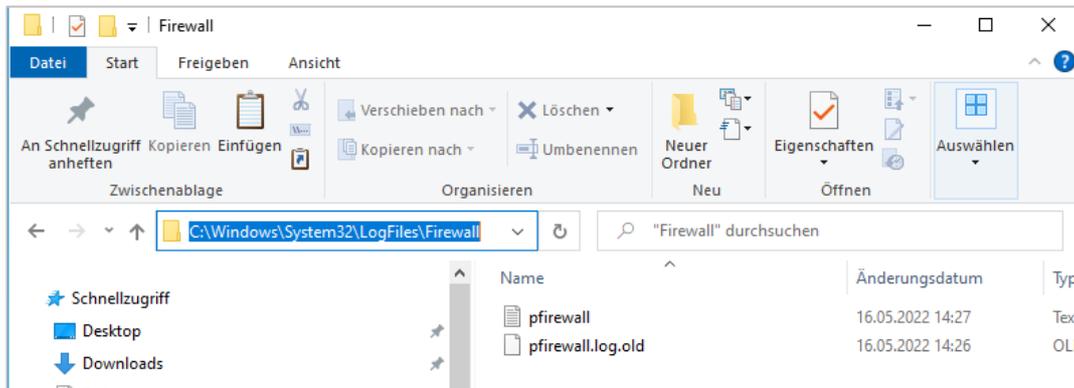
Protokollierung aktivieren mit Auswahl der Eigenschaften der Defender Firewall.



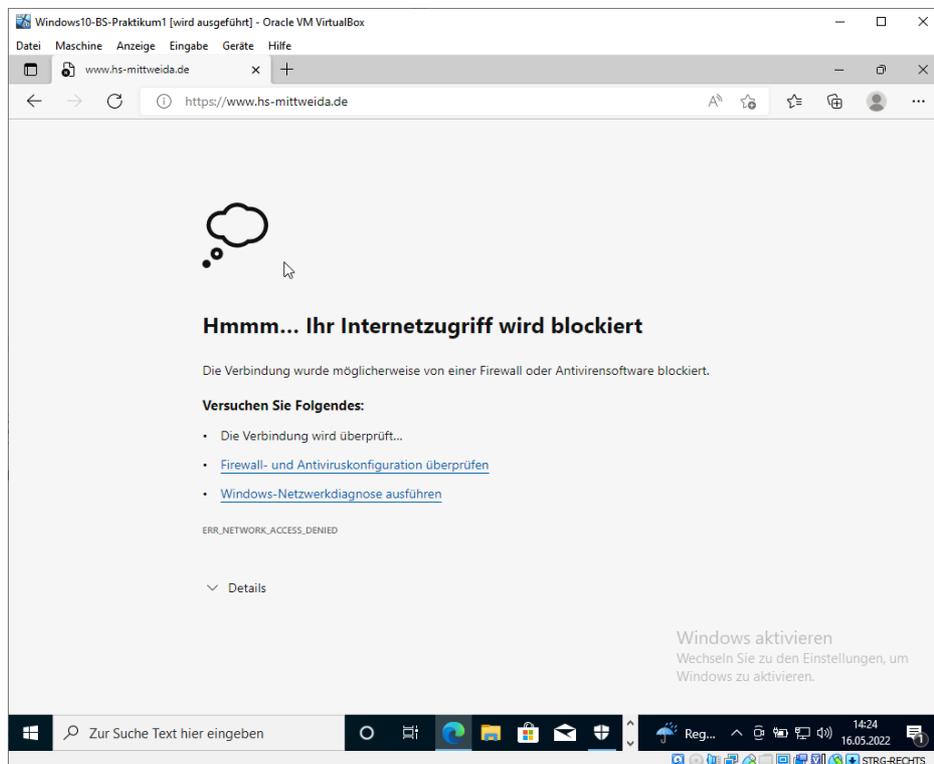
➤ Aktivieren Sie für alle drei Profile das Firewall Log, welches nur blockierte Pakete registrieren soll



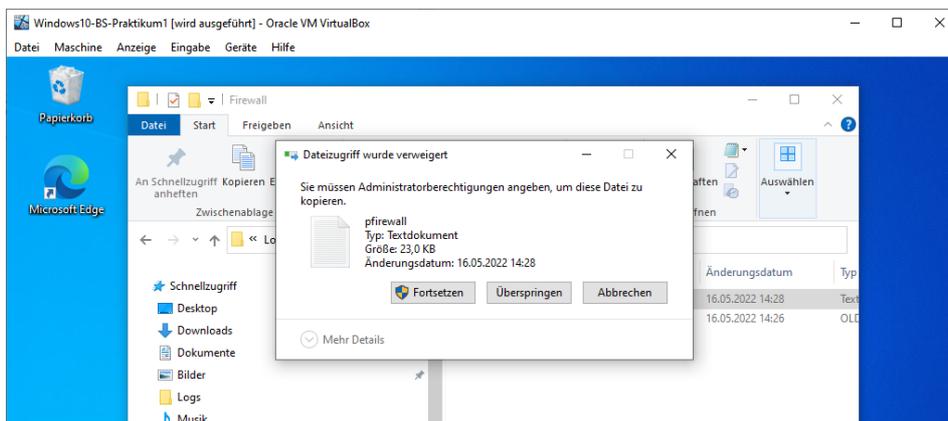
- Öffnen Sie den Windows Explorer und navigieren Sie zum Firewall Log (C:\windows\system32\Logfiles\Firewall)



- Öffnen Sie den Browser und navigieren Sie zu www.hs-mittweida.de, um einen Eintrag im Log zu erzeugen



- Kopieren Sie das Log auf Desktop, da es nicht direkt im laufenden Betrieb geöffnet werden kann



- Ermitteln Sie mit Hilfe der Eingabeaufforderung/Kommandozeile die IP-Adresse der URL www.hs-mittweida.de
- Suchen Sie diese in der Logdatei

```

Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Nutzer1>ping www.hs-mittweida.de

Ping wird ausgeführt für www.hs-mittweida.de [141.55.192.190] mit 32 Bytes Daten:
Antwort von 141.55.192.190: Bytes=32 Zeit=27ms TTL=49
Antwort von 141.55.192.190: Bytes=32 Zeit=28ms TTL=49
Antwort von 141.55.192.190: Bytes=32 Zeit=27ms TTL=49
Antwort von 141.55.192.190: Bytes=32 Zeit=26ms TTL=49

Ping-Statistik für 141.55.192.190:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 26ms, Maximum = 28ms, Mittelwert = 27ms

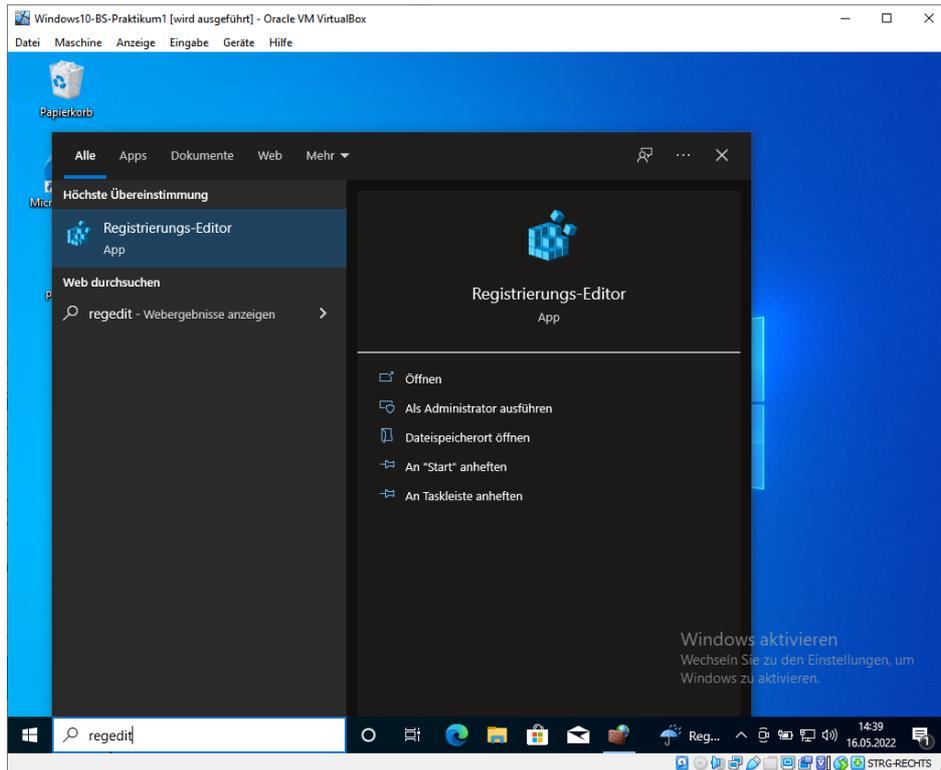
C:\Users\Nutzer1>

```

Datei	Bearbeiten	Format	Ansicht	Hilfe
2022-05-16 14:28:58	DROP	TCP	10.0.2.15 13.107.21.200	51683 443 0 - 0 0 0 - - - SEND
2022-05-16 14:28:58	DROP	TCP	10.0.2.15 204.79.197.200	51684 443 0 - 0 0 0 - - - SEND
2022-05-16 14:28:58	DROP	TCP	10.0.2.15 13.107.21.200	51685 443 0 - 0 0 0 - - - SEND
2022-05-16 14:28:58	DROP	TCP	10.0.2.15 204.79.197.203	51686 443 0 - 0 0 0 - - - SEND
2022-05-16 14:28:59	DROP	TCP	10.0.2.15 204.79.197.200	51687 443 0 - 0 0 0 - - - SEND
2022-05-16 14:28:59	DROP	TCP	10.0.2.15 141.55.192.190	51688 80 0 - 0 0 0 - - - SEND
2022-05-16 14:28:59	DROP	TCP	10.0.2.15 141.55.192.190	51689 80 0 - 0 0 0 - - - SEND
2022-05-16 14:28:59	DROP	TCP	10.0.2.15 141.55.192.190	51690 443 0 - 0 0 0 - - - SEND
2022-05-16 14:28:59	DROP	TCP	10.0.2.15 13.107.21.200	51691 443 0 - 0 0 0 - - - SEND
2022-05-16 14:28:59	DROP	TCP	10.0.2.15 20.73.130.64	51692 443 0 - 0 0 0 - - - SEND
2022-05-16 14:28:59	DROP	TCP	10.0.2.15 20.73.130.64	51693 443 0 - 0 0 0 - - - SEND
2022-05-16 14:29:00	DROP	TCP	10.0.2.15 141.55.192.190	51694 443 0 - 0 0 0 - - - SEND

Firewall-Eintragungen in der Registrierung überprüfen und ändern

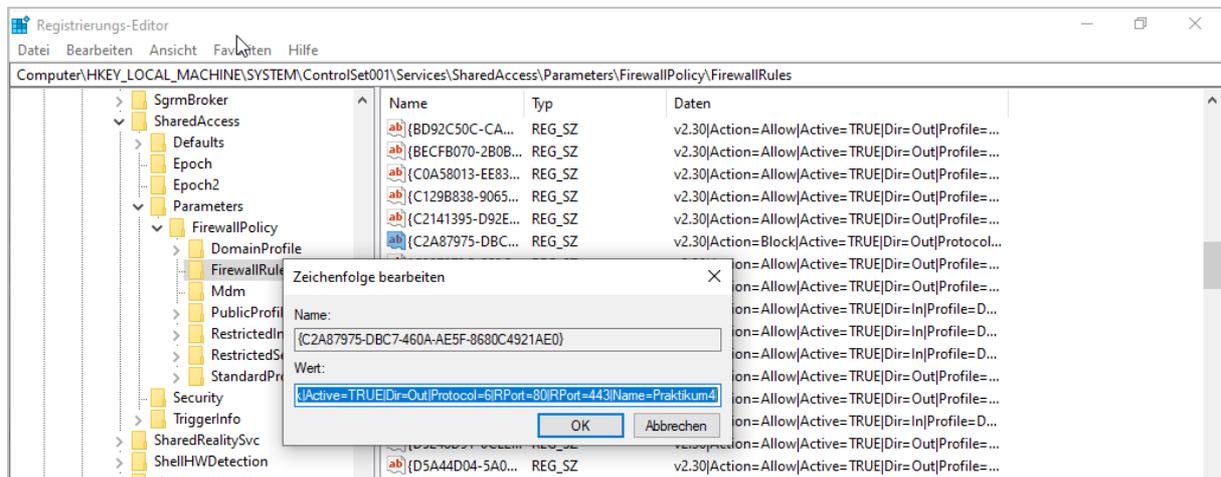
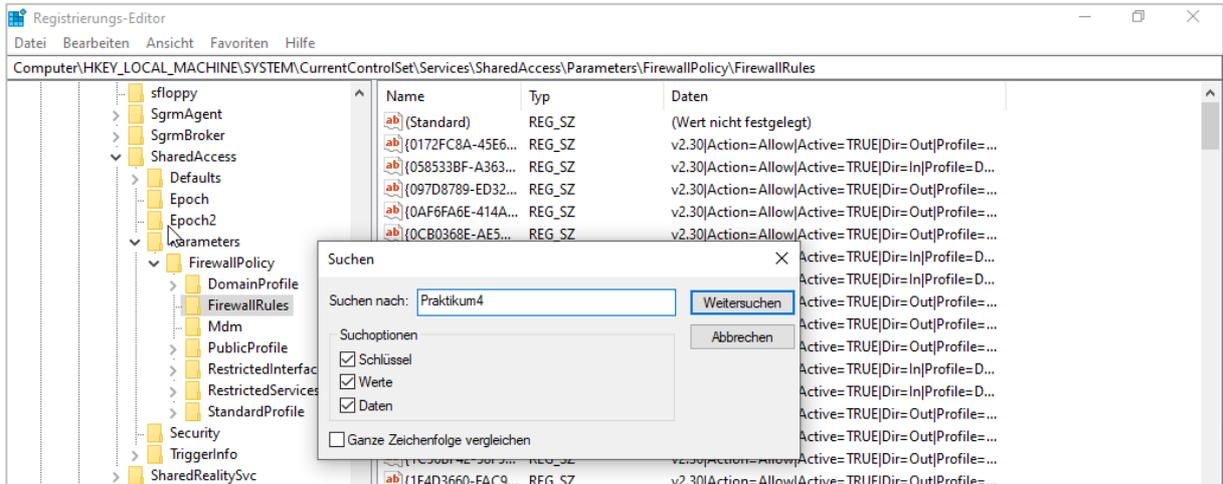
Öffnen Sie den Registrierungseditor **Regedit**.



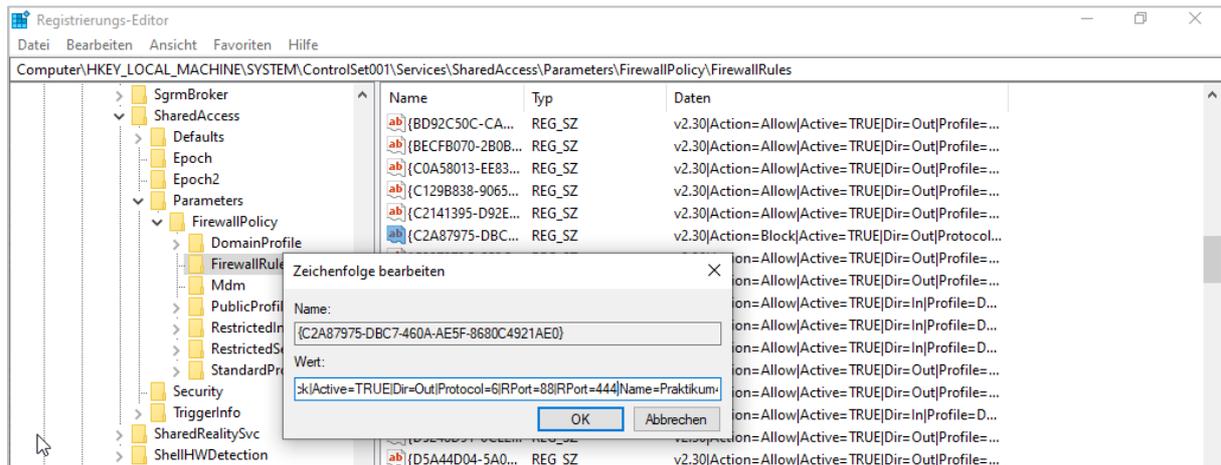
- Suchen Sie sich die Firewall Regeln heraus
- Suchen Sie sich die Regel Praktikum 4 heraus

Registrierungs-Editor			
Datei Bearbeiten Ansicht Favoriten Hilfe			
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules			
	Name	Typ	Daten
	(Standard)	REG_SZ	(Wert nicht festgelegt)
	{0172FC8A-45E6...	REG_SZ	v2.30 Action=Allow Active=TRUE Dir=Out Profile=...
	{058533BF-A363...	REG_SZ	v2.30 Action=Allow Active=TRUE Dir=In Profile=D...
	{097D8789-ED32...	REG_SZ	v2.30 Action=Allow Active=TRUE Dir=Out Profile=...
	{0AF6FA6E-414A...	REG_SZ	v2.30 Action=Allow Active=TRUE Dir=Out Profile=...
	{0CB0368E-AE5...	REG_SZ	v2.30 Action=Allow Active=TRUE Dir=Out Profile=...
	{11600BC6-5DD...	REG_SZ	v2.30 Action=Allow Active=TRUE Dir=In Profile=D...
	{1292C5F4-F7A9...	REG_SZ	v2.30 Action=Allow Active=TRUE Dir=In Profile=D...
	{12DAC17A-370...	REG_SZ	v2.30 Action=Allow Active=TRUE Dir=Out Profile=...
	{13CC6988-834C...	REG_SZ	v2.30 Action=Allow Active=TRUE Dir=Out Profile=...
	{16D7F51E-F4E3...	REG_SZ	v2.30 Action=Allow Active=TRUE Dir=Out Profile=...
	{180EDAB6-4748...	REG_SZ	v2.30 Action=Allow Active=TRUE Dir=In Profile=D...
	{195EBA17-8DF1...	REG_SZ	v2.30 Action=Allow Active=TRUE Dir=In Profile=D...
	{1B7919C8-8440...	REG_SZ	v2.30 Action=Allow Active=TRUE Dir=Out Profile=...
	{1C2C8DBC-9D4...	REG_SZ	v2.30 Action=Allow Active=TRUE Dir=Out Profile=...
	{1C56BF42-58F5...	REG_SZ	v2.30 Action=Allow Active=TRUE Dir=Out Profile=...

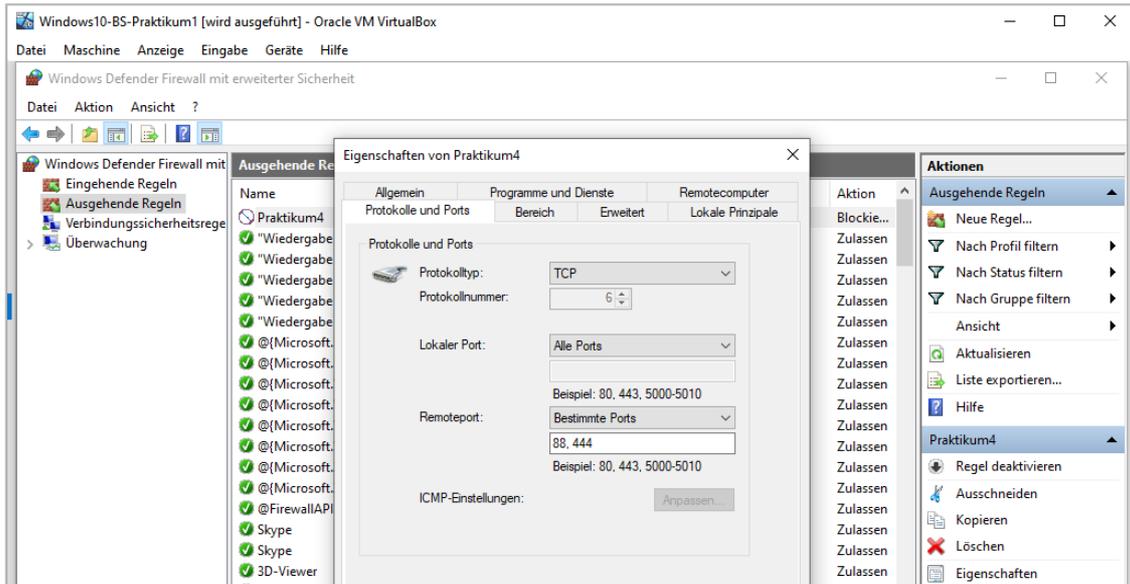
➤ Bearbeiten > Suchen > Praktikum4



➤ Ändern Sie im Schlüssel die Werte Port 80 > 88 und Port 443 > 444

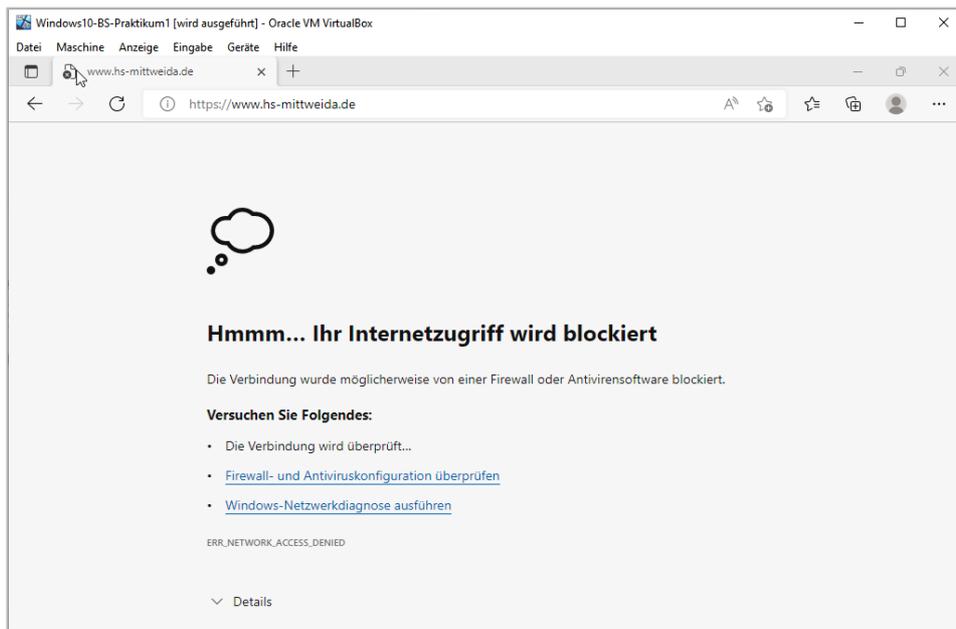


➤ Schließen Sie das Firewall Fenster und öffnen Sie es erneut



Geht der Browser?

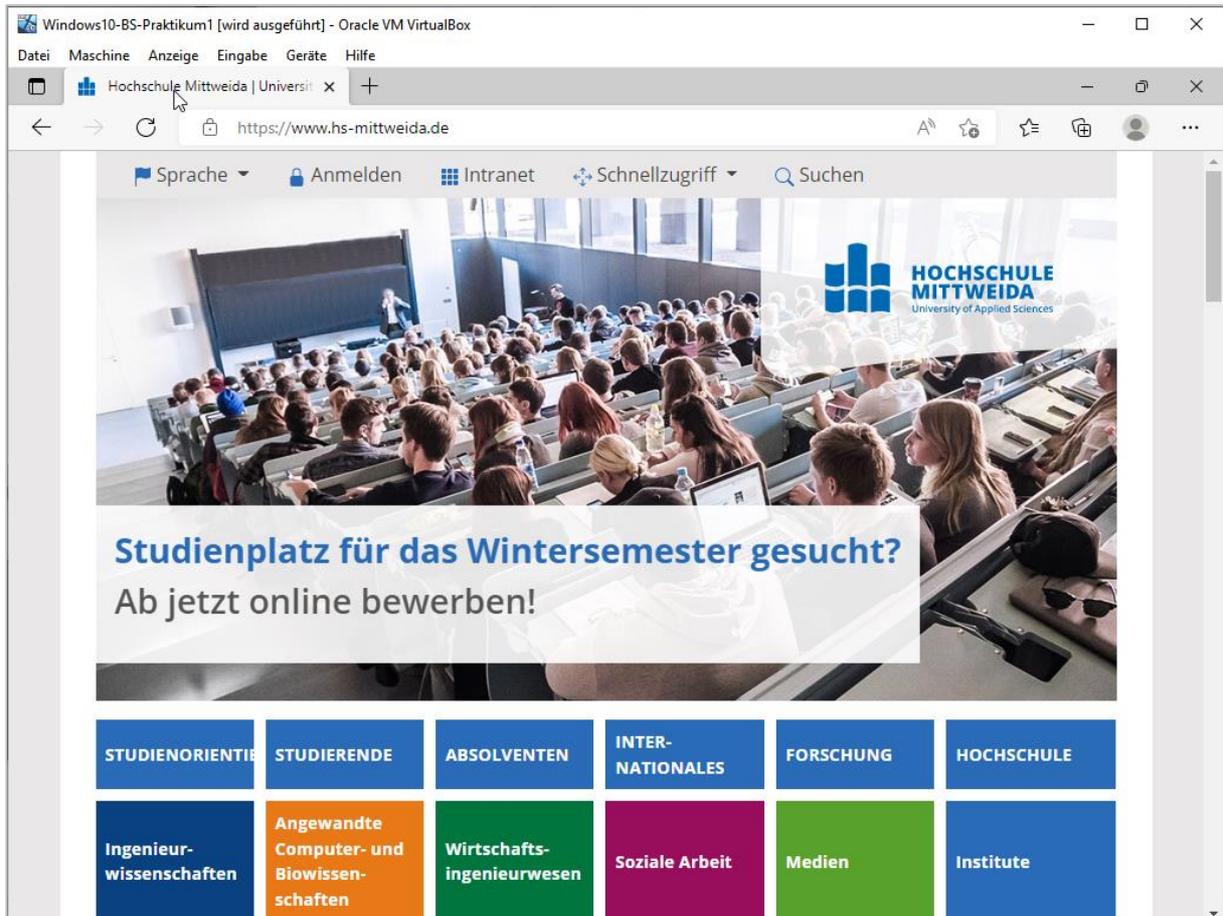
- Rufen Sie dazu die URL www.hs-mittweida.de auf



➤ Nein!

- ✓ **Ursache:** die Firewall Eintragungen werden beim Starten gelesen oder beim Ändern durch den Firewall Regel Editor, jedoch nicht durch Änderungen in der Registry.

- Starten Sie Windows neu und versuchen Sie es erneut

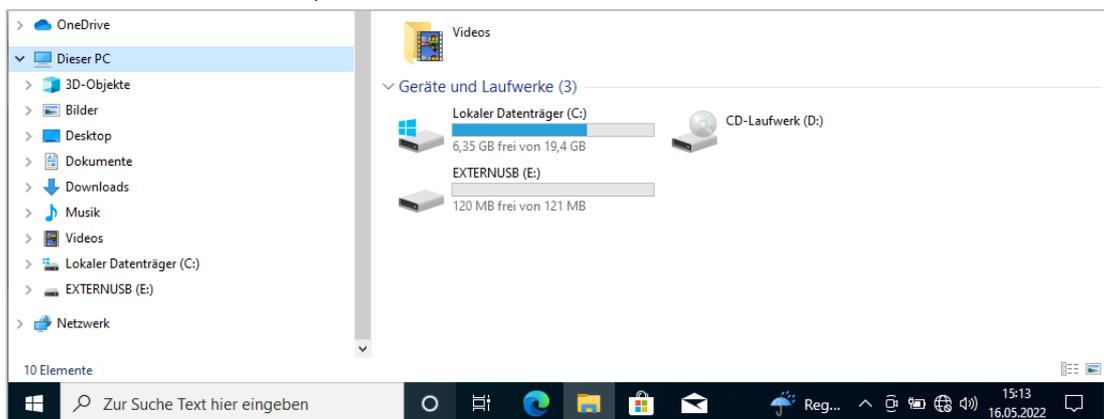


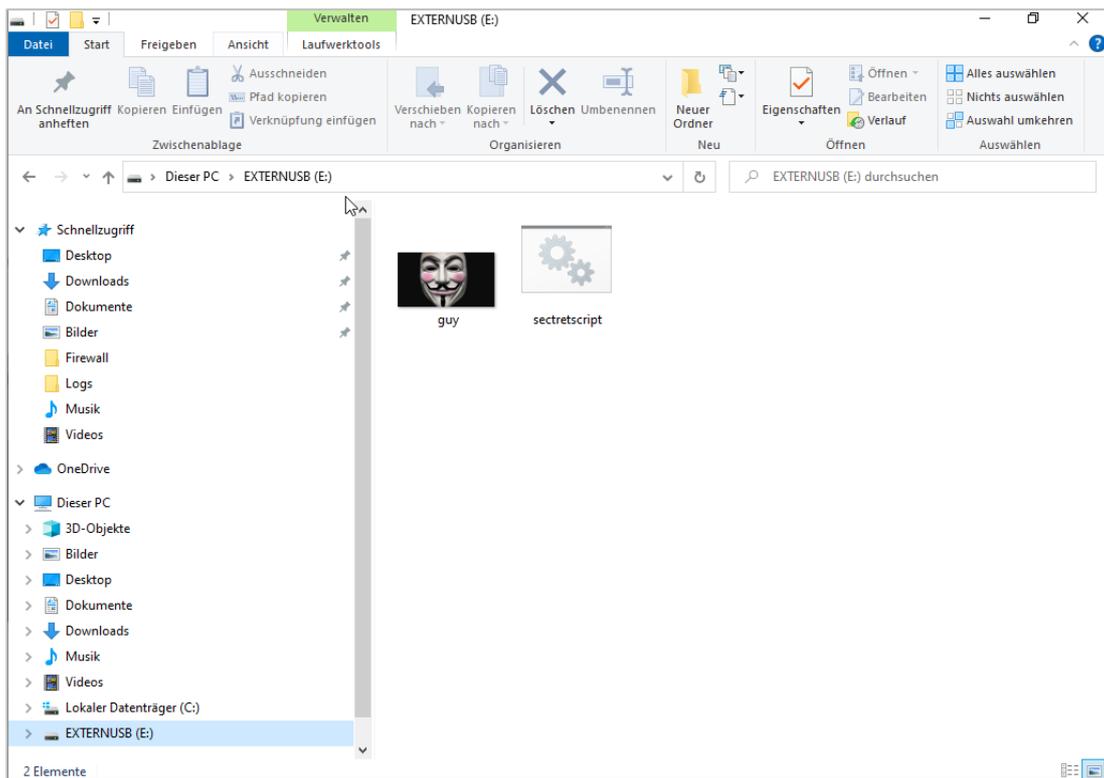
Recent/Verlaufs-Eintragungen

Recent-Eintragungen anlegen

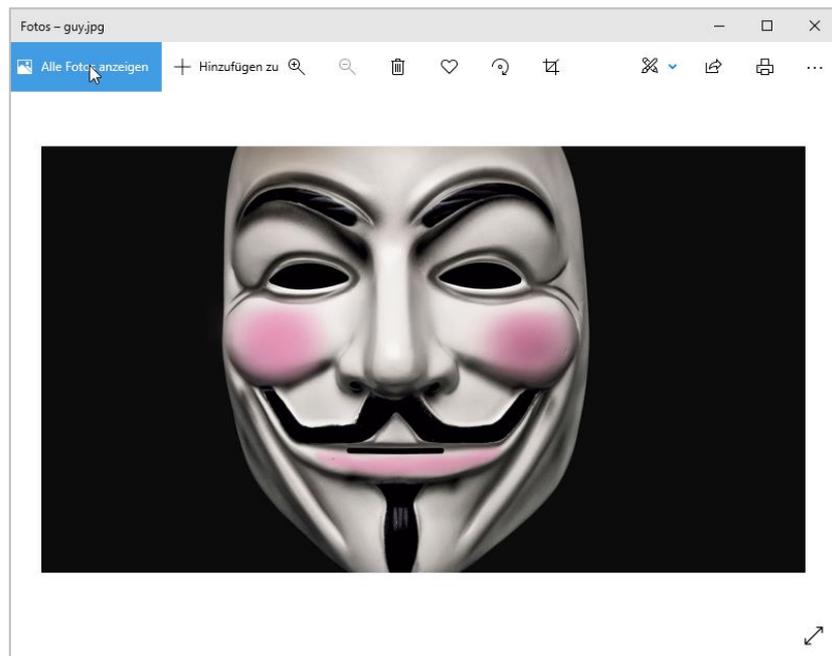
Schließen Sie alle offenen Anwendungen und Fenster.

- Öffnen Sie den Windows Explorer und wechseln Sie auf das externe Laufwerk EXTERNUSB

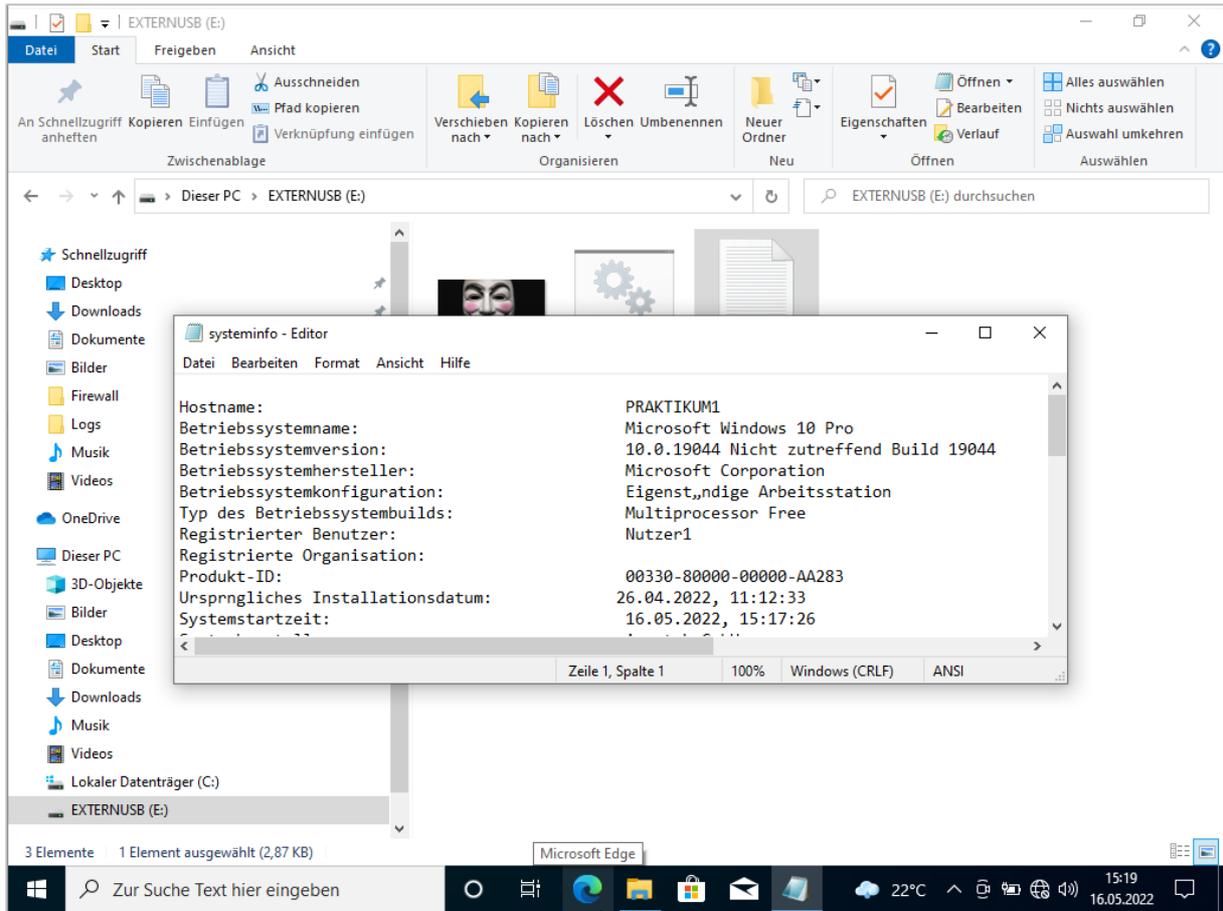




➤ Schauen Sie sich die Bilddatei an

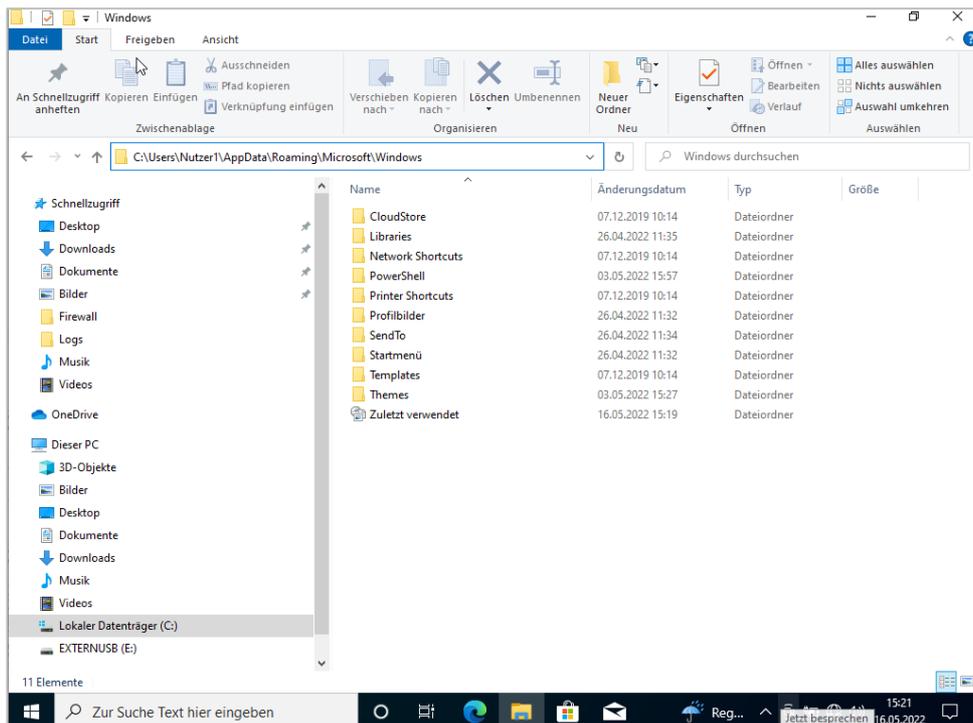


➤ Starten Sie durch Doppelklick zudem die BAT-Datei und Öffnen Sie danach die neu erstellte Datei Systeminfo.txt

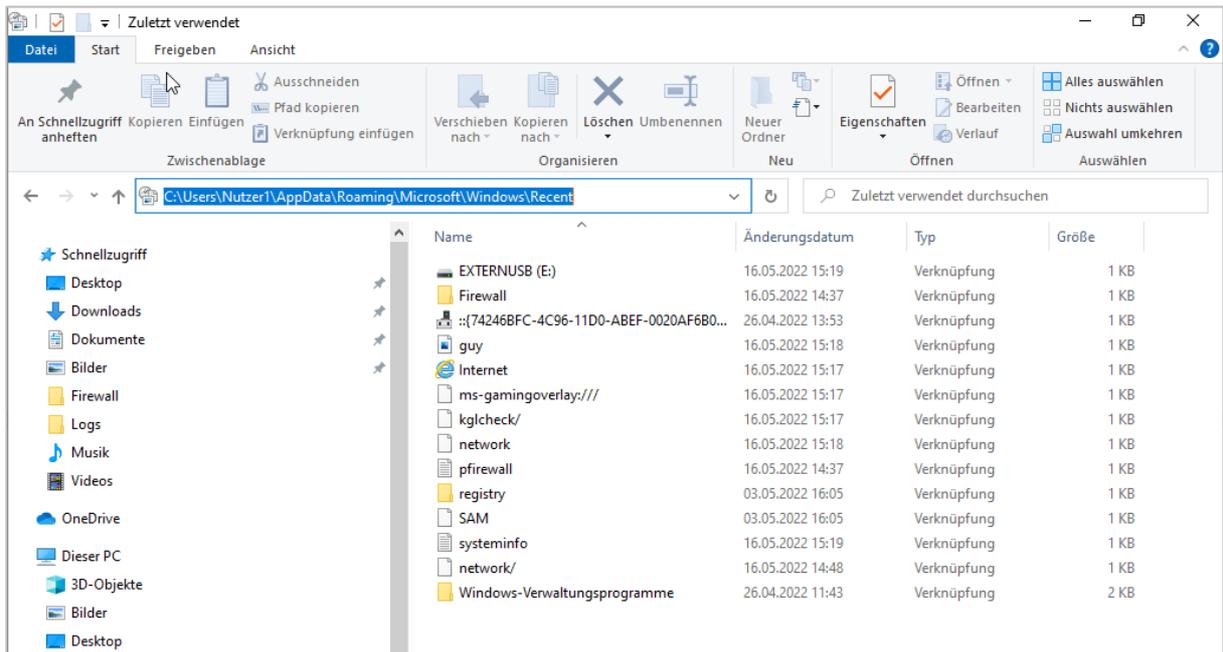


Recent-Dateien lesen

Wechseln Sie jetzt in das Verzeichnis **C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows**.

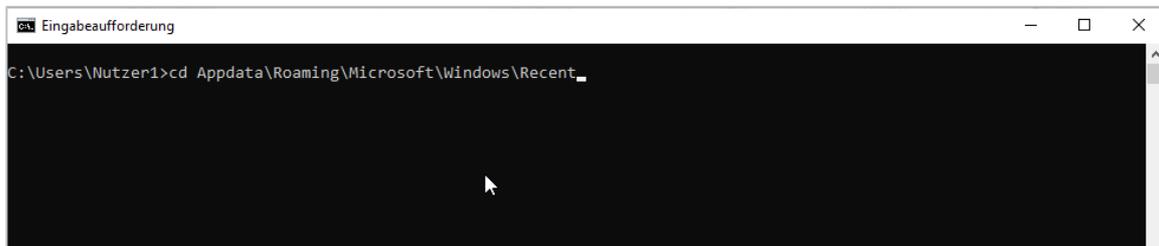


➤ Sehen Sie einen Recent Ordner? Wechseln Sie in diesen

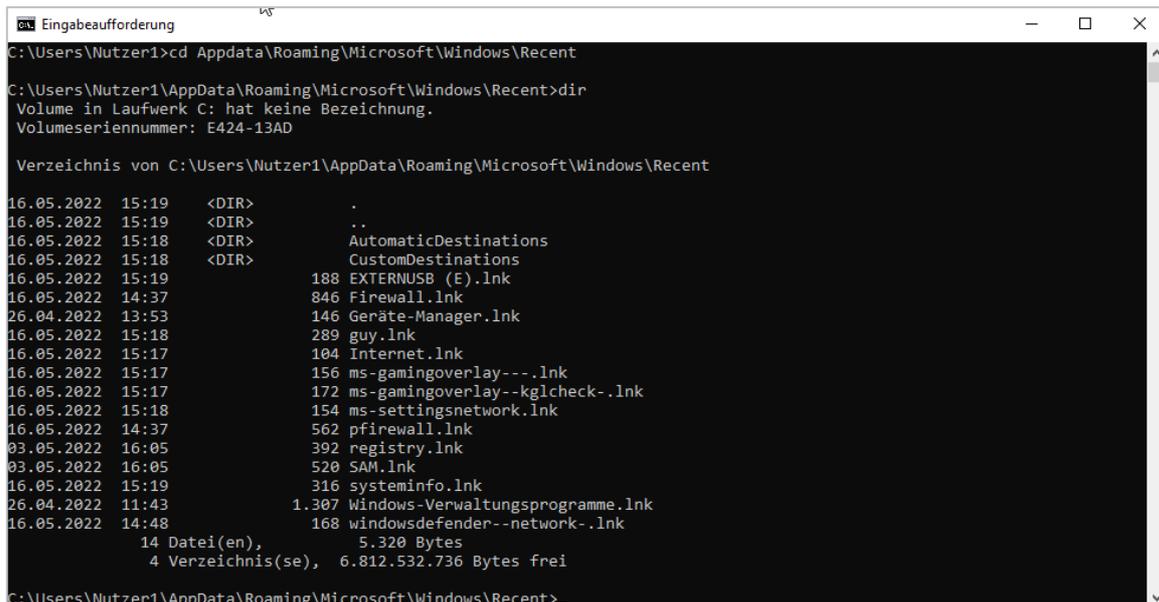


➤ Können Sie viel mit dieser Ansicht anfangen?

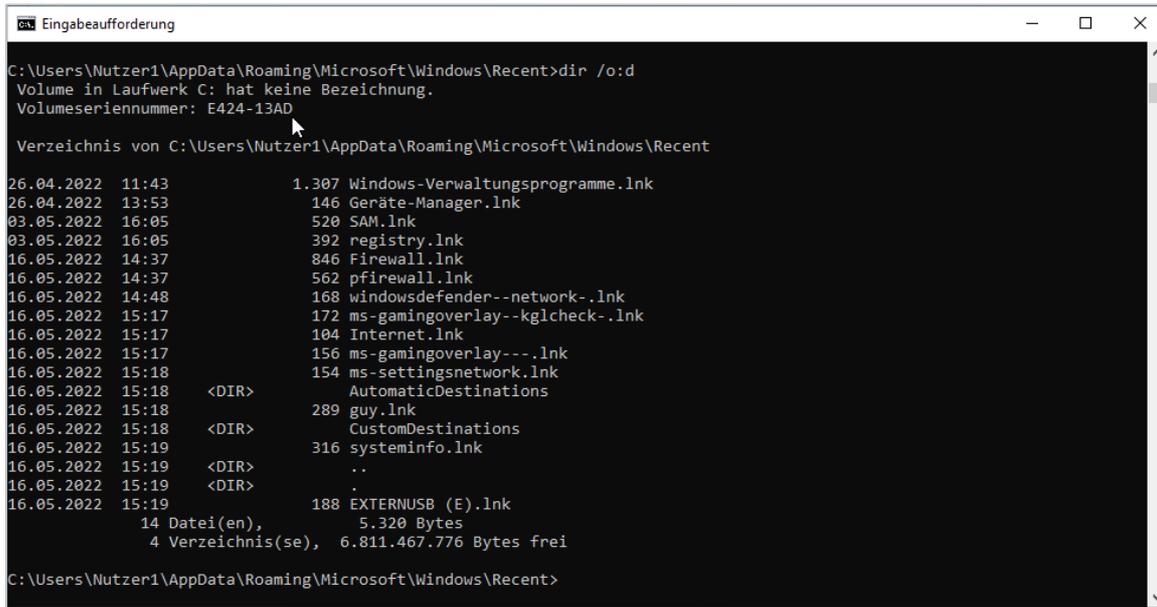
Öffnen Sie die Eingabeaufforderung/Kommandozeile `cmd.exe` ohne Administratorrechte. Wechseln Sie danach mit dem `cd` Befehl in das Verzeichnis `C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent`.



➤ Listen Sie den Ordnerinhalt mit `dir` auf



➤ Geben Sie die Dateien nach Erstellungszeit sortiert aus mit **dir /o:d**



```

C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent>dir /o:d
Volume in Laufwerk C: hat keine Bezeichnung.
Volumenseriennummer: E424-13AD

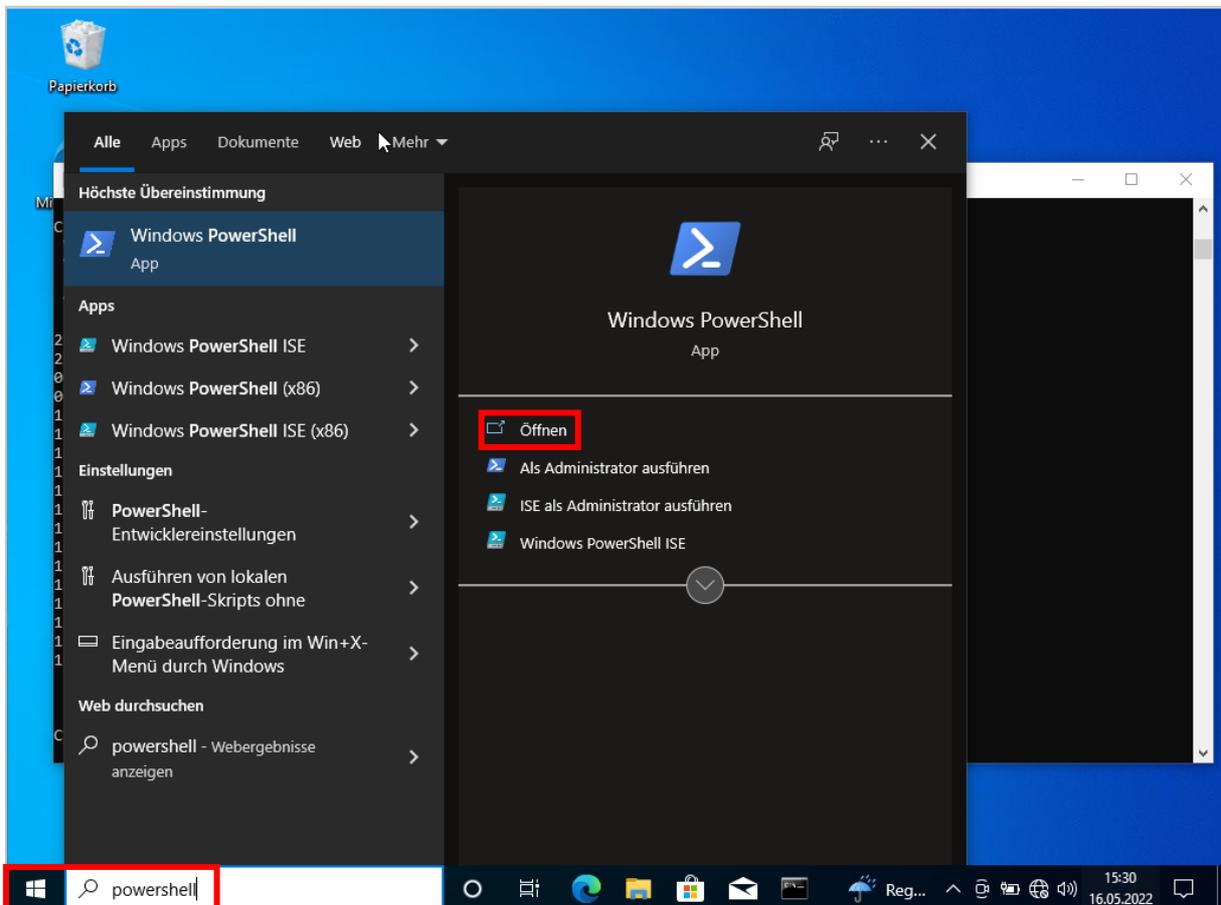
Verzeichnis von C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent

26.04.2022  11:43                1.307 Windows-Verwaltungsprogramme.lnk
26.04.2022  13:53                146 Geräte-Manager.lnk
03.05.2022  16:05                520 SAM.lnk
03.05.2022  16:05                392 registry.lnk
16.05.2022  14:37                846 Firewall.lnk
16.05.2022  14:37                562 pfirewall.lnk
16.05.2022  14:48                168 windowsdefender--network-.lnk
16.05.2022  15:17                172 ms-gamingoverlay--kglicheck-.lnk
16.05.2022  15:17                104 Internet.lnk
16.05.2022  15:17                156 ms-gamingoverlay--.lnk
16.05.2022  15:18                154 ms-settingsnetwork.lnk
16.05.2022  15:18                <DIR> AutomaticDestinations
16.05.2022  15:18                289 guy.lnk
16.05.2022  15:18                <DIR> CustomDestinations
16.05.2022  15:19                316 systeminfo.lnk
16.05.2022  15:19                <DIR> ..
16.05.2022  15:19                <DIR> .
16.05.2022  15:19                188 EXTERNUSB (E).lnk
                14 Datei(en),          5.320 Bytes
                4 Verzeichnis(se), 6.811.467.776 Bytes frei

C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent>

```

Öffnen Sie eine Powershell durch den Startbutton und der Eingabe von Powershell.



➤ Wechseln Sie danach mit dem **cd** Befehl in das Verzeichnis **C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent**

Schauen Sie sich mit dem Powershell Befehle **Format-Hex** den Inhalt der Datei **guy.lnk** an.

```

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

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

PS C:\Users\Nutzer1> format-hex C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent\guy.lnk

Pfad: C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent\guy.lnk

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 4C 00 00 00 01 14 02 00 00 00 00 00 00 00 00 00 L.....Ä...
00000010 00 00 00 46 93 00 20 00 20 00 00 00 00 96 4C 15 ...F@. . . . @L.
00000020 15 69 D8 01 00 B0 37 1F A7 68 D8 01 00 B8 12 FB .i0..°7.sh0...ù
00000030 14 69 D8 01 F5 45 01 00 00 00 00 01 00 00 00 .i0.ðE.....
00000040 00 00 00 00 00 00 00 00 00 00 00 00 85 00 14 00 .....@...
00000050 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 .PàOð è:i.¢0..+0
00000060 30 9D 19 00 2F 45 3A 5C 00 00 00 00 00 00 00 00 00./E:\.....
00000070 00 00 00 00 00 00 00 00 00 00 00 00 56 00 32 00 F5 .....V.2.ð
00000080 45 01 00 B0 54 CC 58 20 00 47 55 59 2E 4A 50 47 E..°TIX .GUY.JPG
00000090 00 40 00 09 00 04 00 EF BE B0 54 E4 58 AF 54 00 .@.....i%°TäX`T.
000000A0 B0 2E 00 00 00 A0 00 40 00 00 00 00 00 00 00 00 °....@.....
000000B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 67 .....g
000000C0 00 75 00 79 00 2E 00 6A 00 70 00 67 00 00 00 16 .u.y...j.p.g...
000000D0 00 00 00 42 00 00 00 1C 00 00 00 01 00 00 00 1C ...B.....
000000E0 00 00 00 36 00 00 00 00 00 00 00 41 00 00 00 1A ...6.....A...
000000F0 00 00 00 03 00 00 00 B2 15 DB 84 10 00 00 00 45 .....².Ü@....E
00000100 58 54 45 52 4E 55 53 42 00 45 3A 5C 67 75 79 2E XTERNUSB.E:\guy.
00000110 6A 70 67 00 00 03 00 45 00 3A 00 5C 00 00 00 00 jpg...E.:.\....

PS C:\Users\Nutzer1>

```

- Erkennen Sie von wo aus die Datei geöffnet wurde?
- Wiederholen Sie dies für die Datei **systeminfo.txt**

```

Auswählen Windows PowerShell
PS C:\Users\Nutzer1> format-hex C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent\systeminfo.lnk

Pfad: C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent\systeminfo.lnk

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 4C 00 00 00 01 14 02 00 00 00 00 00 C0 00 00 00 L.....Ä...
00000010 00 00 00 46 93 00 20 00 20 00 00 00 20 30 C5 7F ...F@. . . . 0Äo
00000020 27 69 D8 01 00 B0 37 1F A7 68 D8 01 00 27 69 82 'i0..°7.sh0..'i@
00000030 27 69 D8 01 81 08 00 00 00 00 00 01 00 00 00 'i0.ð.....
00000040 00 00 00 00 00 00 00 00 00 00 00 99 00 14 00 .....@...
00000050 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 .PàOð è:i.¢0..+0
00000060 30 9D 19 00 2F 45 3A 5C 00 00 00 00 00 00 00 00 00./E:\.....
00000070 00 00 00 00 00 00 00 00 00 00 6A 00 32 00 81 .....j.2.ð
00000080 0B 00 00 B0 54 61 6A 20 00 53 59 53 54 45 4D 7E ...°Taj ,SYSTEM~
00000090 31 2E 54 58 54 00 00 4E 00 09 00 04 00 EF BE B0 1.TXT..N....i%°
000000A0 54 5D 6A AF 54 00 B0 2E 00 00 00 E0 01 40 00 00 Tjj`T.°....à@..
000000B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000C0 00 00 00 00 73 00 79 00 73 00 74 00 65 00 6D .....s.y.s.t.e.m
000000D0 00 69 00 6E 00 66 00 6F 00 2E 00 74 00 78 00 74 .i.n.f.o...t.x.t
000000E0 00 00 00 1C 00 00 00 49 00 00 00 1C 00 00 00 01 .....I.....
000000F0 00 00 00 1C 00 00 00 36 00 00 00 00 00 00 48 .....6.....H
00000100 00 00 00 1A 00 00 00 03 00 00 00 B2 15 DB 84 10 .....².Ü@....
00000110 00 00 00 45 58 54 45 52 4E 55 53 42 00 45 3A 5C ...EXTERNUSB.E:\
00000120 73 79 73 74 65 6D 69 6E 66 6F 2E 74 78 74 00 00 systeminfo.txt..
00000130 03 00 45 00 3A 00 5C 00 00 00 00 00 ..E.:.\....

PS C:\Users\Nutzer1>

```

- Wiederholen Sie dies für die Datei **ExternUSB...lnk** (Nutzen Sie die Tab-Taste, um den Dateinamen auszuschreiben)

```

Windows PowerShell
PS C:\Users\Nutzer1> format-hex 'C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent\EXTERNUSB (E).lnk'

Pfad: C:\users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent\EXTERNUSB (E).lnk

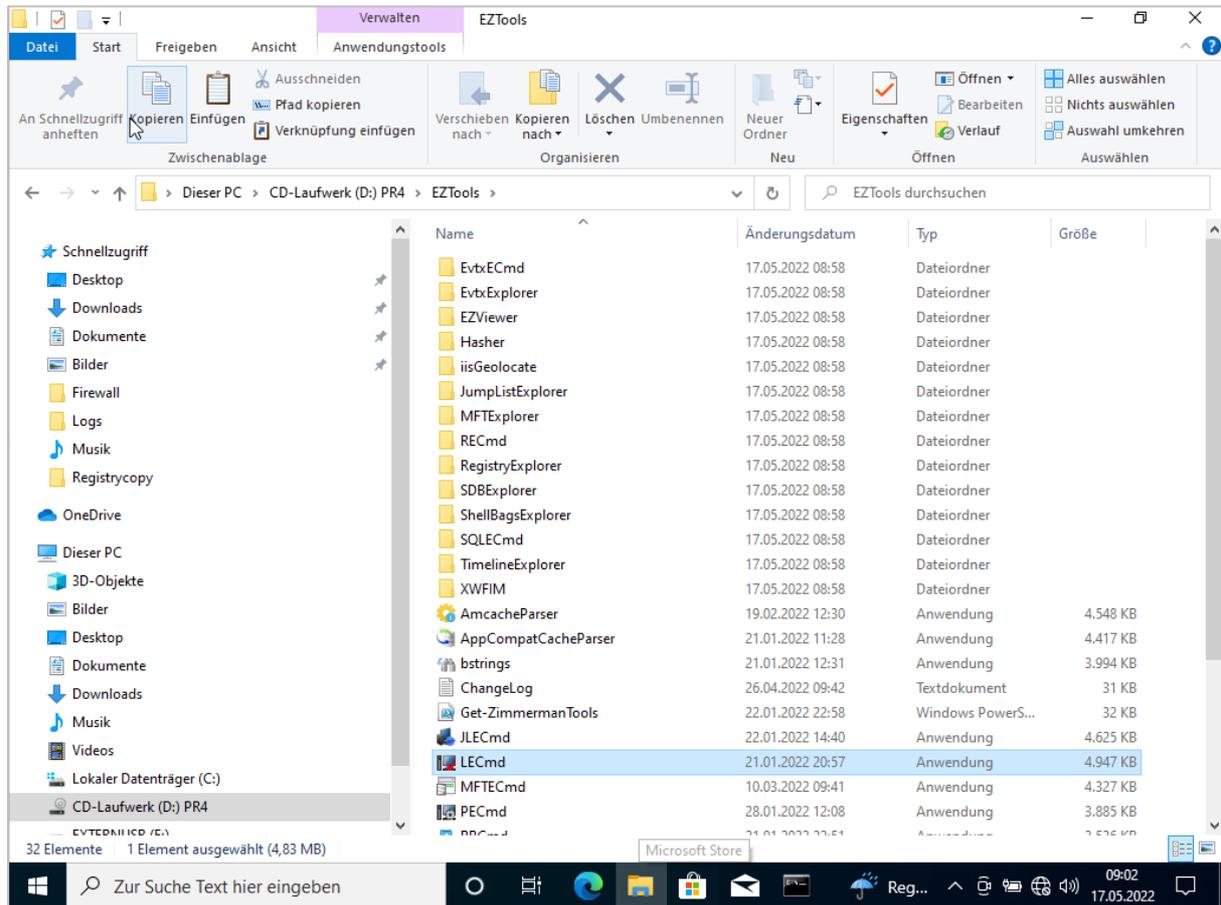
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000 4C 00 00 00 01 14 02 00 00 00 00 00 C0 00 00 00 L.....Ä...
00000010 00 00 00 46 83 00 20 00 10 00 00 00 00 80 4C 1E ..F. ....°L.
00000020 8F E7 A8 01 00 B0 4C 1E 8F E7 A8 01 00 B0 4C 1E 0ç".."ç".."°L.
00000030 8F E7 A8 01 00 00 00 00 00 00 00 00 01 00 00 00 0ç".....
00000040 00 00 00 00 00 00 00 00 00 00 00 00 2F 00 14 00 ...../...
00000050 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 .Pa00 è:i.ç0..+0
00000060 30 9D 19 00 2F 45 3A 5C 00 00 00 00 00 00 00 00 00./E:\.....
00000070 00 00 00 00 00 00 00 00 00 00 00 00 00 3B 00 00 .....;..
00000080 00 1C 00 00 00 01 00 00 00 1C 00 00 00 36 00 00 .....6..
00000090 00 00 00 00 00 3A 00 00 00 1A 00 00 00 03 00 00 .....:.....
000000A0 00 B2 15 DB 84 10 00 00 00 45 58 54 45 52 4E 55 .².Ü. ....EXTERNU
000000B0 53 42 00 45 3A 5C 00 00 00 00 00 00 00 00 00 00 SB.E:\.....

PS C:\Users\Nutzer1>

```

Wechseln Sie zum Windows Explorer und schauen Sie sich den Inhalt der CD im Verzeichnis **EZTools** an.



- Hier gibt es eine Anwendung LECmd.exe
- Führen Sie diese Datei vom CD-Laufwerk aus, indem Sie den Befehl in der Eingabeaufforderung (im Hintergrund oder neu Öffnen) auf dem Laufwerk der CD ausführen:
 - <LW-Buchstabe>:\EZTools\LECmd.exe

```

Windows10-BS-Praktikum1 [wird ausgeführt] - Oracle VM VirtualBox
Datei Maschine Anzeige Eingabe Geräte Hilfe
Eingabeaufforderung
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. Alle Rechte vorbehalten.
C:\Users\Nutzer1>d:\EZTools\LECmd.exe
Description:
  LECmd version 1.5.0.0

  Author: Eric Zimmerman (saericzimmerman@gmail.com)
  https://github.com/EricZimmerman/LECmd

Examples: LECmd.exe -f "C:\Temp\foobar.lnk"
  LECmd.exe -f "C:\Temp\somelink.lnk" --json "D:\jsonOutput" --jsonpretty
  LECmd.exe -d "C:\Temp" --csv "c:\temp" --html c:\temp --xml c:\temp\xml -q
  LECmd.exe -f "C:\Temp\some other link.lnk" --nid --neb
  LECmd.exe -d "C:\Temp" --all

  Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes

Usage:
  LECmd [options]

Options:
  -f <f>           File to process. Either this or -d is required
  -d <d>           Directory to recursively process. Either this or -f is required
  -r               Only process lnk files pointing to removable drives [default: False]
  -q               Only show the filename being processed vs all output. Useful to speed up exporting to json and/or csv
                  [default: False]
  --all           Process all files in directory vs. only files matching *.lnk [default: False]
  --csv <csv>    Directory to save CSV formatted results to. Be sure to include the full path in double quotes
  --csvf <csvf>  File name to save CSV formatted results to. When present, overrides default name
  --xml <xml>    Directory to save XML formatted results to. Be sure to include the full path in double quotes
  --html <html>  Directory to save xhtml formatted results to. Be sure to include the full path in double quotes
  --json <json>  Directory to save json representation to. Use --pretty for a more human readable layout
  --pretty       When exporting to json, use a more human readable layout [default: False]
  --nid          Suppress Target ID list details from being displayed [default: False]
  --neb         Suppress Extra blocks information from being displayed [default: False]
  --dt <dt>     The custom date/time format to use when displaying time stamps. See https://goo.gl/CNVq0k for options
                  [default: yyyy-MM-dd HH:mm:ss]
  --mp          Display higher precision for time stamps [default: False]
  --debug       Show debug information during processing [default: False]
  --trace       Show trace information during processing [default: False]
  --version     Show version information
  -?, -h, --help Show help and usage information
  
```

- Wenden Sie dieses Tool an, um die LNK-Dateien aus dem Recent Verzeichnis zu lesen
- `...:\EZTools\LECmd.exe -f systeminfo.txt`

```

C:\Users\Nutzer1>d:\EZTools\LECmd.exe -f C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent\systeminfo.lnk
LECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd

Command line: -f C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent\systeminfo.lnk

Warning: Administrator privileges not found!

Processing C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent\systeminfo.lnk

Source file: C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent\systeminfo.lnk
Source created: 2022-05-16 13:19:25
Source modified: 2022-05-16 13:19:25
Source accessed: 2022-05-17 07:05:20

--- Header ---
Target created: 2022-05-16 13:18:57
Target modified: 2022-05-16 13:19:02
Target accessed: 2022-05-15 22:00:00

File size: 2.945
Flags: HasTargetIdList, HasLinkInfo, HasWorkingDir, IsUnicode, DisableKnownFolderTracking
File attributes: FileAttributeArchive
Icon index: 0
Show window: SwNormal (Activates and displays the window. The window is restored to its original size and position if the w
indow is minimized or maximized.)

Working Directory: E:\

--- Link information ---
Flags: VolumeIdAndLocalBasePath
>> Volume information
Drive type: Fixed storage media (Hard drive)
Serial number: 84DB15B2
Label: EXTERNUSB
Local path: E:\systeminfo.txt

--- Target ID information (Format: Type ==> Value) ---

Absolute path: My Computer\E:\systeminfo.txt

-Root folder: GUID ==> My Computer

-Drive letter ==> E:

-File ==> systeminfo.txt
Short name: SYSTEM~1.TXT
Modified: 2022-05-16 13:19:02
Extension block count: 1

----- Block 0 (Beef0004) -----
Long name: systeminfo.txt
Created: 2022-05-16 13:18:58
Last access: 2022-05-15 22:00:00
MFT entry/sequence #: 4194784/null (0x4001E0/0xnull)

--- End Target ID information ---

----- Processed C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent\systeminfo.lnk in 0,18730150 seconds -----

```

➤ ...:\EZTools\LECmd.exe -f „EXTERNUSB (...)”.lnk

```

Eingabeaufforderung

Processing C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent\EXTERNUSB (E).lnk
Source file: C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent\EXTERNUSB (E).lnk
Source created: 2022-05-16 13:18:33
Source modified: 2022-05-16 13:19:25
Source accessed: 2022-05-17 07:06:22

--- Header ---
Target created: 1979-12-31 22:00:00
Target modified: 1979-12-31 22:00:00
Target accessed: 1979-12-31 22:00:00

File size: 0
Flags: HasTargetIdList, HasLinkInfo, IsUnicode, DisableKnownFolderTracking
File attributes: FileAttributeDirectory
Icon index: 0
Show window: SwNormal (Activates and displays the window. The window is restored to its original size and position if the window is minimized or maximized.)

--- Link information ---
Flags: VolumeIdAndLocalBasePath

>> Volume information
Drive type: Fixed storage media (Hard drive)
Serial number: 84DB15B2
Label: EXTERNUSB
Local path: E:\

--- Target ID information (Format: Type ==> Value) ---

Absolute path: My Computer\E:

-Root folder: GUID ==> My Computer

-Drive letter ==> E:

--- End Target ID information ---

----- Processed C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent\EXTERNUSB (E).lnk in 0,16282160 seconds -----

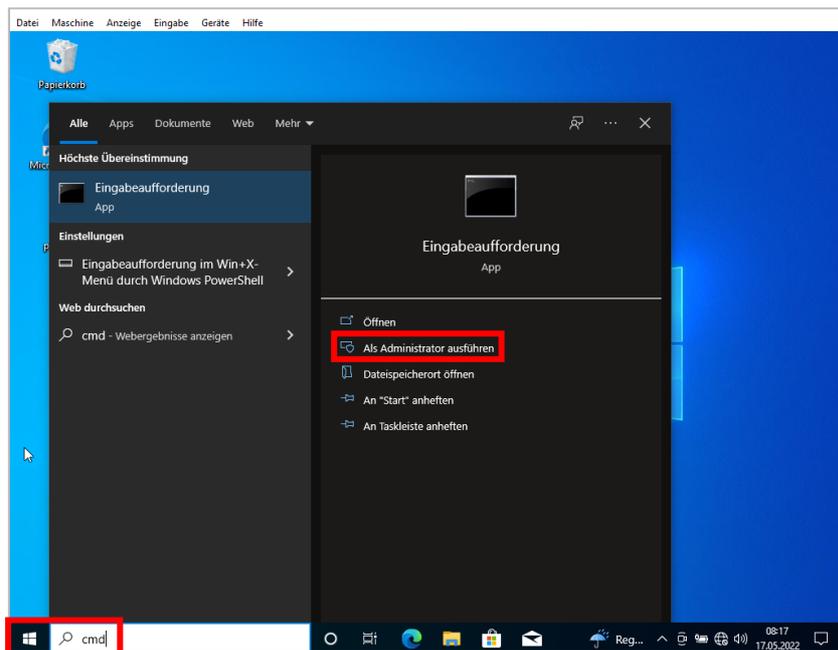
```

Volumenschattenkopien

VSS anlegen

Schließen Sie alle offenen Fenster und Anwendungen.

Starten Sie eine Eingabeaufforderung/Kommandozeile cmd als Administrator.



- Lassen Sie sich in der Eingabeaufforderung alle Schattenkopien anzeigen, mittels **vssadmin list shadows**

```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>vssadmin list shadows
vssadmin 1.1 - Verwaltungsbefehlszeilenprogramm des Volumeschattenkopie-Dienstes
(C) Copyright 2001-2013 Microsoft Corp.

Es wurde keine Ergebnisse für die Abfrage gefunden.

C:\Windows\system32>
```

- Sind Schattenkopien vorhanden?
- Legen Sie eine neue Schattenkopie mit dem Befehl **vssadmin create shadow for=C:** an

```
Administrator: Eingabeaufforderung

C:\Windows\system32>vssadmin create shadow for=c:\
vssadmin 1.1 - Verwaltungsbefehlszeilenprogramm des Volumeschattenkopie-Dienstes
(C) Copyright 2001-2013 Microsoft Corp.

Fehler: Ungültiger Befehl.

---- Unterstützte Befehle ----

Delete Shadows      - Löscht Volumeschattenkopien.
List Providers      - Zeigt die registrierten Volumeschattenkopie-Anbieter an.
List Shadows        - Zeigt bestehende Volumeschattenkopien an.
List ShadowStorage  - Zeigt Volumeschattenkopie-Speicherassoziationen an.
List Volumes        - Zeigt Volumes an, auf denen Volumeschattenkopien
                    erstellt werden können.
List Writers        - Zeigt abonnierte Volumeschattenkopie-Verfasser an.
Resize ShadowStorage - Ändert die Größe
                    einer Schattenkopie-Speicherassoziation.

C:\Windows\system32>
```

War dies erfolgreich? Recherchieren Sie, warum dies nicht erfolgreich ist.

Antwort: Schattenkopien lassen sich mittels VSSADMIN nur auf Server Betriebssystemen anlegen!

- Legen Sie stattdessen eine Schattenkopie mittels des Befehls **wmic shadowcopy call create Volume=C:** an

```
Administrator: Eingabeaufforderung

C:\Windows\system32>wmic shadowcopy call create Volume=C:\
(Win32_ShadowCopy)->create() wird ausgeführt
Methode wurde ausgeführt.
Ausgabeparameter:
instance of __PARAMETERS
{
    ReturnValue = 0;
    ShadowID = "{DC9794B7-07F3-474F-9359-BFF068DB12BF}";
};

C:\Windows\system32>
```

- Lassen Sie sich in der Eingabeaufforderung die Schattenkopien erneut anzeigen, mittels **vssadmin list shadows**

```

Administrator: Eingabeaufforderung

C:\Windows\system32>wmic shadowcopy call create Volume=C:\
(Win32_ShadowCopy)->create() wird ausgeführt
Methode wurde ausgeführt.
Ausgabeparameter:
instance of __PARAMETERS
{
    ReturnValue = 0;
    ShadowID = "{DC9794B7-07F3-474F-9359-BFF068DB12BF}";
};

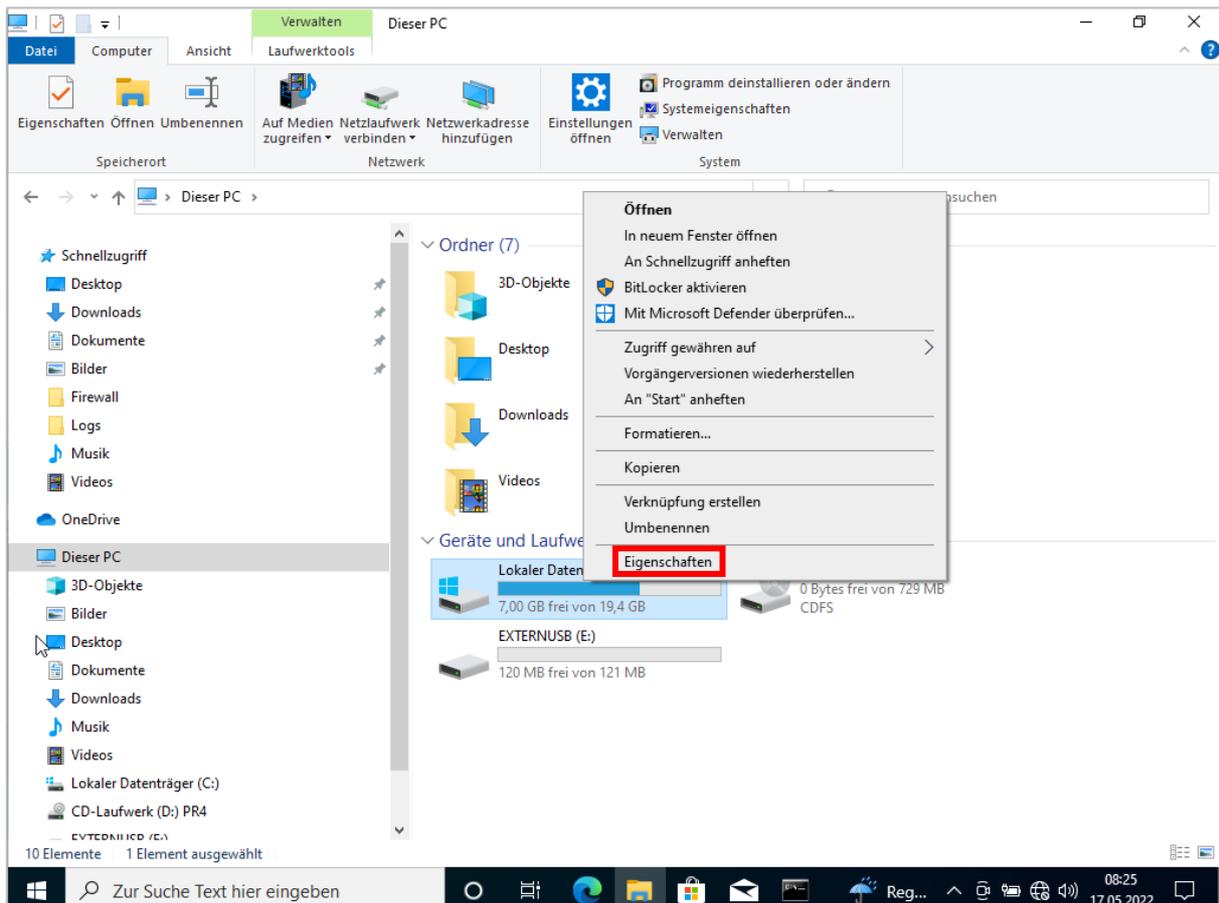
C:\Windows\system32>vssadmin list shadows
vssadmin 1.1 - Verwaltungsbefehlszeilenprogramm des Volumeschattenkopie-Dienstes
(C) Copyright 2001-2013 Microsoft Corp.

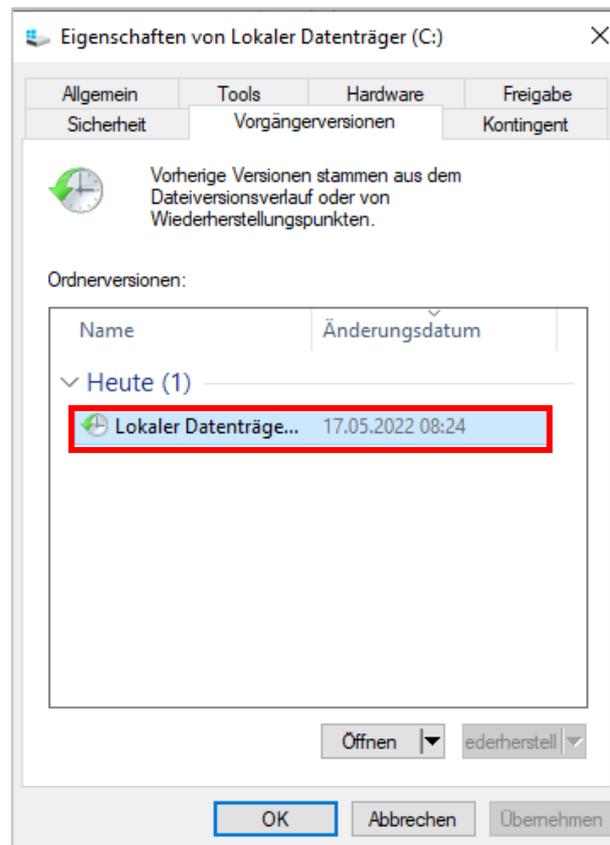
Inhalte der Schattenkopiersatzkennung: {9f5971d9-cc2d-4303-a75c-6c744a4b8ef4}
1 Schattenkopie(n) war(en) enthalten bei der Erstellungszeit:
    17.05.2022 08:24:30
Schattenkopienkennung: {dc9794b7-07f3-474f-9359-bff068db12bf}
Ursprüngliches Volume: (C:)\?\?\Volume{633a5b69-0000-0000-0000-300300000000}\
Schattenkopievolumen: \?\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2
Quellcomputer: PRAKTIKUM1
Dienstcomputer: PRAKTIKUM1
Anbieter: "Microsoft Software Shadow Copy provider 1.0"
Typ: ClientAccessible
Attribute: Permanent, Clientzugänglich, Keine automatische Freigabe, Keine Verfasser, Differenziell

C:\Windows\system32>

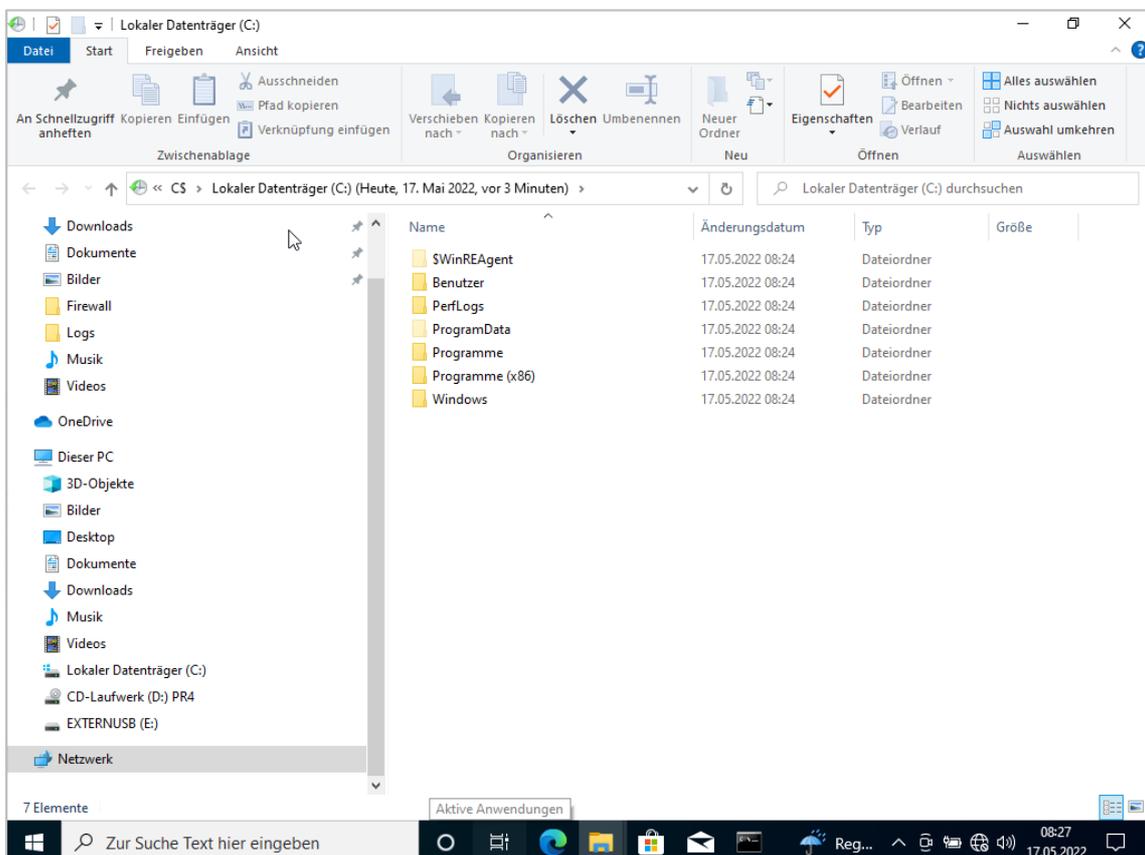
```

Prüfen Sie dies im Windows Explorer in dem Sie sich die Eigenschaften von Laufwerk C:\ anzeigen lassen.

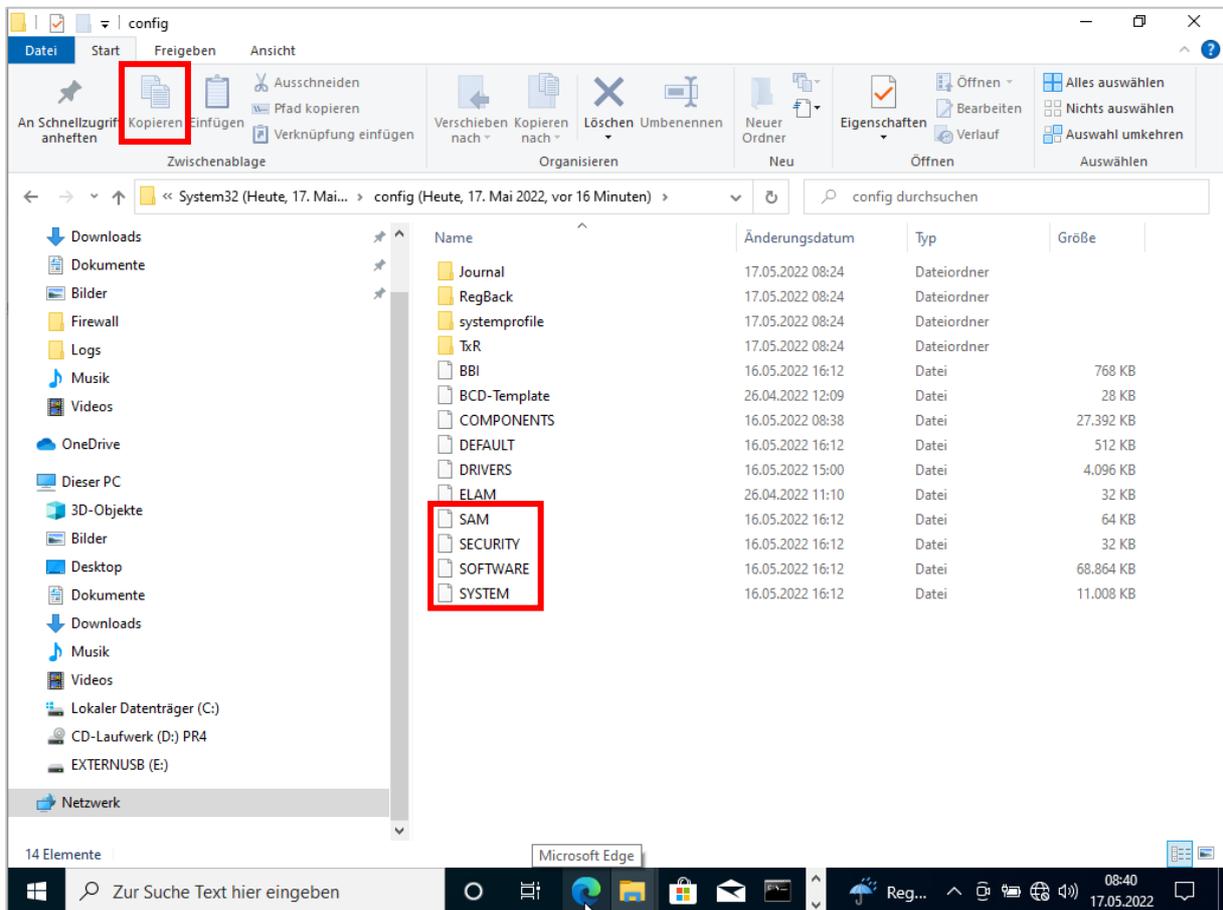




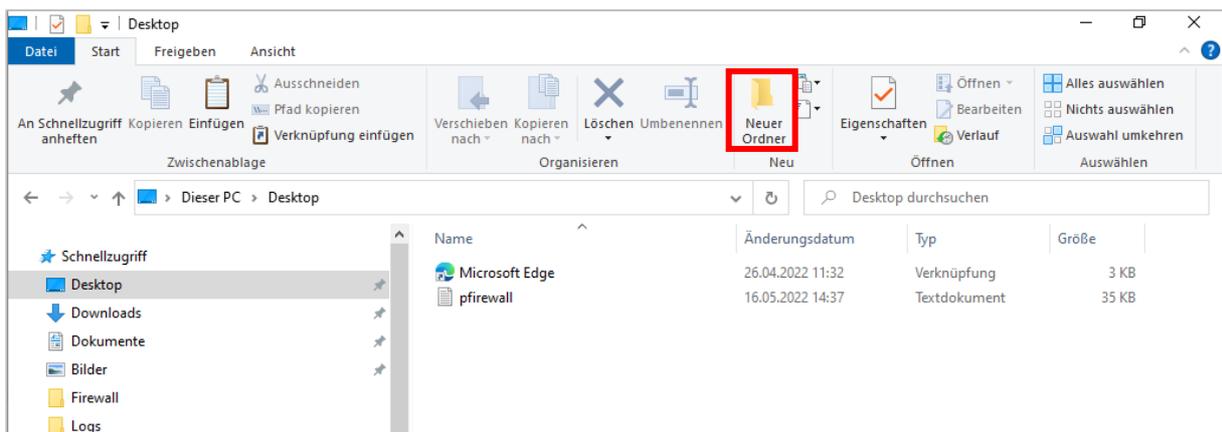
Öffnen Sie die Schattenkopie mit einem Doppelklick darauf.



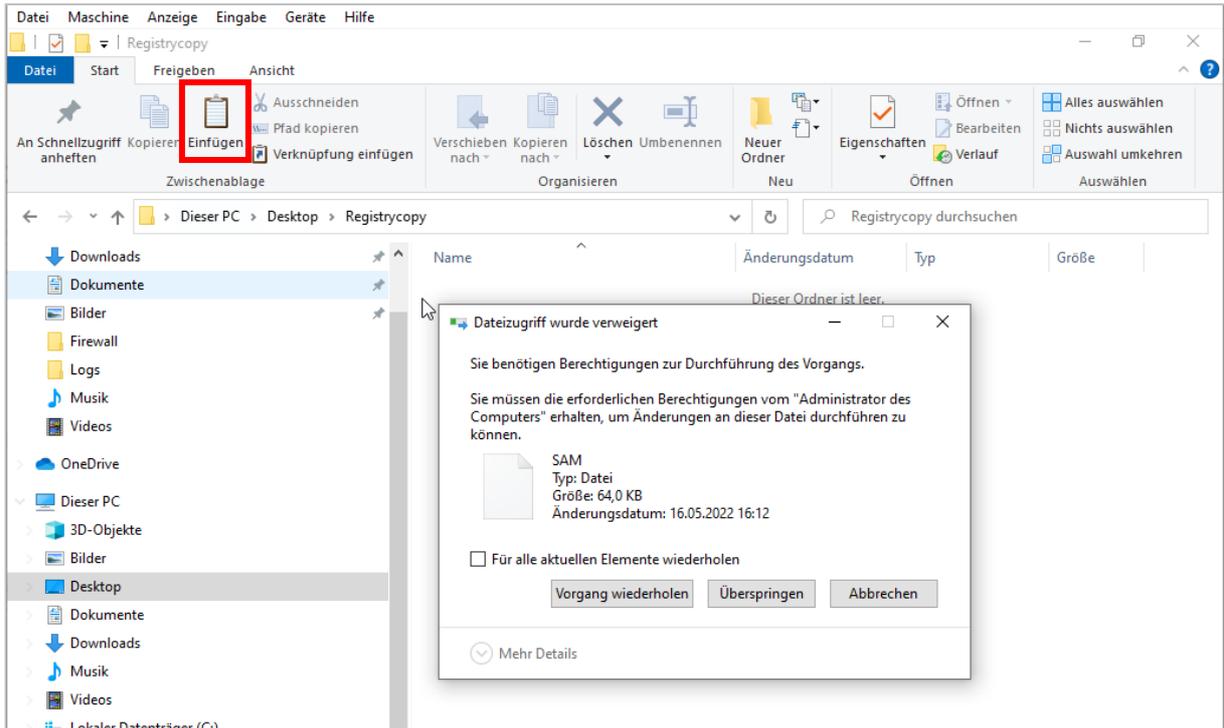
- Wechseln Sie in der Schattenkopie in das Verzeichnis **C\$\Windows\System32\Config**
- Wählen Sie hier die Dateien **SAM, SECURITY, SOFTWARE, SYSTEM** und kopieren Sie diese



- Wechseln Sie auf den **Desktop** und erstellen Sie einen **Neuen Ordner** mit der Bezeichnung **RegistryKopie**



- Fügen Sie die vorher kopierten Dateien ein

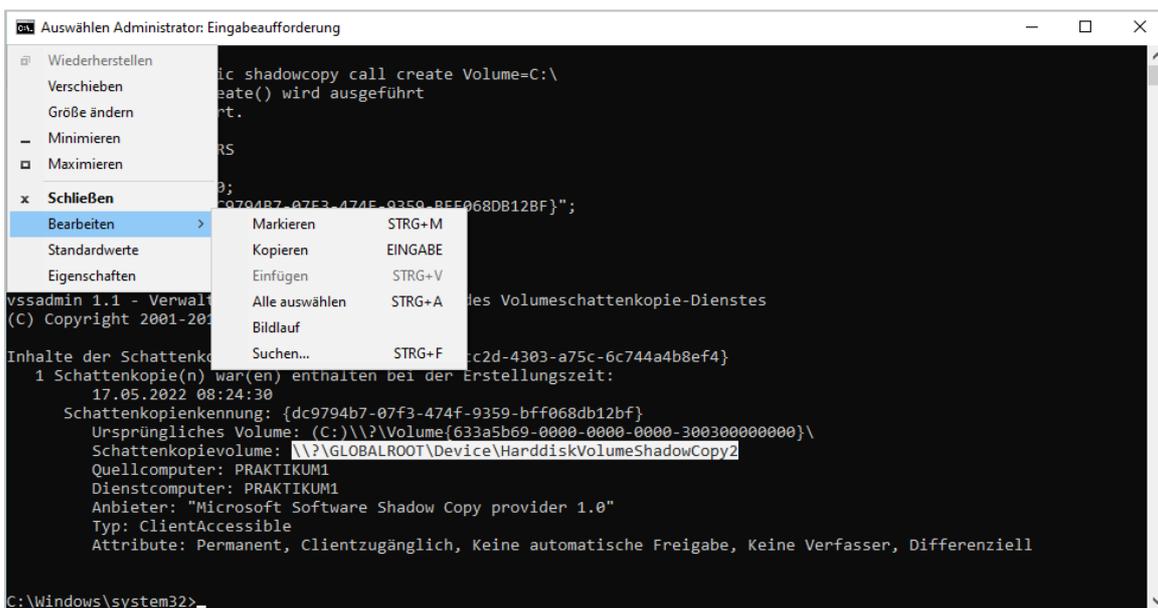


- Leider fehlen Ihnen dazu die Berechtigungen!

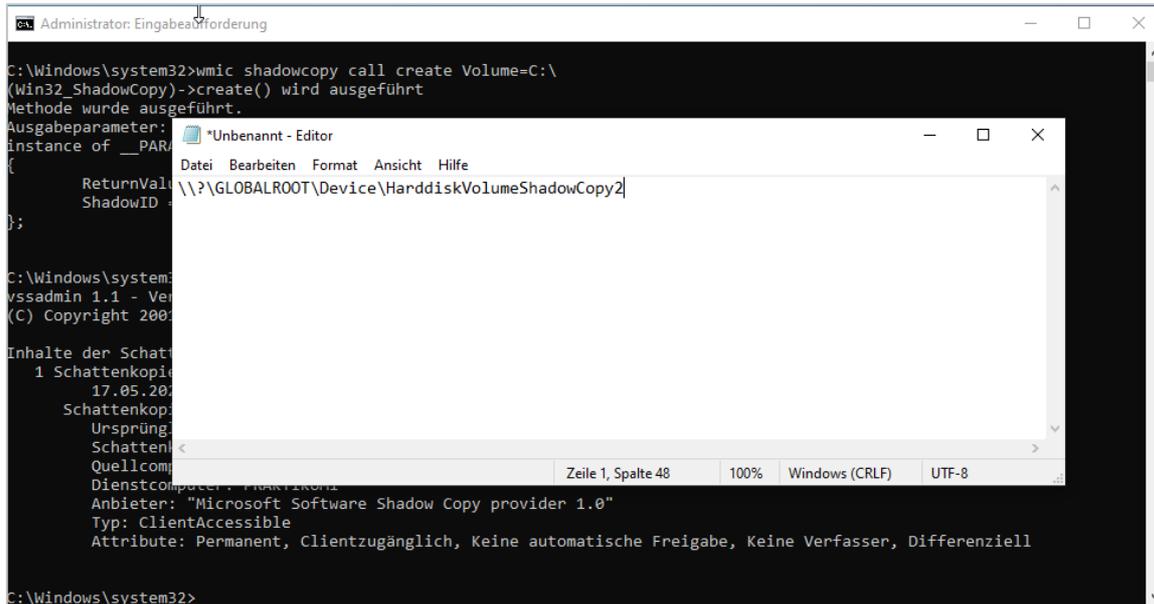
Auf Volumenschattenkopien zugreifen

Wechseln Sie zurück zur Eingabeaufforderung / Kommandozeile oder öffnen Sie diese erneut mit Administratorberechtigungen.

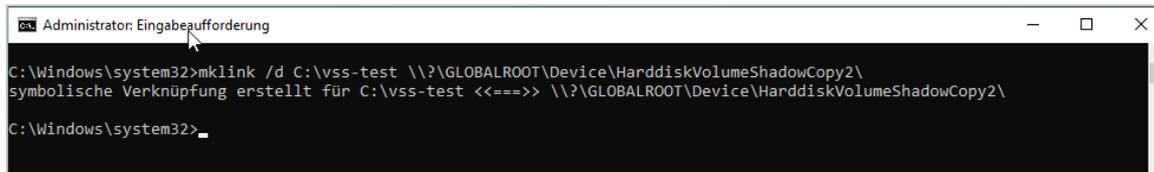
- Lassen Sie sich die Volumen Schattenkopien erneut anzeigen oder Nutzen Sie die Anzeige in der noch geöffneten Eingabeaufforderung
- Markieren Sie den Eintrag des Globalroot Harddisk Objektes der Schattenkopie (`\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1`)
- Kopieren Sie diesen Eintrag aus dem Fenster oder über STRG+C



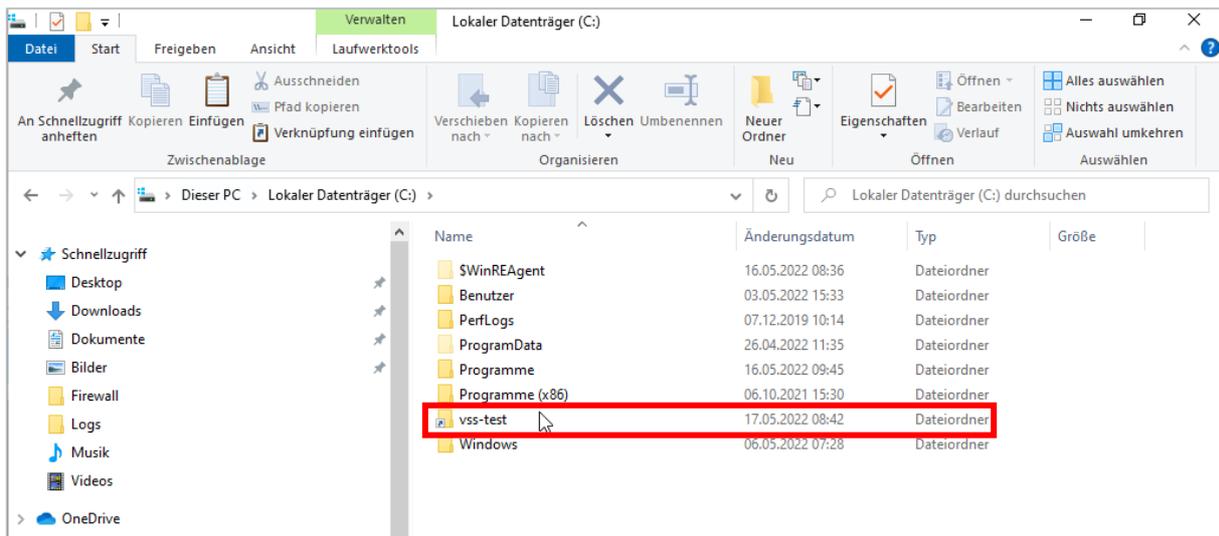
- Überprüfen Sie ob das Kopieren funktioniert über den Editor und fügen Sie in diesen den Globalroot Eintrag ein



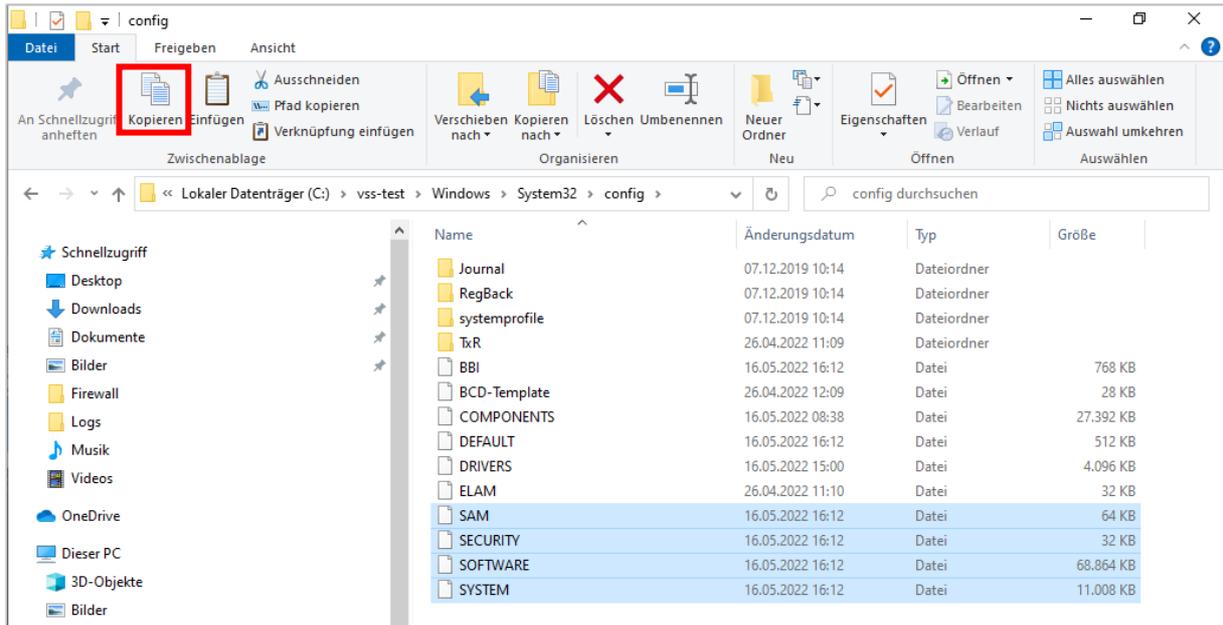
- Erstellen Sie einen Link Eintrag auf den Globalroot im Verzeichnis **C:\vss-test** mit dem Befehl **mklink /d C:\vss-test globalroot <identifizier>** (vergessen Sie den Backslash am Ende nicht!)



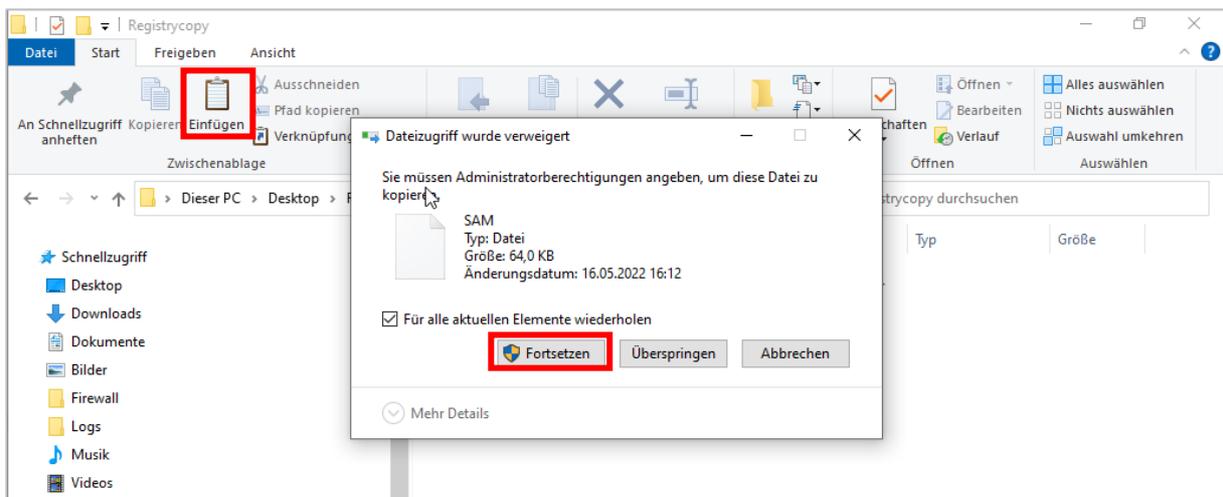
Öffnen Sie jetzt den **Windows Explorer** und navigieren Sie in das Verzeichnis **C:\vss-test**.



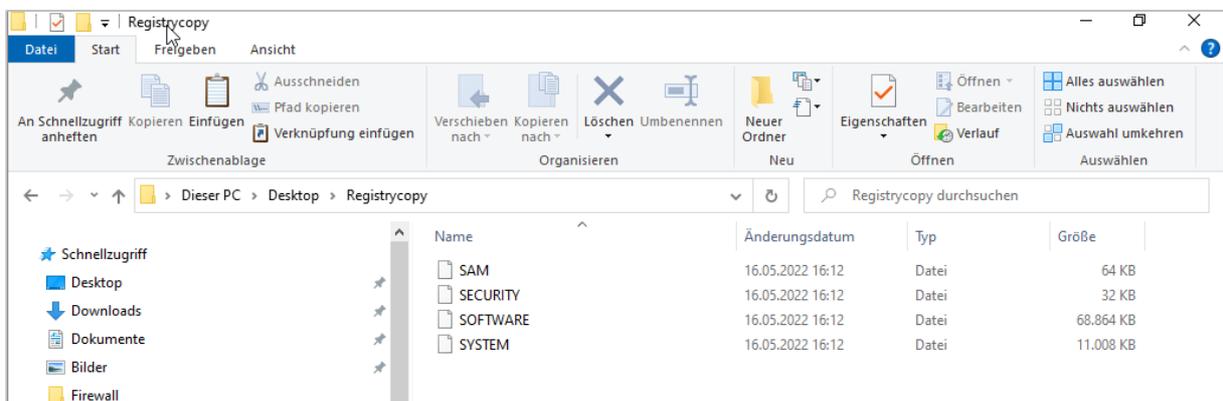
- Wechseln Sie in das Verzeichnis Wechseln Sie in der Schattenkopie in das Verzeichnis **C:\vss-test\Windows\System32\Config**
- Wählen Sie hier die Dateien **SAM, SECURITY, SOFTWARE, SYSTEM** und kopieren Sie diese



- Wechseln Sie auf den **Desktop** und fügen Sie die vorher kopierten Dateien in das Verzeichnis **RegistryKopie** ein
- Bestätigen Sie den Kopierdialog mit Fortsetzen

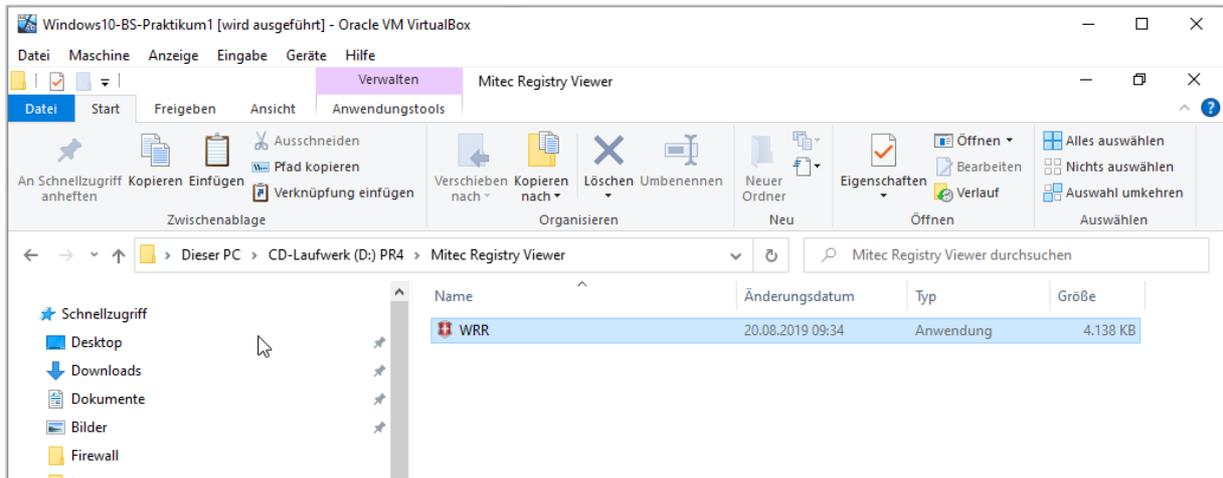


- Jetzt hat das Kopieren funktioniert

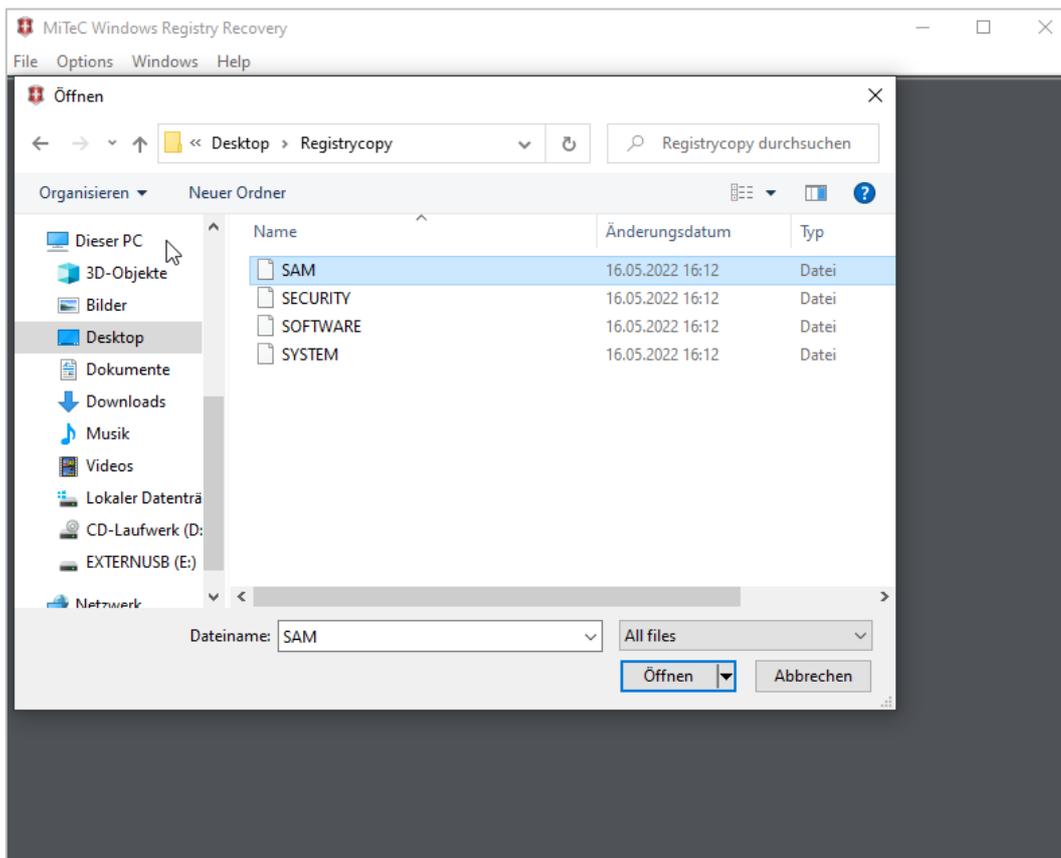


Registryinformationen der Schattenkopie lesen

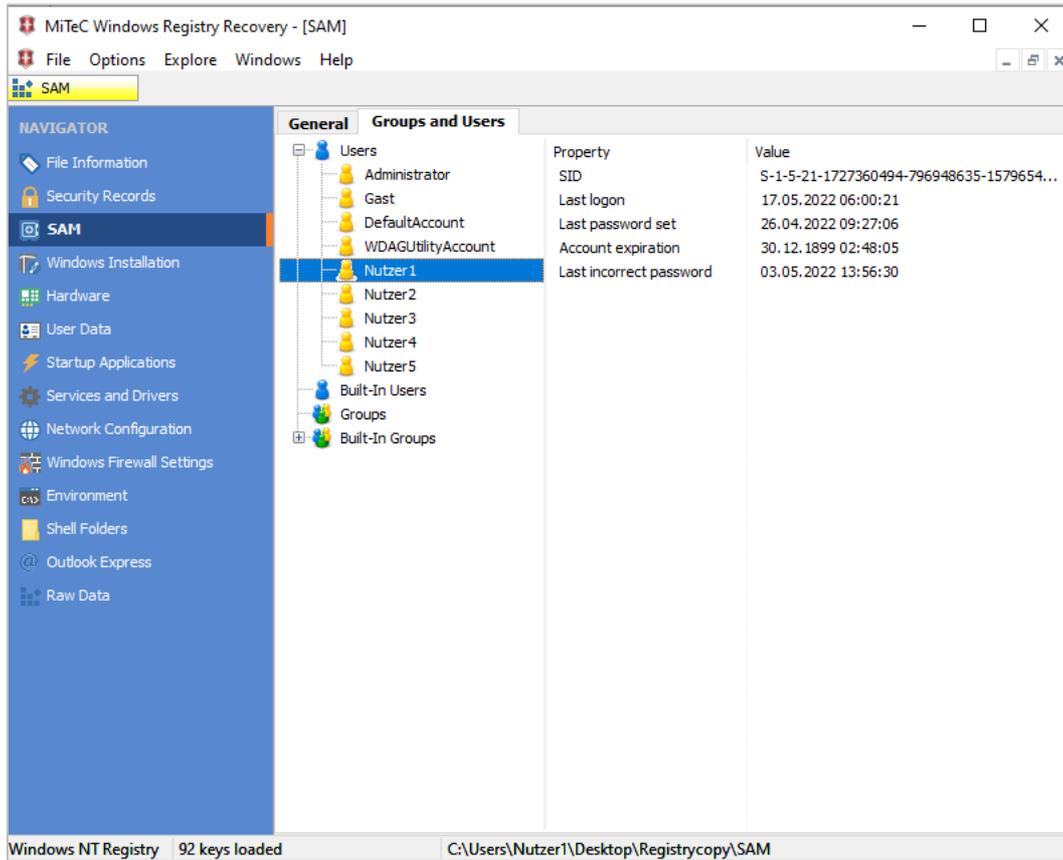
Wechseln Sie im Windows Explorer auf die CD und Starten Sie den **WRR** im Verzeichnis **Mitec Registry Recovery**.



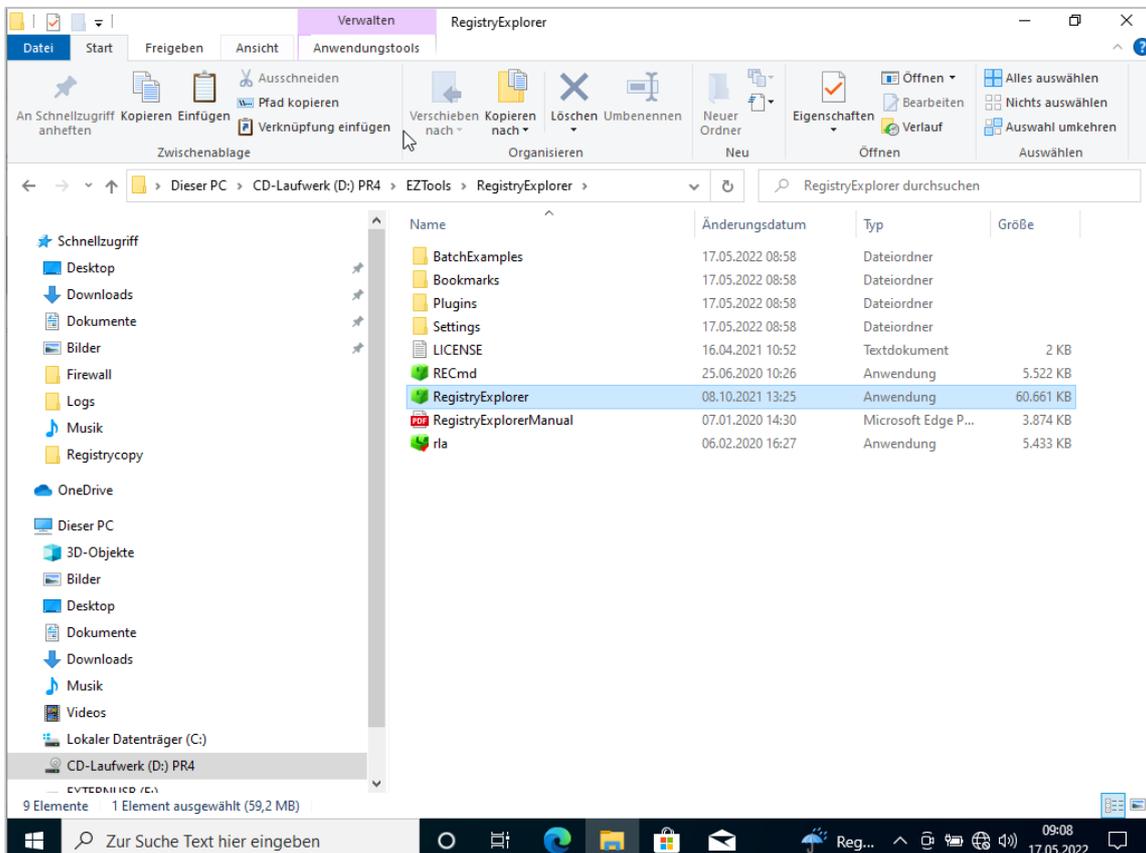
➤ Laden Sie den **SAM Hive** aus dem Verzeichnis **RegistryCopy**



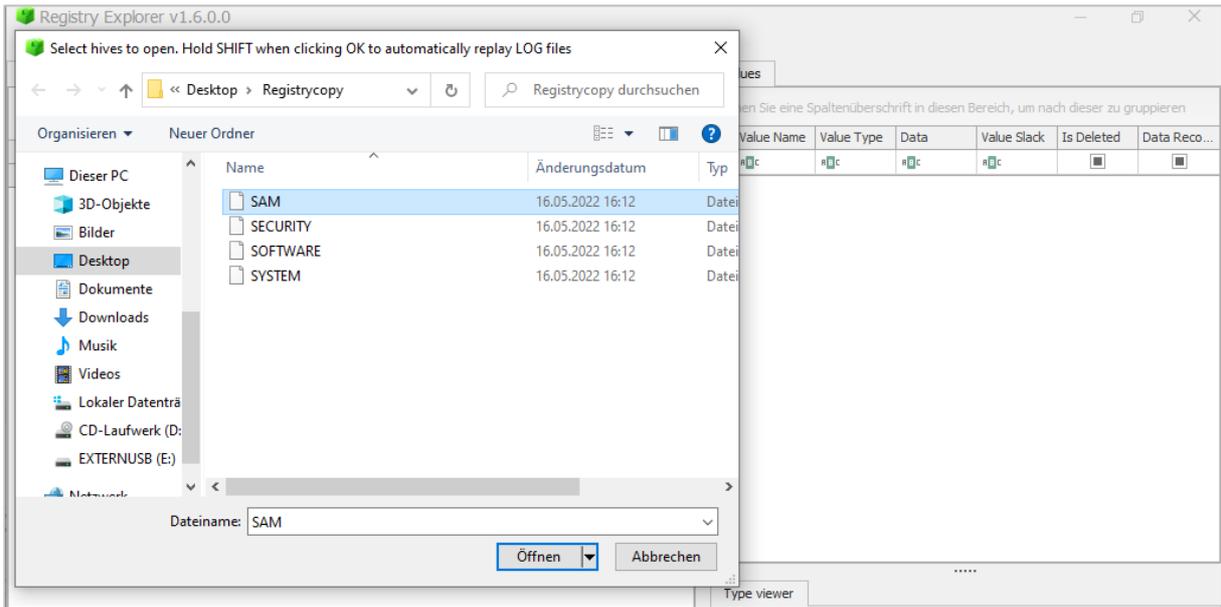
➤ Schauen Sie die Informationen das **SAM Hive** näher an



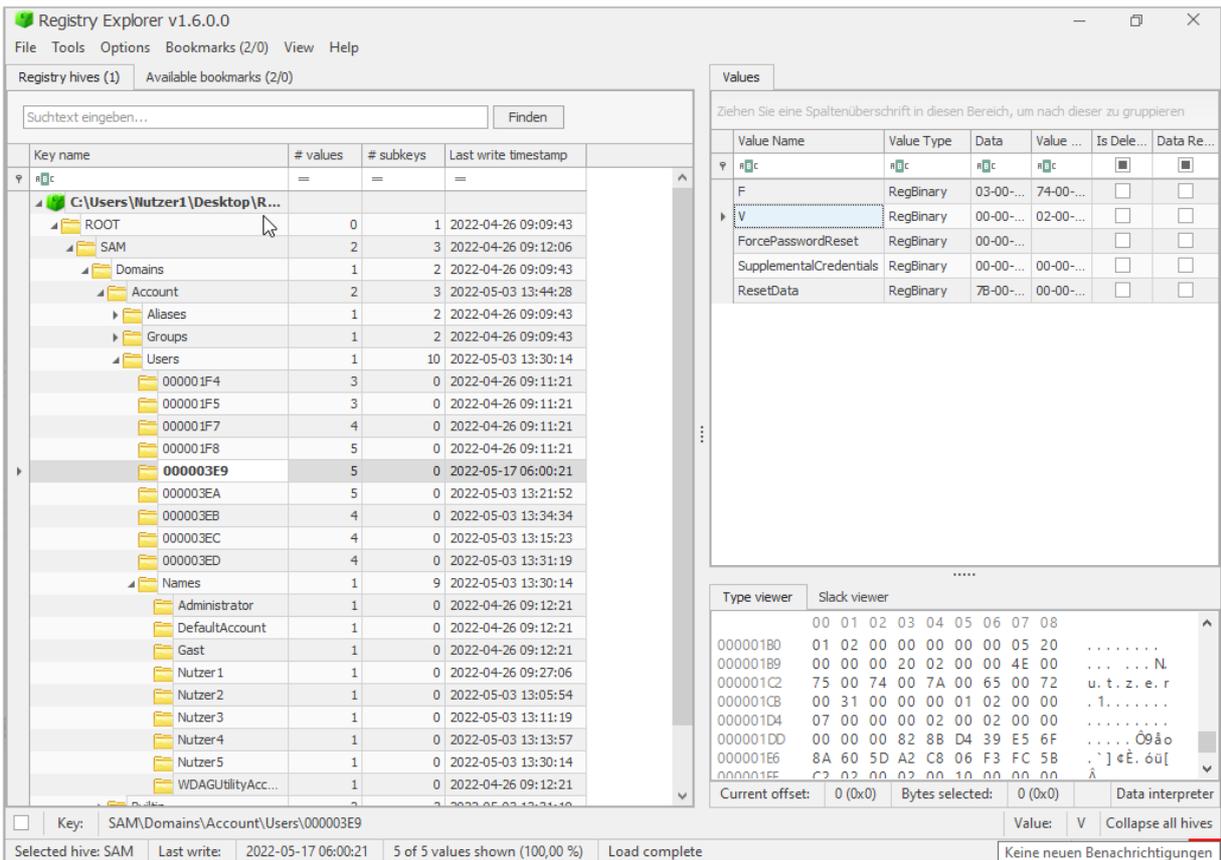
Wechseln Sie im Windows Explorer auf die CD und starten Sie den **RegistryExplorer** im Verzeichnis **EZTools\RegistryExplorer**.



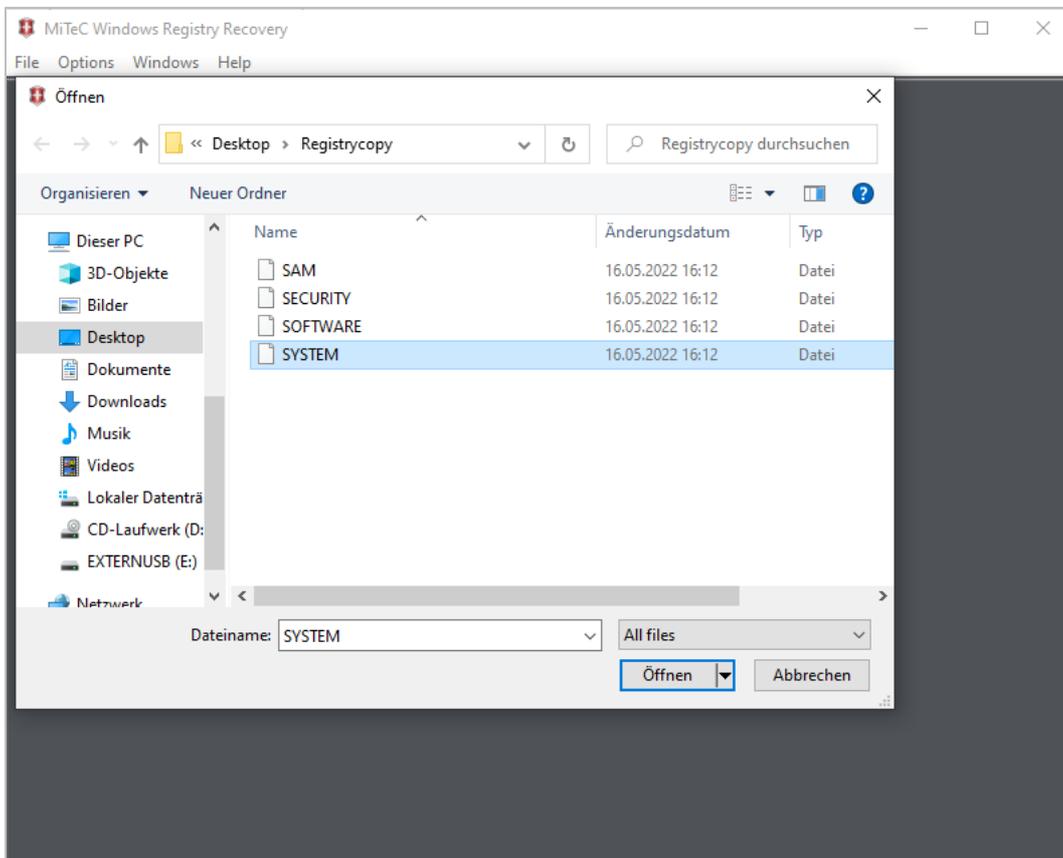
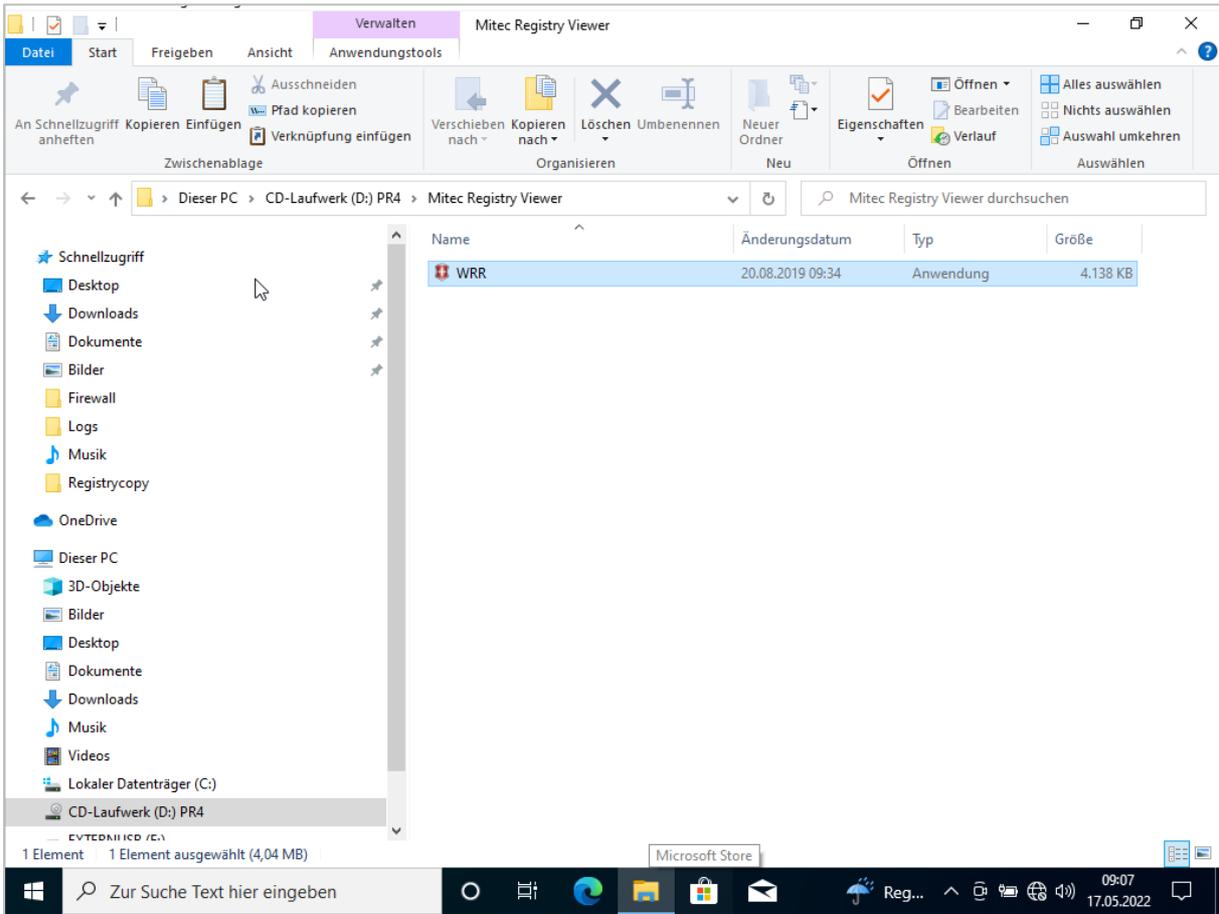
➤ Laden Sie den **SAM Hive** aus dem Verzeichnis **RegistryCopy**



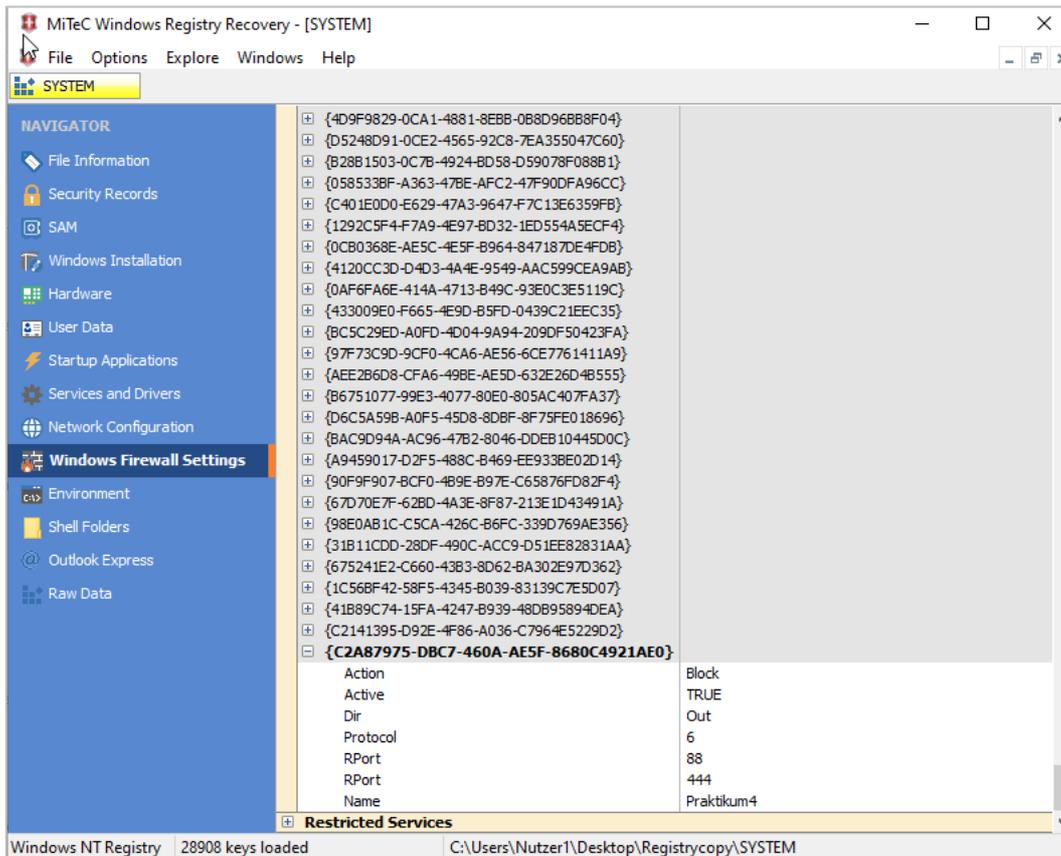
➤ Schauen Sie die Informationen das **SAM Hive** auch hier näher an.



Untersuchen Sie den **SYSTEM Hive** mit dem **WRR** aus dem Verzeichnis **Mitec Registry Recovery** der CD.



➤ Öffnen Sie die Windows Firewall Settings und betrachten Sie den letzten Schlüssel



➤ Kommt Ihnen das bekannt vor?

Untersuchen Sie den **SOFTWARE** Hive mit dem **WRR**.

