Studienprogramm Sachbearbeiter:in Digitale Forensik
Praktikum Betriebssysteme
Dozent: Leander Hossfeld
hossfeld@hs-mittweida.de
Stand: 06.06.2024

HOCHSCHULE MITTWEIDA
University of Applied Sciences

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-Eintragungen 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

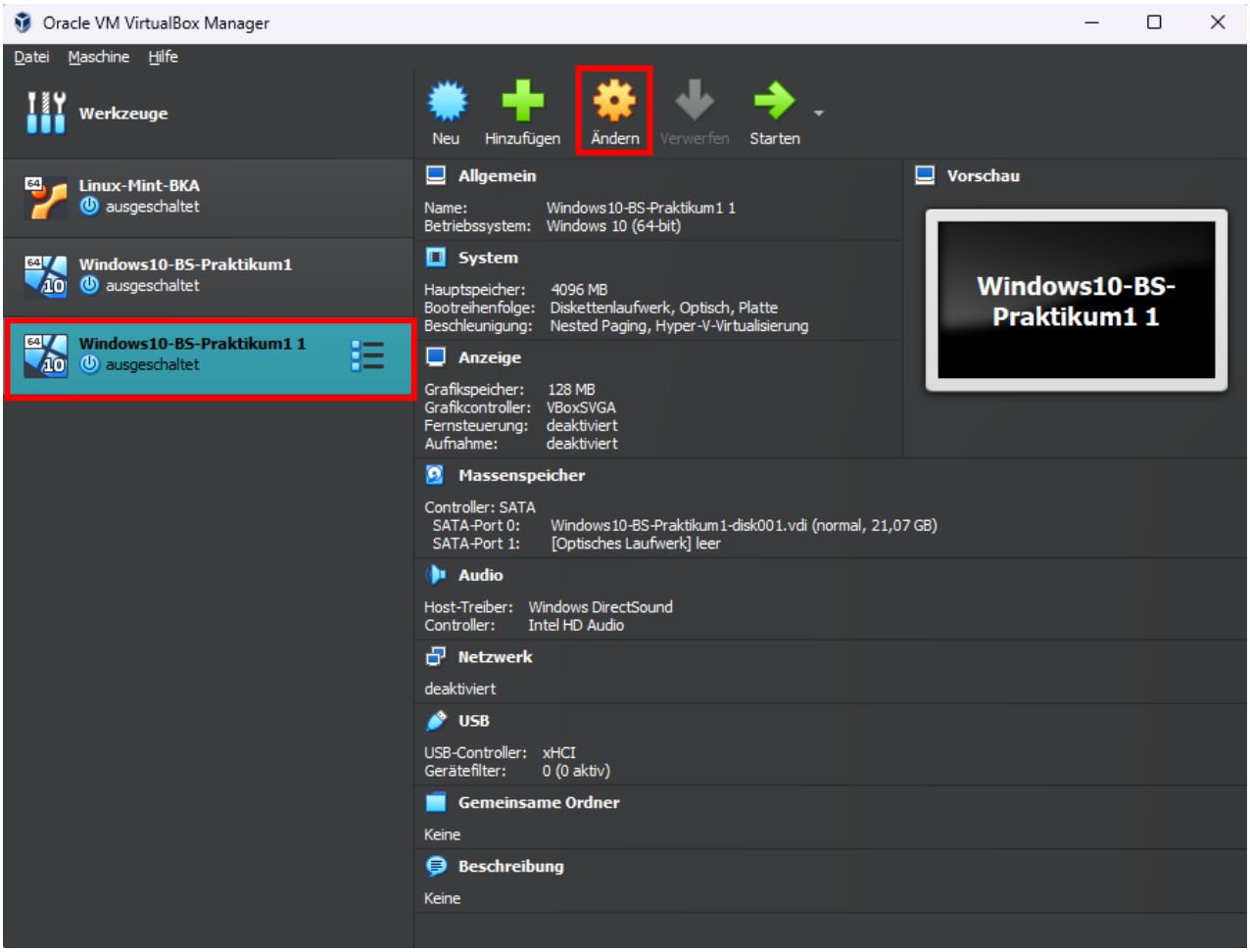
Allgemeine Hinweise

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.

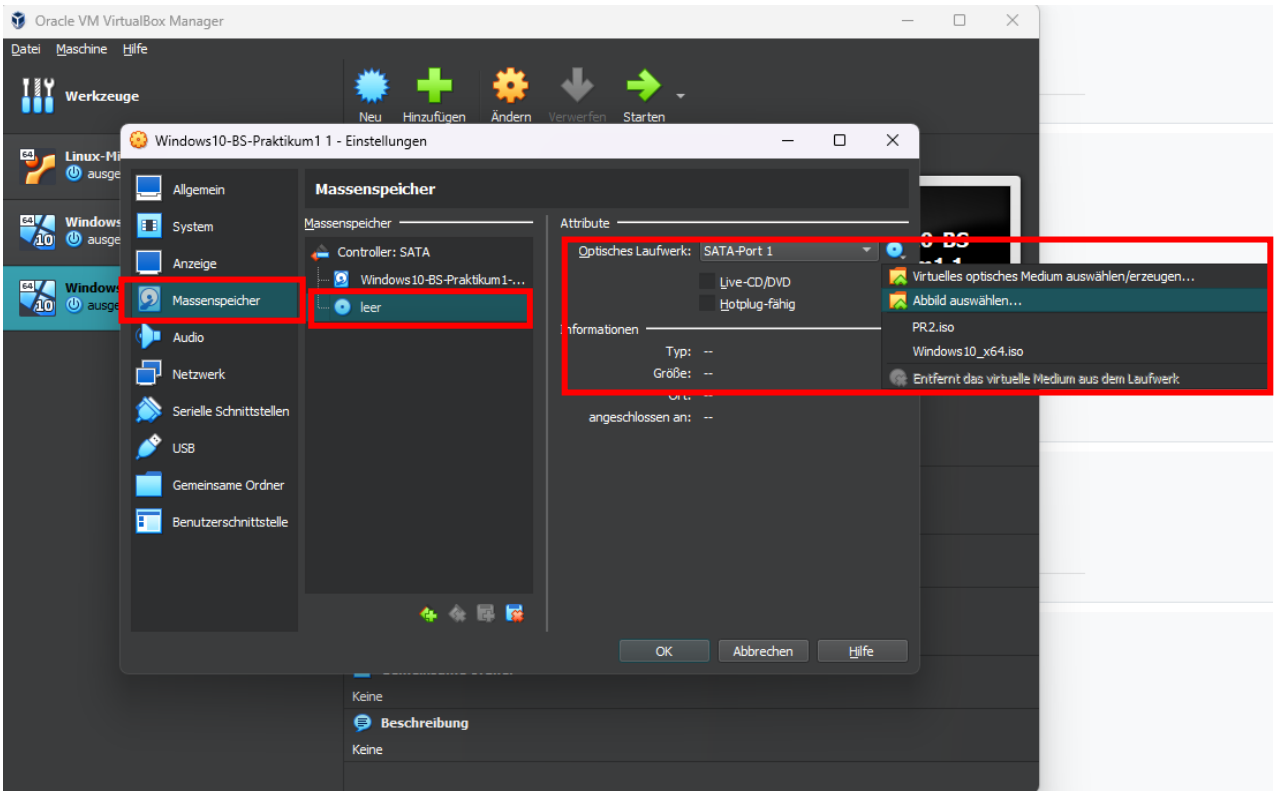
Einbindung der PR4.iso und VMDK-Datei

Öffnen Sie Virtualbox.

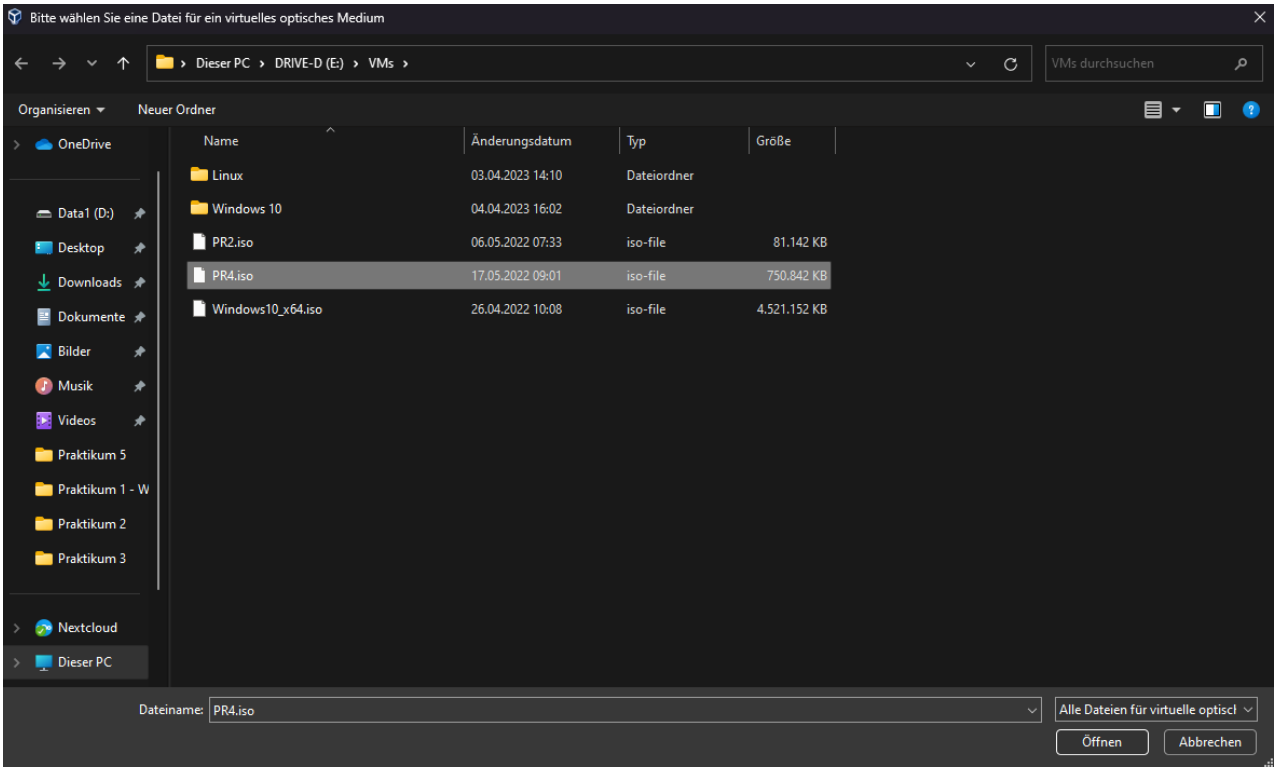
Wählen Sie die im Praktikum 1 angelegte VM aus oder importieren Sie zuerst die OVA-Datei wählen dann die VM des Praktikum 1 aus. Gehen Sie auf **Ändern** (nicht Doppelklicken auf die VM, das würde diese Starten).

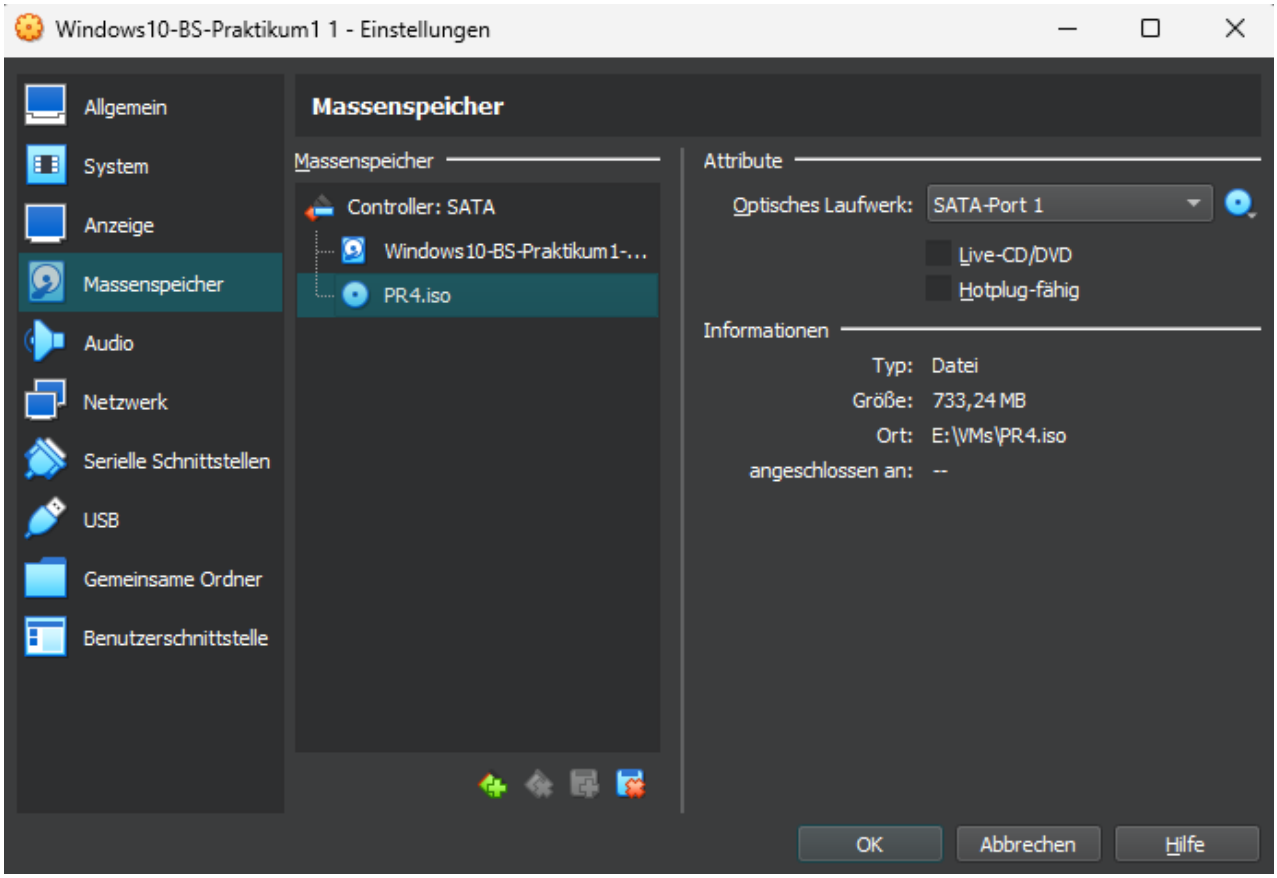


- Wählen Sie den Massenspeicher aus

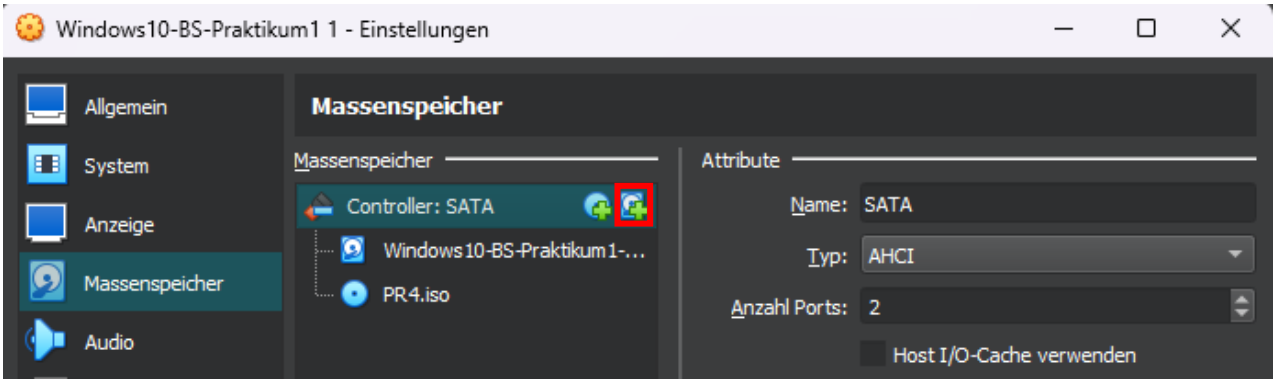


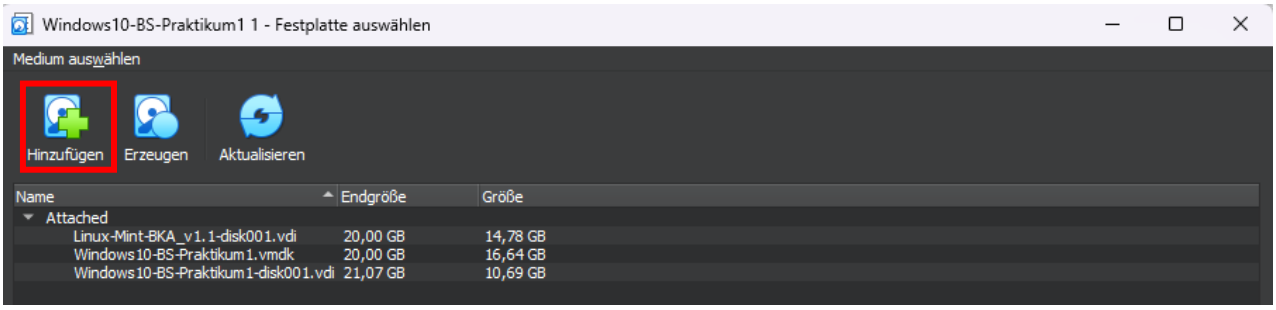
- Binden Sie bei der CD die heruntergeladene Abbilddatei **PR4.iso** ein

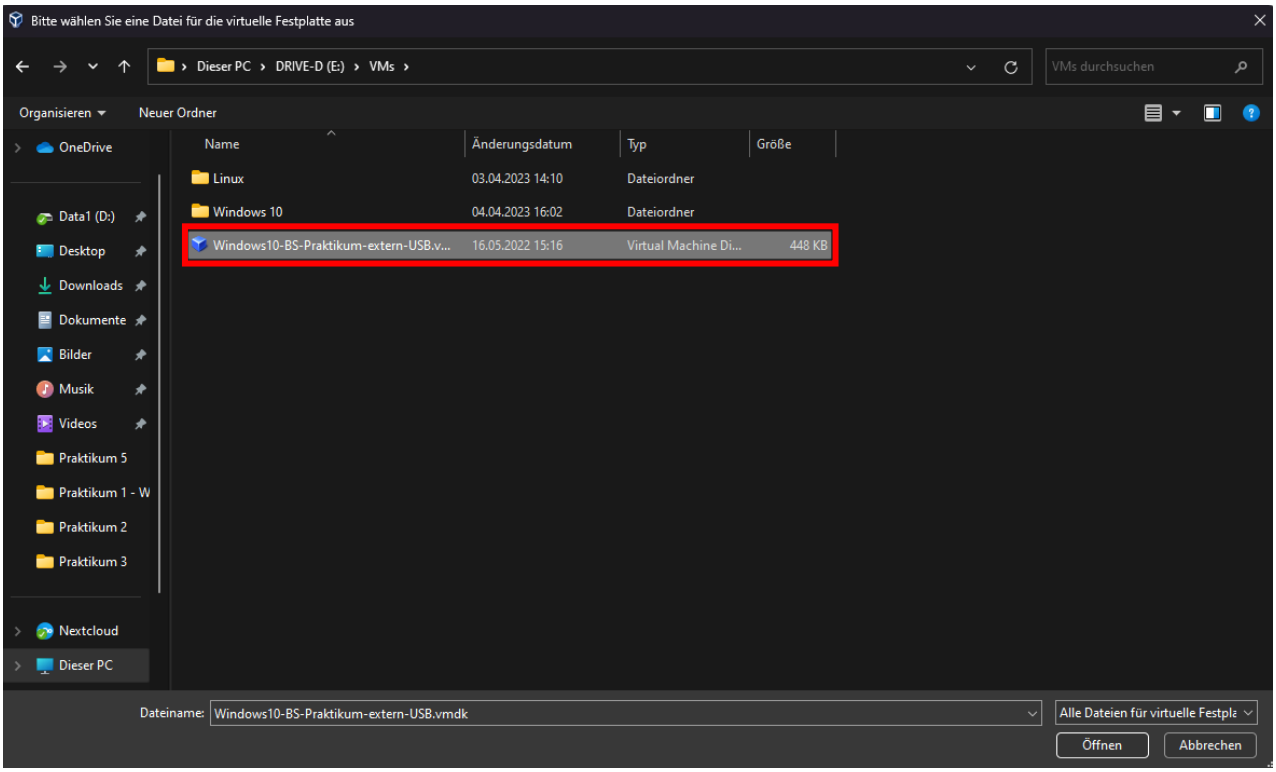


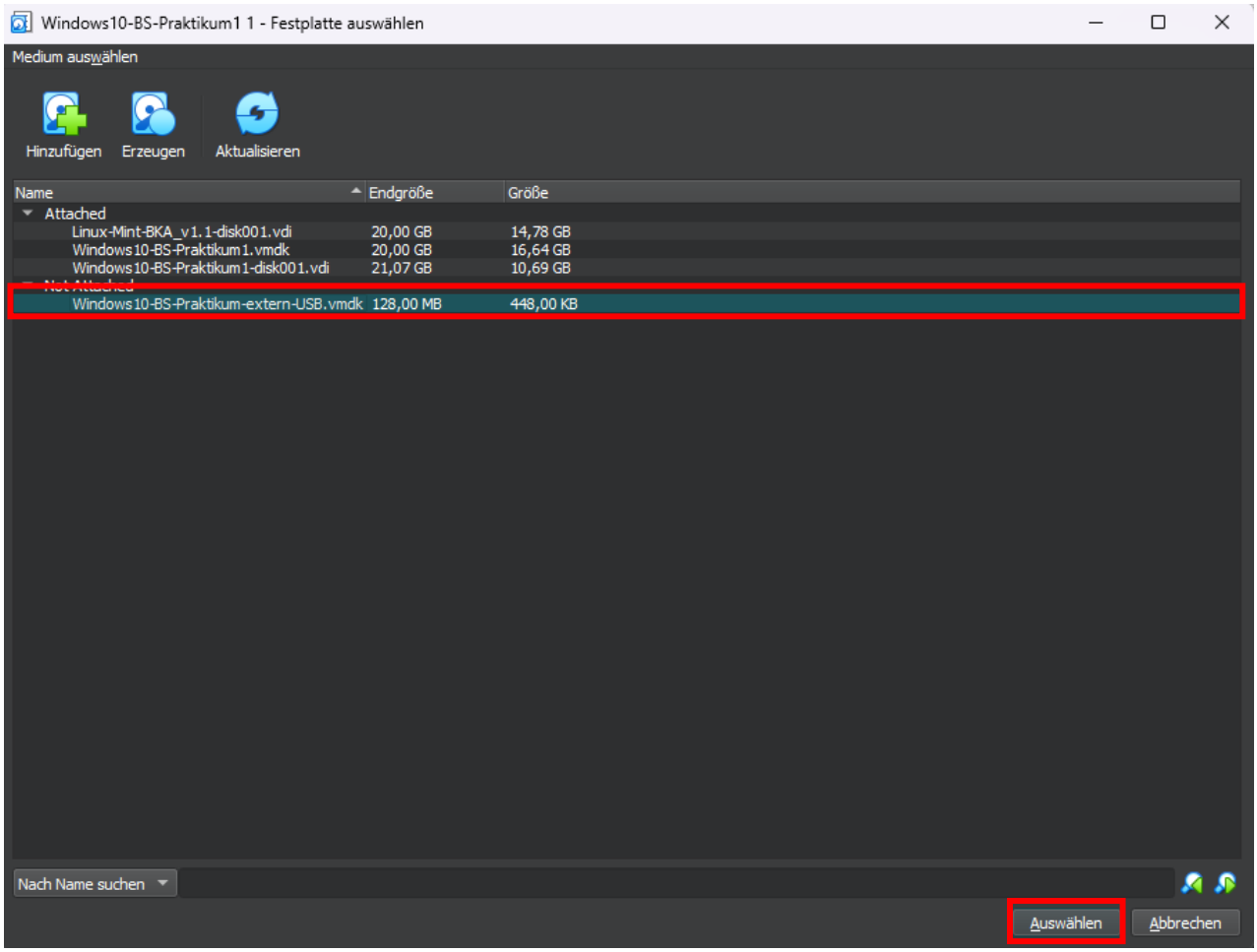


- Fügen Sie die VMDK-Datei …extern-USB.vmdk als Massenspeicher zur VM hinzu

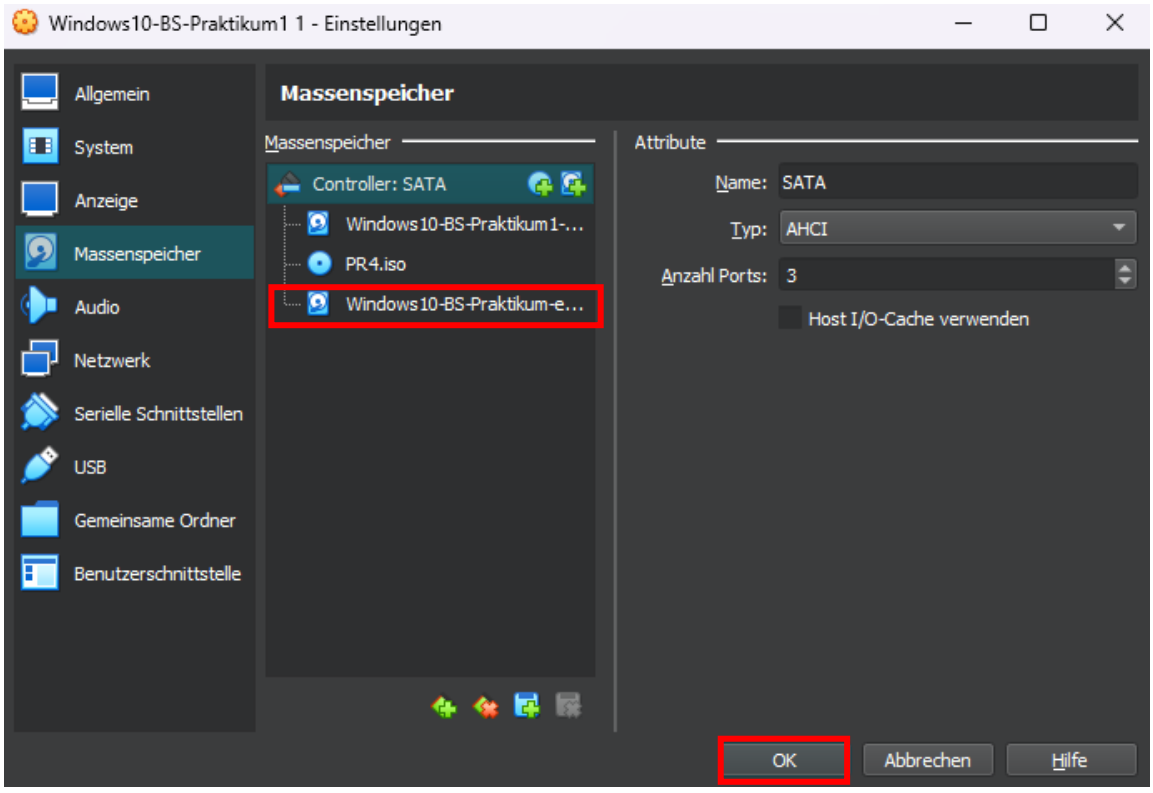






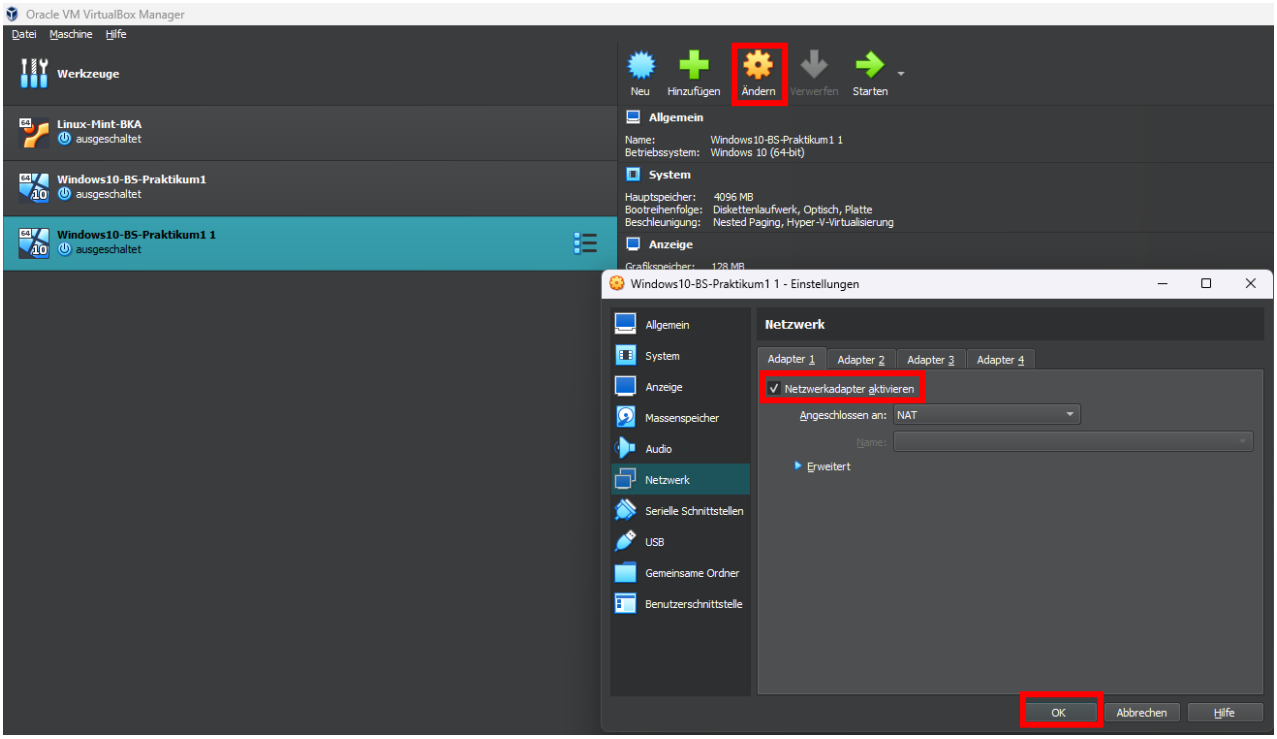


➢ Bestätigen Sie die Änderungen mit OK

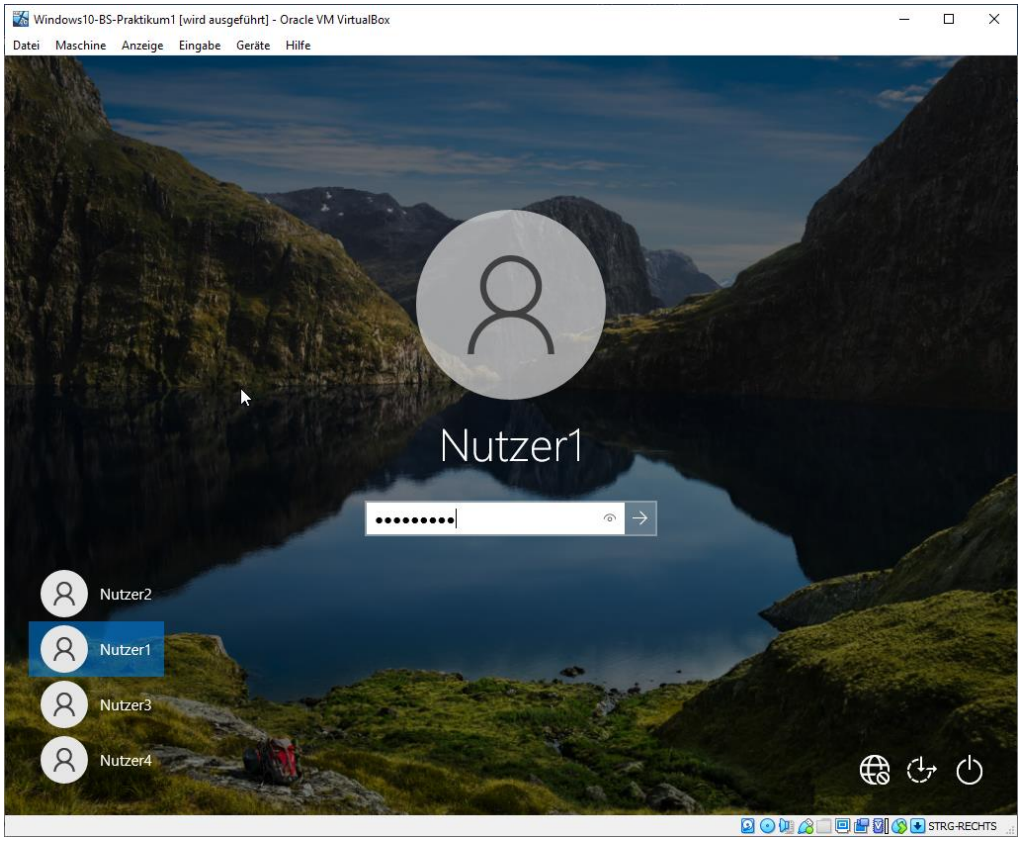


Die Firewall Einstellungen

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“.**



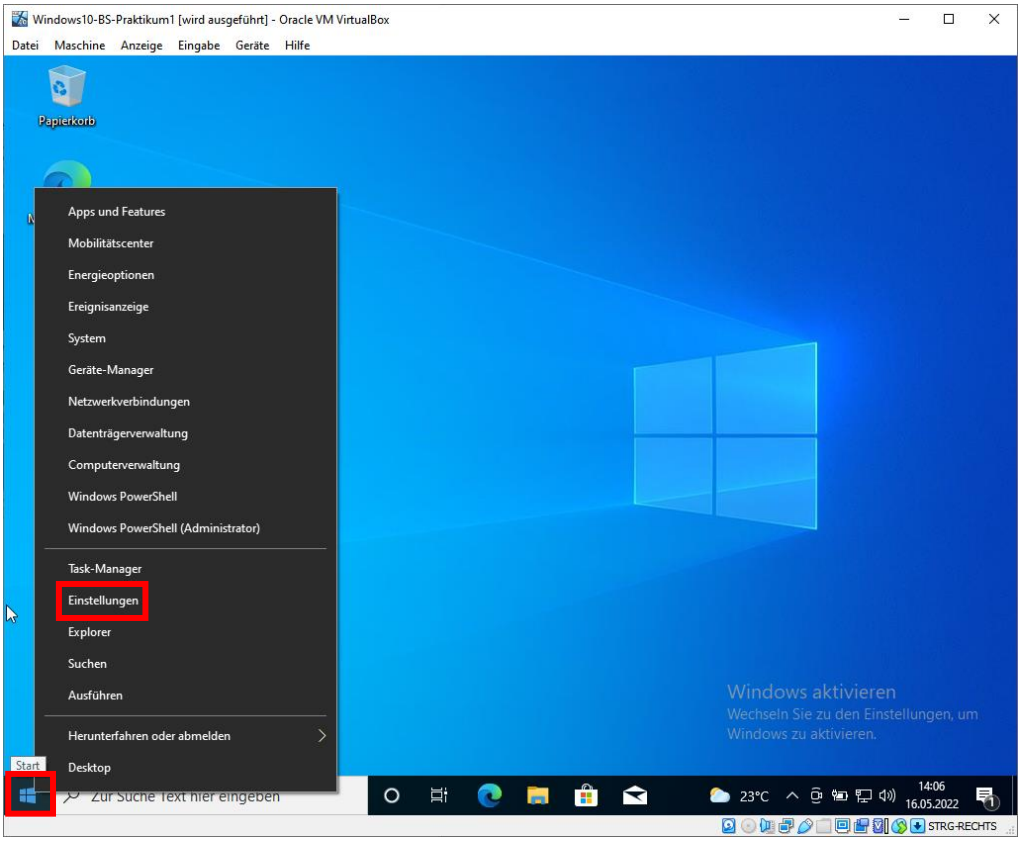
Starten Sie jetzt die VM und loggen sich als **Nutzer1** mit **Kennwort1** ein.



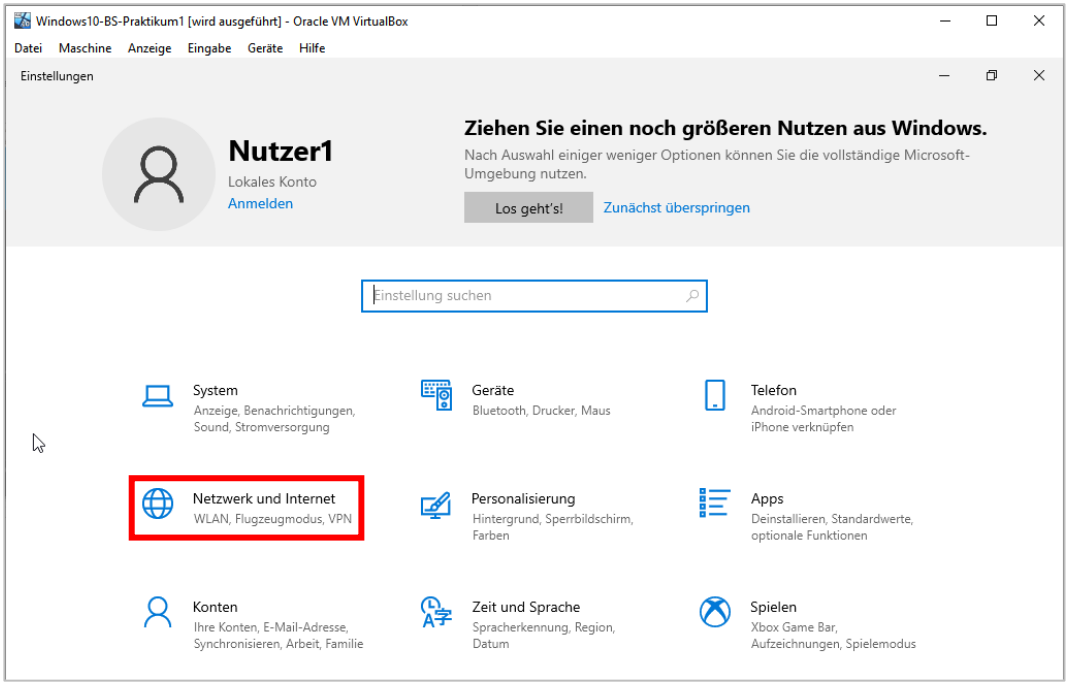
Öffnen Sie im Schritt 2 den **MS Edge** als Browser und bestätigen Sie die kommenden Dialoge**.**

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

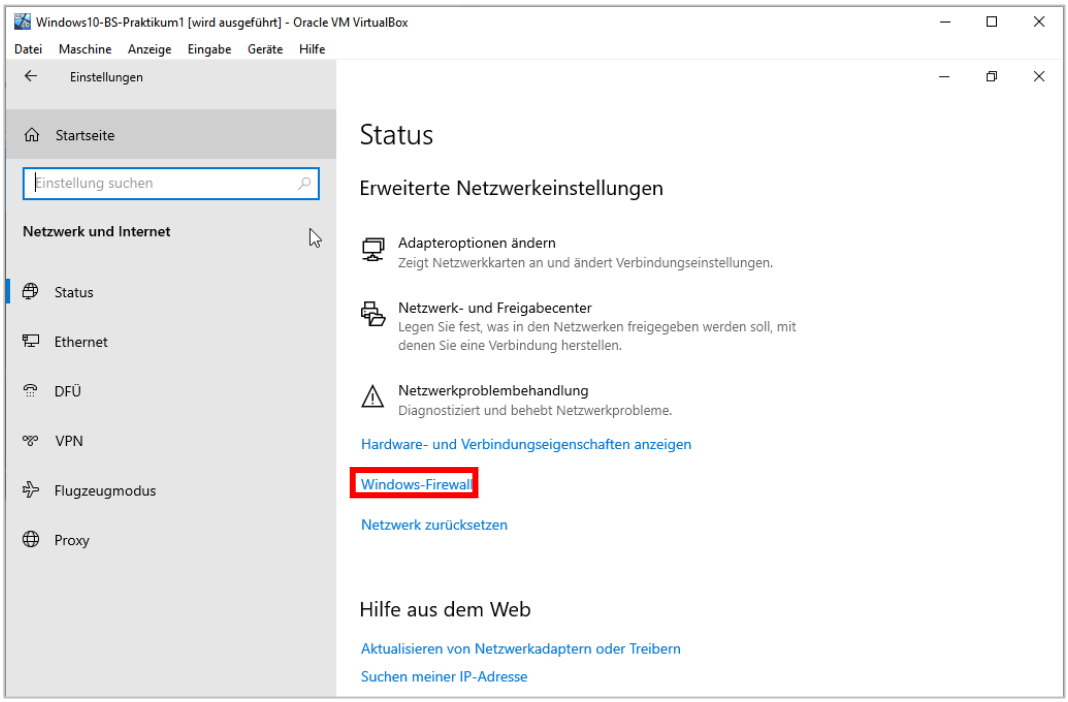
Rufen Sie die Einstellungen mit rechter Maustaste auf den Windows Start Button auf.



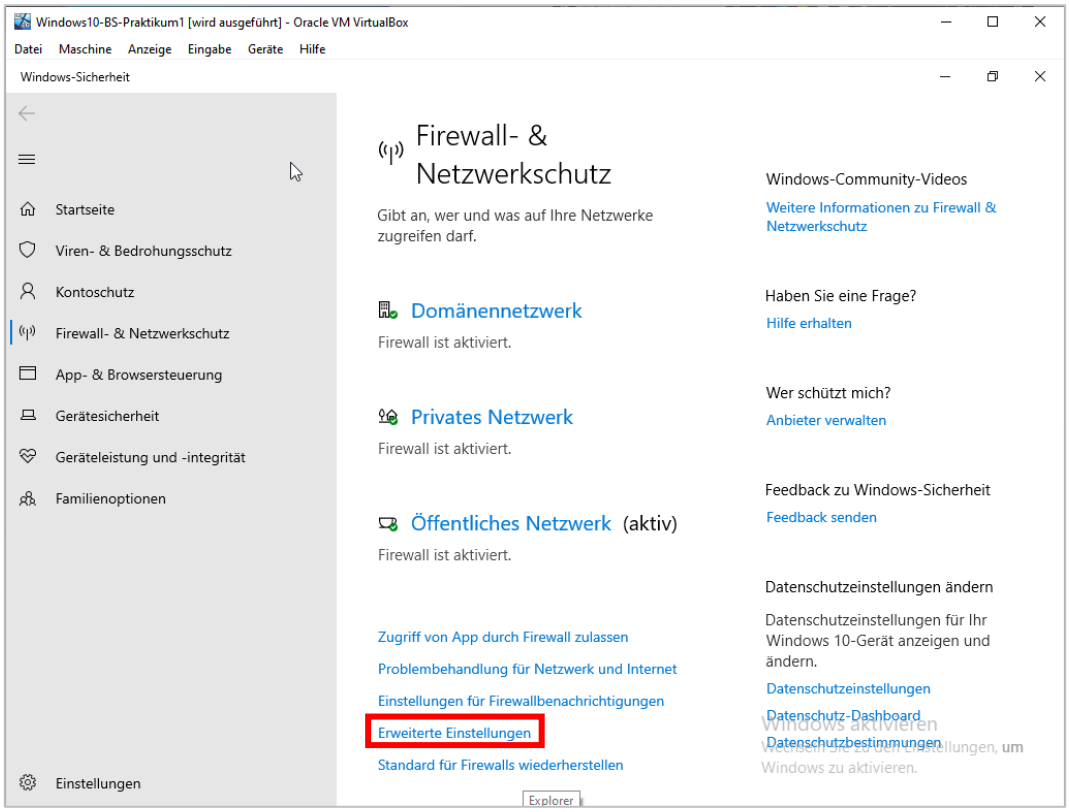
➢ Wählen Sie in den Einstellungen Netzwerk aus



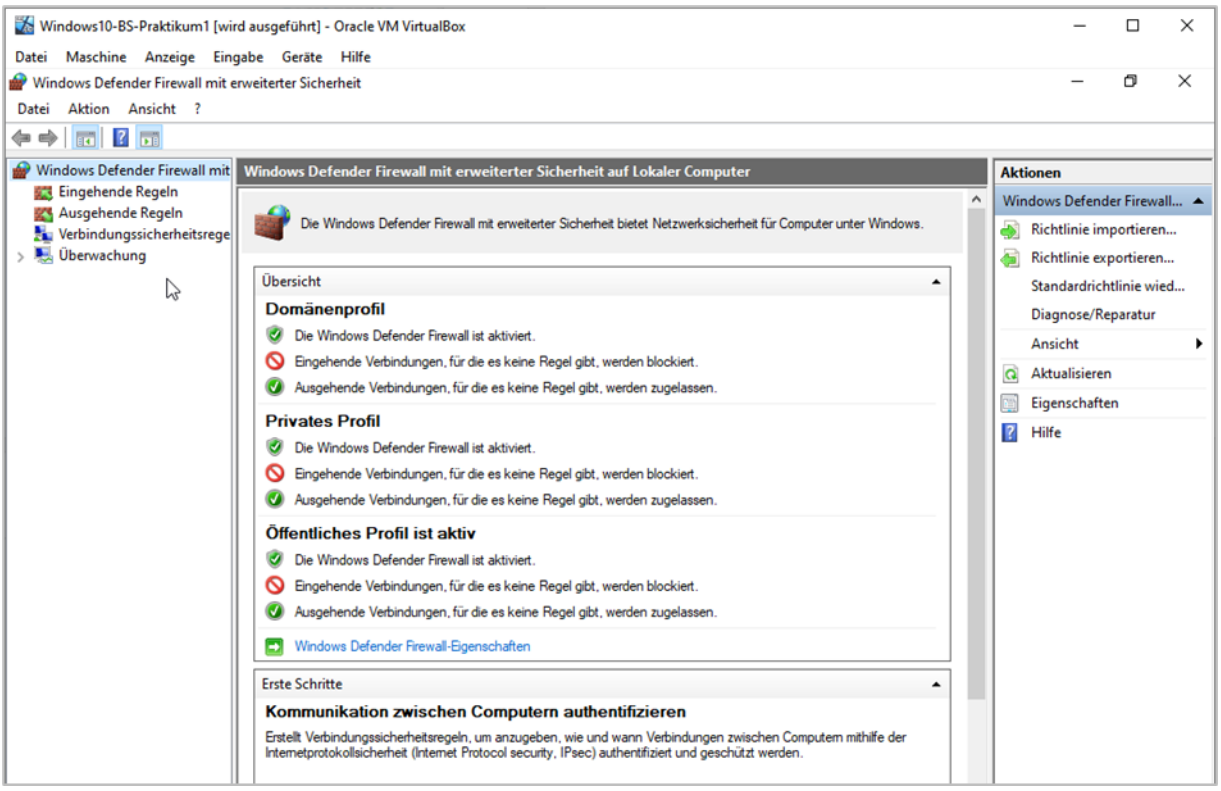
➢ Öffnen Sie die Windows Firewall



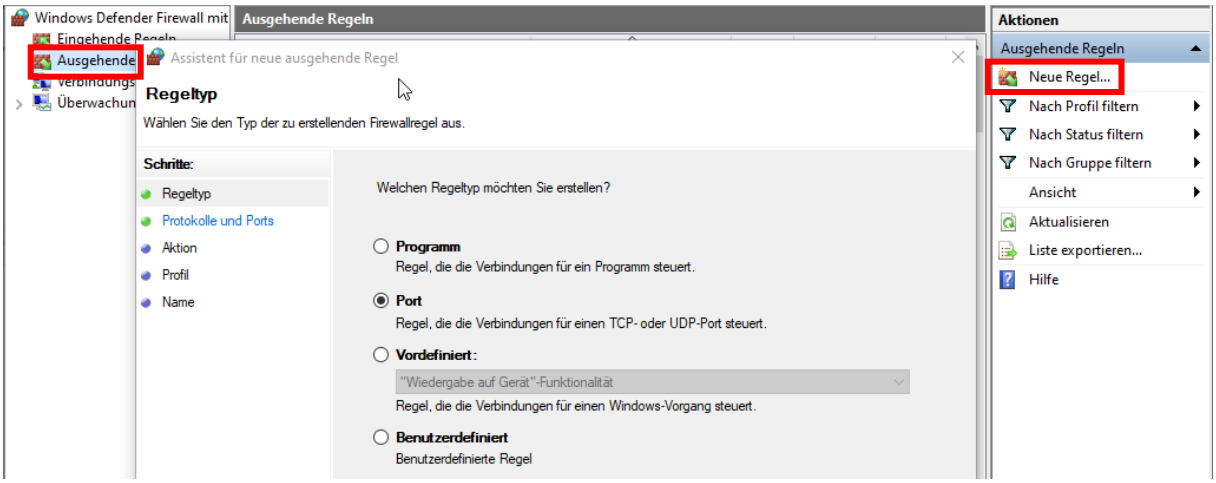
➢ Wählen Sie hier Erweiterte Einstellungen



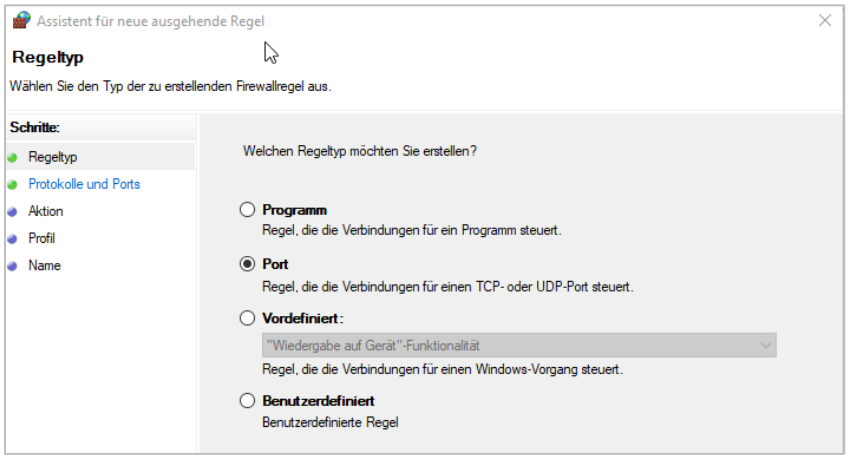
- Achtung es gibt beim Aufrufen einen Bug in der Ansicht
- Erweitere Einstellungen sind im Hintergrund – Alt+TAB zum Hervorholen wählen

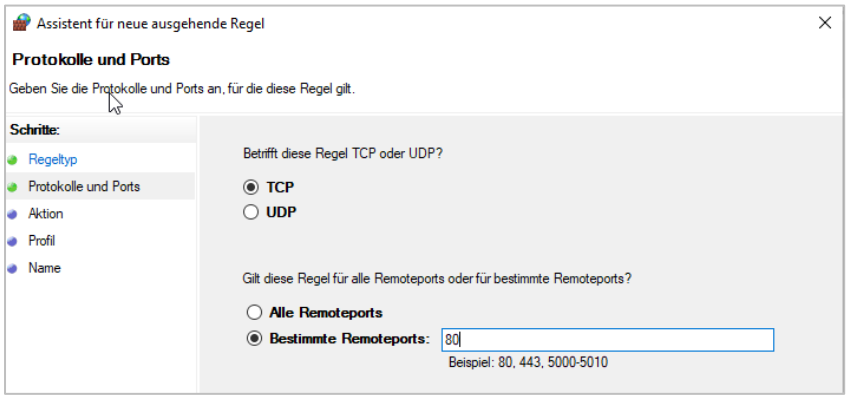


➢ Gehen Sie auf Ausgehende Regeln und Wählen mit dem Seiten-Menü **Neue Regel**

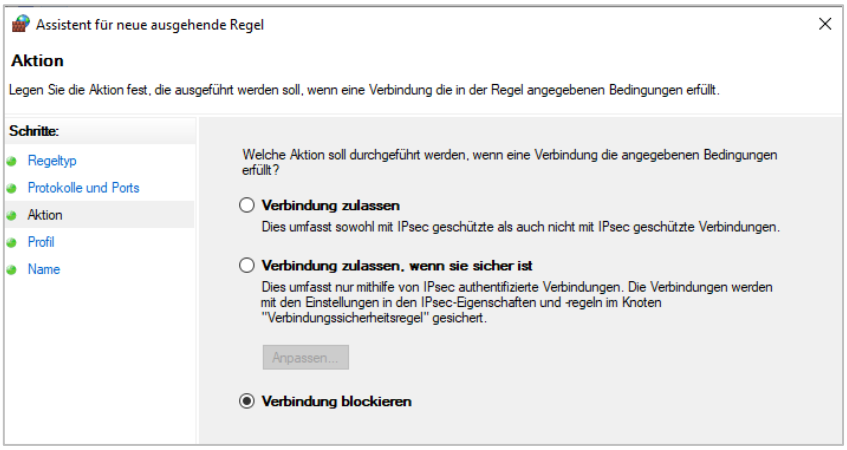


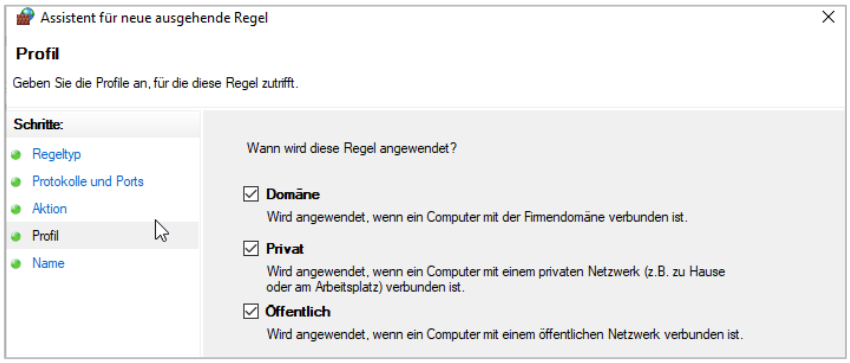
➢ In der Neuen Regel wählen Sie bitte Port aus und tragen dann Port 80 ein



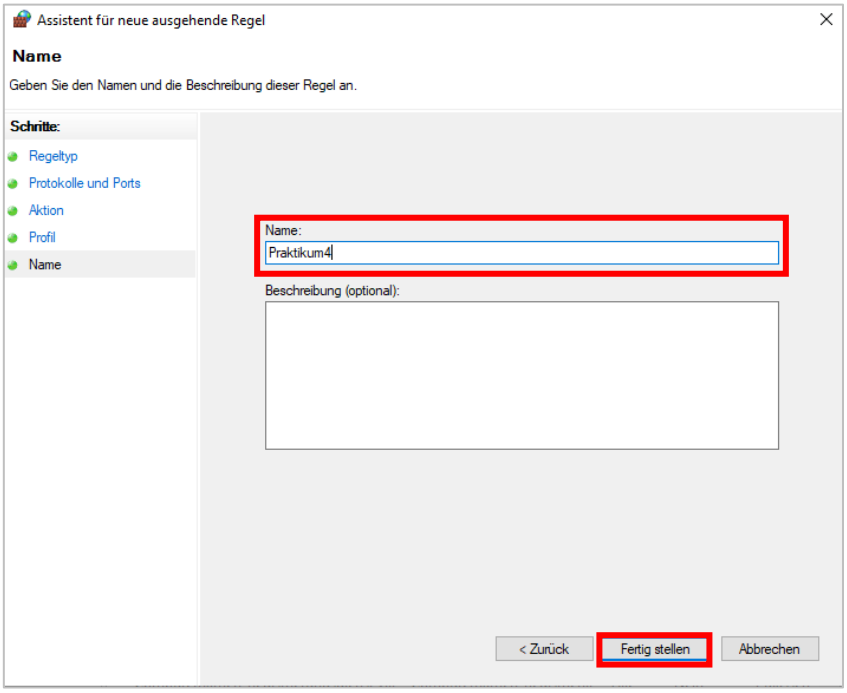


➢ Wählen Sie **Verbindung blockieren** und tragen dies **für alle Profile** ein

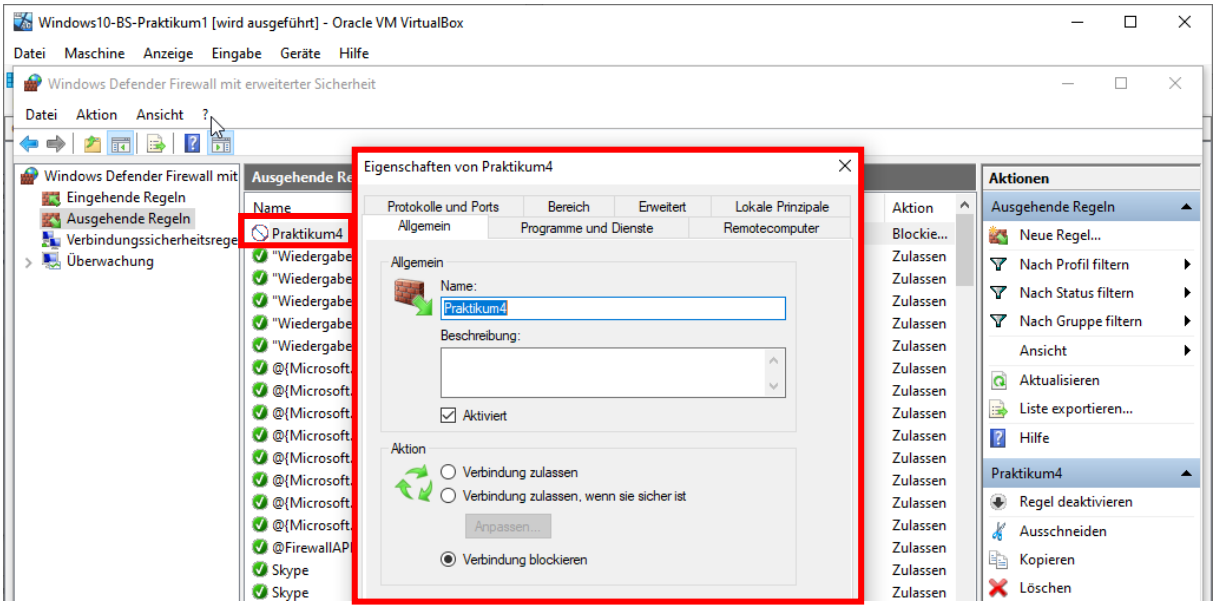




➢ Benennen Sie diese Regel mit **Praktikum4**

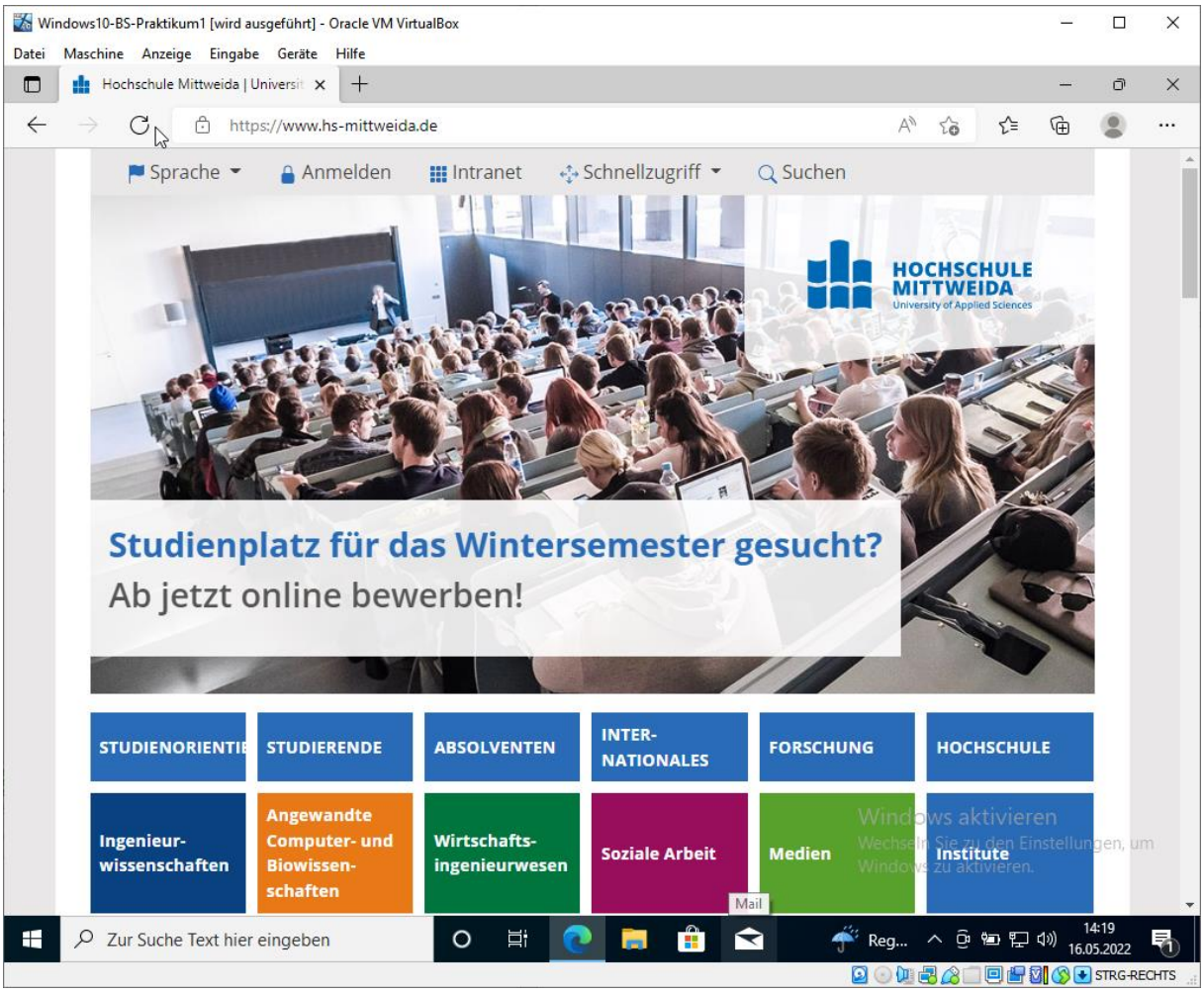


- Überprüfen Sie die so erstellte Regel



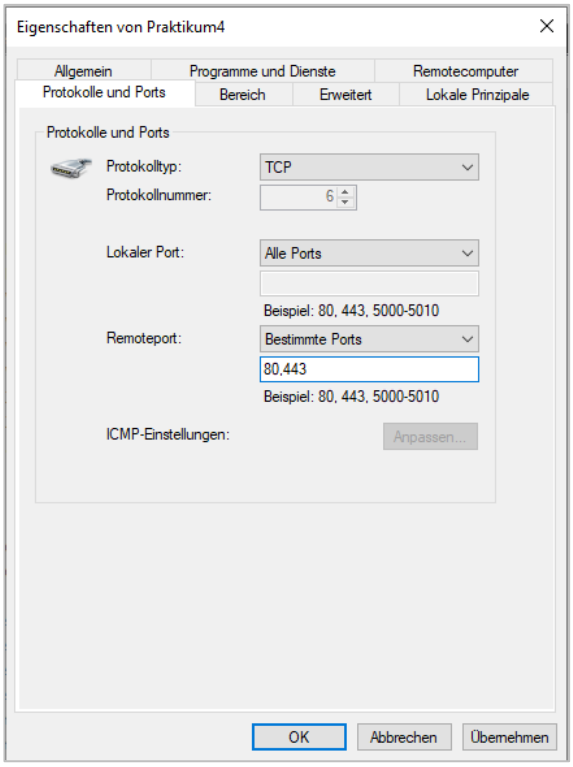
- Hat alles funktioniert?

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

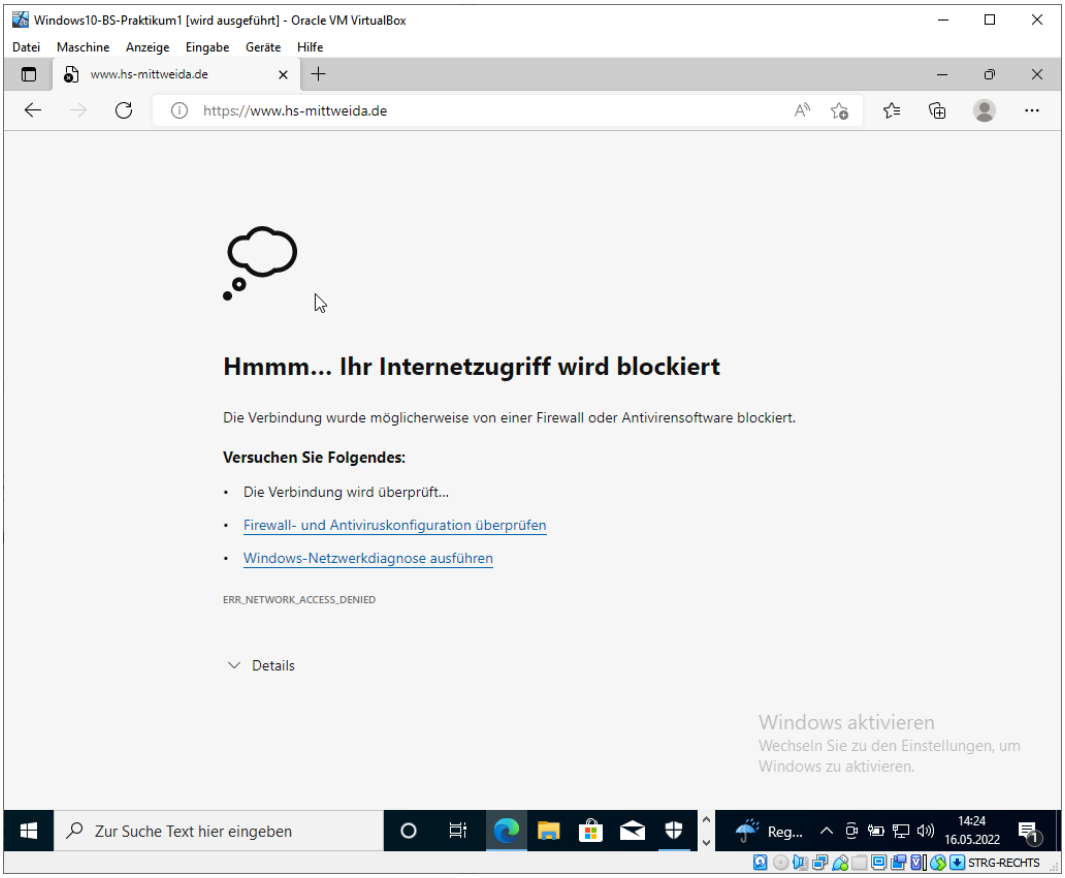


Warum ist der Abruf möglich?

- 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

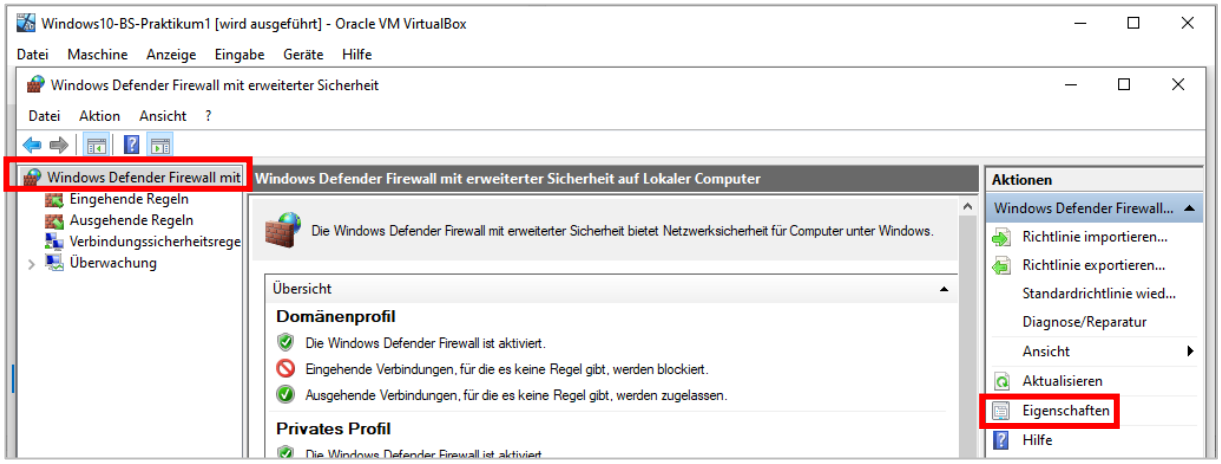


- Nun sollte der Zugriff auf die Webseite blockiert sein

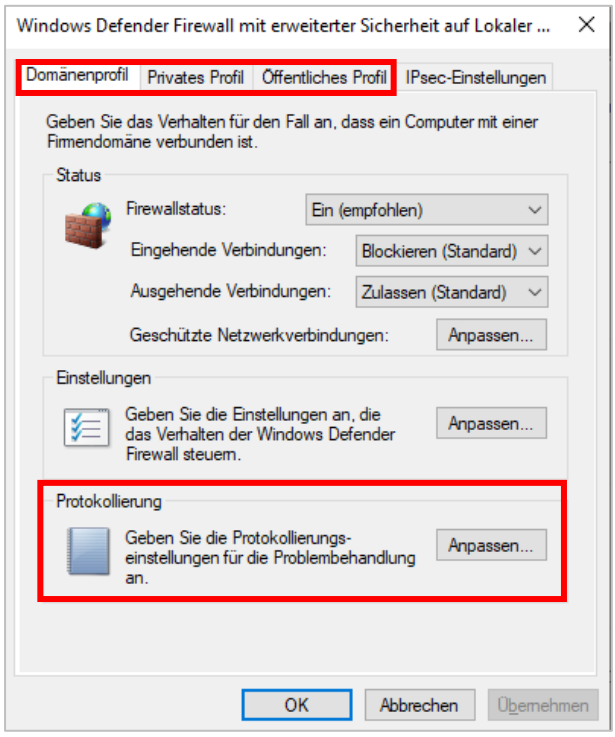


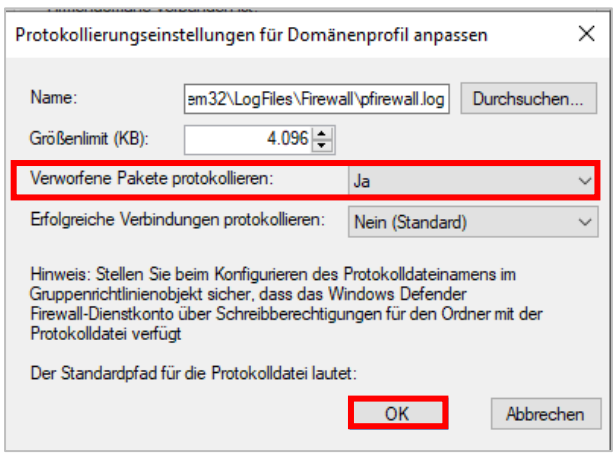
Firewall-Log Dateien einrichten und prüfen

Protokollierung aktivieren mit Auswahl der Eigenschaften der Defender Firewall.

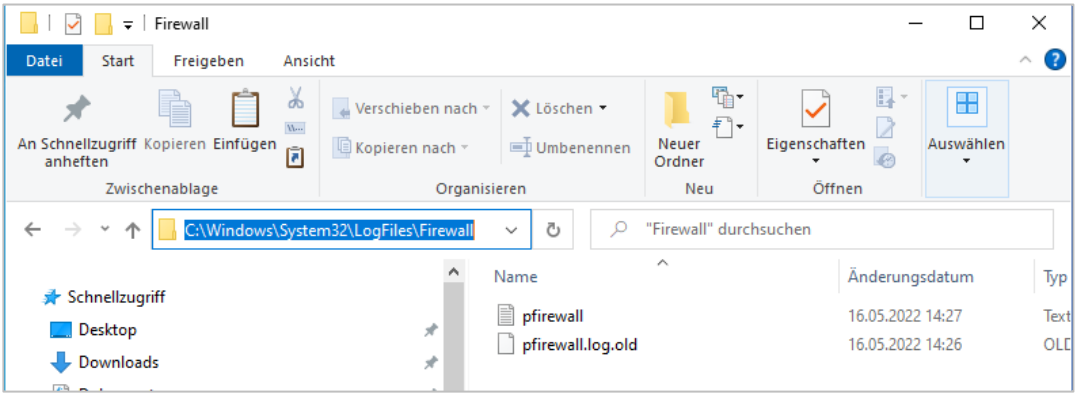


➢ Aktivieren Sie für alle drei Profile das Firewall Log, welches nur blockierte Pakete registrieren soll

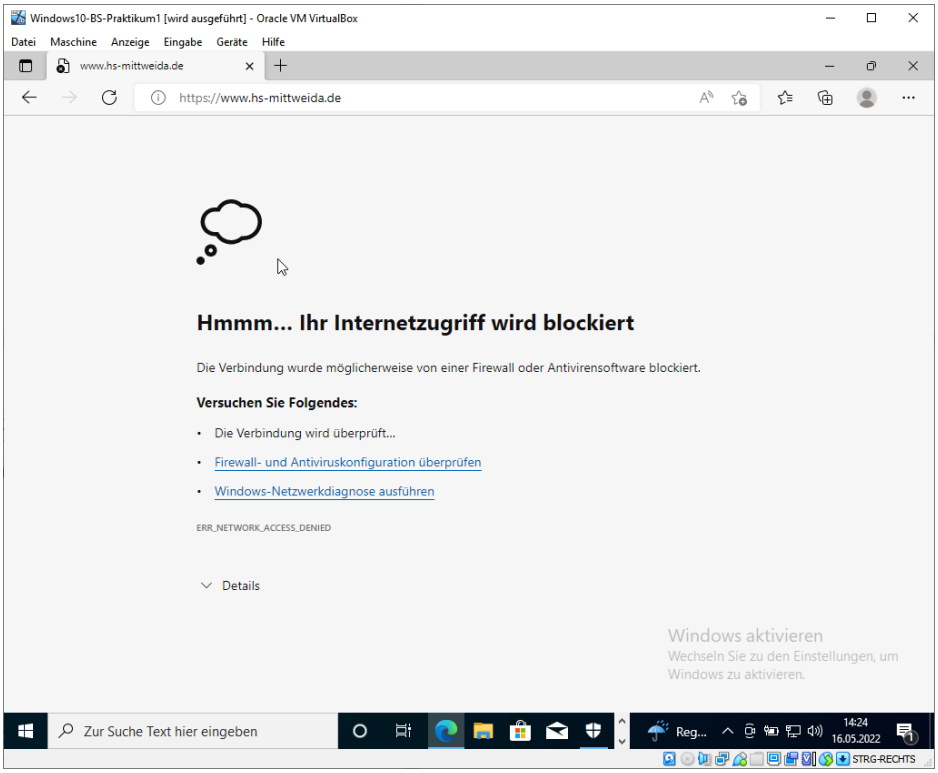




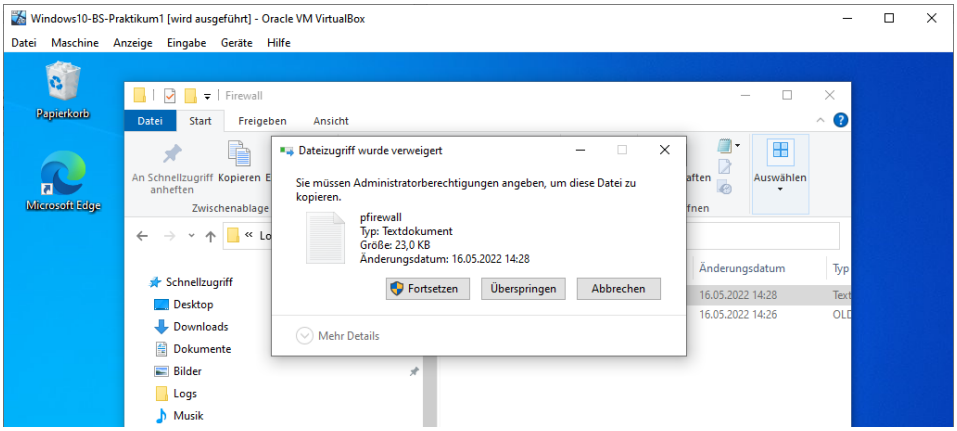
➢ Öffnen Sie zum Windows Explorer und navigieren Sie zum Firewall Log (C:\windows\system32\Logfiles\Firewall\)



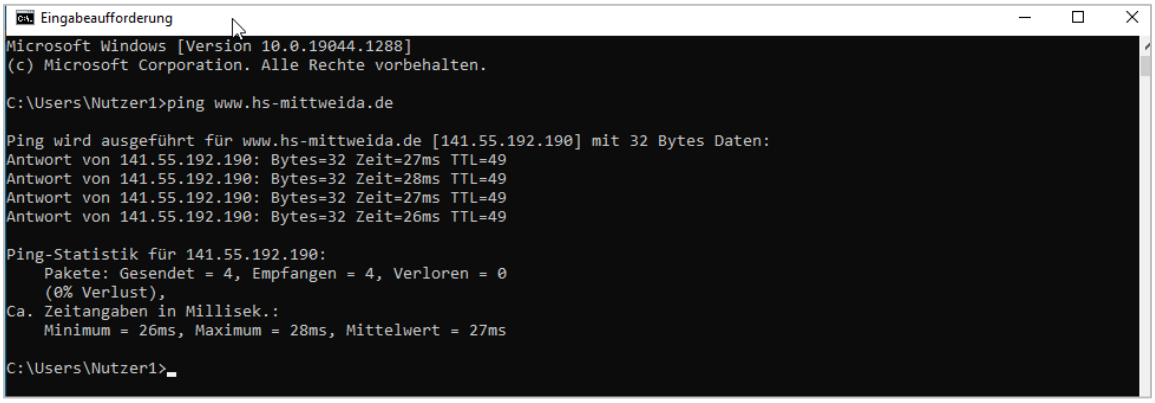
➢ Öffnen Sie den Browser und navigieren Sie zu www.hs-mittweida.de , um einen Eintrag im Log zu erzeugen

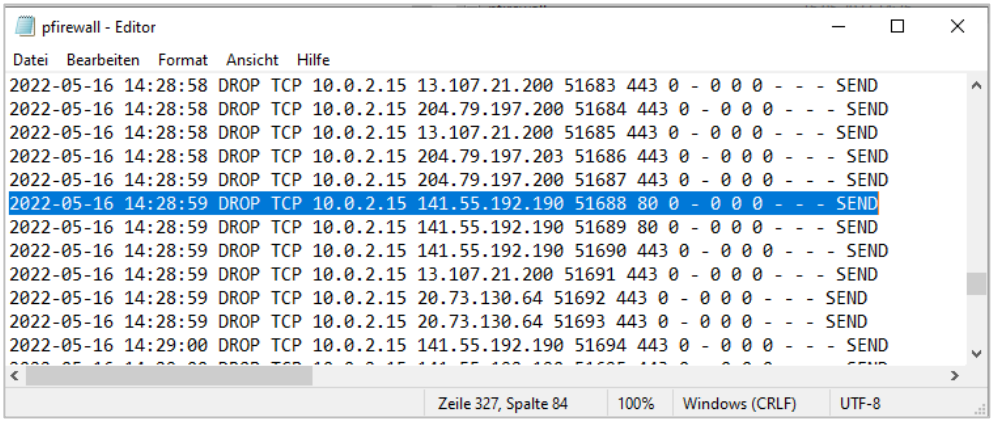


➢ Kopieren Sie das Log auf Desktop, da es nicht direkt im laufenden Betrieb geöffnet werden kann



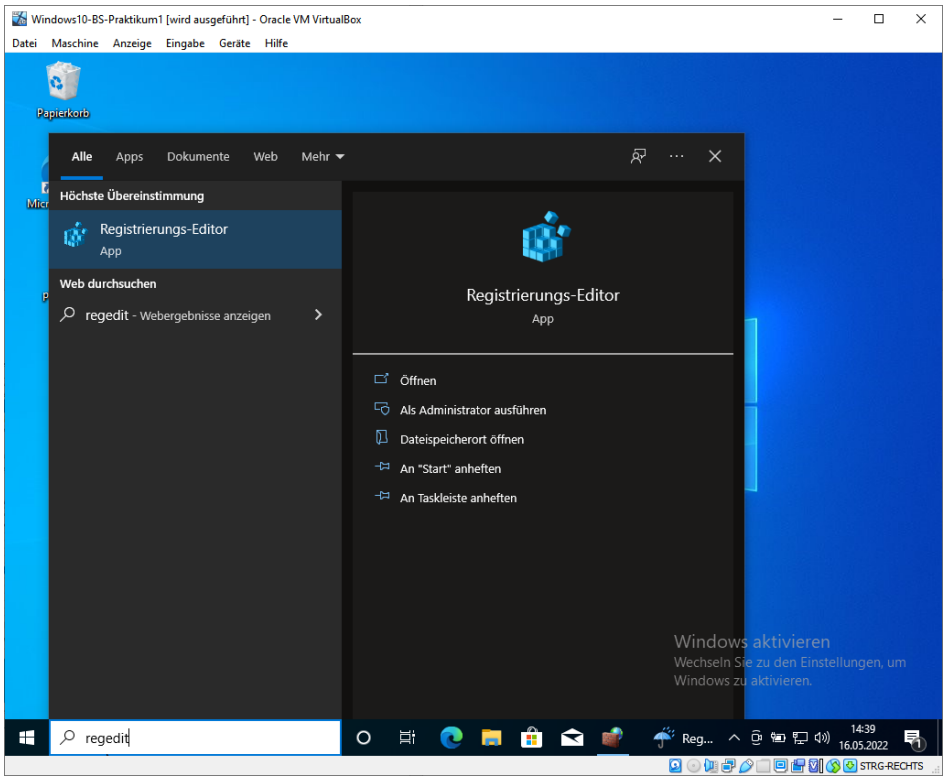
- Ermitteln Sie mit Hilfe der Eingabeaufforderung/Kommandozeile die IP-Adresse der URL www.hs-mittweida.de
- Suchen Sie diese in der Logdatei



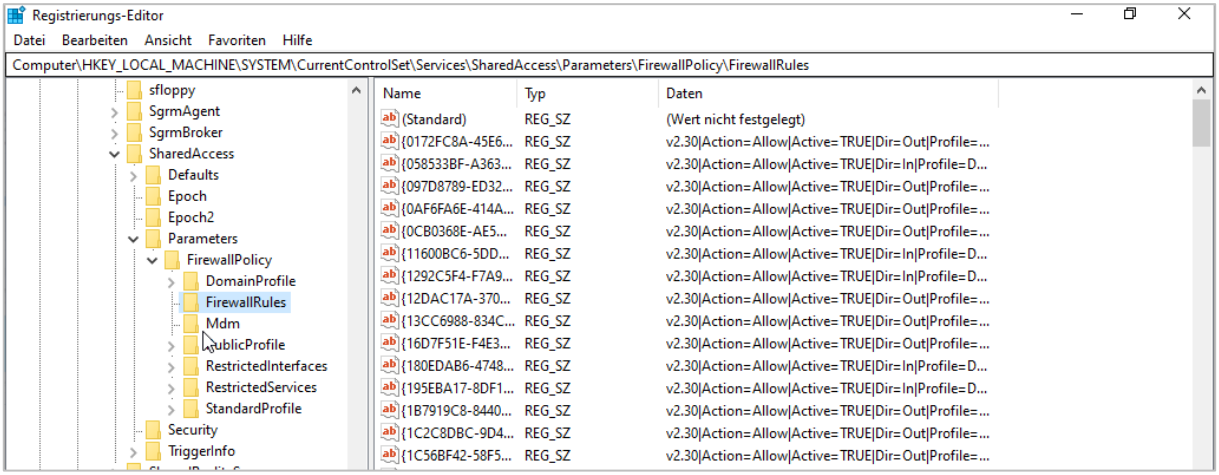


Firewall-Eintragungen in der Registrierung überprüfen und ändern

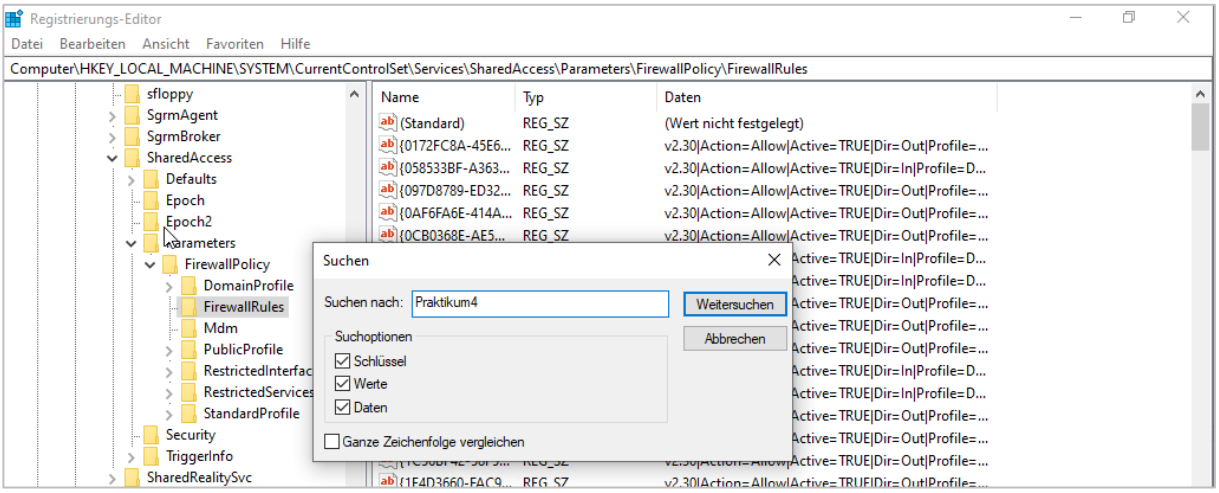
Öffnen Sie den Registrierungseditor **Regedit**.

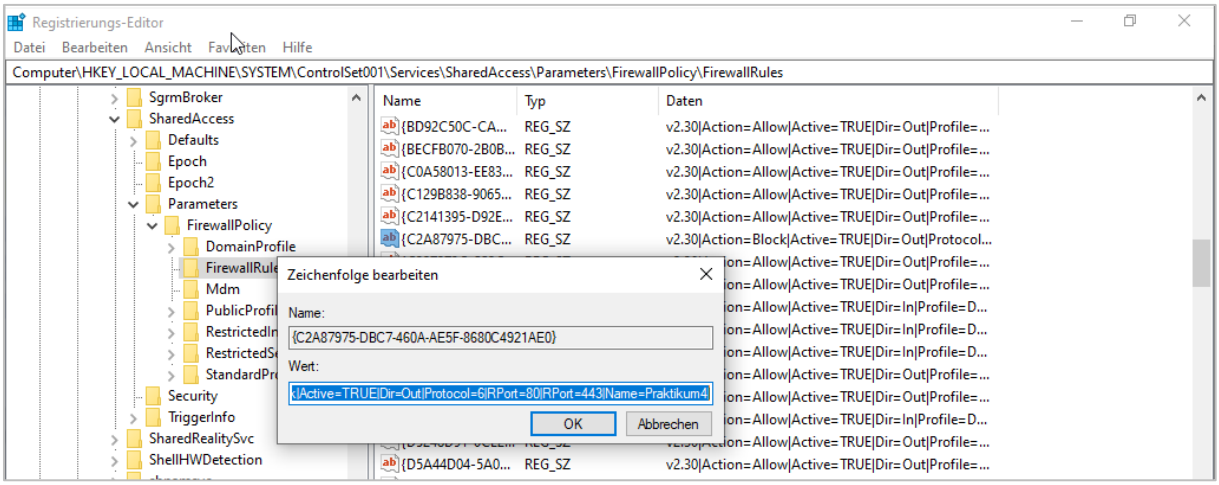


- Suchen Sie sich die Firewall Regeln heraus
- Suchen Sie Sich die Regel Praktikum 4 heraus

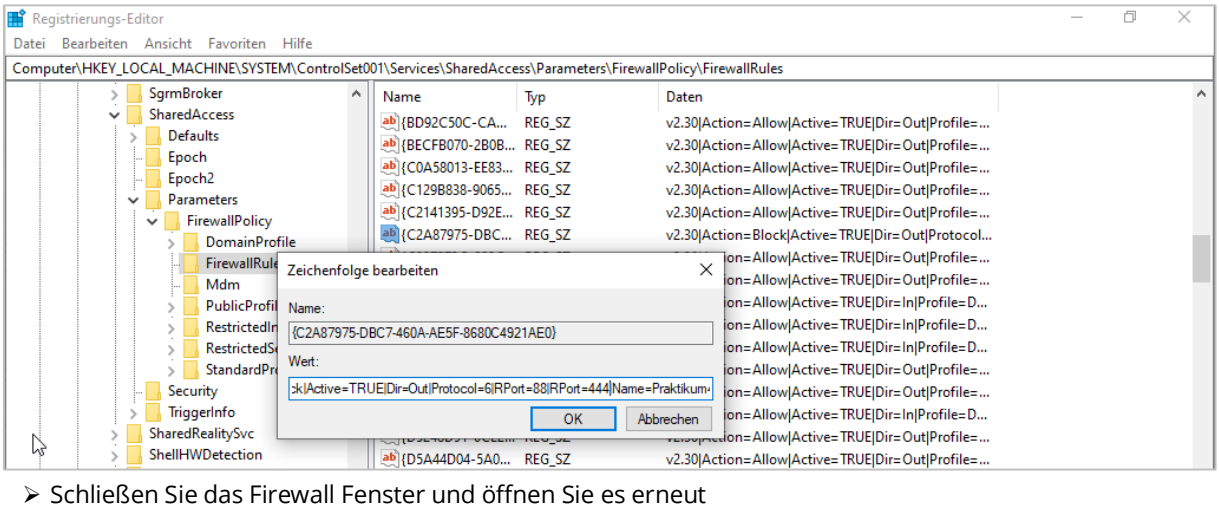


➢ Bearbeiten > Suchen > Praktikum4

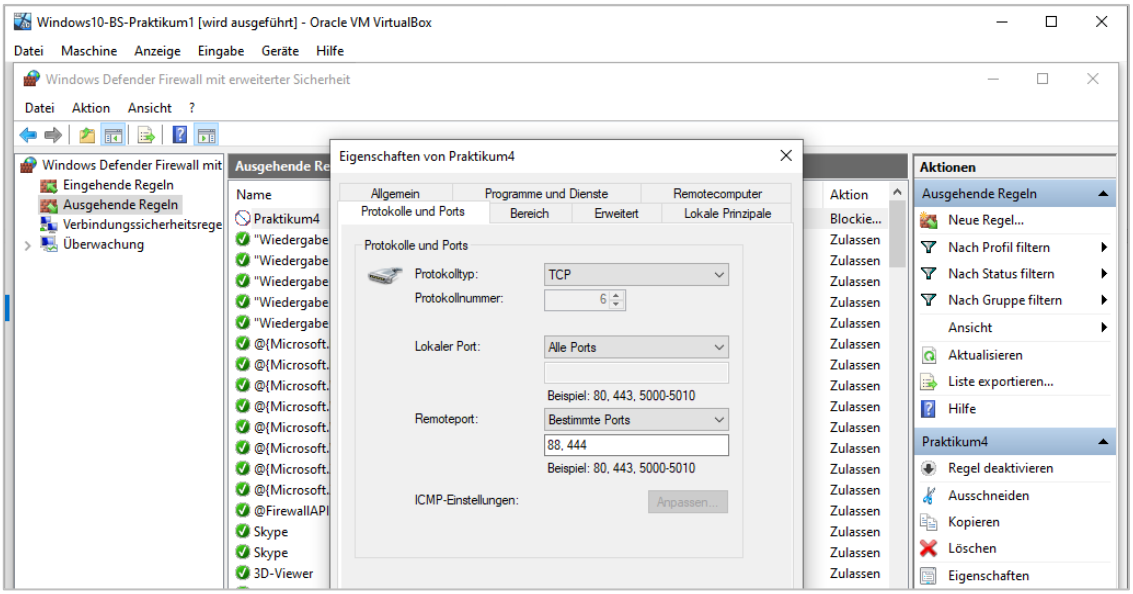




➢ Ändern Sie im Schlüssel die Werte Port 80 > 88 und Port 443 > 444

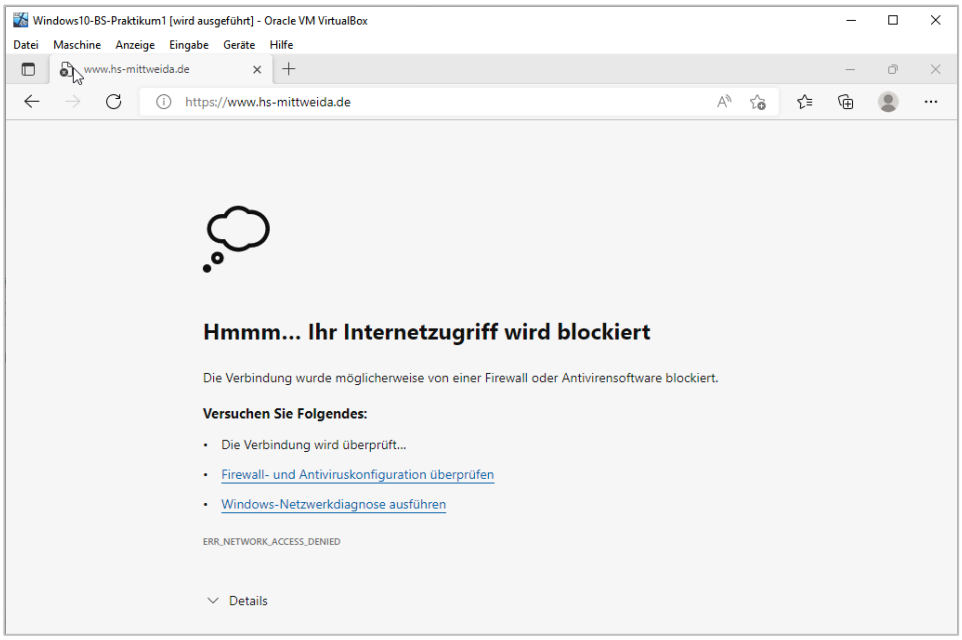


➢ Schließen Sie das Firewall Fenster und öffnen Sie es erneut



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.

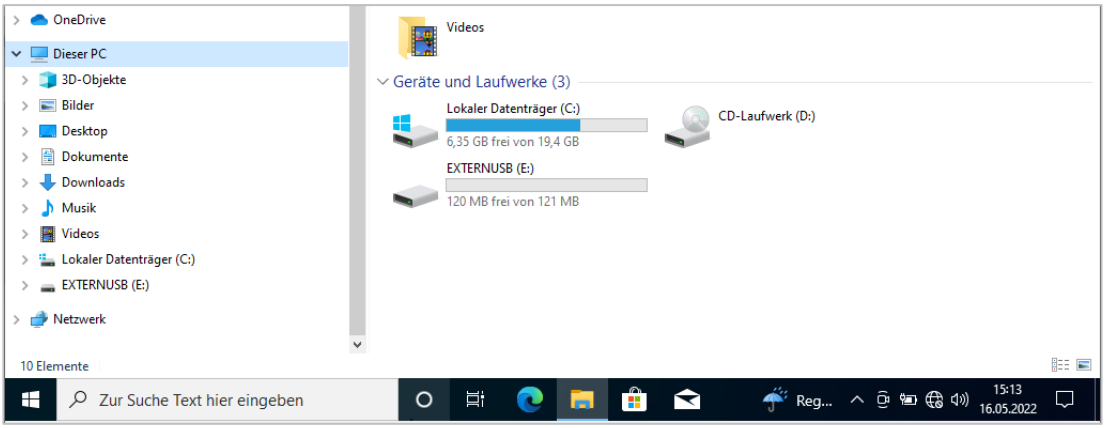
- Starten Sie Windows neu und versuchen Sie es erneut

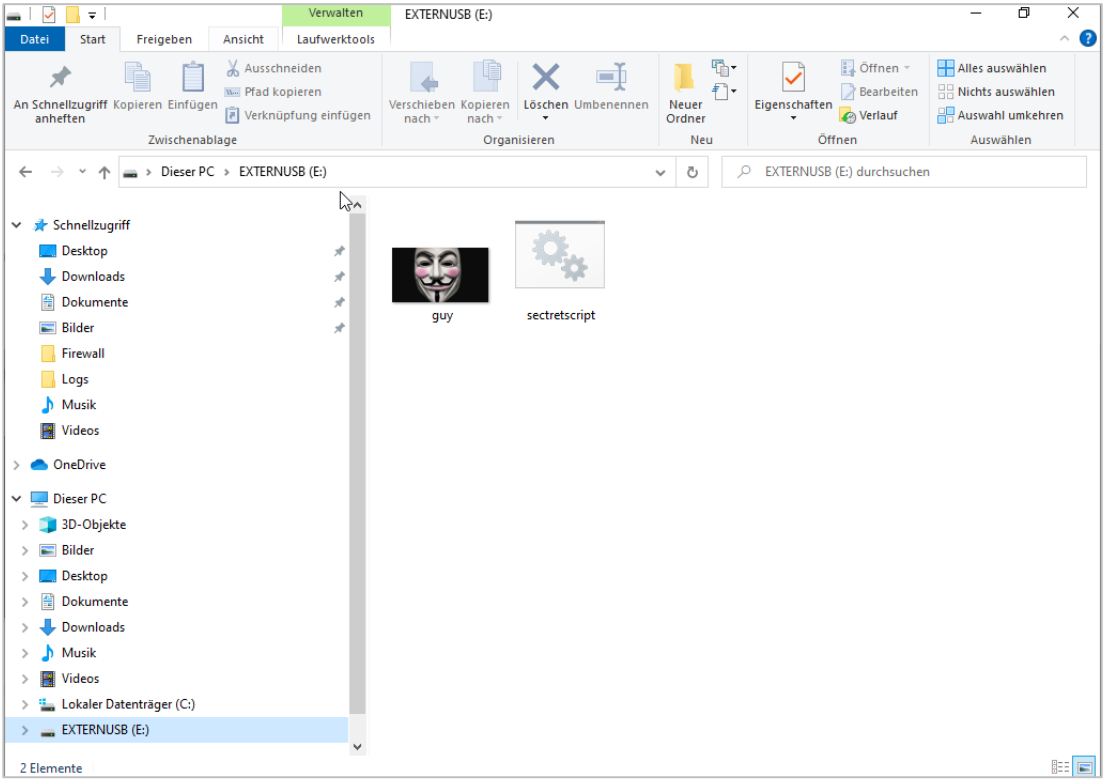
Recent/Verlaufs-Eintragungen

Recent-Eintragungen anlegen

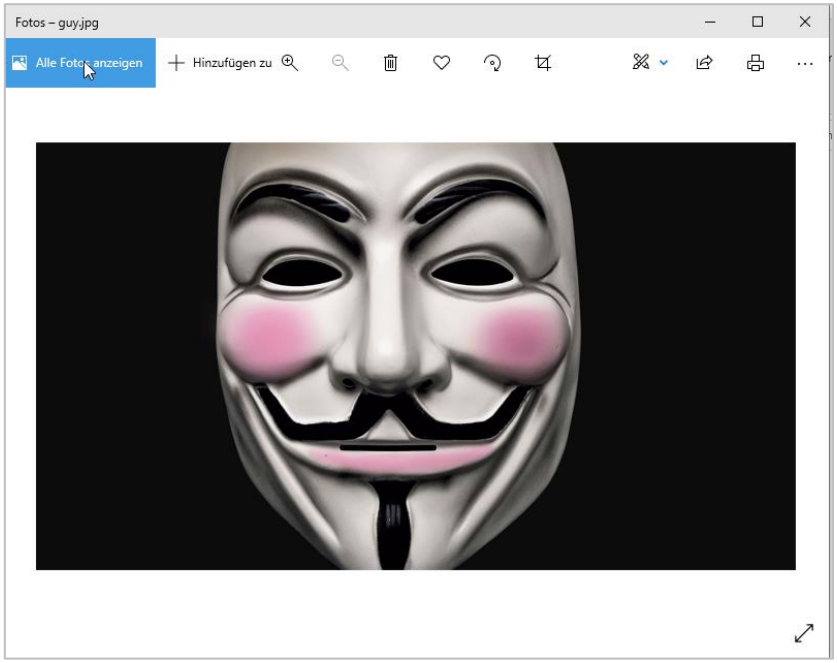
Schließen Sie alle offenen Anwendungen und Fenster.

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

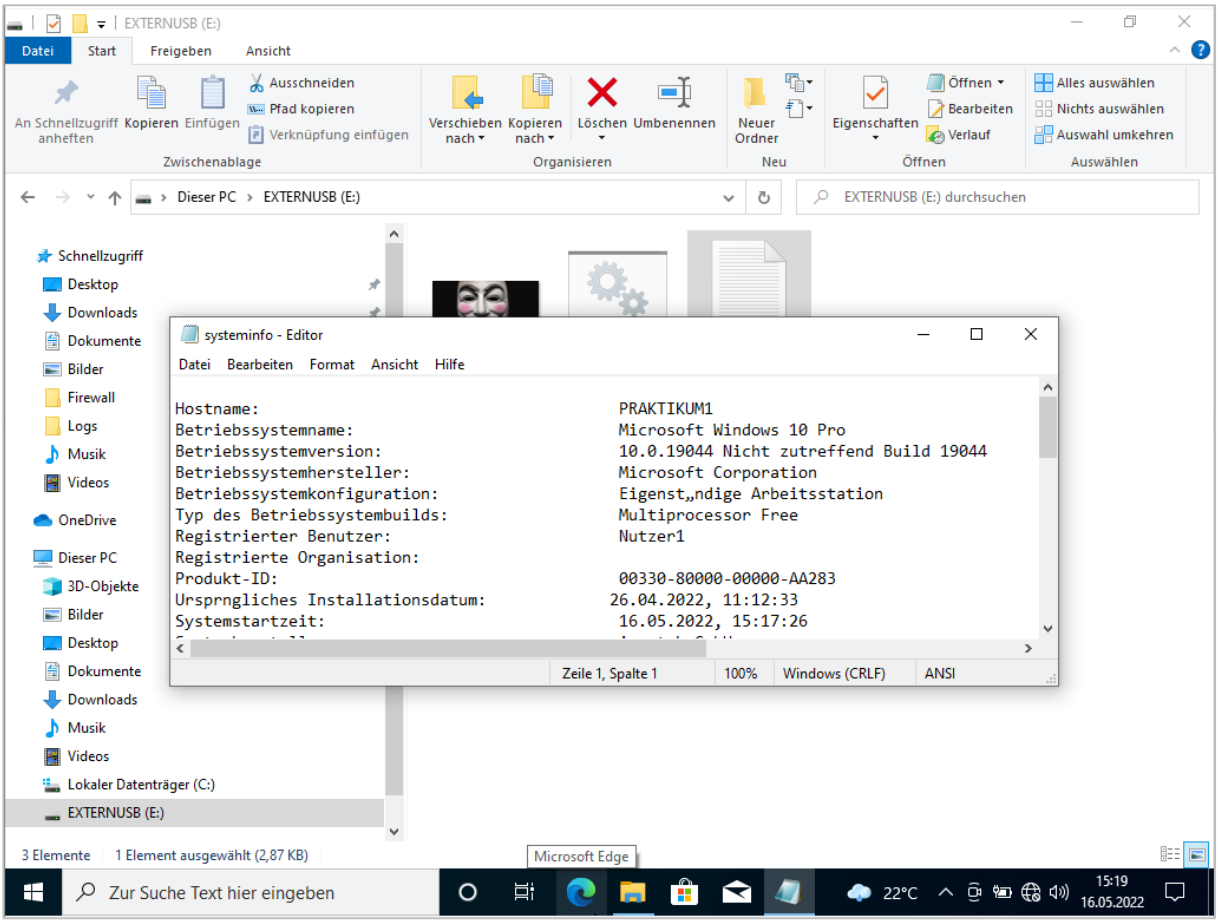




➢ Schauen Sie sich die Bilddatei an

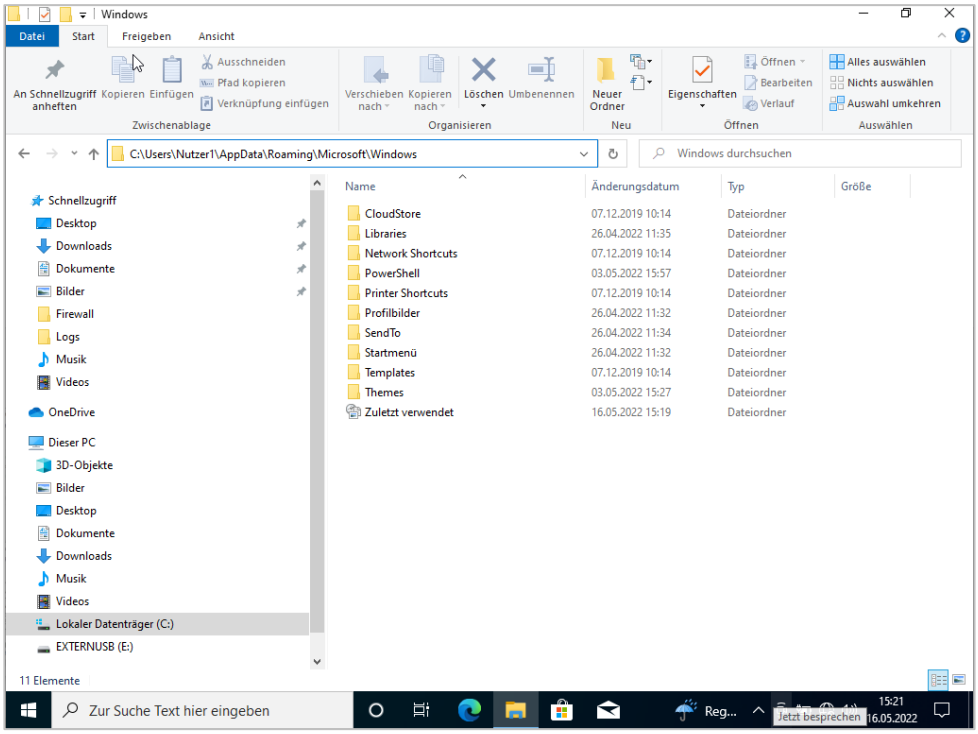


➢ Starten Sie durch Doppelklick zudem die BAT-Datei und Öffnen Sie danach die neu erstellte Datei Systeminfo.txt

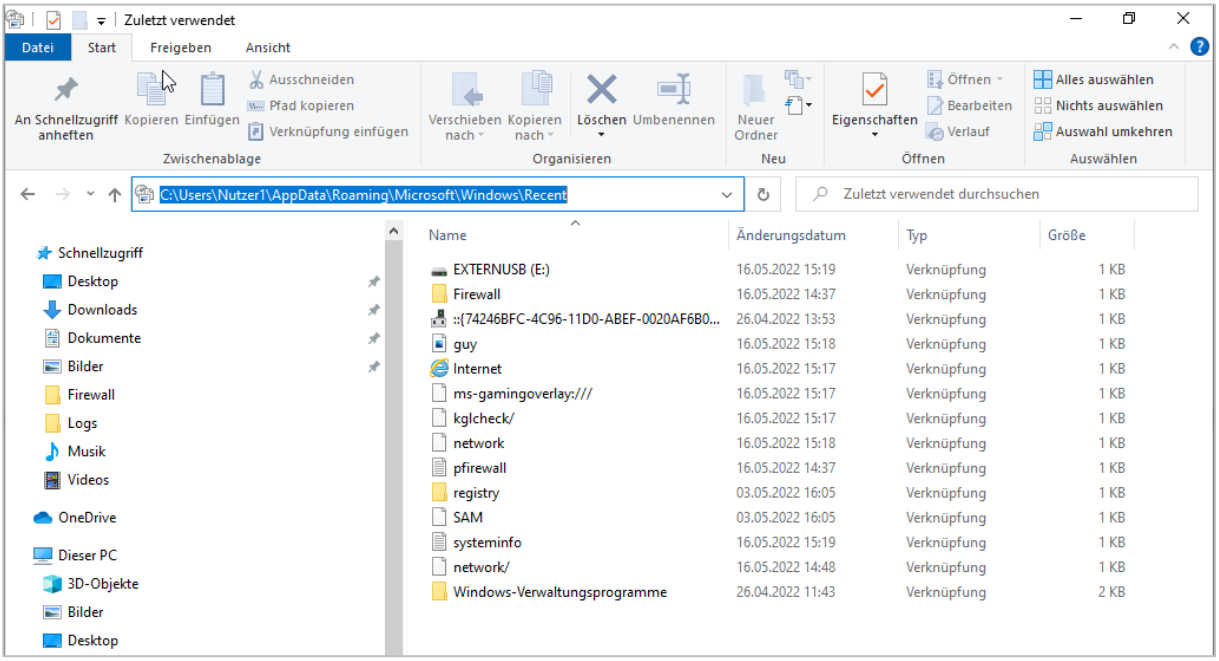


Recent-Dateien lesen

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

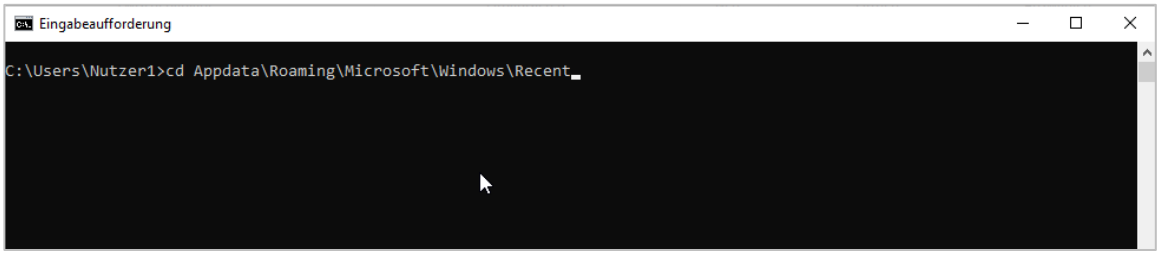


- Sehen Sie einen Recent Ordner? Wechseln Sie in diesen

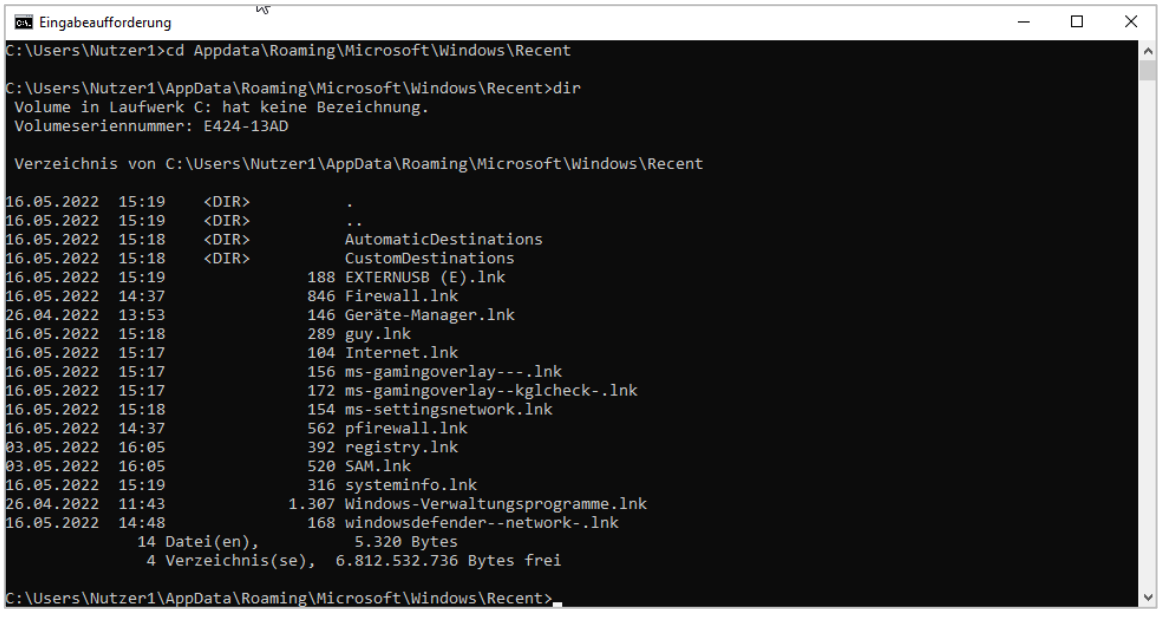


- Können Sie viel mit dieser Ansicht anfangen?

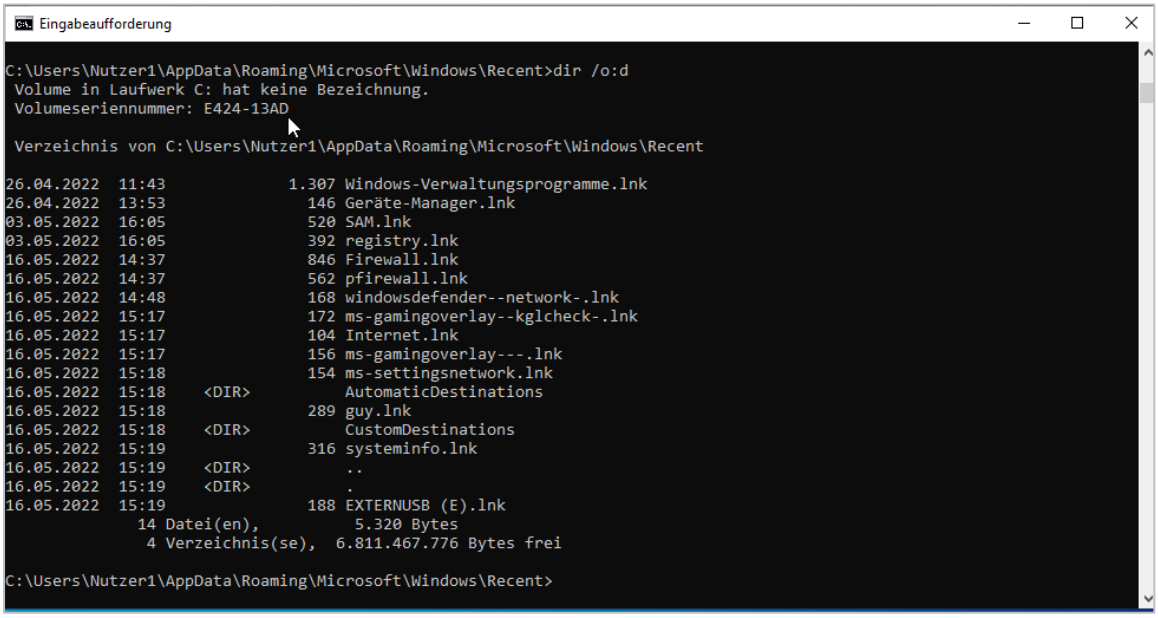
Öffnen Sie die Eingabeaufforderung/Kommandozeile cmd.exe ohne Administratorrechte. Wechseln Sie danach mit dem **cd** Befehl in das Verzeichnis **C:\Users\Nutzer1\AppData\Roaming\Microsoft\Windows\Recent.**



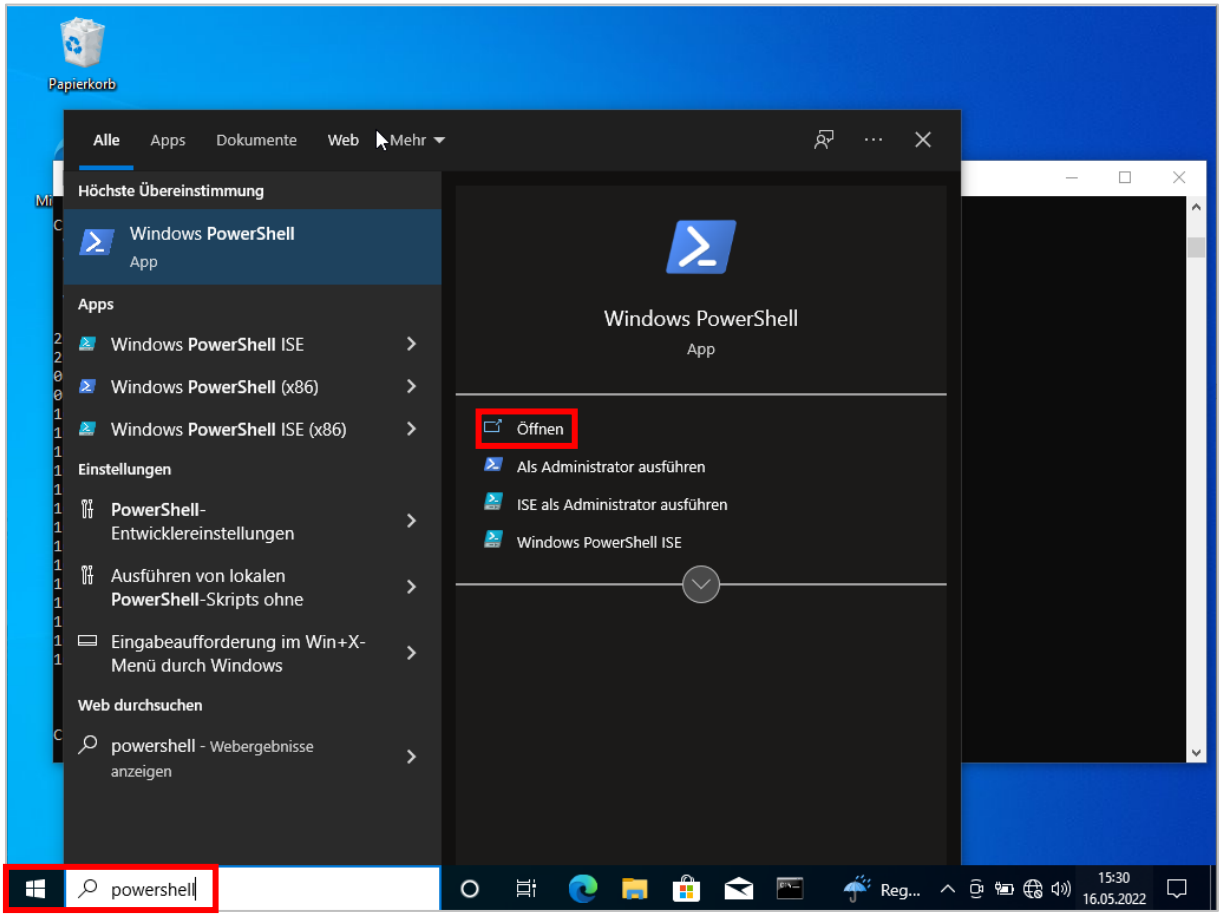
- Listen Sie den Ordnerinhalt mit **dir** auf



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

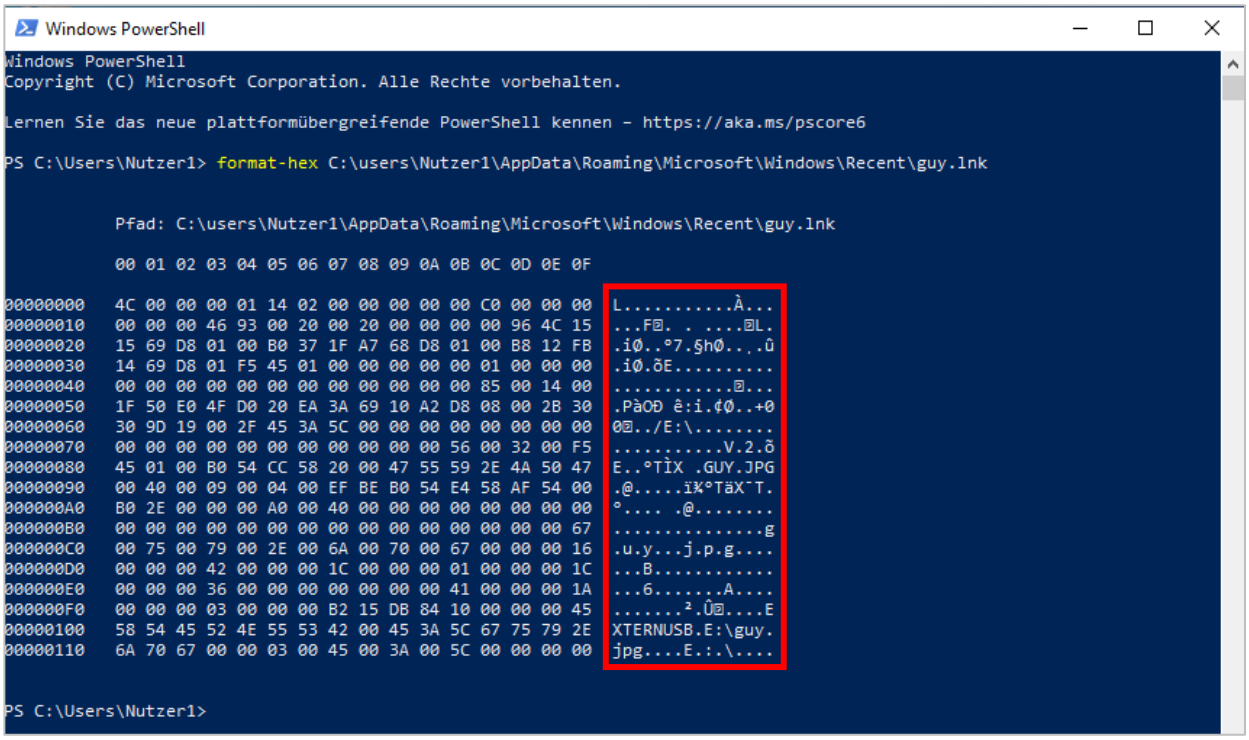


Öffnen Sie eine Powershell durch den Startbutton und der Eingabe von Powershell.

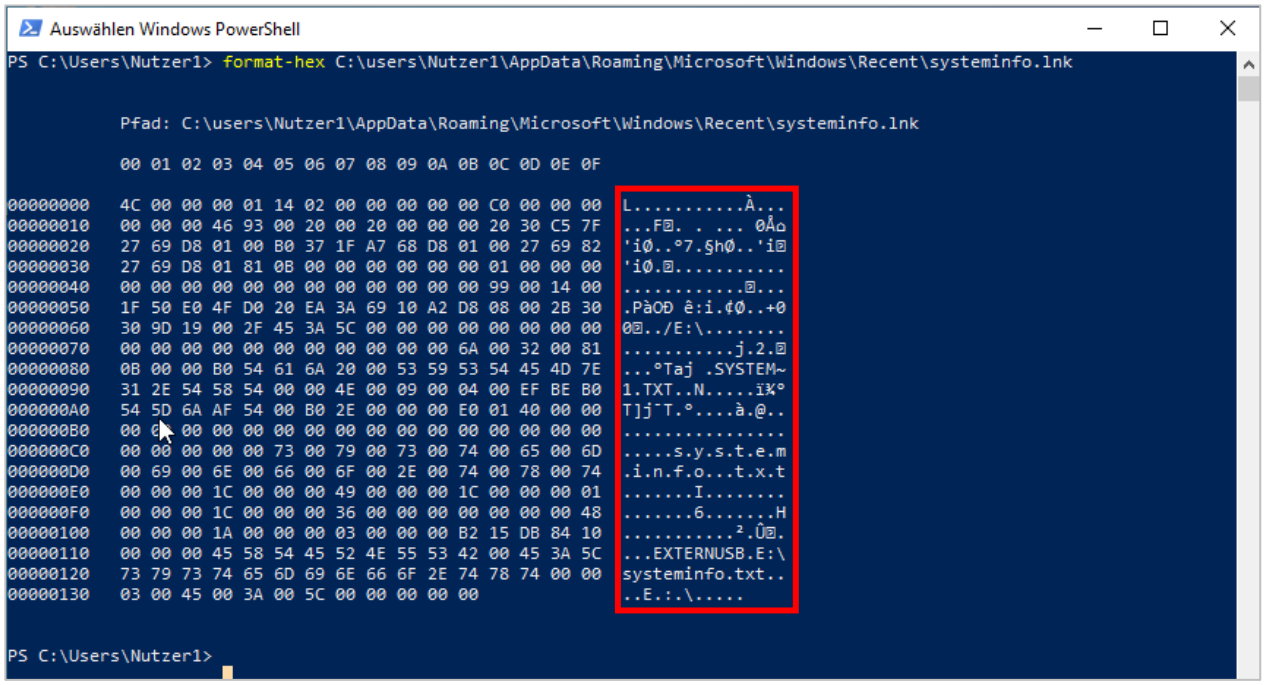


➢ Wechseln Sie danach mit dem **cd** Befehl in das Verzeichnis **C:\Users\Nutzer1\AppData\Roaming\Microsoft\ Windows\Recent**

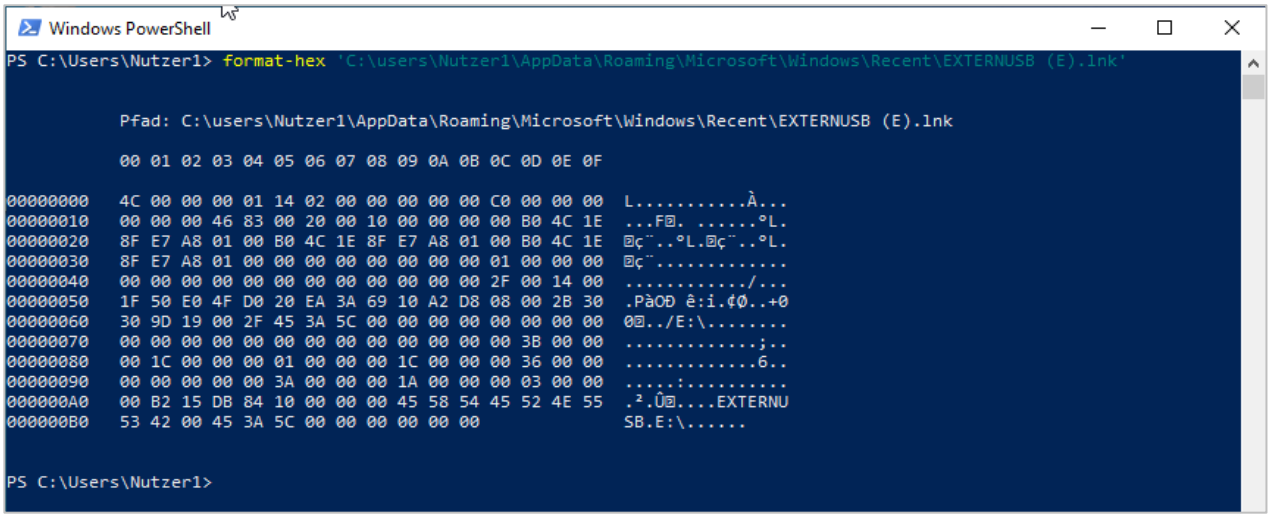
Schauen Sie sich mit dem Powershell Befehle **Format-Hex** den Inahlt der Datei **guy.lnk** an.



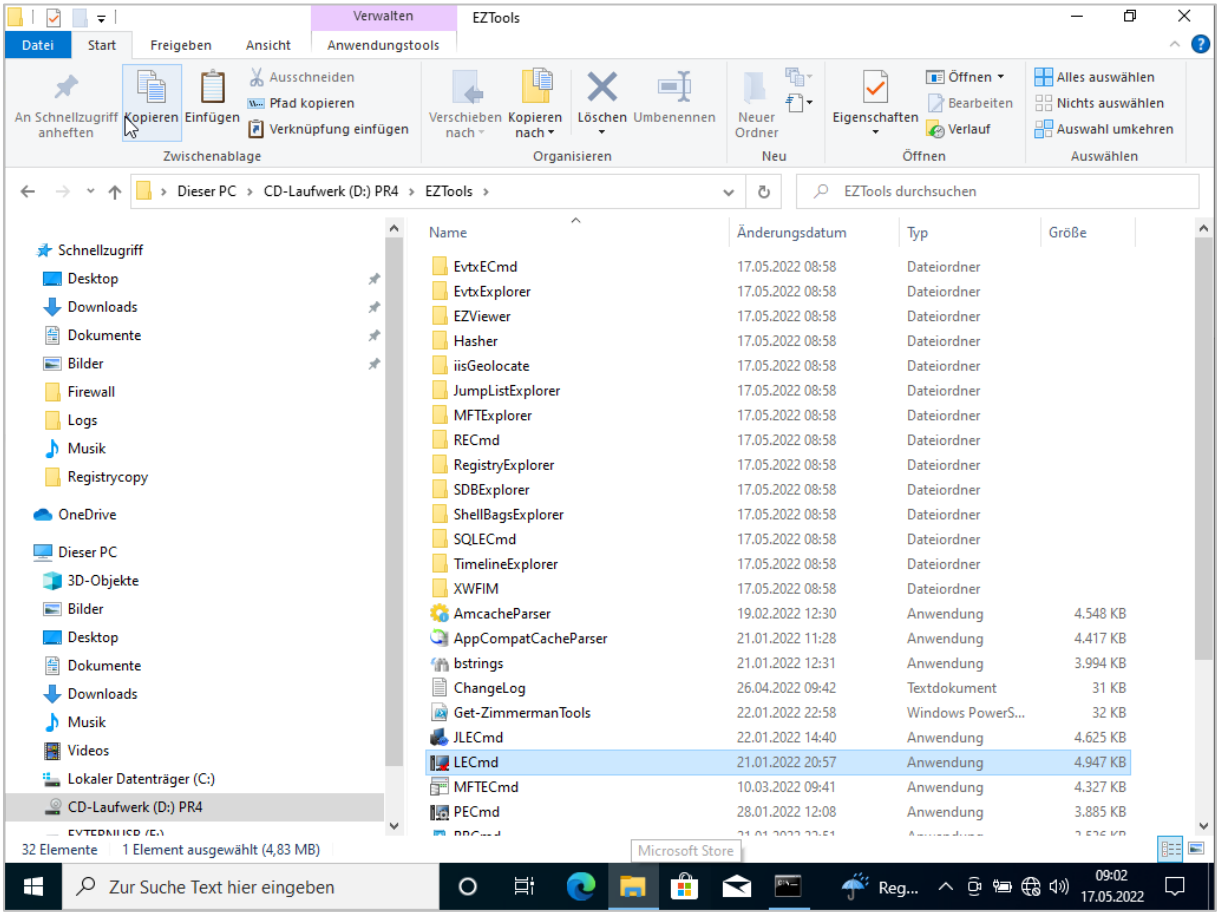
- Erkennen Sie von wo aus die Datei geöffnet wurde?
- Wiederholen Sie dies für die Datei **systeminfo.txt**



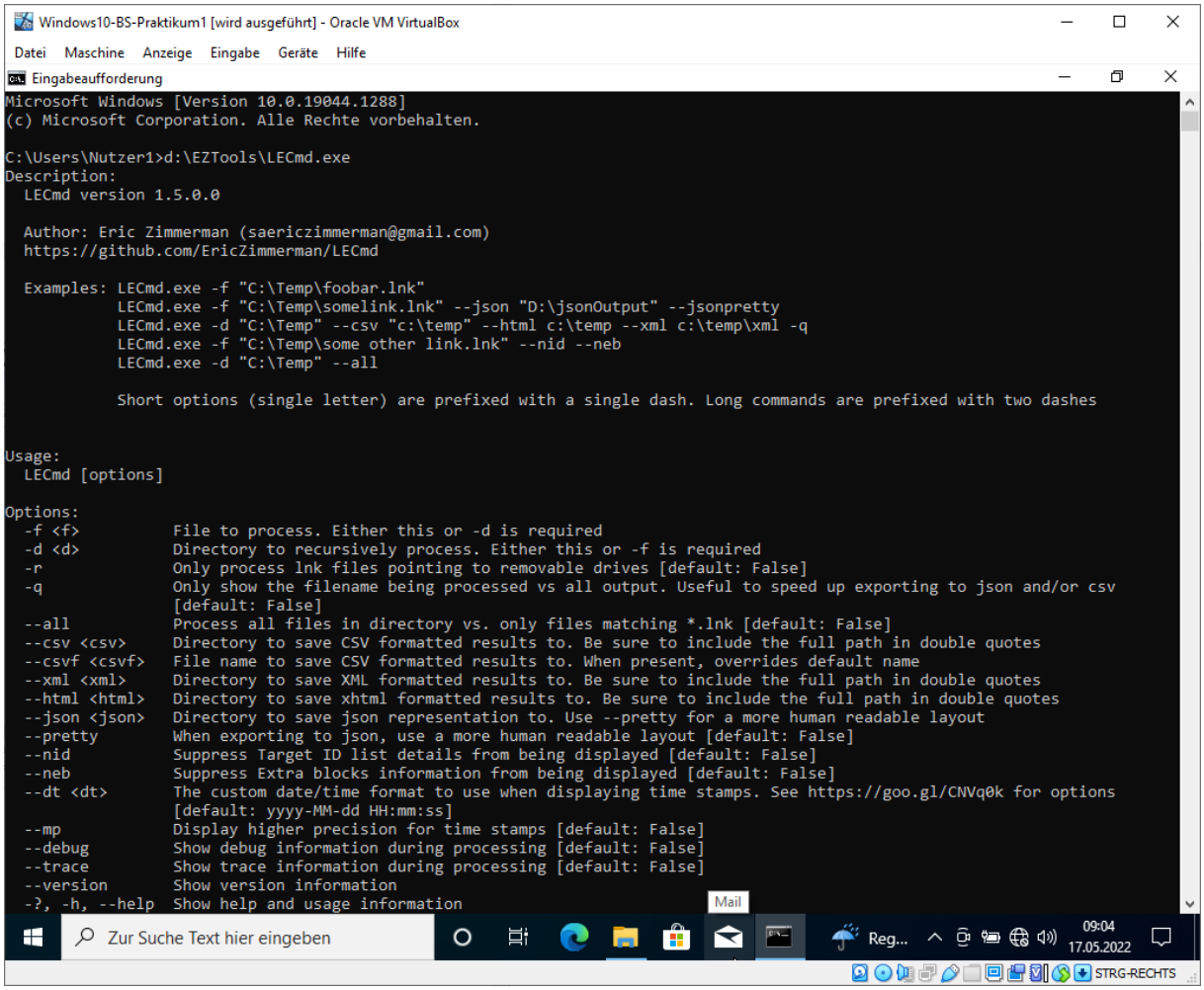
- Wiederholen Sie dies für die Datei **ExternUSB...lnk** (Nutzen Sie die Tab-Taste, um den Dateinamen auszuschreiben)



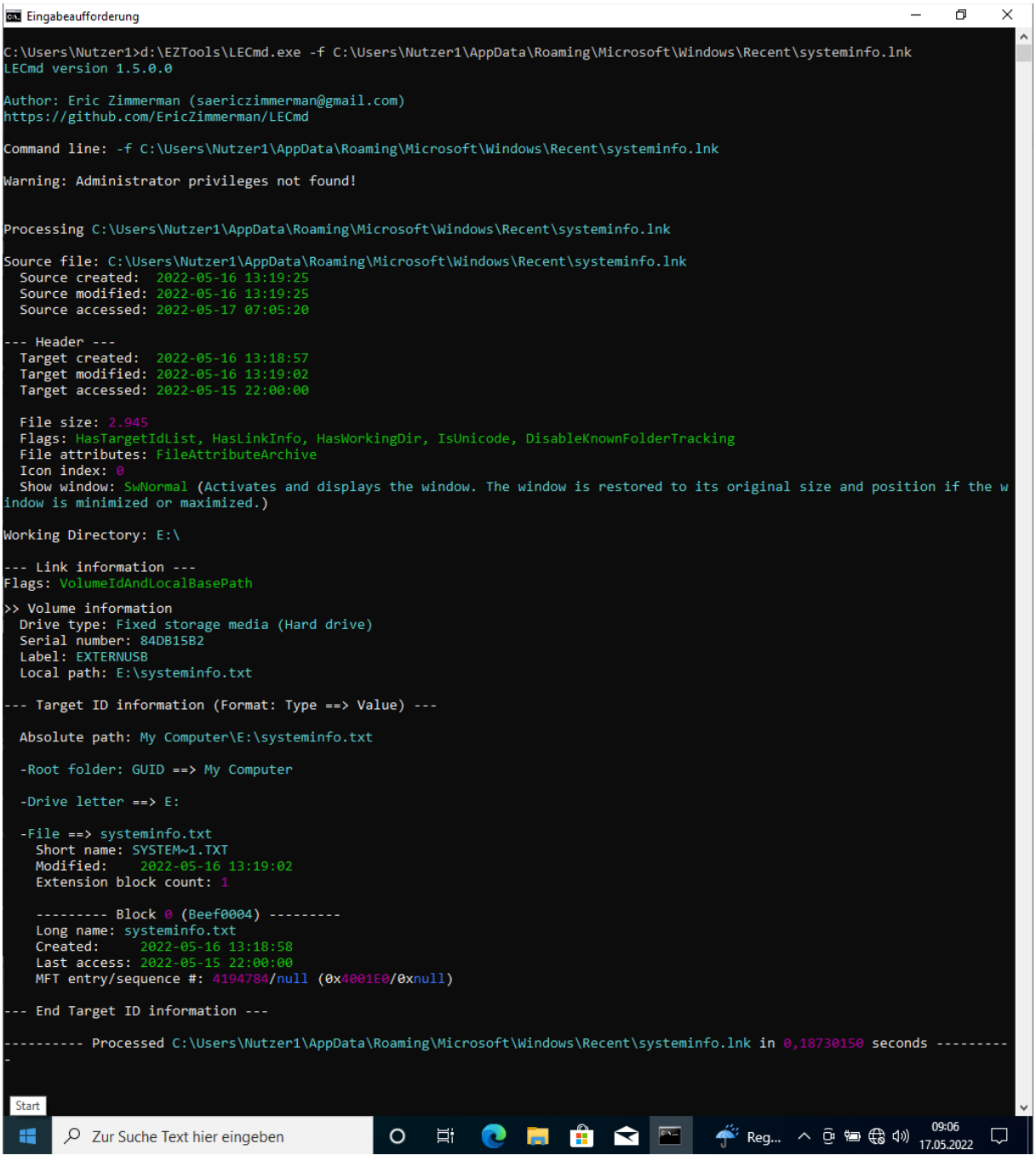
Wechseln Sie zum Windows Explorer und schauen Sie sich den Inhalt der CD im Verzeichnis **EZTools** an.



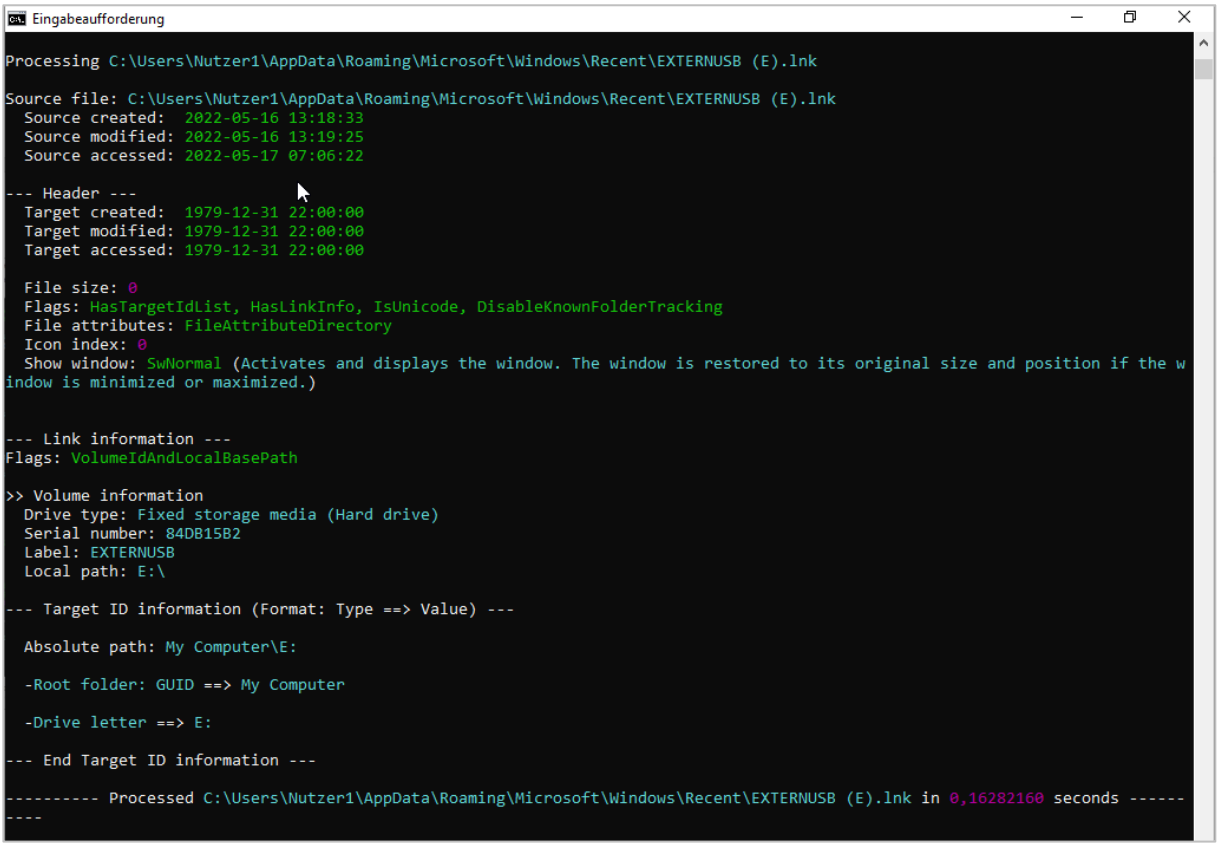
- Hier gibt es eine Anwendung LECmd.exe
- Führen Sie diese Datei vom CD-Laufwerk aus, indem Sie den Befehl in der Eingabeaufforderung (im Hintergrund oder neu Öffnen) auf dem Laufwerk der CD ausführen:
  - **`<LW-Buchstabe>:\EZTools\LECmd.exe`**



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



- **…:\EZTools\LECmd.exe –f „EXTERNUSB (…).lnk**

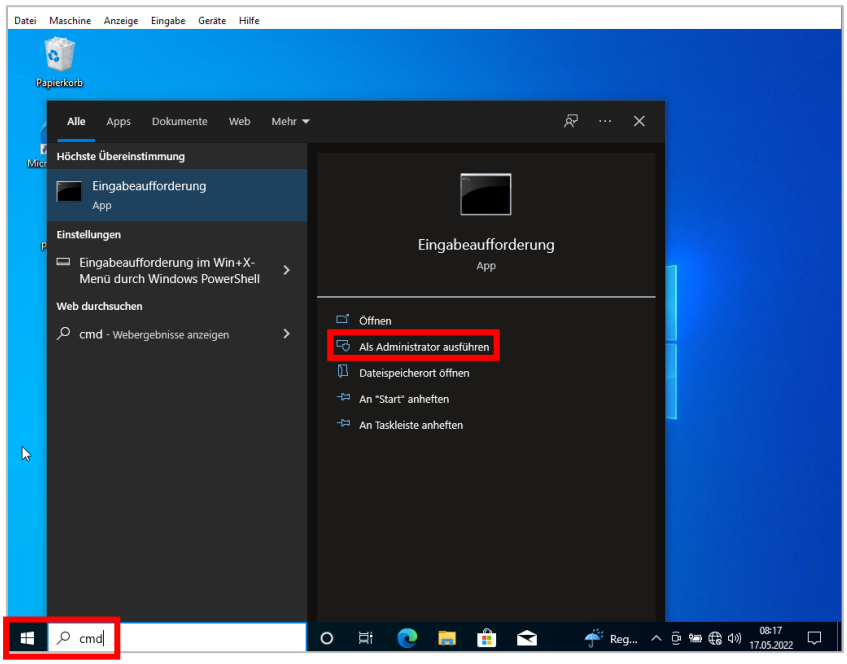


Volumenschattenkopien

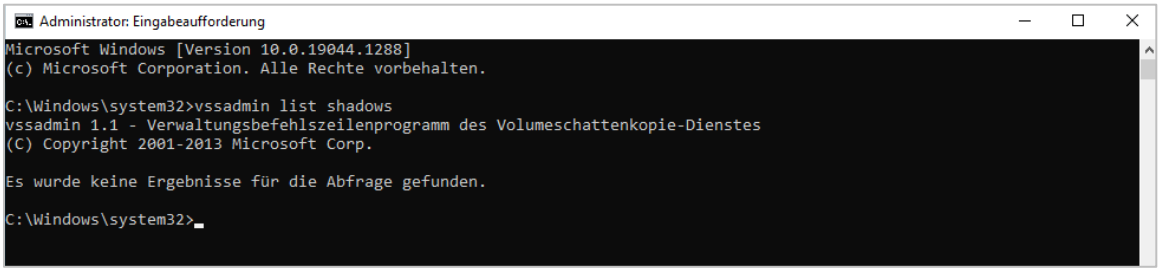
VSS anlegen

Schließen Sie alle offenen Fenster und Anwendungen.

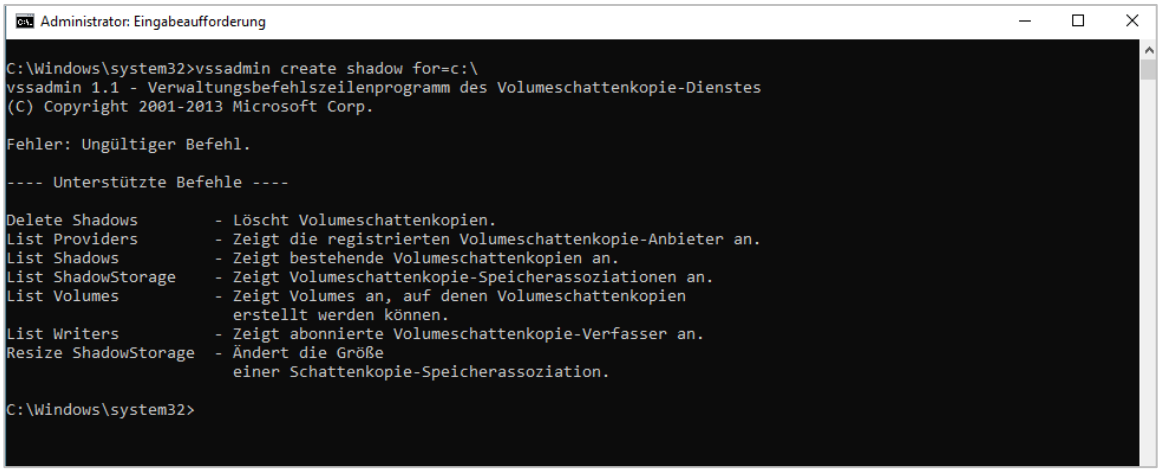
Starten Sie eine Eingabeaufforderung/Kommandozeile cmd als Administrator.



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



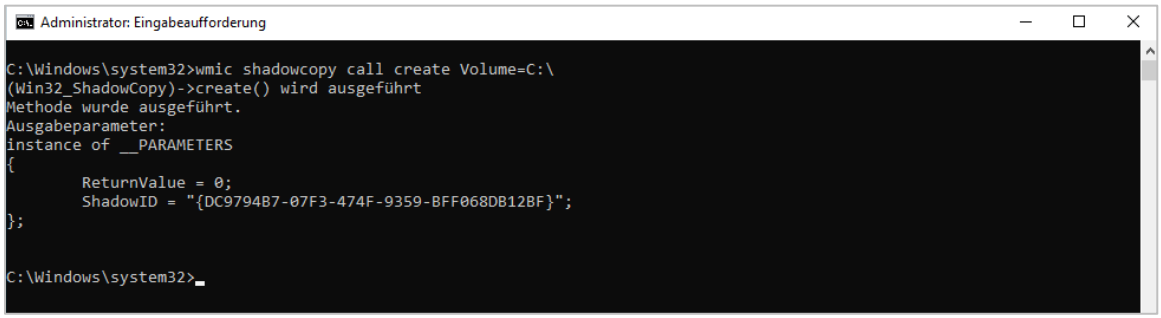
- Sind Schattenkopien vorhanden?
- Legen Sie eine neue Schattenkopie mit dem Befehl **vssadmin create shadow for=C:** an



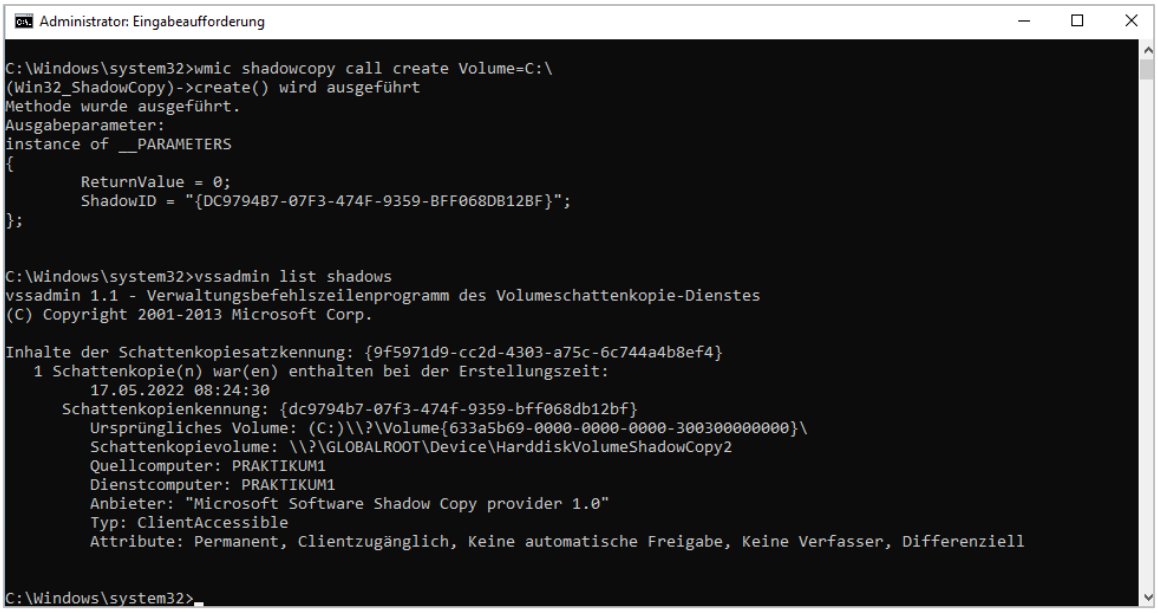
War dies erfolgreich? Recherchieren Sie, warum dies nicht erfolgreich ist.

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

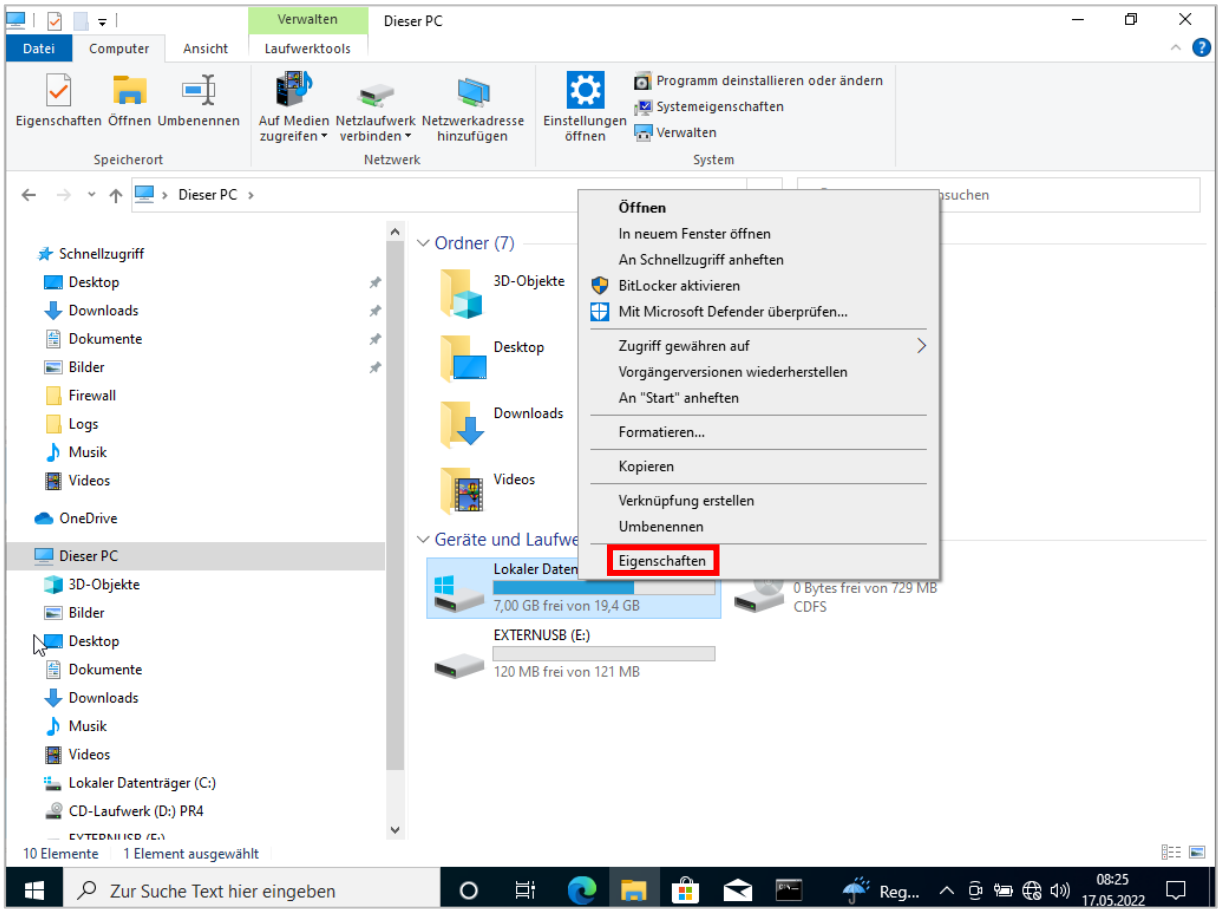
- Legen Sie stattdessen eine Schattenkopie mittels des Befehls **wmic shadowcopy call create Volume=C:** an

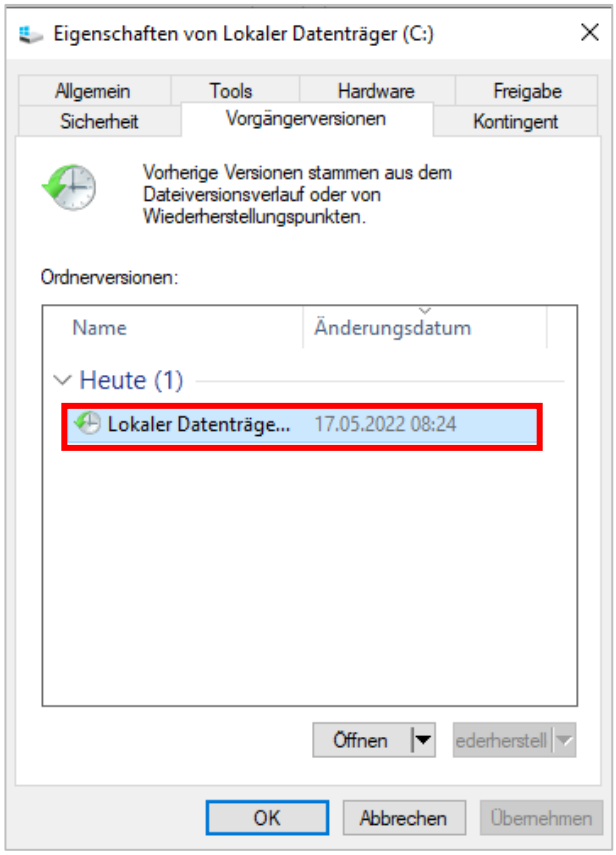


- Lassen Sie sich in der Eingabeaufforderung die Schattenkopien erneut anzeigen, mittels **vssadmin list shadows**

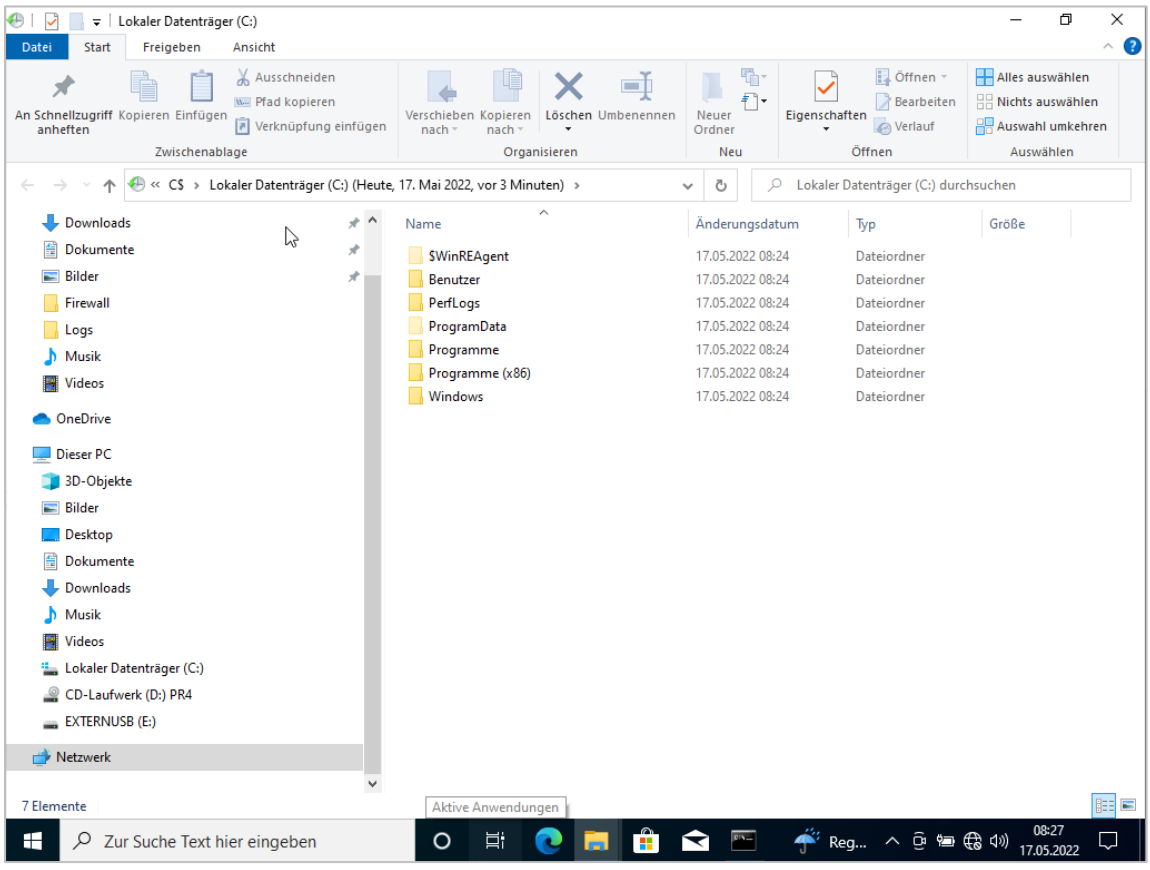


Prüfen Sie dies im Windows Explorer in dem Sie sich die Eigenschaften von Laufwerk C:\ anzeigen lassen.

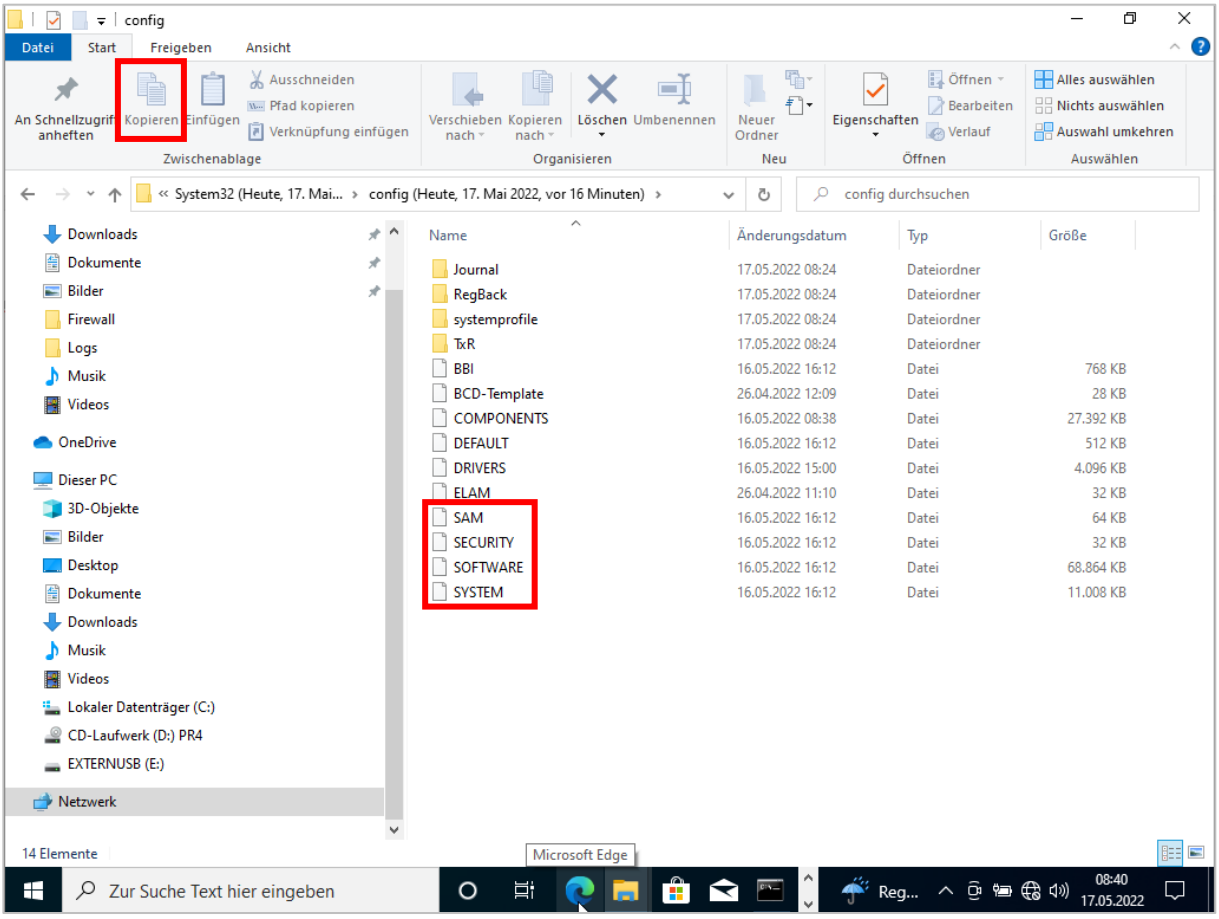




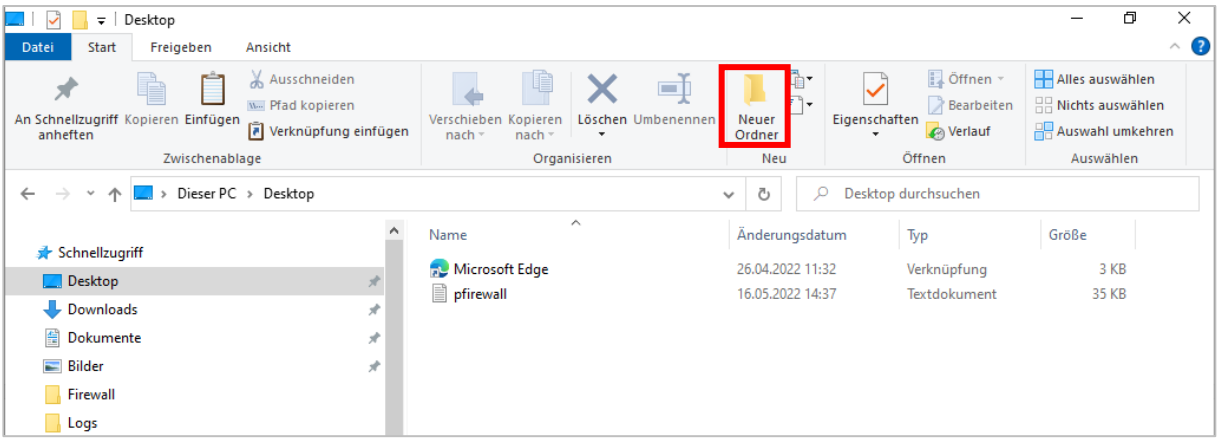
Öffnen Sie die Schattenkopie mit einem Doppelklick darauf.



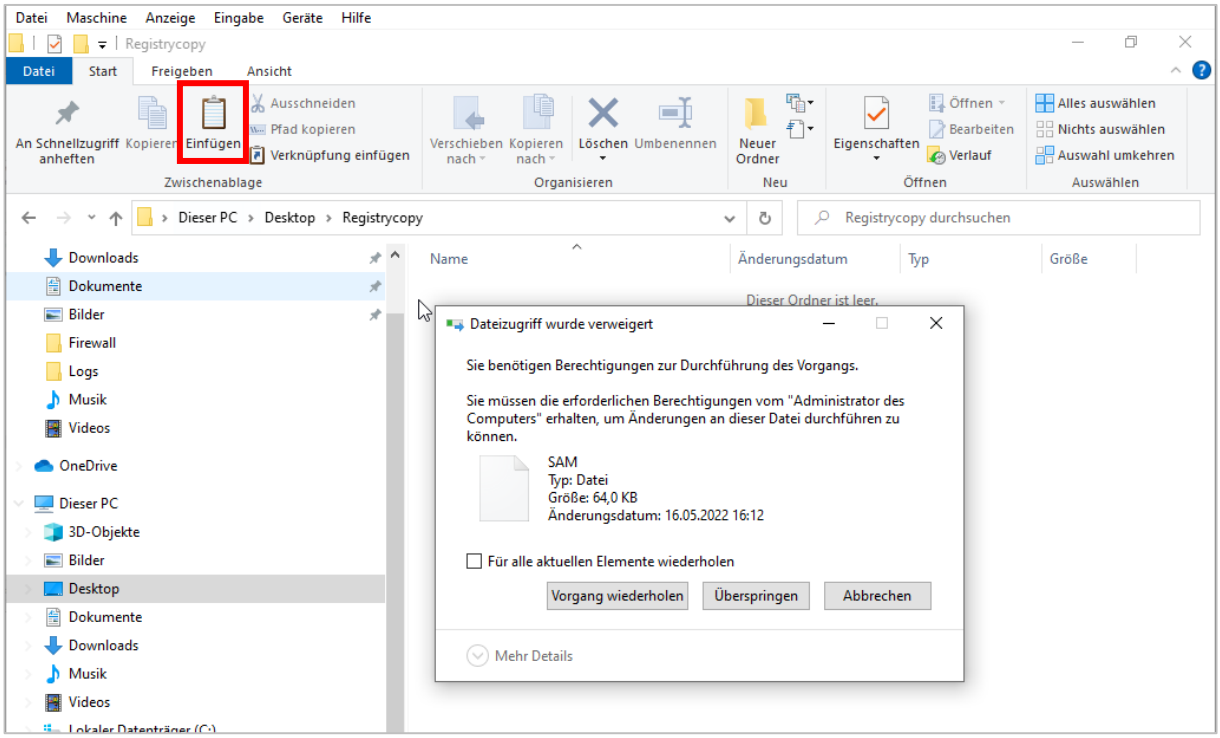
- Wechseln Sie in der Schattenkopie in das Verzeichnis **C$:\Windows\System32\Config**
- Wählen Sie hier die Dateien **SAM, SECURITY, SOFTWARE, SYSTEM** und kopieren Sie diese



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



- Fügen Sie die vorher kopierten Dateien ein

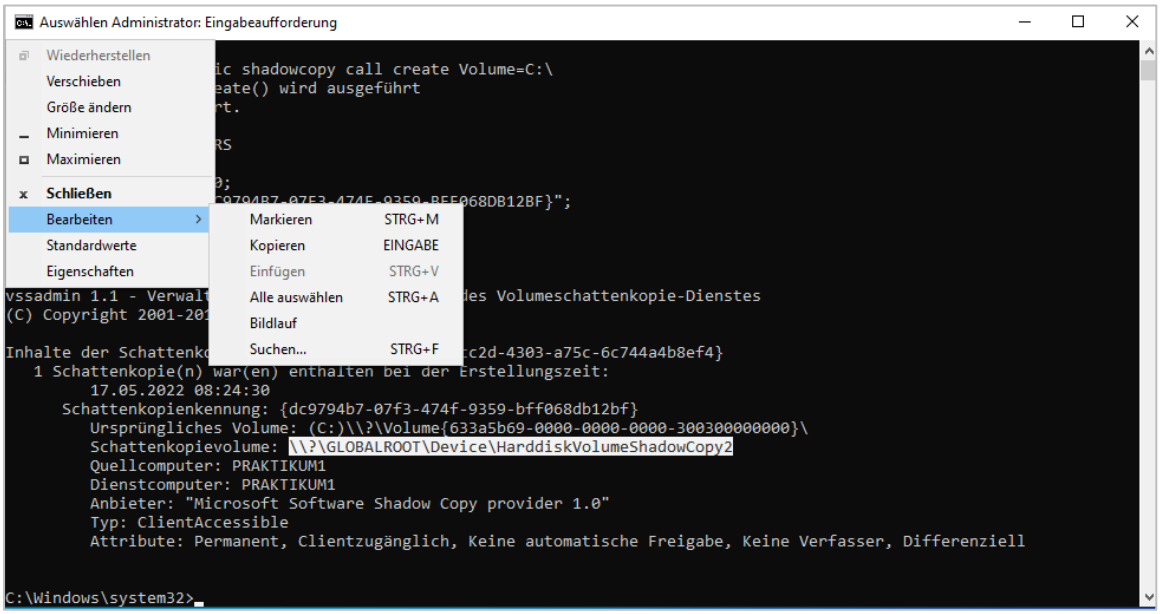


➢ Leider fehlen Ihnen dazu die Berechtigungen!

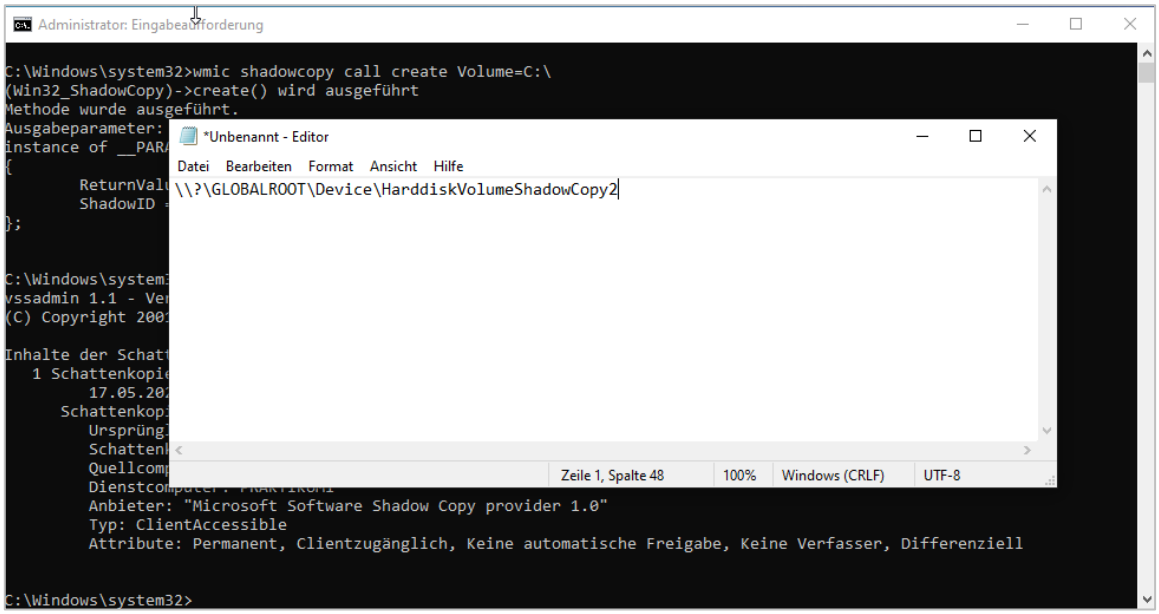
Auf Volumenschattenkopien zugreifen

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

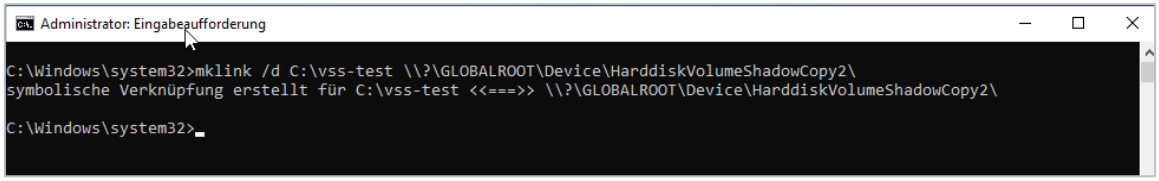
➢ Lassen Sie sich die Volumen Schattenkopien erneut anzeigen oder Nutzen Sie die Anzeige in der noch geöffneten Eingabeaufforderung
➢ Markieren Sie den Eintrag des Globalroot Harddisk Objektes der Schattenkopie (\\?\GLOBALROOT\Device\HarddiskVolumeSchadowCopy1)
➢ Kopieren Sie diesen Eintrag aus dem Fenster oder über STRG+C



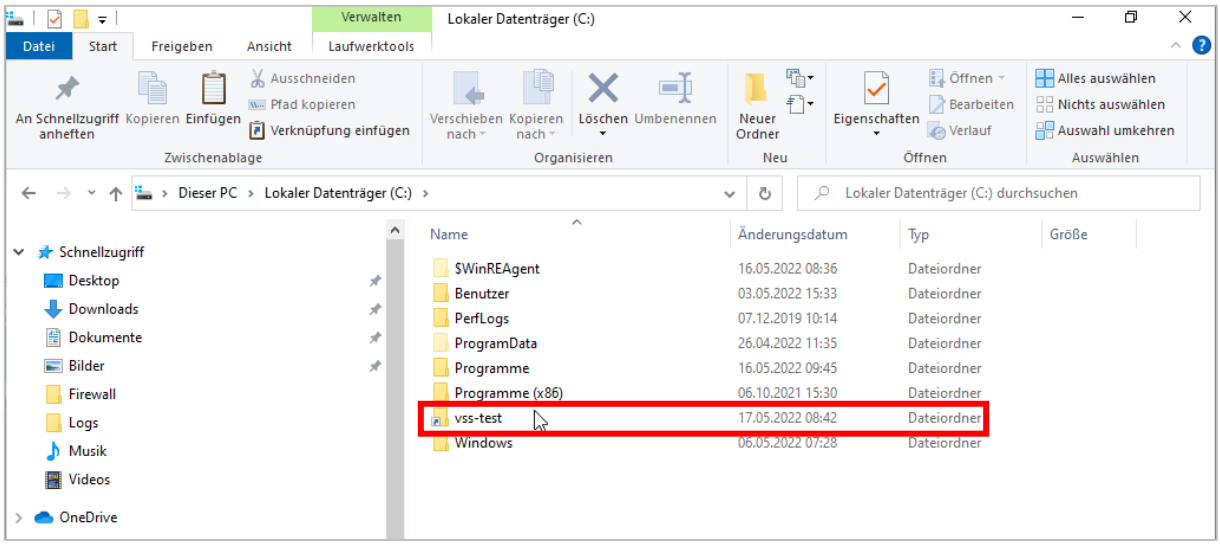
- Überprüfen Sie ob das Kopieren funktioniert über den Editor und fügen Sie in diesen den Globalroot Eintrag ein



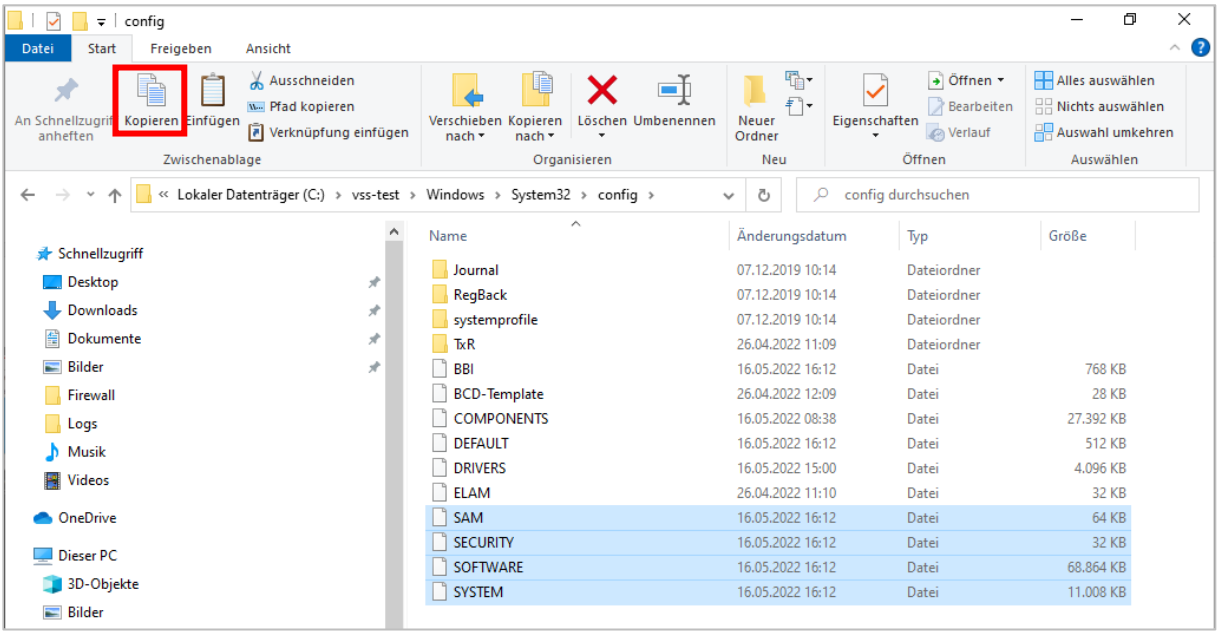
- Erstellen Sie einen Link Eintrag auf den Globalroot im Verzeichnis **C:\vss-test** mit dem Befehl **`mlink /d C:\vss-test globalroot <identifier>\`** (vergessen Sie den Backslash am Ende nicht!)



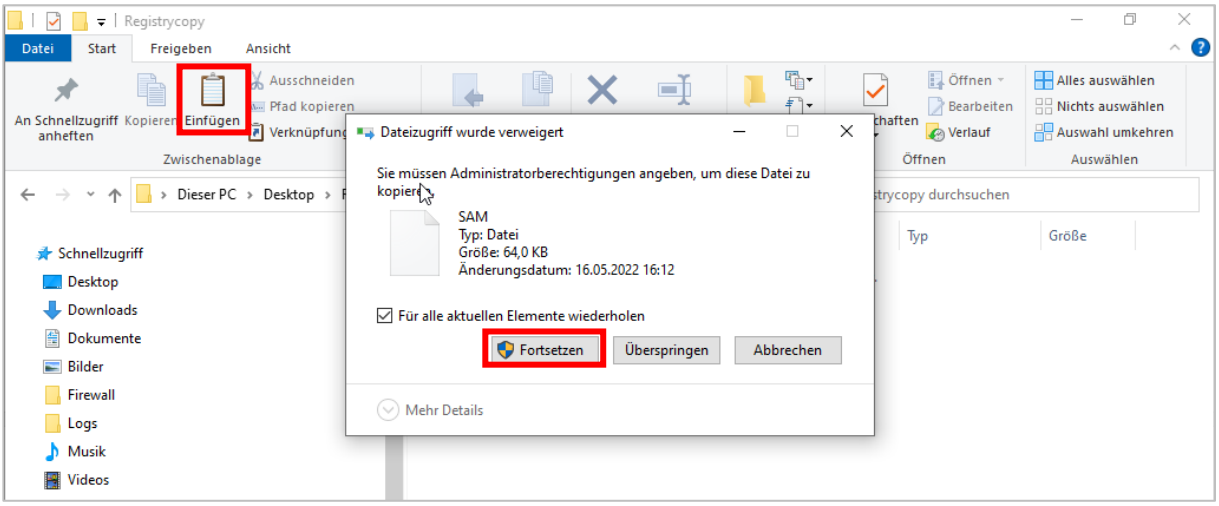
Öffnen Sie jetzt den **Windows Explorer** und navigieren Sie in das Verzeichnis **C:\vss-test**.



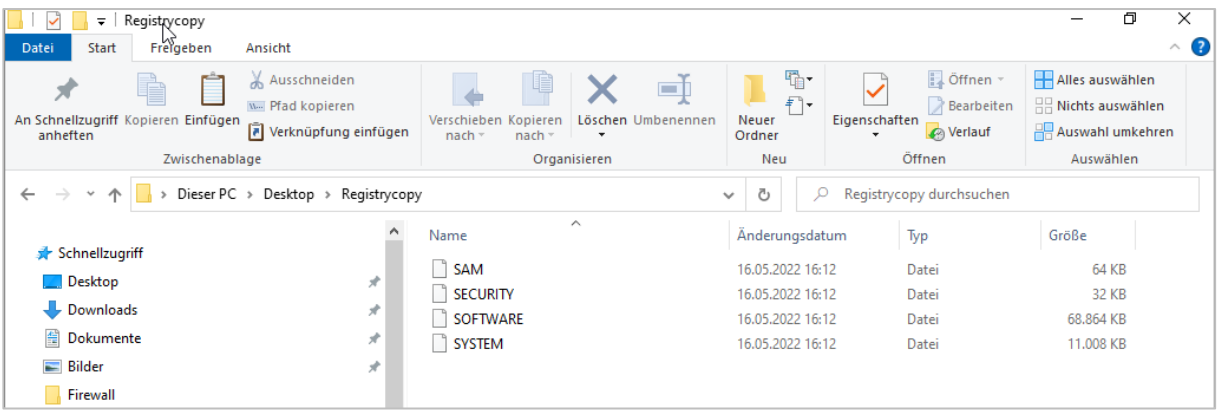
- Wechseln Sie in das Verzeichnis Wechseln Sie in der Schattenkopie in das Verzeichnis **C:\vss-test\Windows\System32\Config**
- Wählen Sie hier die Dateien **SAM, SECURITY, SOFTWARE, SYSTEM** und kopieren Sie diese



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

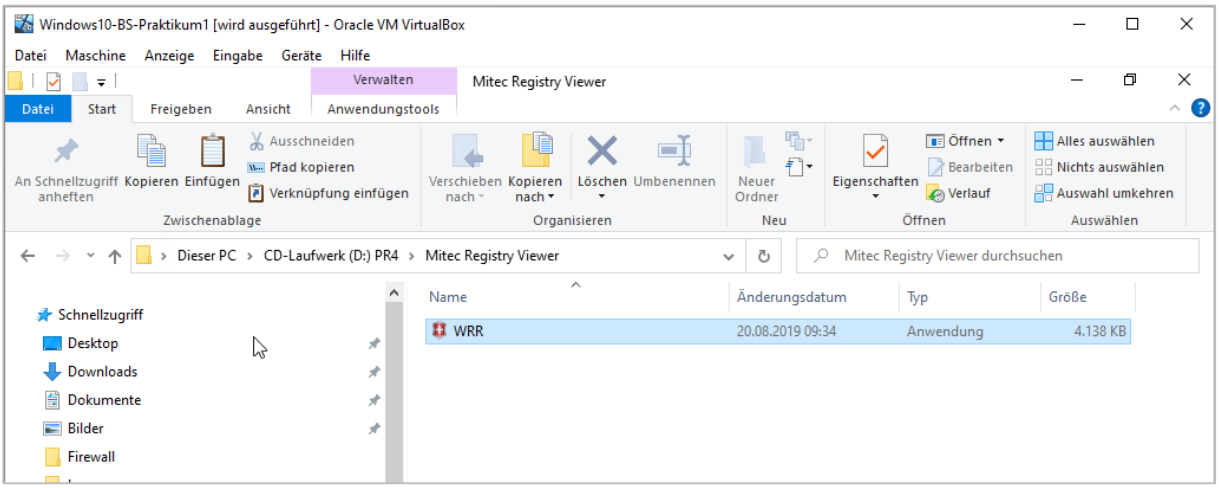


- Jetzt hat das Kopieren funktioniert

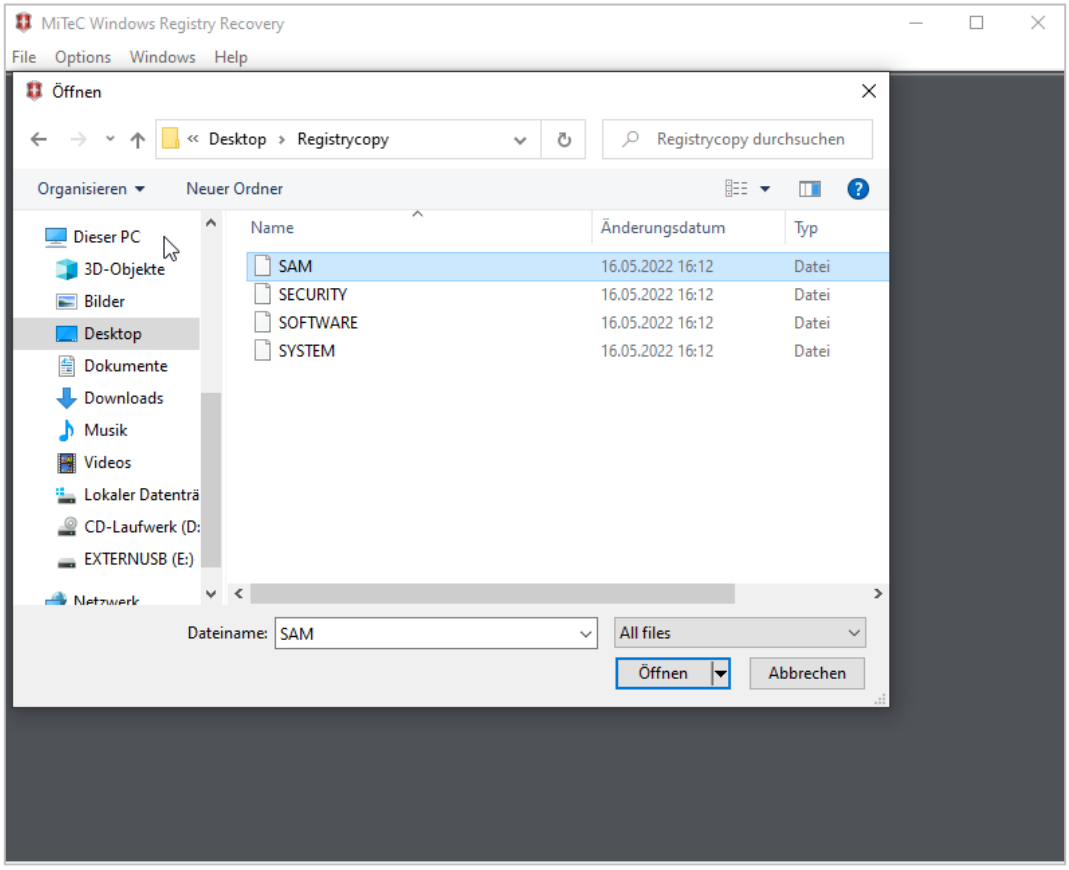


Registryinformationen der Schattenkopie lesen

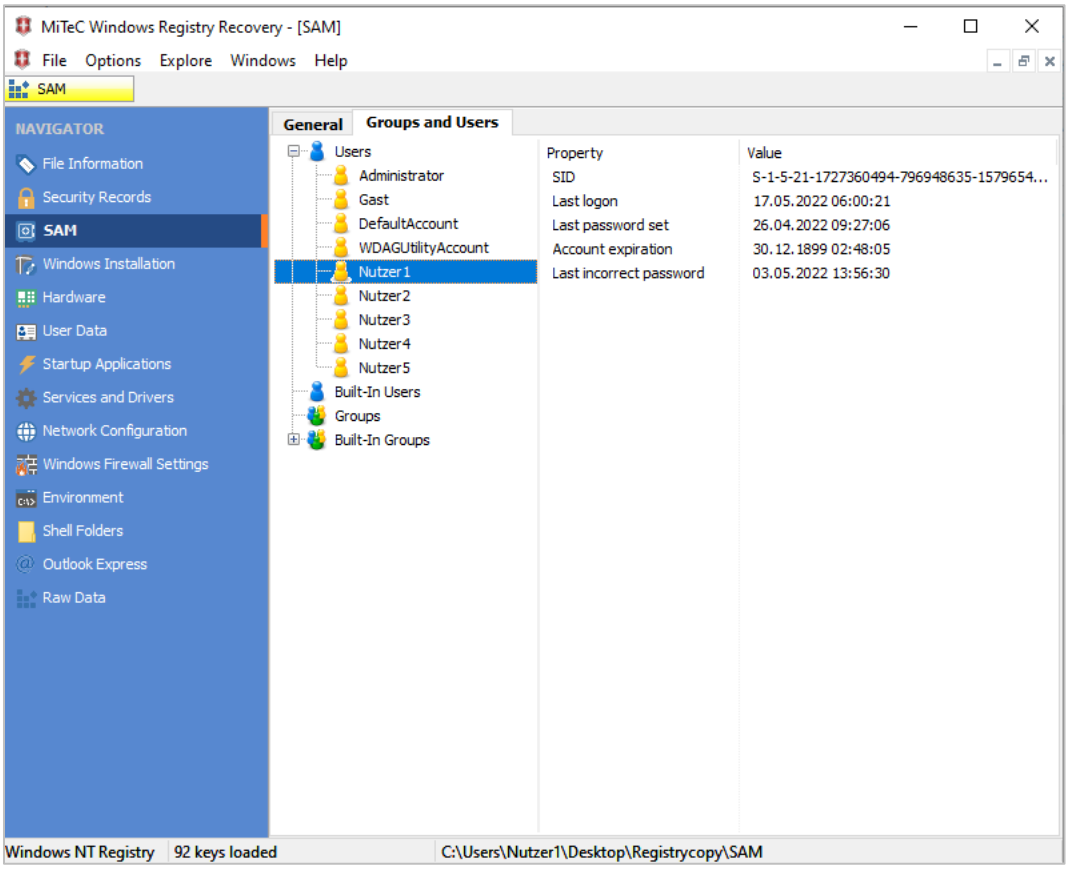
Wechseln Sie im Windows Explorer auf die CD und Starten Sie den **WRR** im Verzeichnis **Mitec Registry Recovery.**



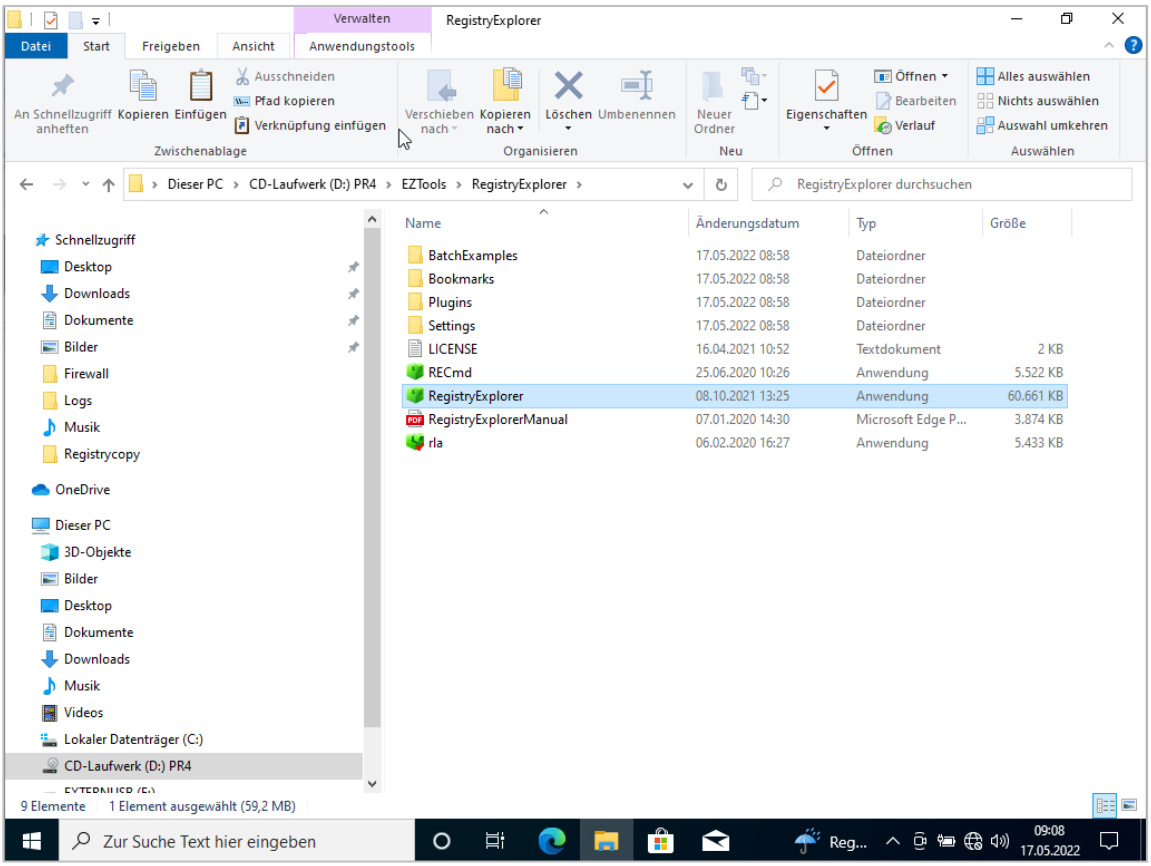
➢ Laden Sie den **SAM Hive** aus dem Verzeichnis **RegistryCopy**



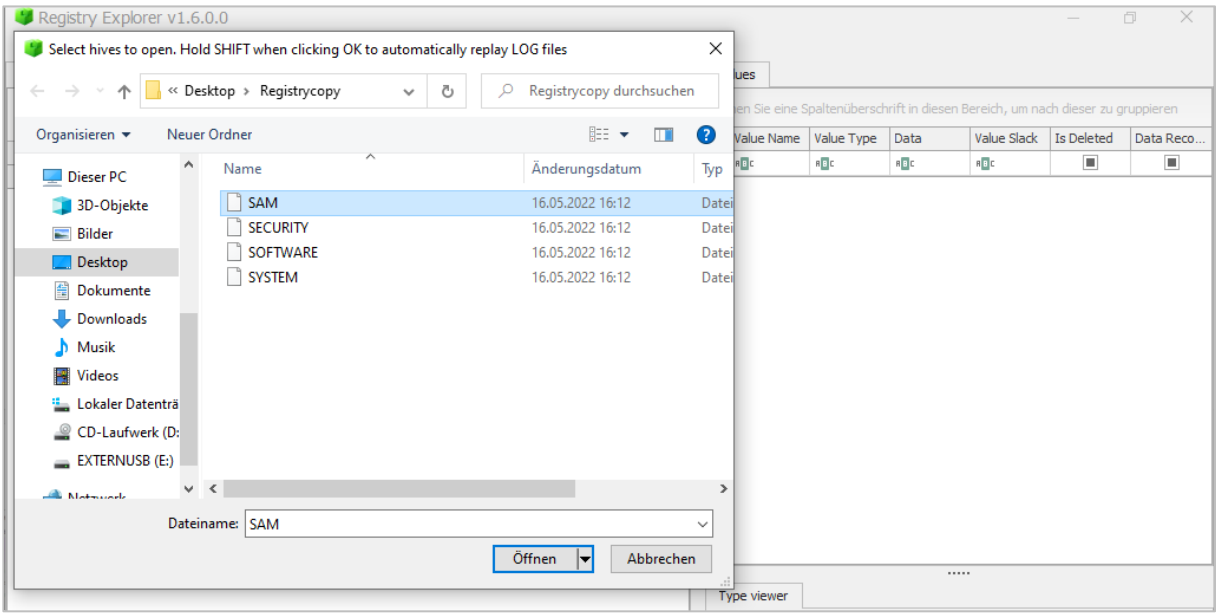
➢ Schauen Sie die Informationen das **SAM Hive** näher an



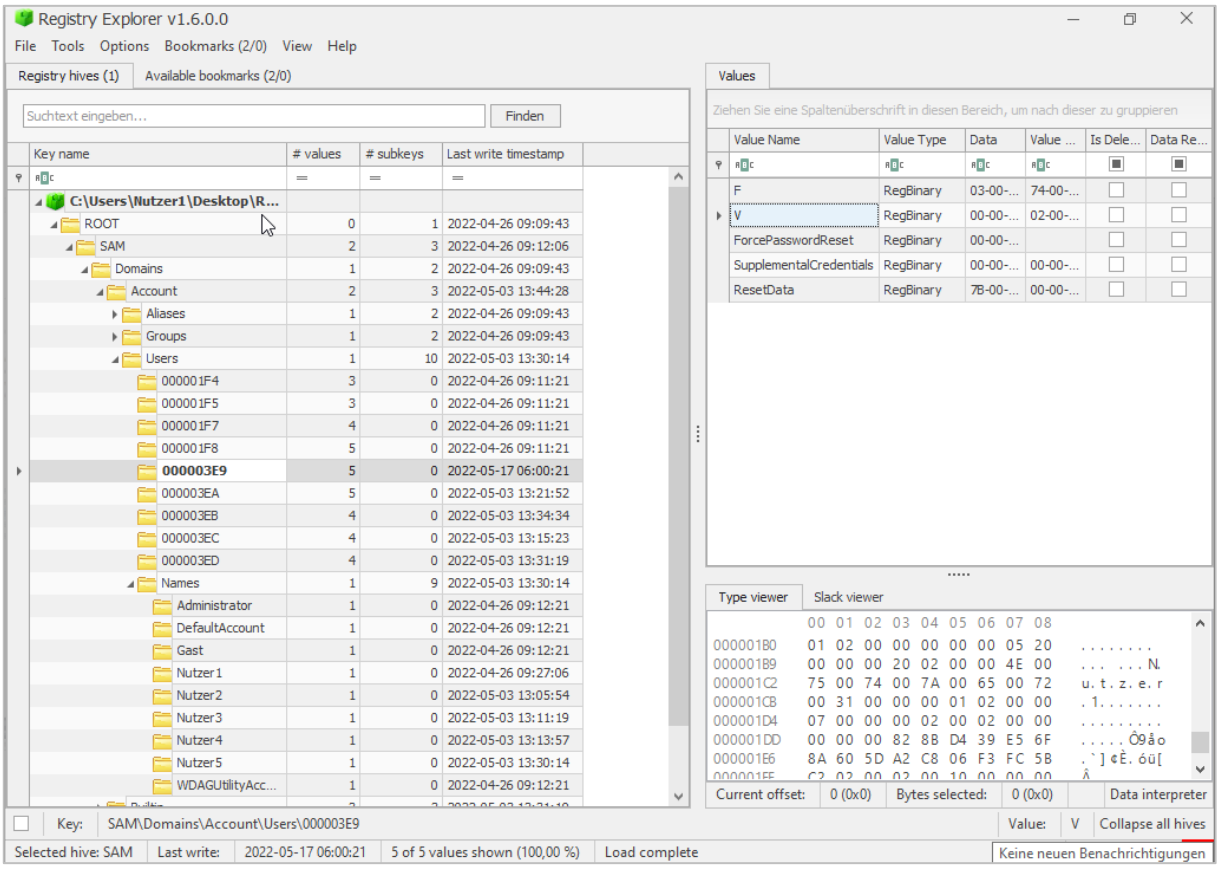
Wechseln Sie im Windows Explorer auf die CD und Starten Sie den **RegistryExplorer** im Verzeichnis **EZTools\RegistryExplorer.**



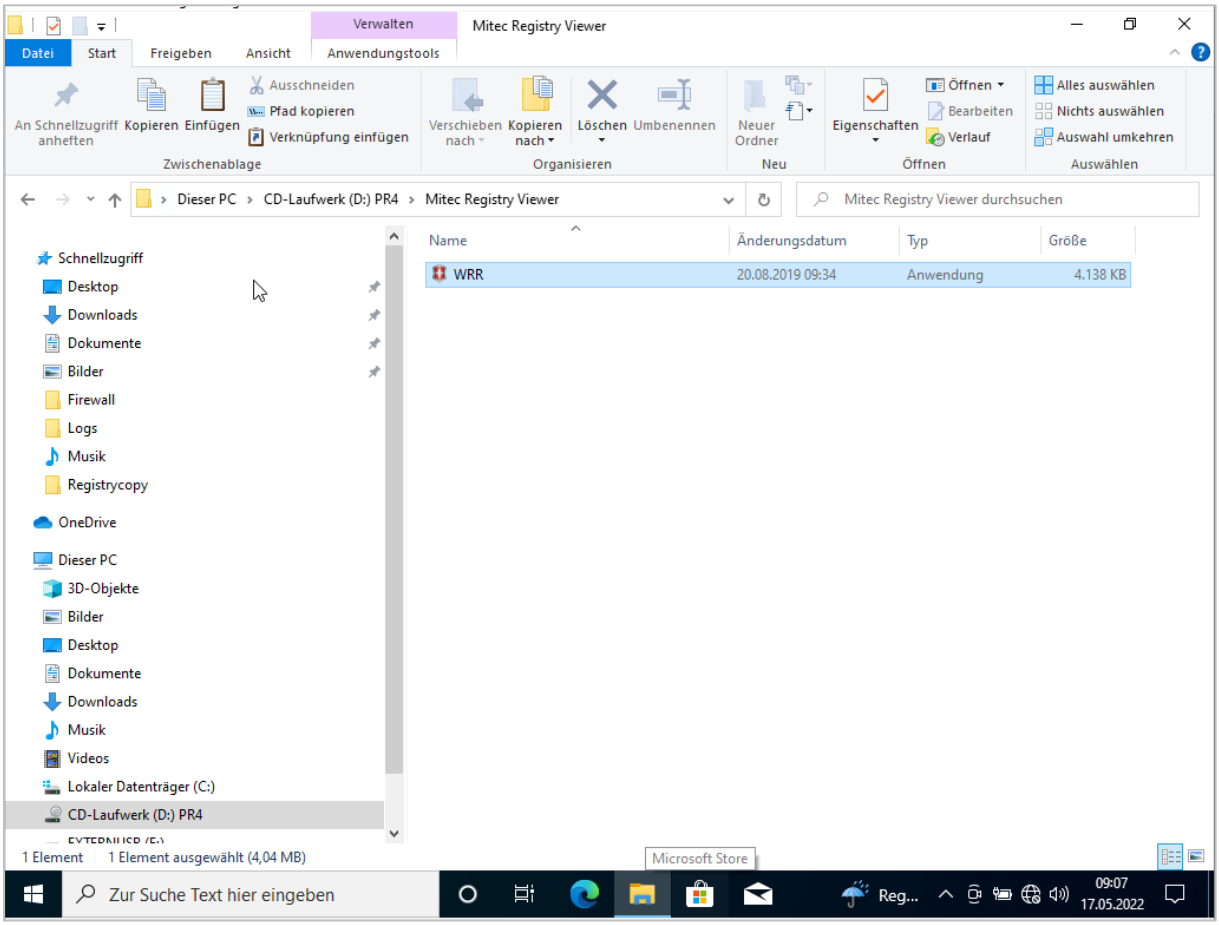
➢ Laden Sie den **SAM Hive** aus dem Verzeichnis **RegistryCopy**

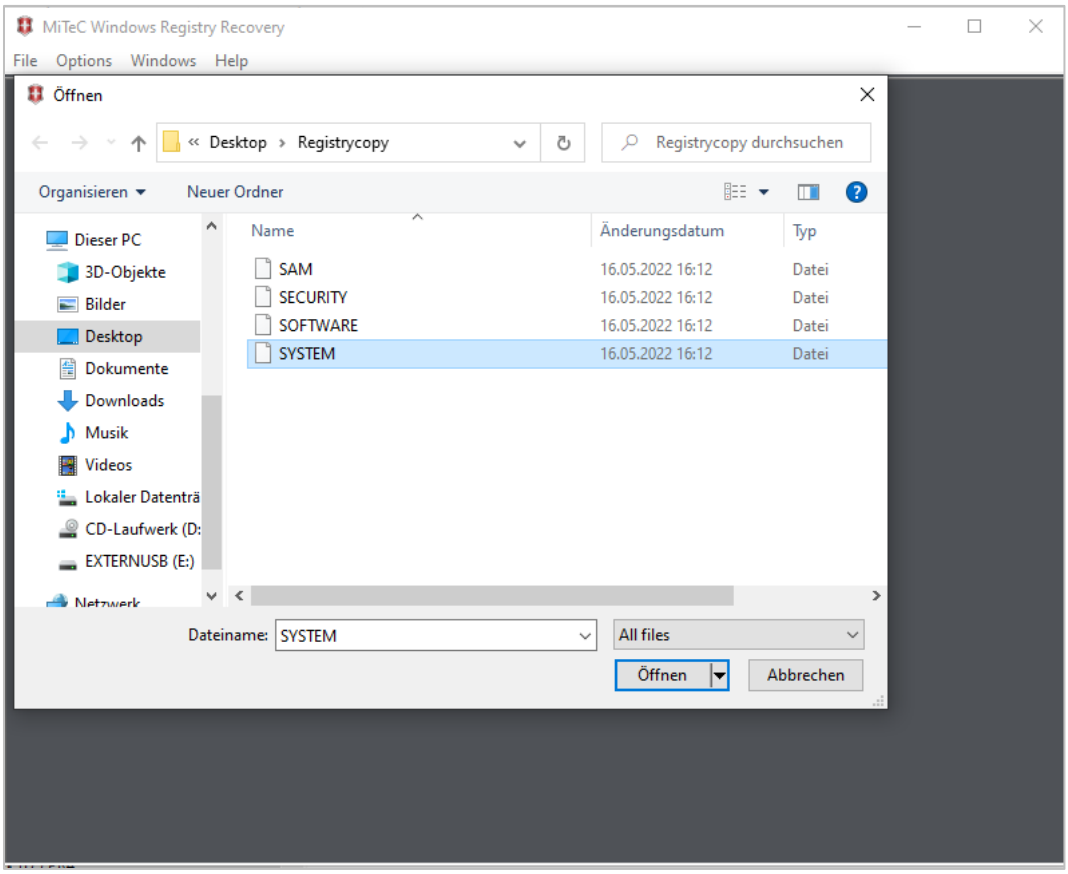


➢ Schauen Sie die Informationen das **SAM Hive** auch hier näher an.

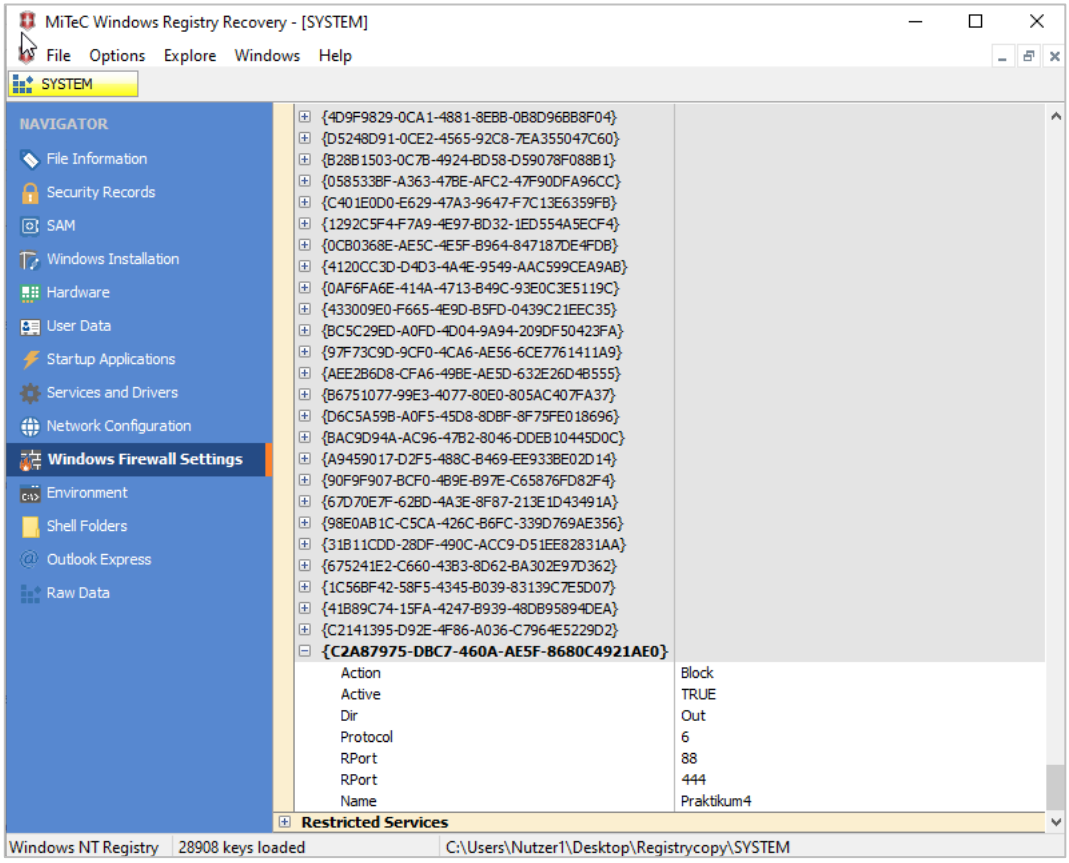


Untersuchen Sie den **SYSTEM Hive** mit dem **WRR** aus dem Verzeichnis **Mitec Registry Recovery** der CD.


Mitec Registry Viewer
Verwalten
Datei
Start
Freigeben
Ansicht
Anwendungstools
Ausschneiden
Pfad kopieren
Verknüpfung einfügen
An Schnellzugriff anheften
Kopieren
Einfügen
Zwischenablage
Verschieben nach
Kopieren nach
Löschen
Umbenennen
Organisieren
Neuer Ordner
Neu
Eigenschaften
Öffnen
Bearbeiten
Verlauf
Öffnen
Alles auswählen
Nichts auswählen
Auswahl umkehren
Auswählen
Dieser PC › CD-Laufwerk (D:) PR4 › Mitec Registry Viewer
Mitec Registry Viewer durchsuchen
Schnellzugriff
Desktop
Downloads
Dokumente
Bilder
Firewall
Logs
Musik
Registrycopy
OneDrive
Dieser PC
3D-Objekte
Bilder
Desktop
Dokumente
Downloads
Musik
Videos
Lokaler Datenträger (C:)
CD-Laufwerk (D:) PR4
Name
Änderungsdatum
Typ
Größe
WRR
20.08.2019 09:34
Anwendung
4.138 KB
1 Element
1 Element ausgewählt (4,04 MB)
Microsoft Store
Zur Suche Text hier eingeben
Reg...
09:07
17.05.2022


MiTeC Windows Registry Recovery
File
Options
Windows
Help
Öffnen
« Desktop › Registrycopy
Registrycopy durchsuchen
Organisieren
Neuer Ordner
Dieser PC
3D-Objekte
Bilder
Desktop
Dokumente
Downloads
Musik
Videos
Lokaler Datenträ
CD-Laufwerk (D:
EXTERNUSB (E:)
Netzwerk
Name
Änderungsdatum
Typ
SAM
16.05.2022 16:12
Datei
SECURITY
16.05.2022 16:12
Datei
SOFTWARE
16.05.2022 16:12
Datei
SYSTEM
16.05.2022 16:12
Datei
Dateiname:
SYSTEM
All files
Öffnen
Abbrechen

➢ 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**.