Studienprogramm Sachbearbeiter:in Digitale Forensik
Praktikum Blockwoche macOS
Dozenten: Prof. Bodach | Wetterau B.Sc. | Hossfeld B.Sc.
Stand: 10.07.2023

HOCHSCHULE MITTWEIDA
University of Applied Sciences

Betriebssysteme

Praktikum macOS

Inhaltsverzeichnis

1. AUFGABENSTELLUNG VORBEREITUNG

In diesem Praktikum lernen Sie die Einrichtung einer macOS VM kennen. Die Einrichtung dieses Betriebssystems ist durch verschiedene Kniffe nicht trivial und erfordert einige Umwege und besondere Maßnahmen. Zusätzlich sollen Sie erste Schritte in dem Betriebssystem machen und dessen Oberfläche kennenlernen. Auch in diesem Praktikum verwenden wir die Virtualisierungssoftware Oracle VirtualBox, welche Sie schon aus den vorigen Praktika kennen sollten.

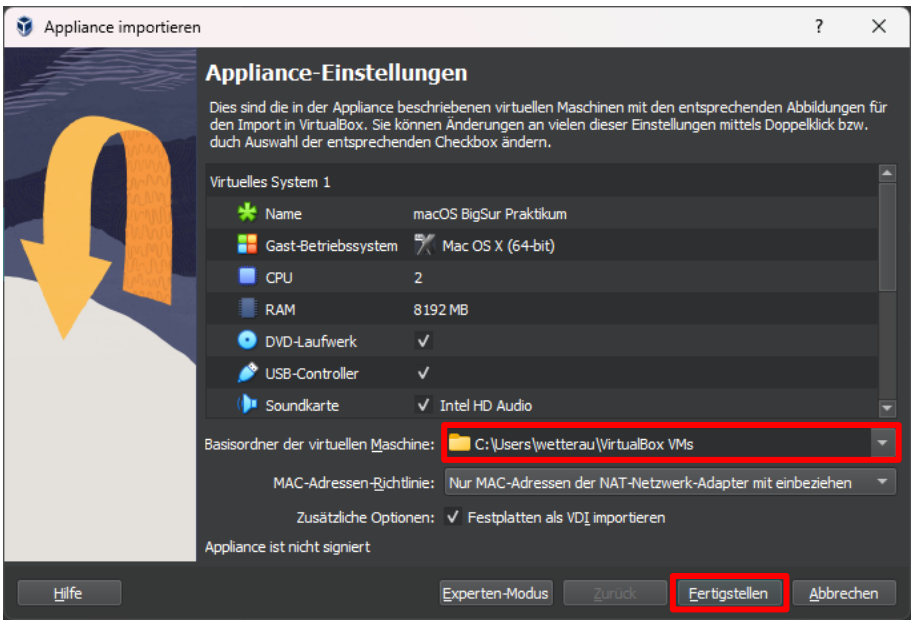
Zur Durchführung des Praktikums nutzen wir das auf den PCs der HSMW installierte Betriebssystem Windows. Weiterhin benötigen wir einige Dateien, welche Ihnen im Laufwerk R: unter folgendem Pfad zur Verfügung stehen:

`R:\CB\Bodach\BKA Studiengang\Betriebssysteme\Praktikum Blockwochen\macOS\`

*Laden Sie sich aus diesem Verzeichnis für dieses Praktikum die Dateien „***`macOS BigSur Praktikum Installiert.ova`***“ und „***`macOS BigSur Praktikum\macOS BigSur Praktikum.nvram`***“ herunter und speichern Sie diese Dateien an einen geeigneten Ort auf Ihrem lokalen System.* (An den PC der HSMW optimalerweise unter D:\)

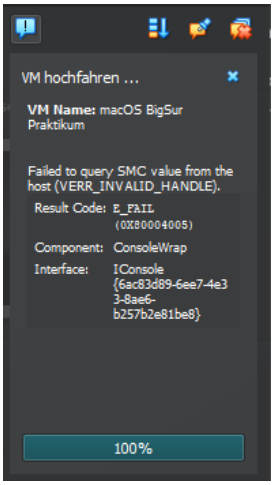
Importieren der OVA-Datei

Nachdem Sie alle Dateien heruntergeladen haben, starten Sie die vorbereitete virtuelle Maschine mit einem Doppelklick auf die OVA-Datei. Daraufhin öffnet sich VirtualBox und fragt nach der Importierung der virtuellen Maschine. Stellen Sie bitte den Basisordner der Datei unten auf einen von Ihnen gewählten Ordner auf Laufwerk



D: um und bestätigen Sie den Dialog mit dem Button „Fertigstellen“.

Danach wird Ihnen die VM importiert, wie Sie es bereits kennen. Sollten Sie nun versuchen die VM ohne Weiteres zu starten, werden Sie höchstwahrscheinlich einen Fehler in VirtualBox bekommen:



Sollte das bei Ihnen nicht der Fall sein, dann haben Sie Glück und können mit dem Kennenlernen der Oberfläche fortfahren. Ansonsten gehen Sie das Praktikum weiter durch und versuchen die Fehler, wie beschrieben zu behandeln. Ein weiterer Fehler kann sein, dass die im EFI-Menü gefangen sind. Dann gehen Sie auch weiter.

Zusätzliche Maßnahmen vornehmen (Fehlerbehandlung)

Damit das Gastbetriebssystem reibungslos auf den Hostsystem laufen kann, müssen noch einige Einstellungen getätigt werden, wenn dies bis hierher nicht der Fall ist. Dazu starten Sie bitte mit einem Rechtsklick auf den Windowsstartbutton eine neue PowerShell (Terminal unter Windows 11). Anschließend geben Sie bitte den folgenden Befehl in die die Befehlszeile ein:

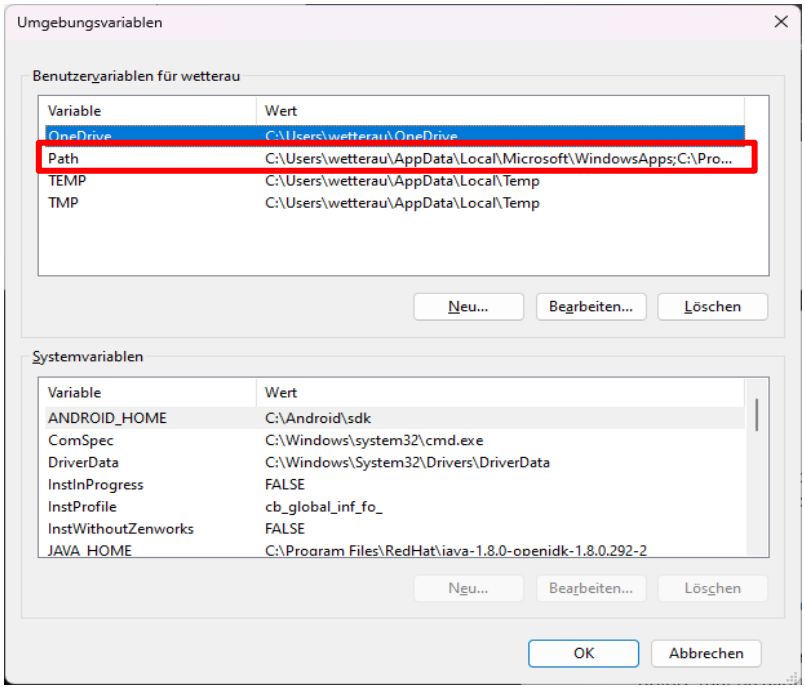
```
$ VBoxManage setextradata "macOS BigSur Praktikum"
   "VBoxInternal/Devices/smc/0/Config/GetKeyFromRealSMC" 0
```

Sollte dieser Befehl bei Ihnen einen Fehler erzeugen, dass der Befehl VBoxManage nicht als Cmdlet registriert ist, fahren Sie bitte mit dem Hinzufügen von VirtualBox zu den Umgebungsvariablen fort (nächtes Kapitel).

Sollten Sie im EFI Bios gefangen sein und macOS nicht starten, so kopieren Sie anschließend die *.nvram-Datei in das Verzeichnis, in dem Sie die VM abgelegt haben, dann sollte dieser Fehler behoben sein.

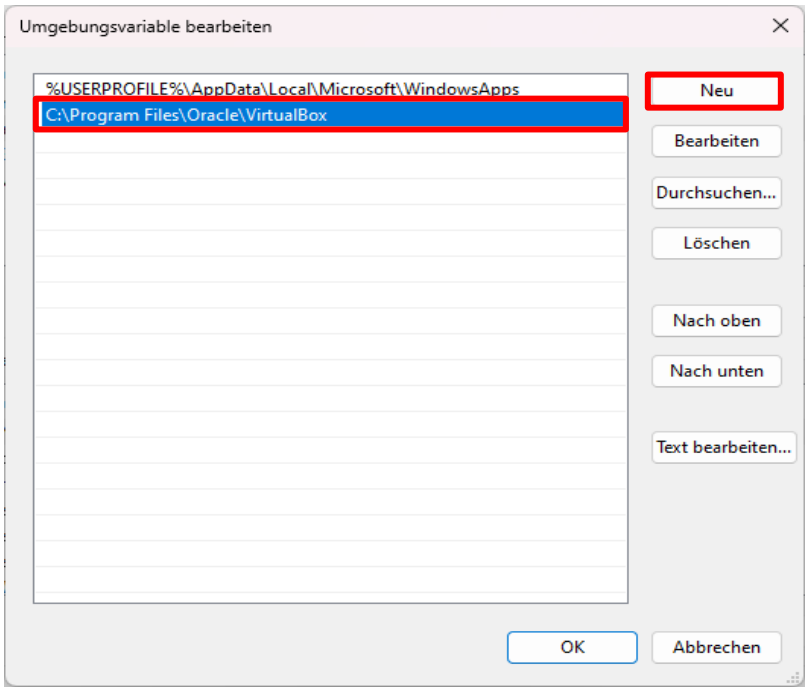
VirtualBox-Pfad zu den Umgebungsvariablen hinzufügen (Optional)

Sollte bei Ihnen der Befehl mit VBoxManage nicht funktionieren, kann eine Abhilfe geschaffen werden, indem Sie den Pfad zu der ausführbaren Datei in die Systemvariable PATH einfügen. Dazu drücken Sie bitte den Windows-



Button und geben den Begriff Umgebungsvariablen ein und wählen den Ergebniseintrag „Umgebungsvariablen für dieses Konto bearbeiten“ aus. Im Folgenden sich öffnenden Fenster klicken Sie bitte doppelt auf die Variable PATH im oberen Fenster.

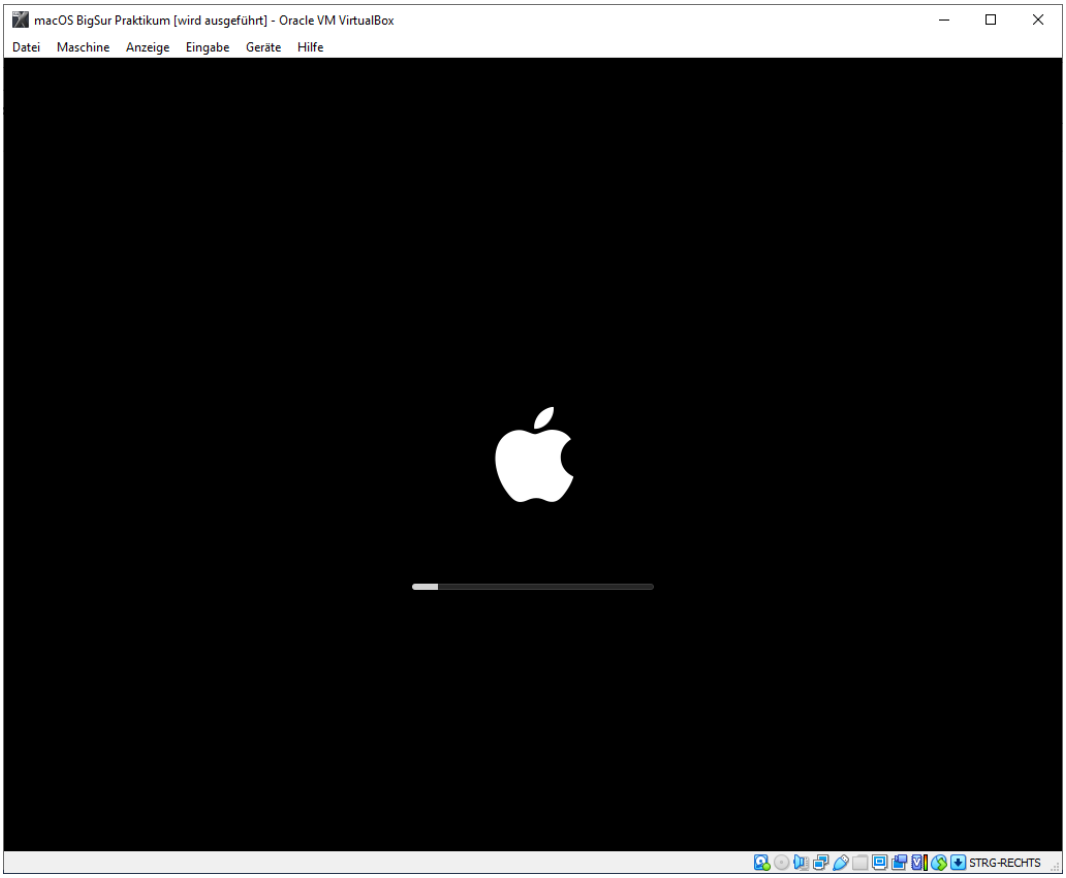
Im sich nun öffnenden Fenster klicken Sie bitte auf „Neu“ und fügen den Pfad „C:\Program Files\Oracle\VirtualBox“ ein:



Anschließend klicken Sie bitte auf „OK“, um Ihre Änderungen zu bestätigen. Nun sollten Sie das Kommando VBoxManage, wie oben beschrieben ausführen können.

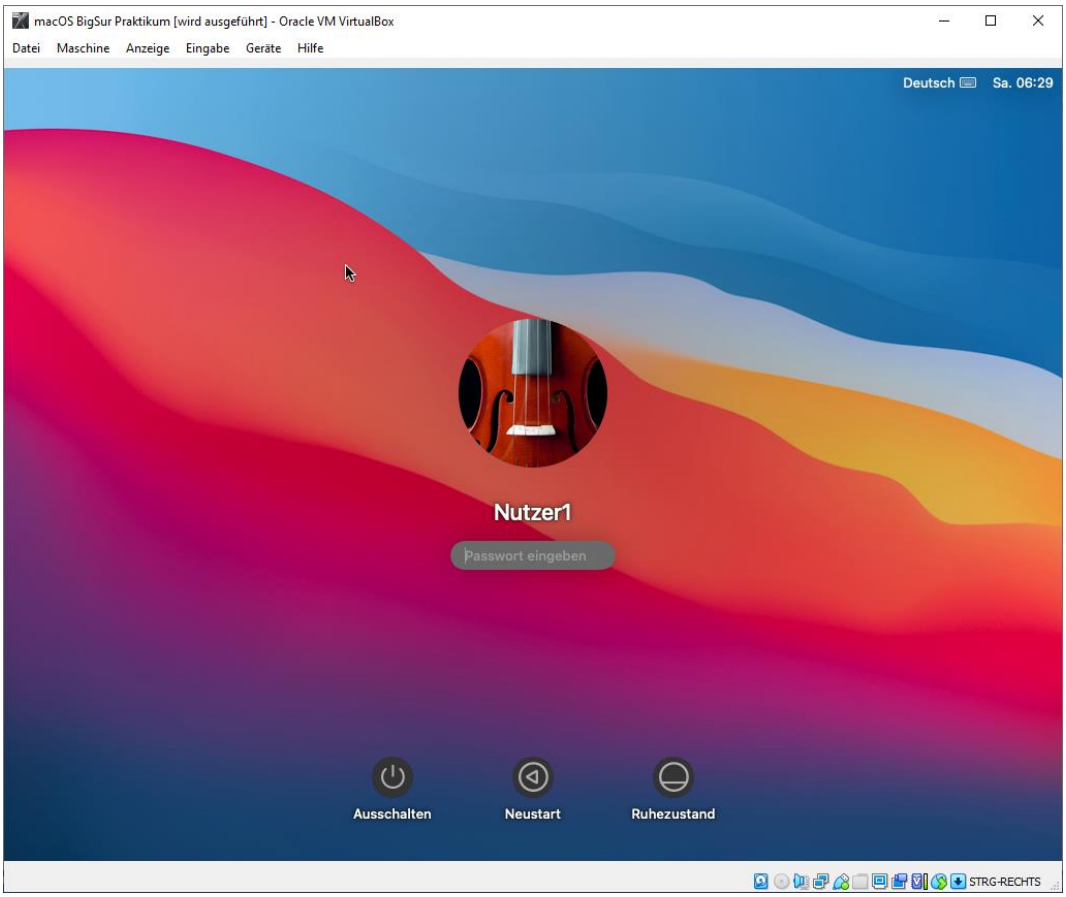
Starten der VM zum weiteren arbeiten

Starten Sie die **macOS Big Sure Praktikum** VM durch Doppelklick oder Starten.

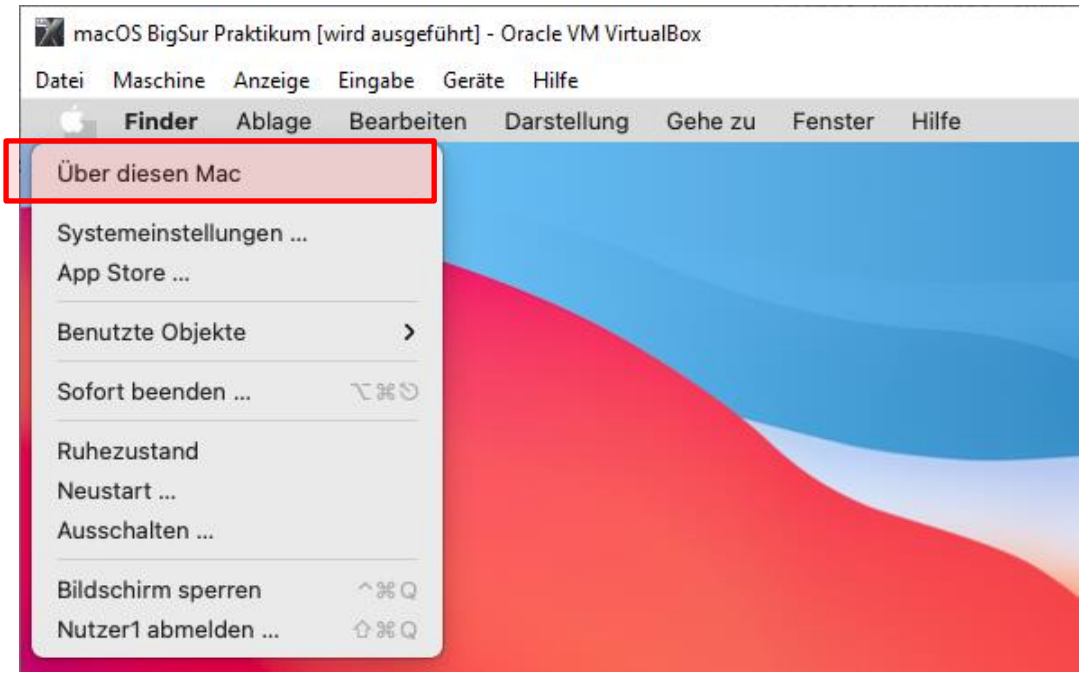


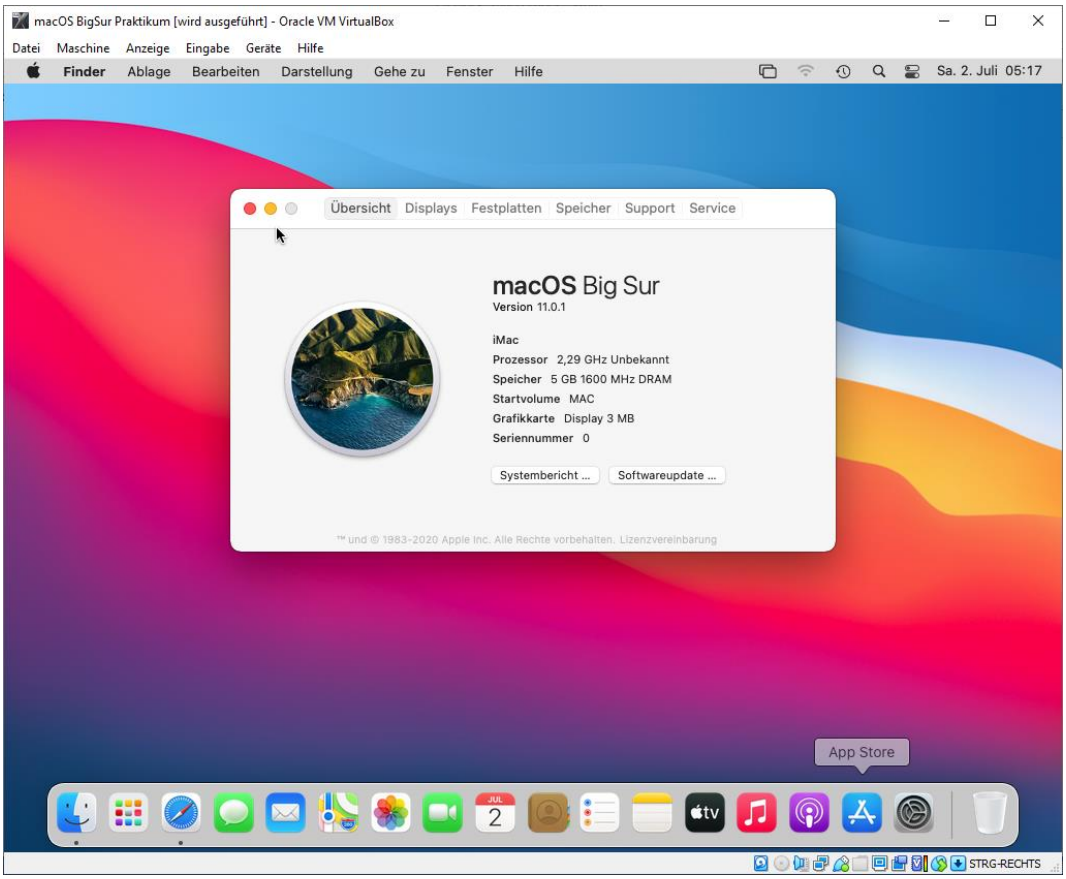
2. KENNENLERNEN VON MACOS AUS BEDIENERSICHT

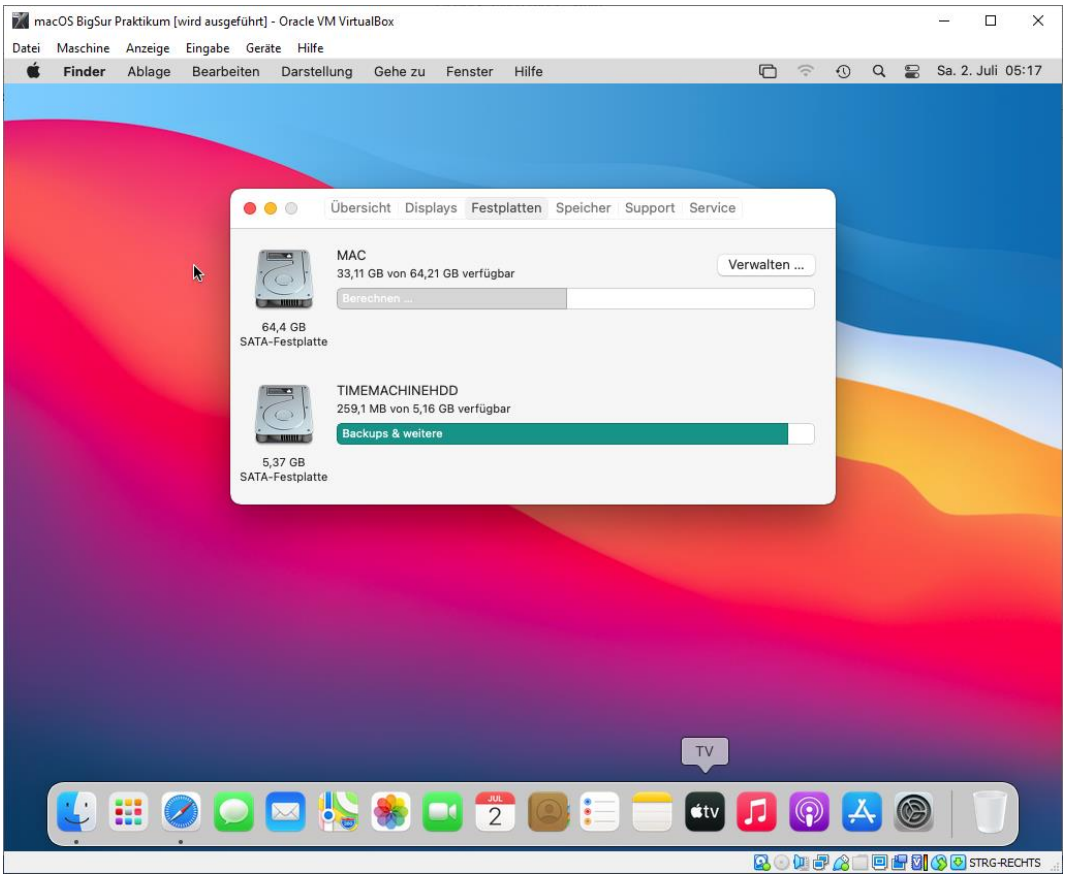
Melden Sie sich als **Nutzer1** mit **Kennwort1** an.



Rufen Sie **Über diesen Mac** auf und schauen Sie sich an, um was für ein System es sich handelt und welches Startvolume eingebunden ist.

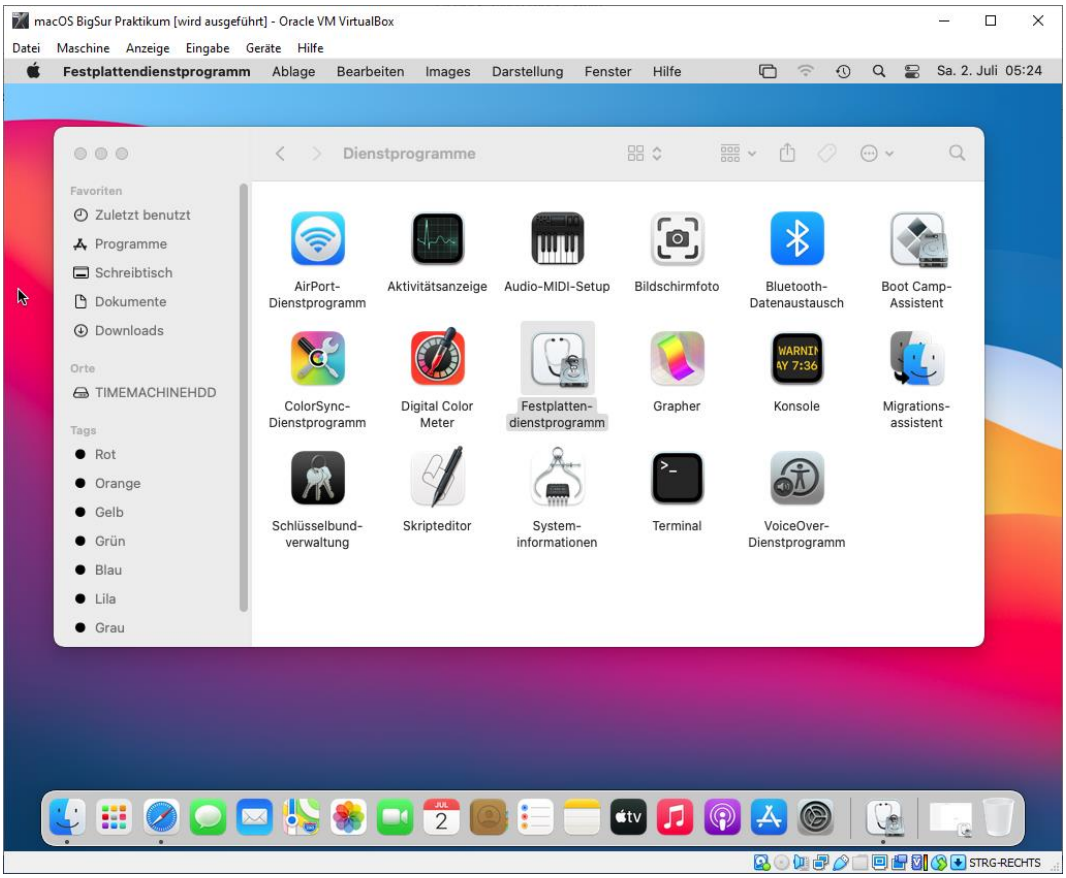




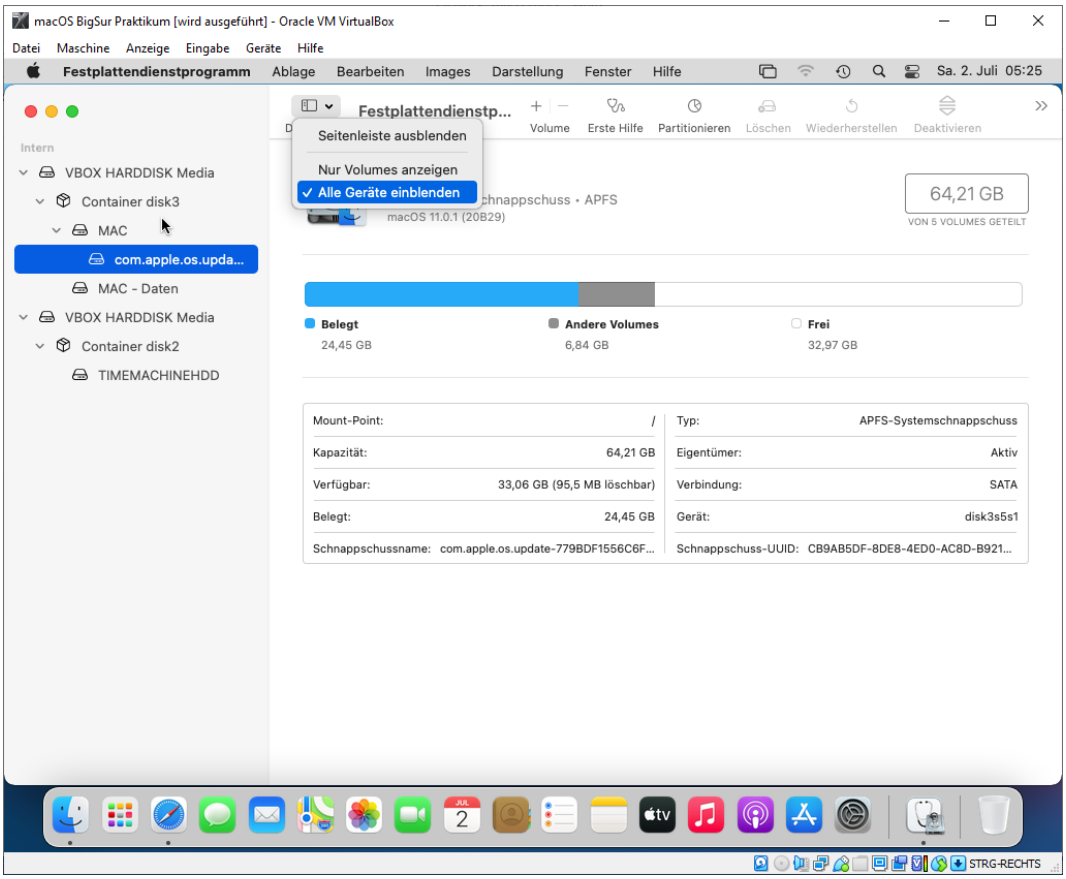

macOS BigSur Praktikum [wird ausgeführt] - Oracle VM VirtualBox
Datei Maschine Anzeige Eingabe Geräte Hilfe
Finder Ablage Bearbeiten Darstellung Gehe zu Fenster Hilfe
Sa. 2. Juli 05:17
Übersicht Displays Festplatten Speicher Support Service
MAC
33,11 GB von 64,21 GB verfügbar
Verwalten ...
Berechnen ...
64,4 GB
SATA-Festplatte
TIMEMACHINEHDD
259,1 MB von 5,16 GB verfügbar
Backups & weitere
5,37 GB
SATA-Festplatte
TV
STRG-RECHTS

Schließen Sie diese Fenster und Öffnen Sie den Finder und navigieren zu Programmen.

Wechseln Sie in Dienstprogramme.



Öffnen Sie das **Festplattendienstprogramm**. Überprüfen Sie ob die Ansicht auf **Alle Geräte anzeigen** eingestellt ist.

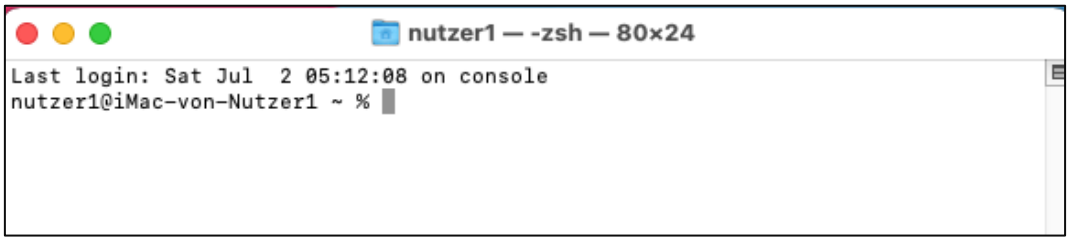


Wählen Sie den Container **disk3** aus und schauen Sie sich die Übersicht der tatsächlich vorhandenen Volumes an.

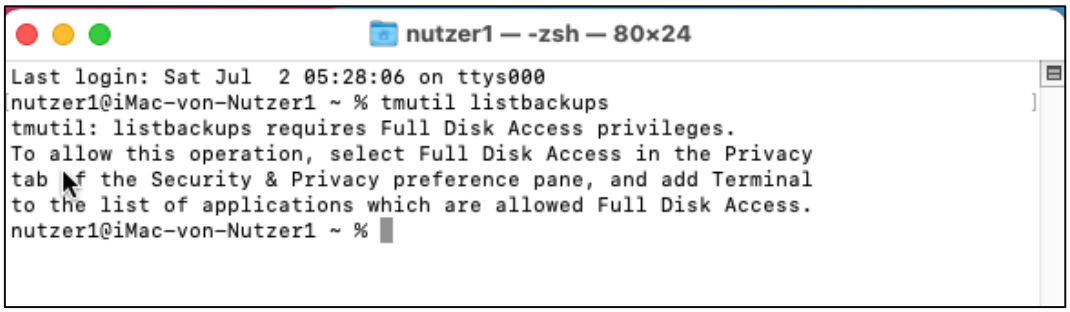
Öffnen Sie das **Terminal** unter **Finder > Programme > Dienstprogramme**.

Schließen Sie das Terminal Fenster und öffnen Sie **Spotlight** über die **Menüleiste**.

Geben Sie hier **Terminal** ein und öffnen Sie das Terminal Fenster erneut.

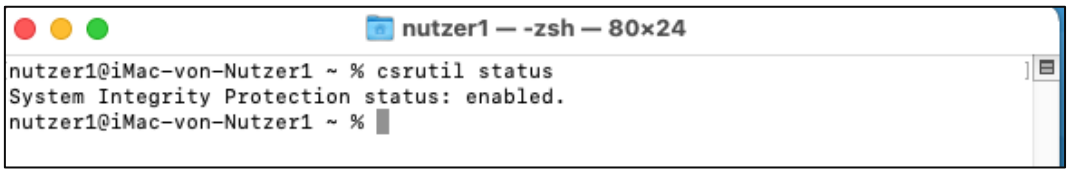


Listen Sie sich alle Backups auf.

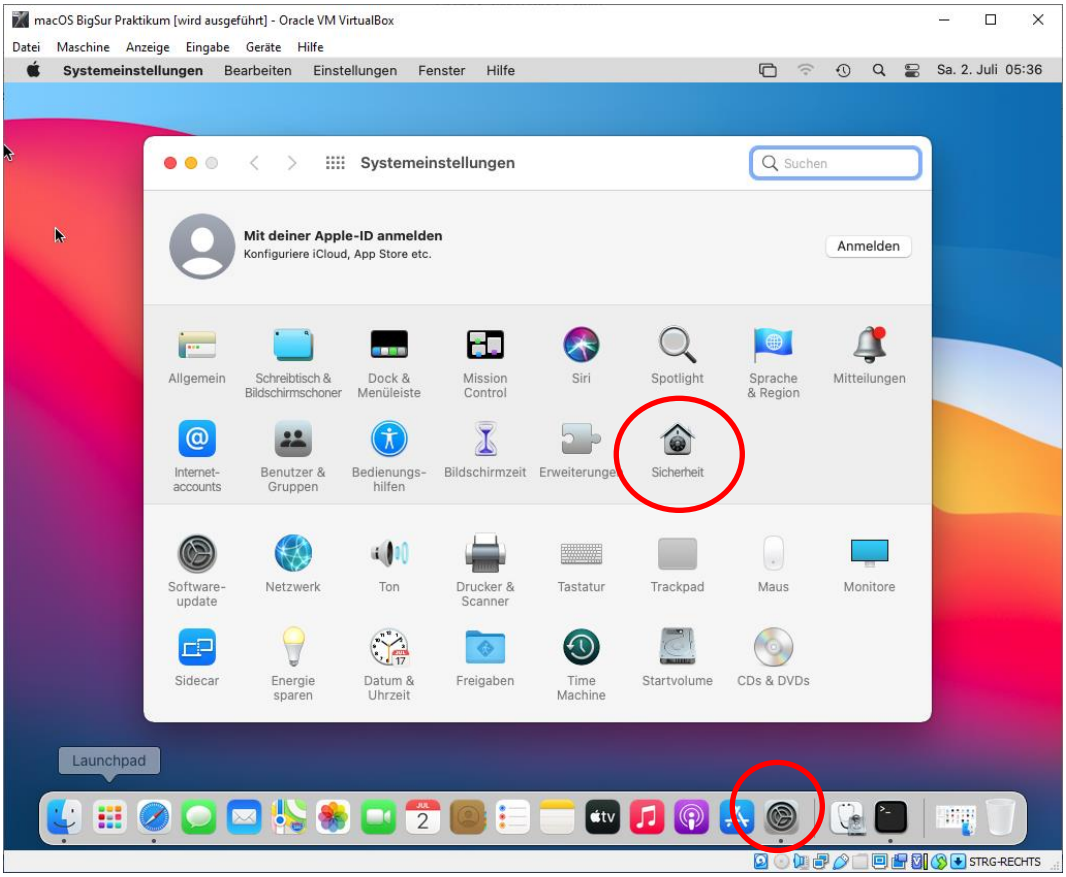


Hier fehlen ihnen die Berechtigungen, da die System Integrity Protection SIP einiges blockiert.

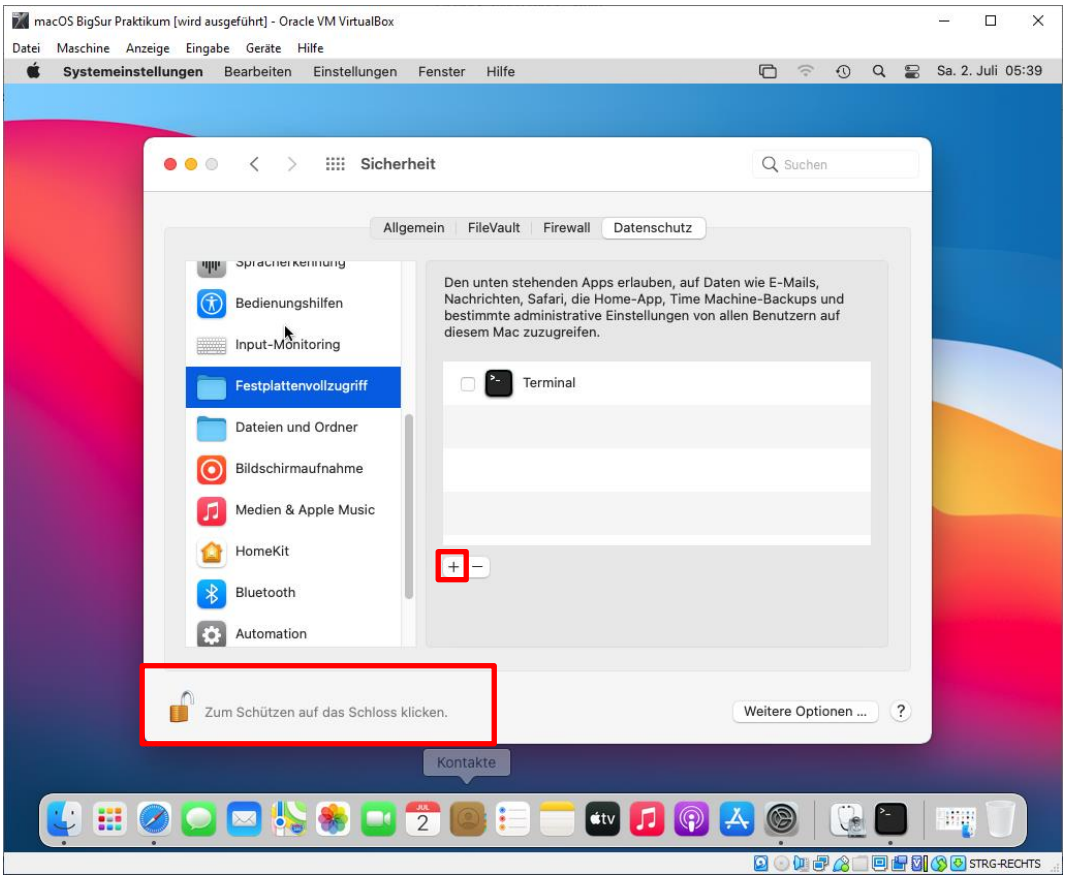
Überprüfen Sie dies mit dem Befehl **csrutil status** im Terminal.



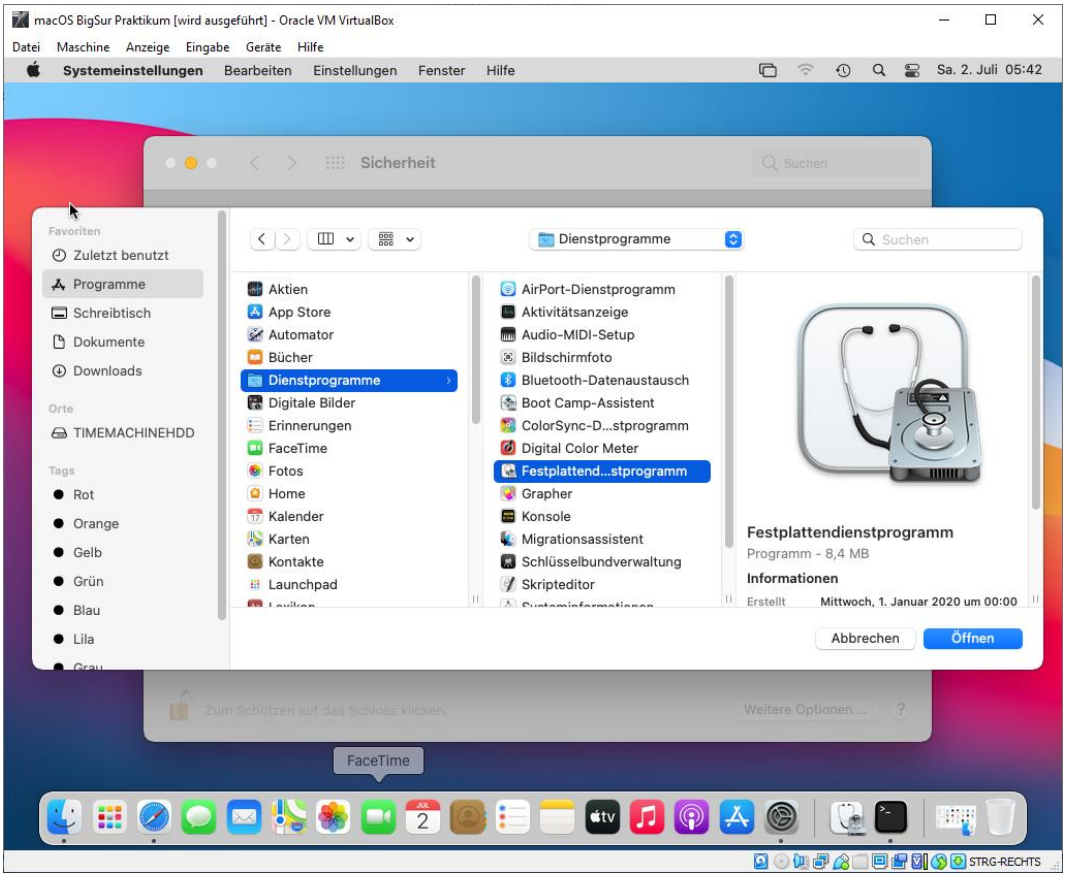
Schließen Sie das Terminal und Öffnen Sie die Systemeinstellungen im Dock.



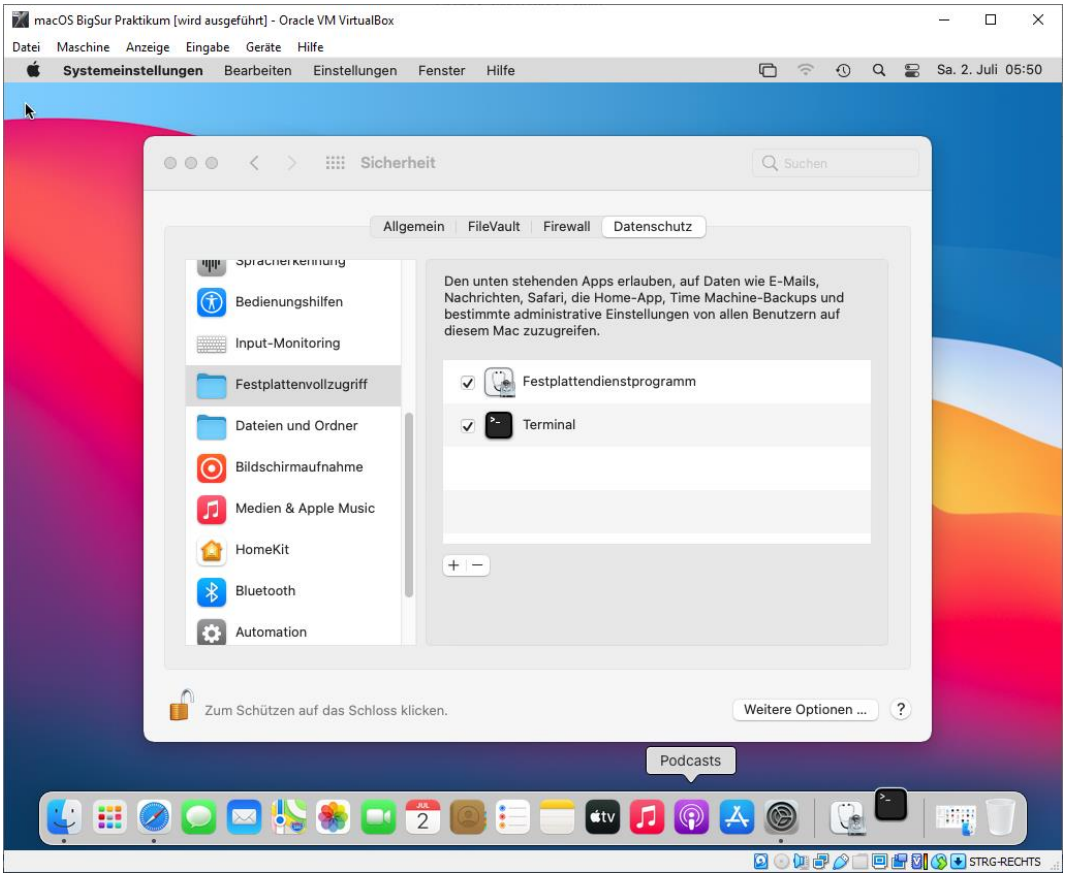
Wählen Sie danach den Punkt Sicherheit und wechseln Sie zu Datenschutz. Hier Wählen Sie bitte Festplattenvollzugriff aus.



Klicken Sie auf das Schlosssymbol und fügen Sie hier das Festplattendienstprogramm hinzu über das (+).

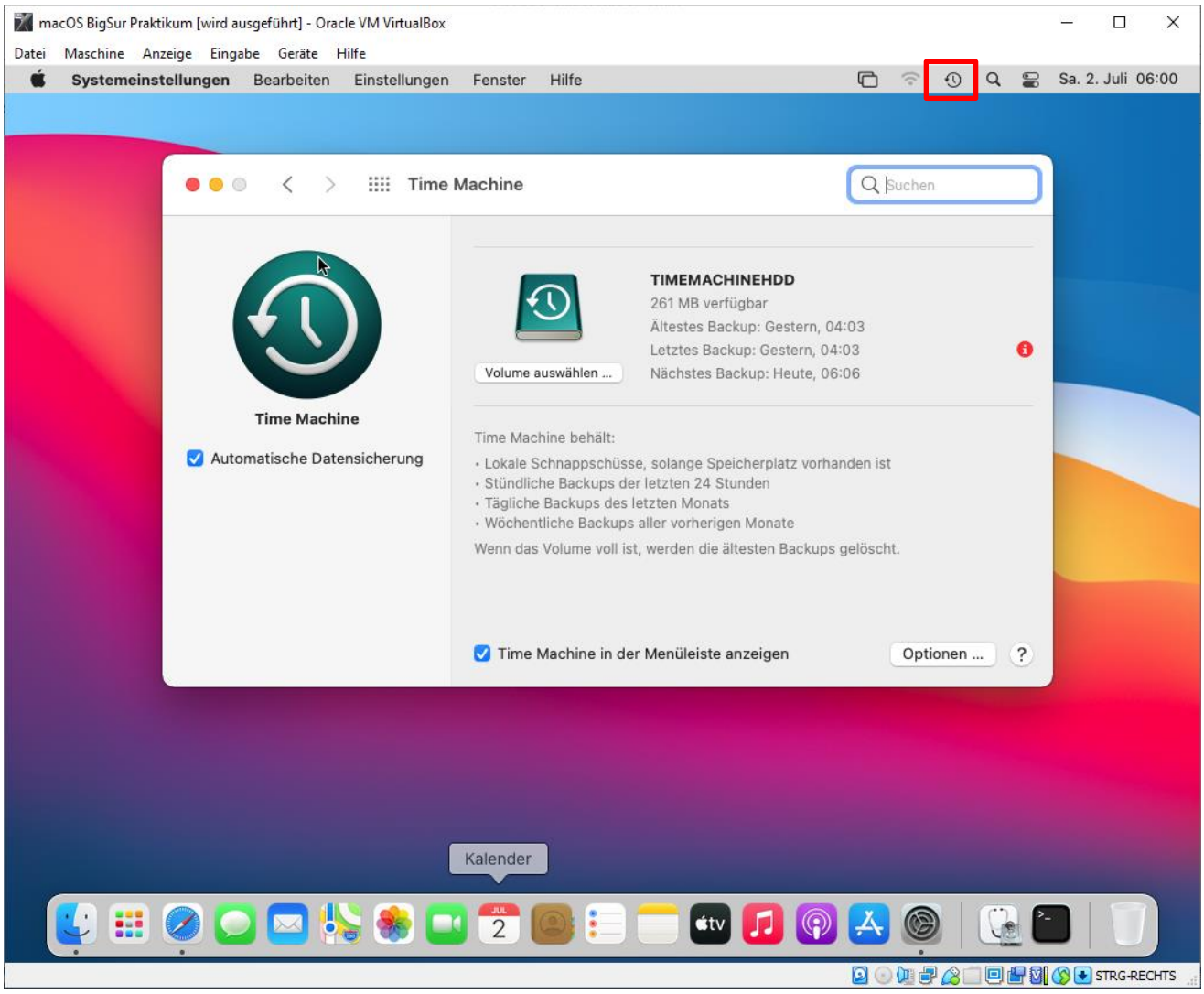


Setzen Sie zudem den **Haken** bei **Terminal**.

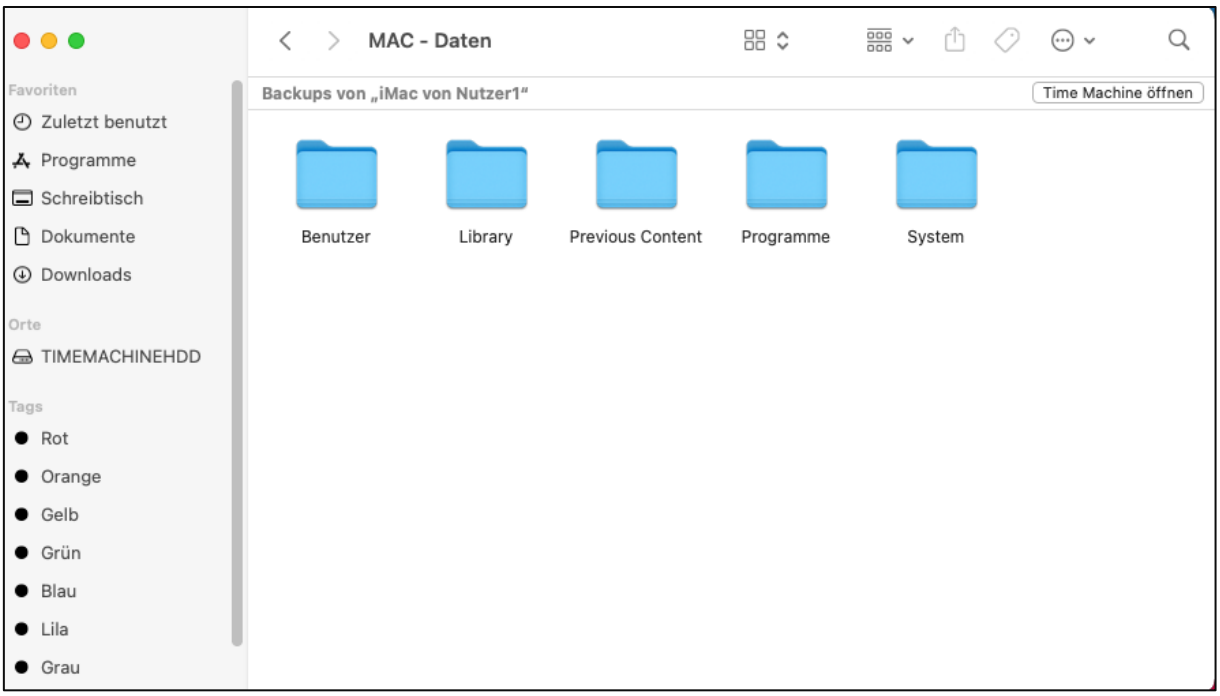


Öffnen Sie das **Terminal** Listen Sie sich das Time Machine Laufwerk, alle Backups und die lokalen Backups auf.

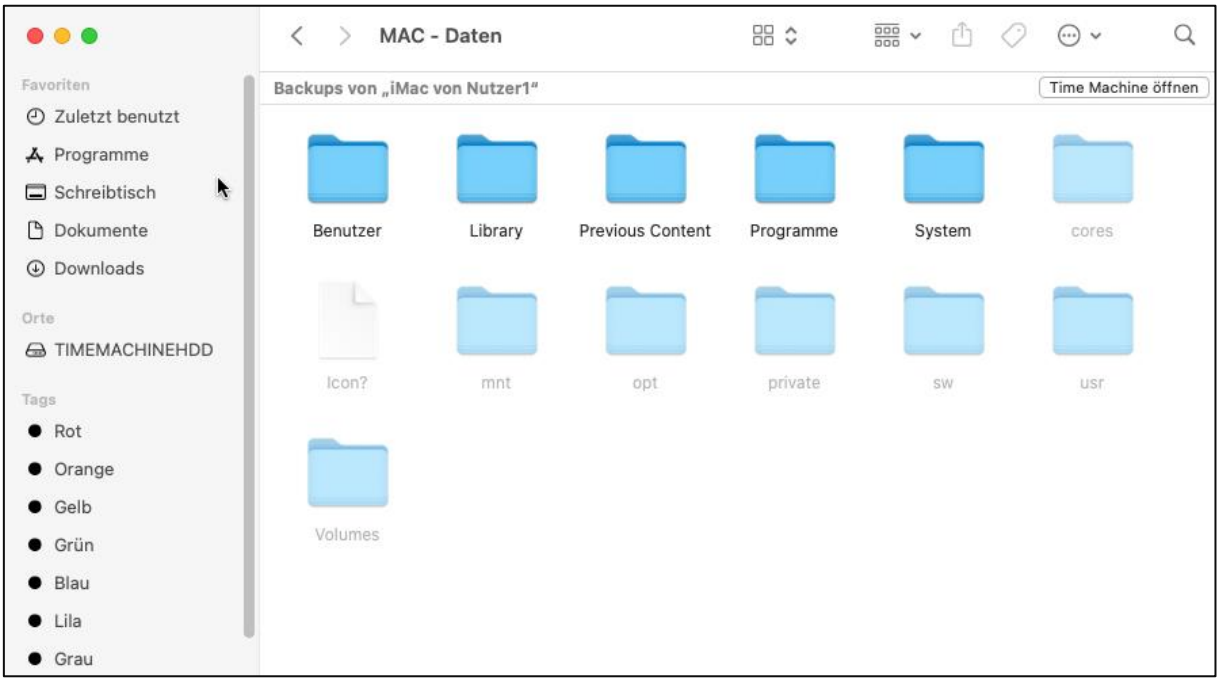
Öffnen Sie die **TimeMachine Systemeinstellungen** über das Icon in der Menüleiste.



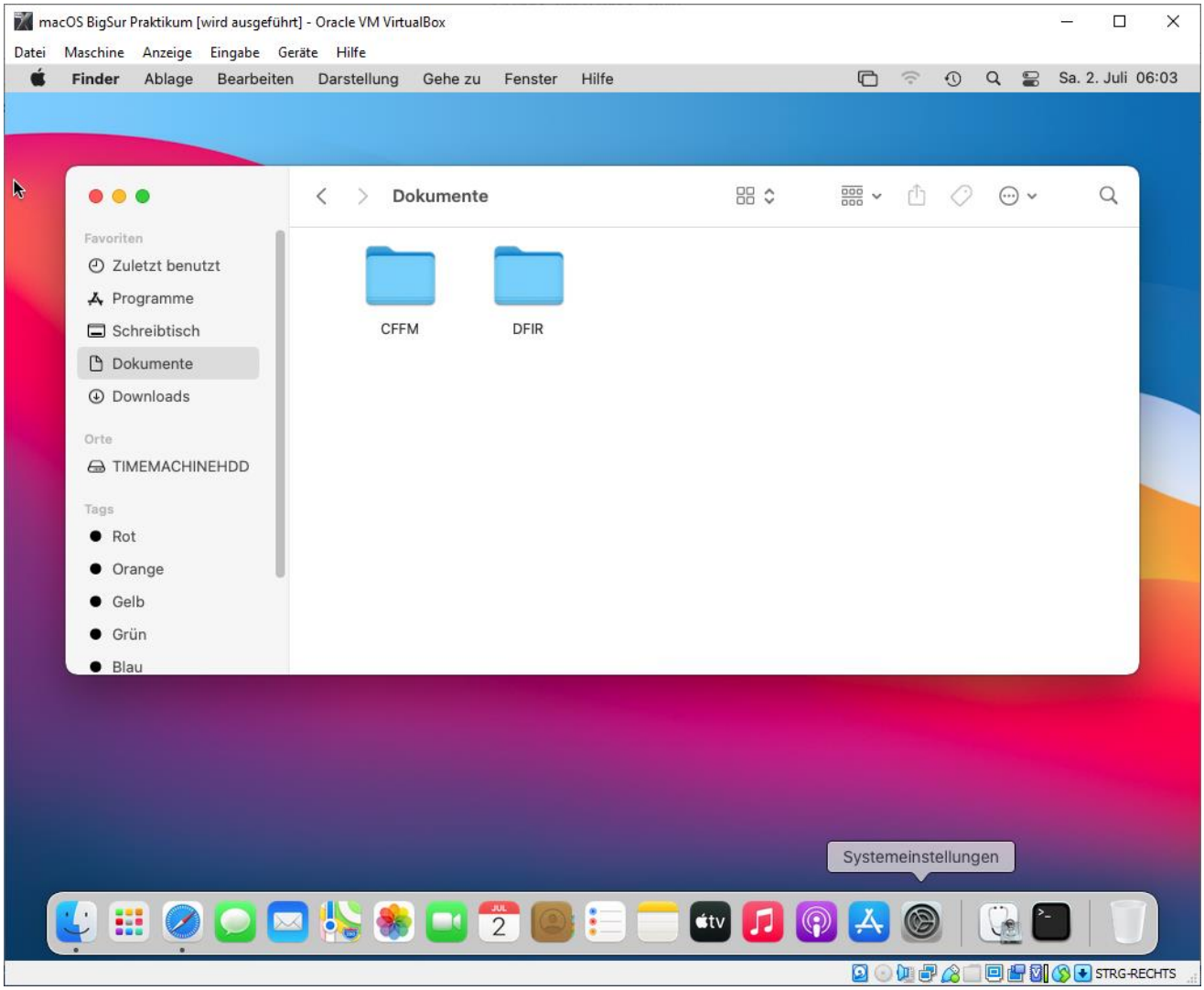
Schauen Sie auf dem Time Machine Laufwerk die Speicherstruktur an (Finder TIMMACHINEHDD).



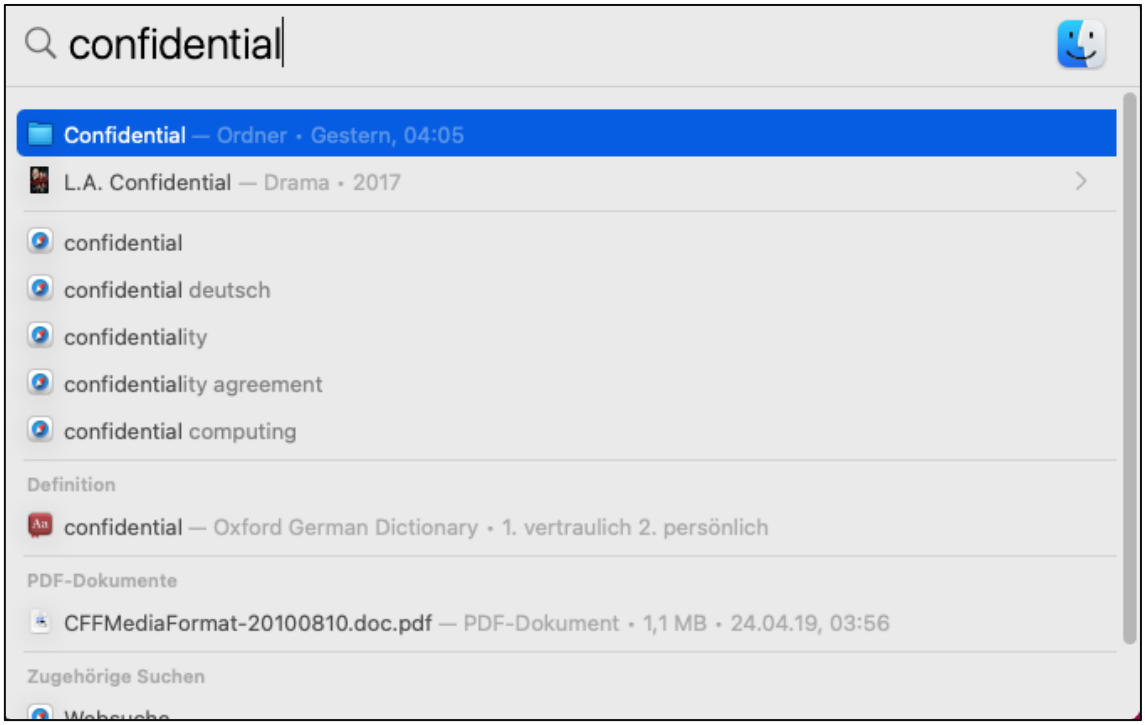
Aktivieren Sie die Ansicht der versteckten Dateien und Ordner durch **SHIFT+WINDOWS Taste + [.]**.



Öffnen Sie den Finder und schauen Sie sich in den **Dokumenten** des **Nutzers1** um.



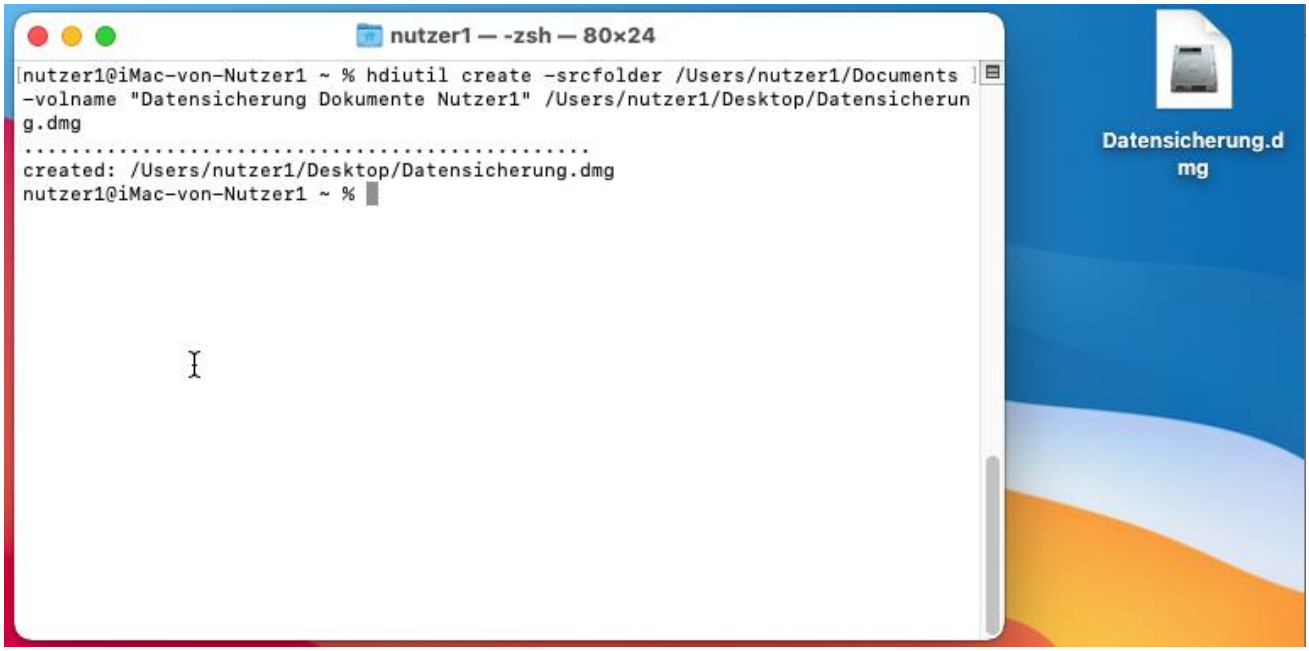
Sie suchen eine Datei die das Wort **Confidential** enthält. Nutzen Sie dazu **Spotlight** über die **Menüleiste**.



Sichern Sie die Dokumente von Nutzer1 in einem DMG Container.

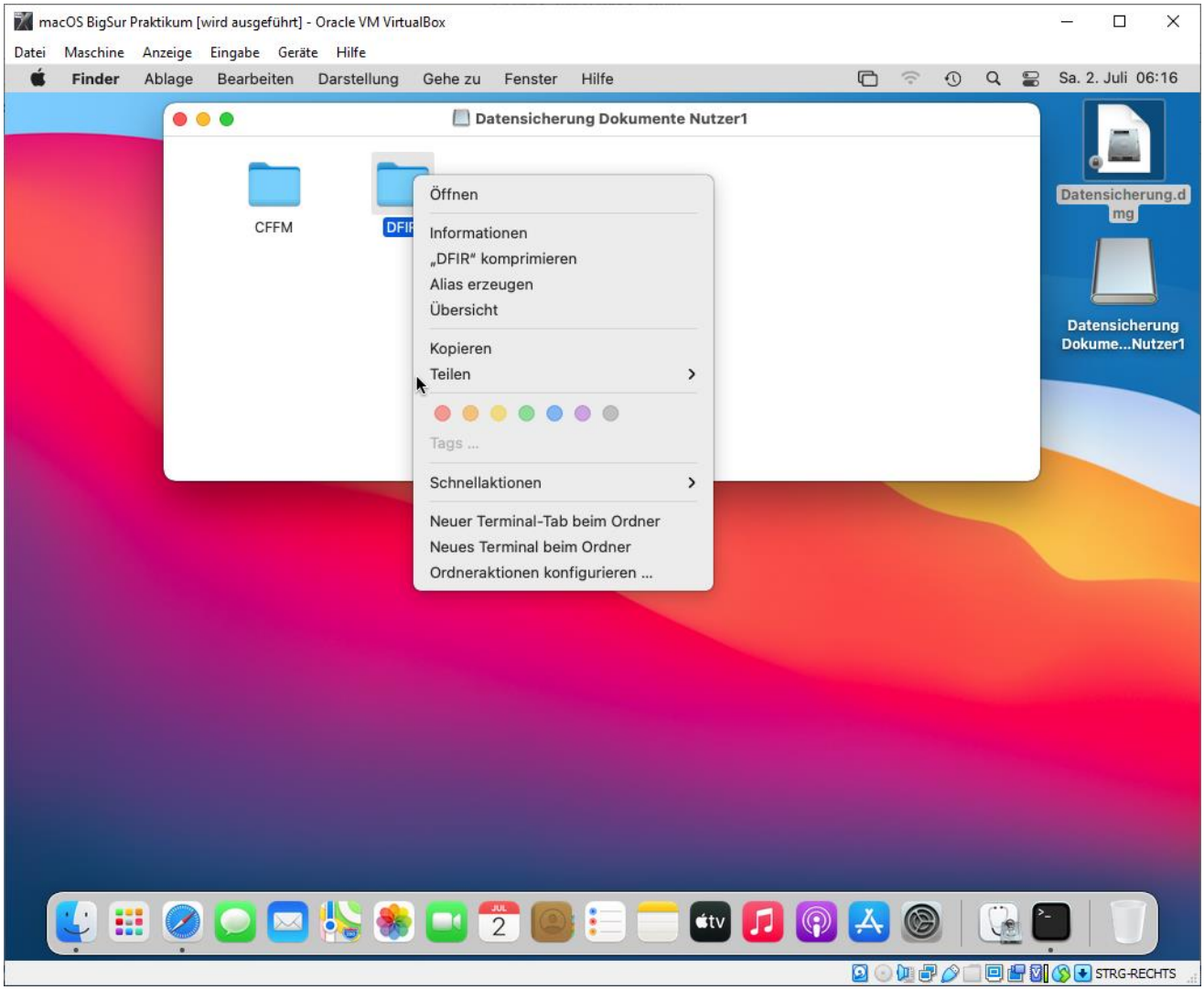
Öffnen Sie dazu das Teminal und nutzen Sie den Befehl

hdiutil create -srcfolder /Users/nutzer1/Dokumente -volname „Datensicherung Dokumente Nutzer1“ /Users/nutzer1/Desktop/Datensicherung.dmg



Zeigen Sie sich die Informationen zur Datei **Datensicherung.dmg an.**

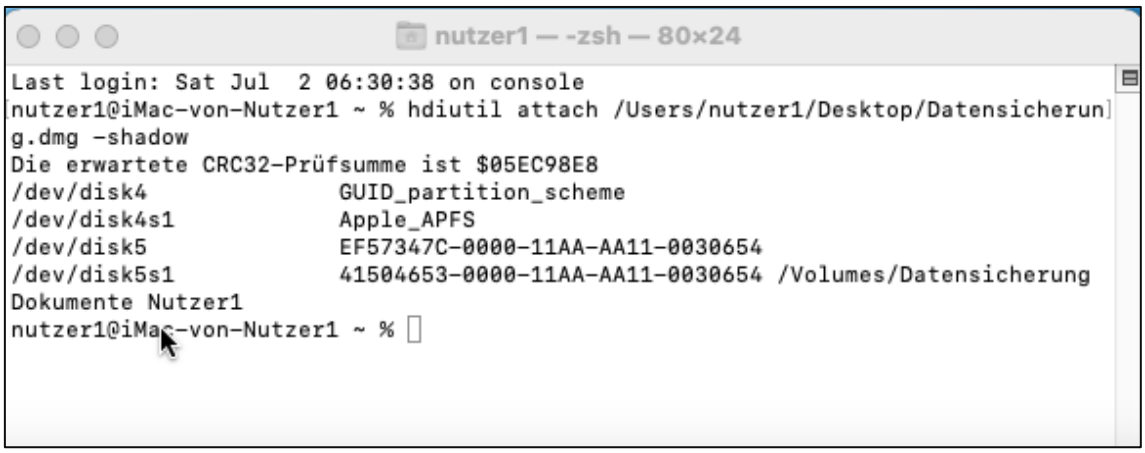
Binden Sie das Image **Datensicherung.dmg** im System ein und greifen Sie auf die Dateien zu.

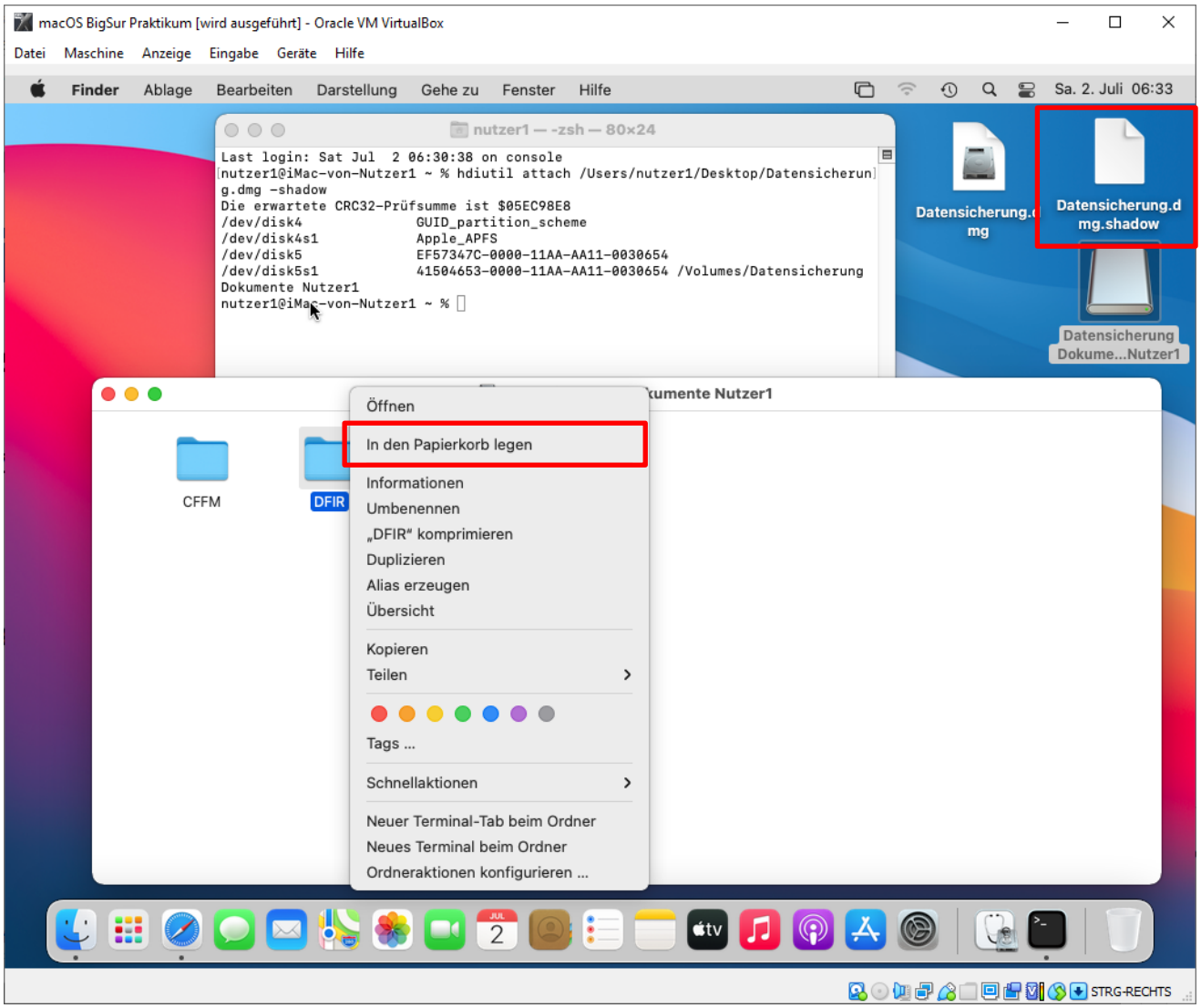


Wird das Image Schreibgeschützt eingebunden oder ist von Haus aus Schreibgeschützt, können Sie über das Kontext Menü keine Daten löschen!

Werfen Sie das gemountete Volume aus und binden Sie es über das Terminal erneut ein mit dem folgenden Befehl:

```
hdiutil attach /Users/nutzer1/Desktop/Datensicherung.dmg -shadow
```





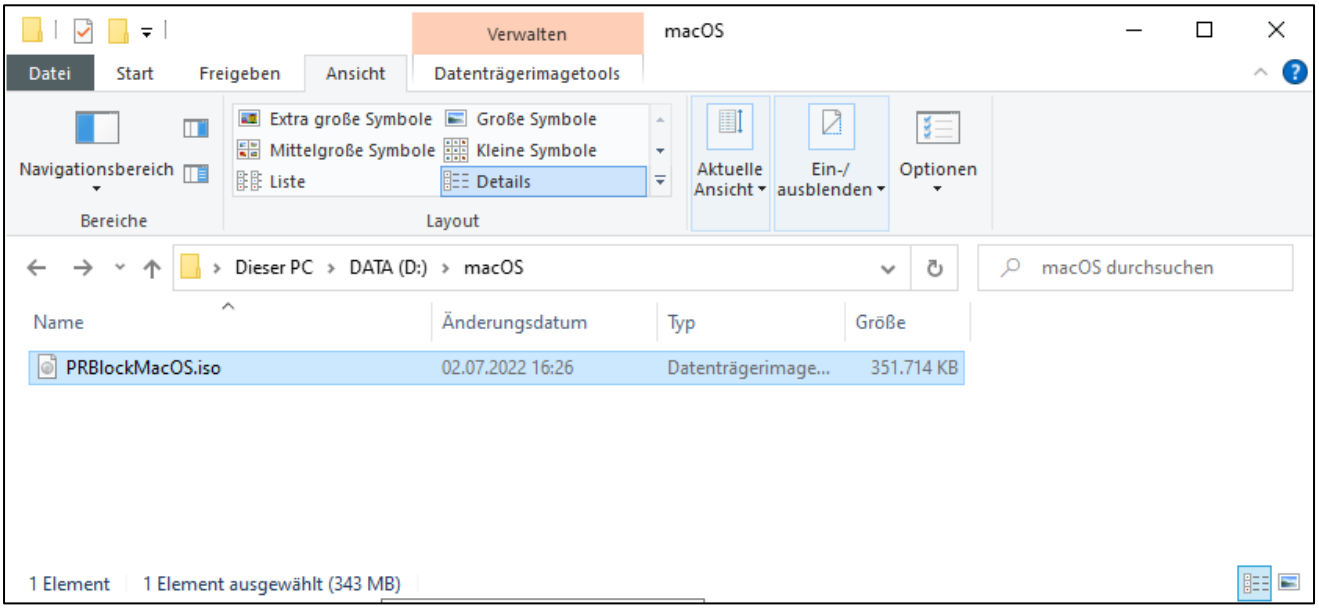
Jetzt wird zusätzlich eine **Shadow Datei** erzeugt, welche die Änderungen aufnimmt.

Dies sieht man daran, dass Dateien auch gelöscht werden können.

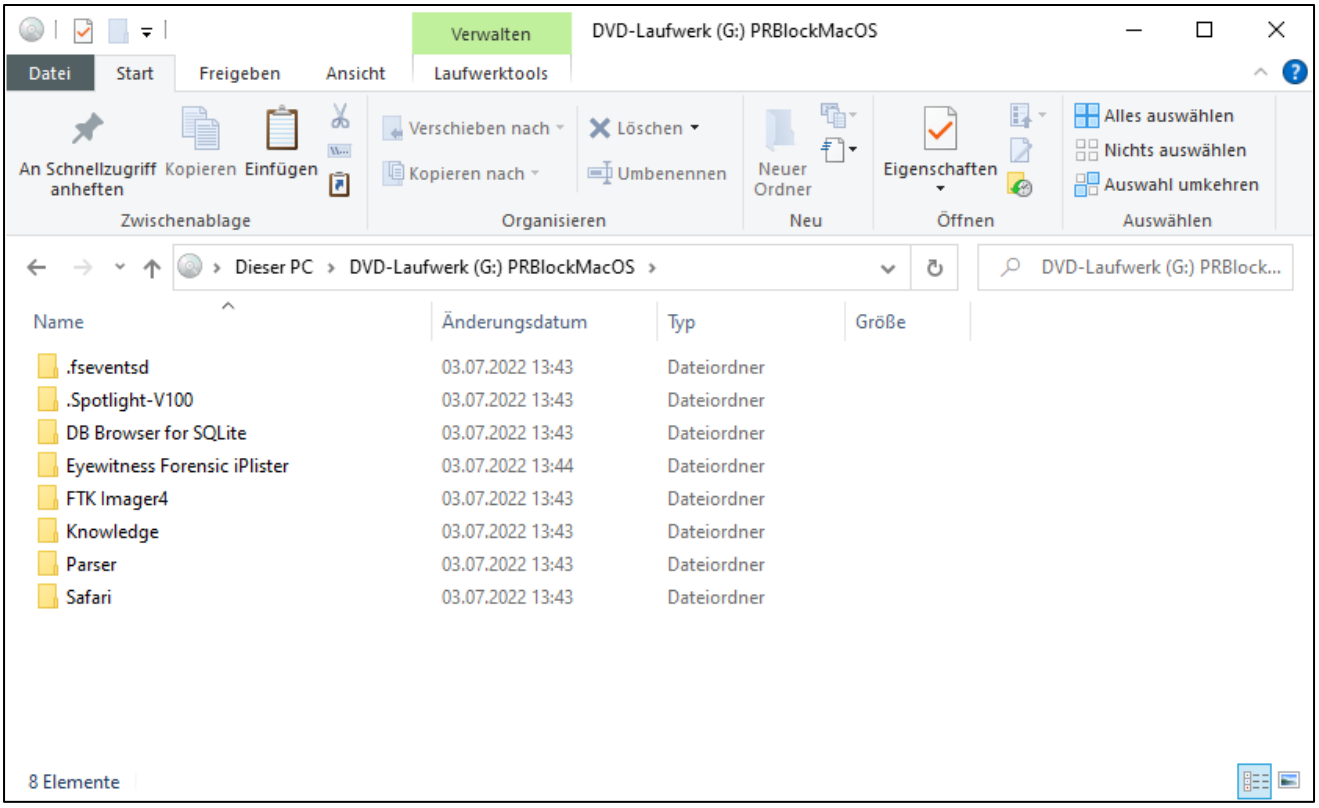
3. UNTERSUCHUNG DER MACOS ARTEFAKTE UND DIGITALER SPUREN IN EXTERNEM BETRIEBSSYSTEM

Zur Vorbereitung erstellen Sie auf Laufwerk D:\ ein Verzeichnis **macOS** und kopieren dahin die **PRBlockMacOS.iso** Datei.

Binden Sie zum Bearbeiten der Daten die auf die lokale Festplatte kopierte ISO Datei **PRBlockMacOS.iso** durch Doppelklick ein.

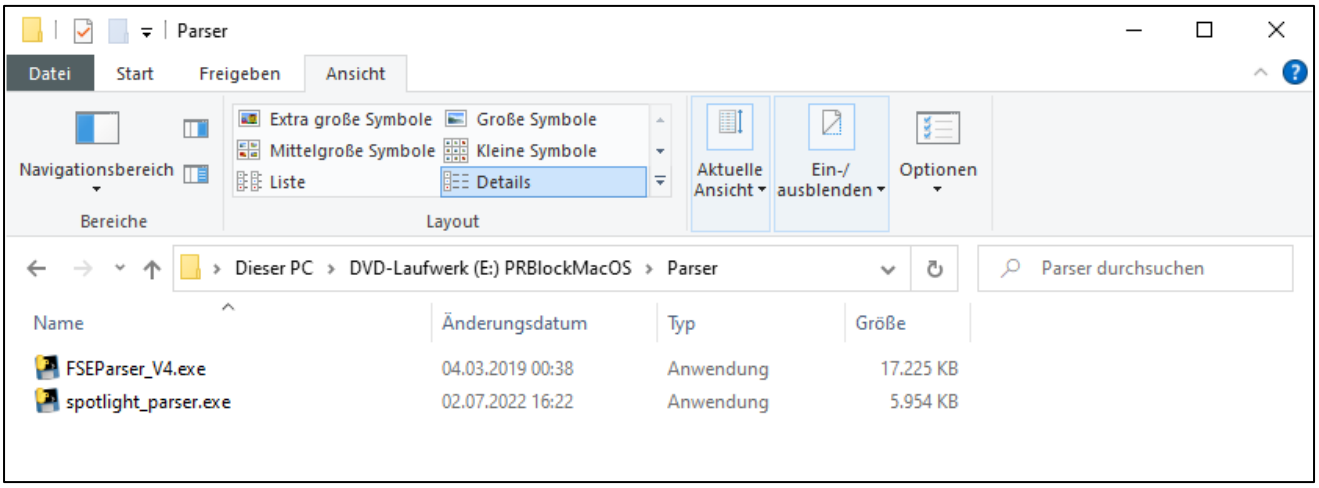


Auf der eingebundenen CD finden Sie alle nötigen Tools und auch die bereits gesicherten Daten des macOS.

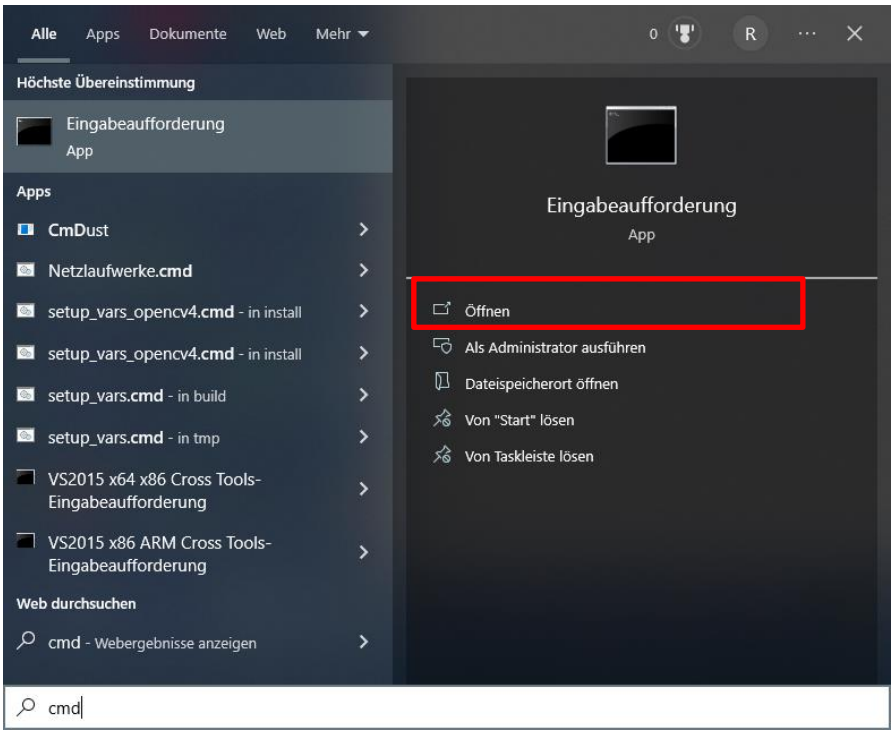


3.1. SPOTLIGHT UNTERSUCHUNG MIT PYTHON PARSER

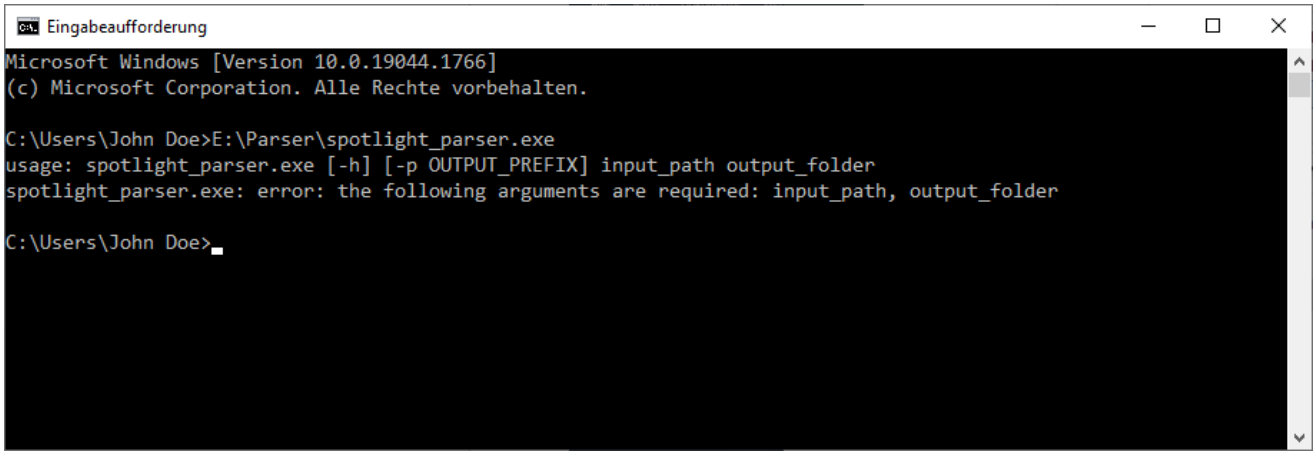
Rufen Sie den das Verzeichnis Parser auf der CD auf. Her befinden sich zwei in Python gechriebene Parser für Spotlight und FSEvents.



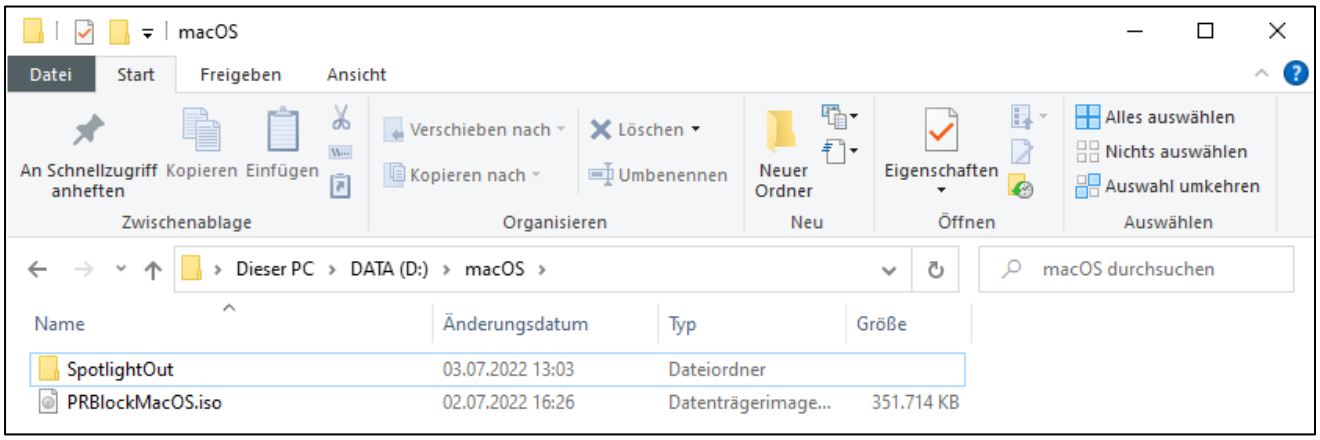
Öffnen Sie eine Eingabeaufforderung durch Klicken auf den Start Button und Eingabe von CMD. Es reicht eine Eingabeaufforderung ohne Admin Rechte.



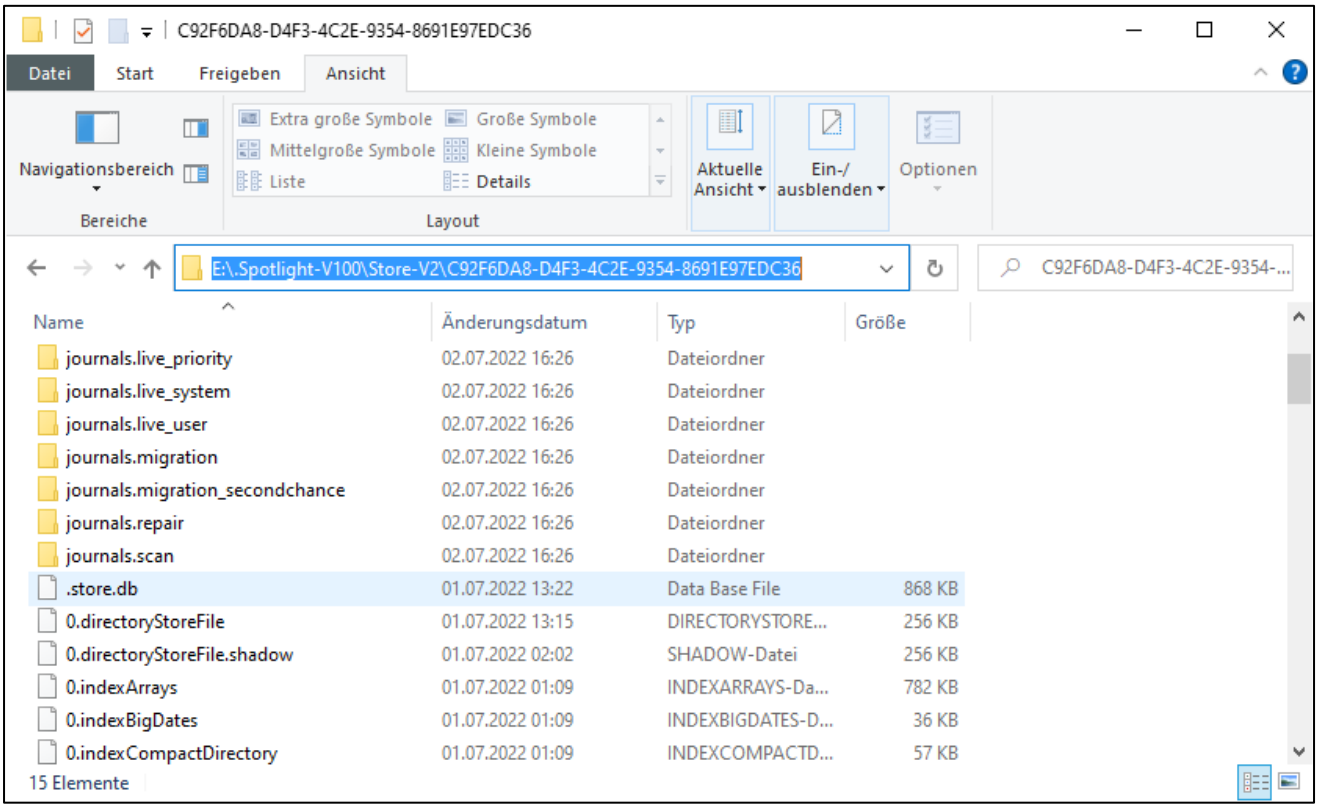
Starten Sie den SpotlightParser in der Eingabeaufforderung.



Der SpotlightParser benötigt zur Ausgabe ein Verzeichnis, welches vor Nutzung angelegt werden muss.

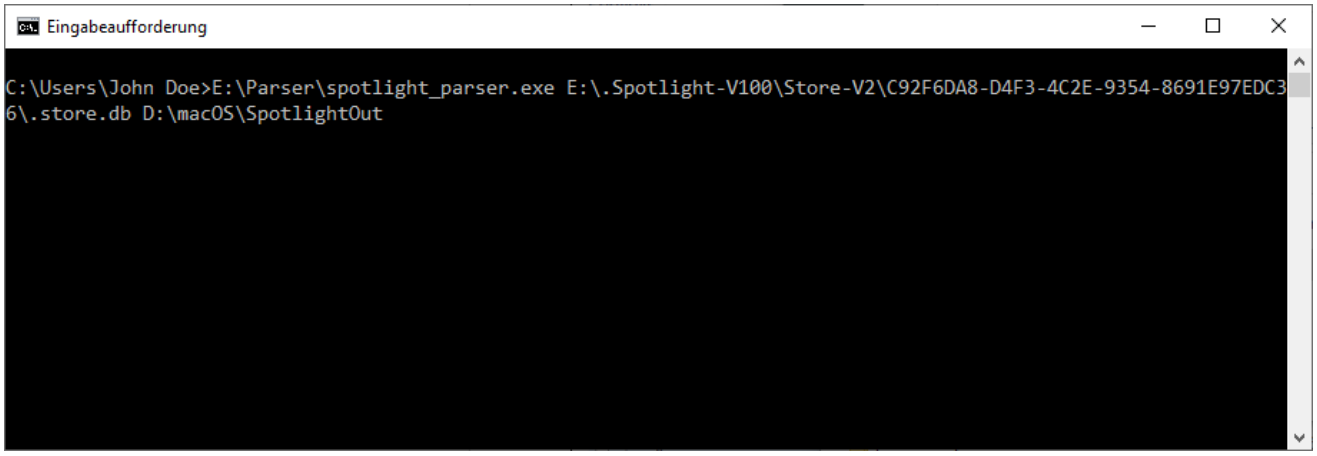


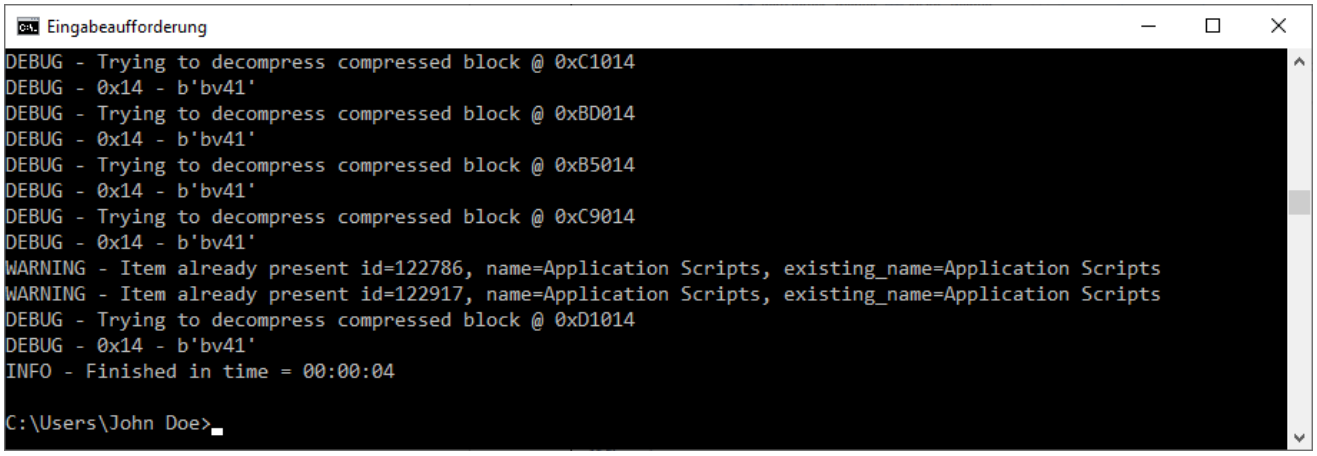
Die zu untersuchende Spotlight Datenbank Datei finden Sie unter \.Spotlight-V100\Store-V2\C92F6DA8-D4F3-4C2E-9354-8691E97EDC36\.store.db



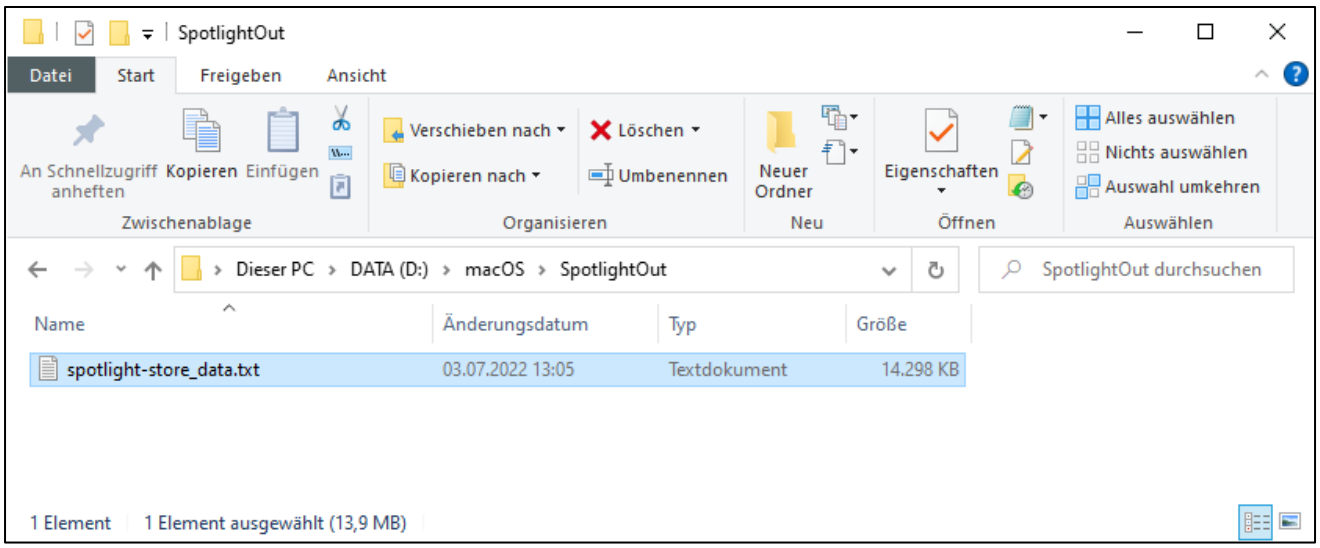
Mit folgendem Befehl kann der Spotlight Parser gestartet werden:

```
\Parser\spotlight_parser.exe G:\.Spotlight-V100\Store-V2\C92F6DA8-D4F3-4C2E-9354-
8691E97EDC36\.store.db D:\macOS\SpotlightOut
```

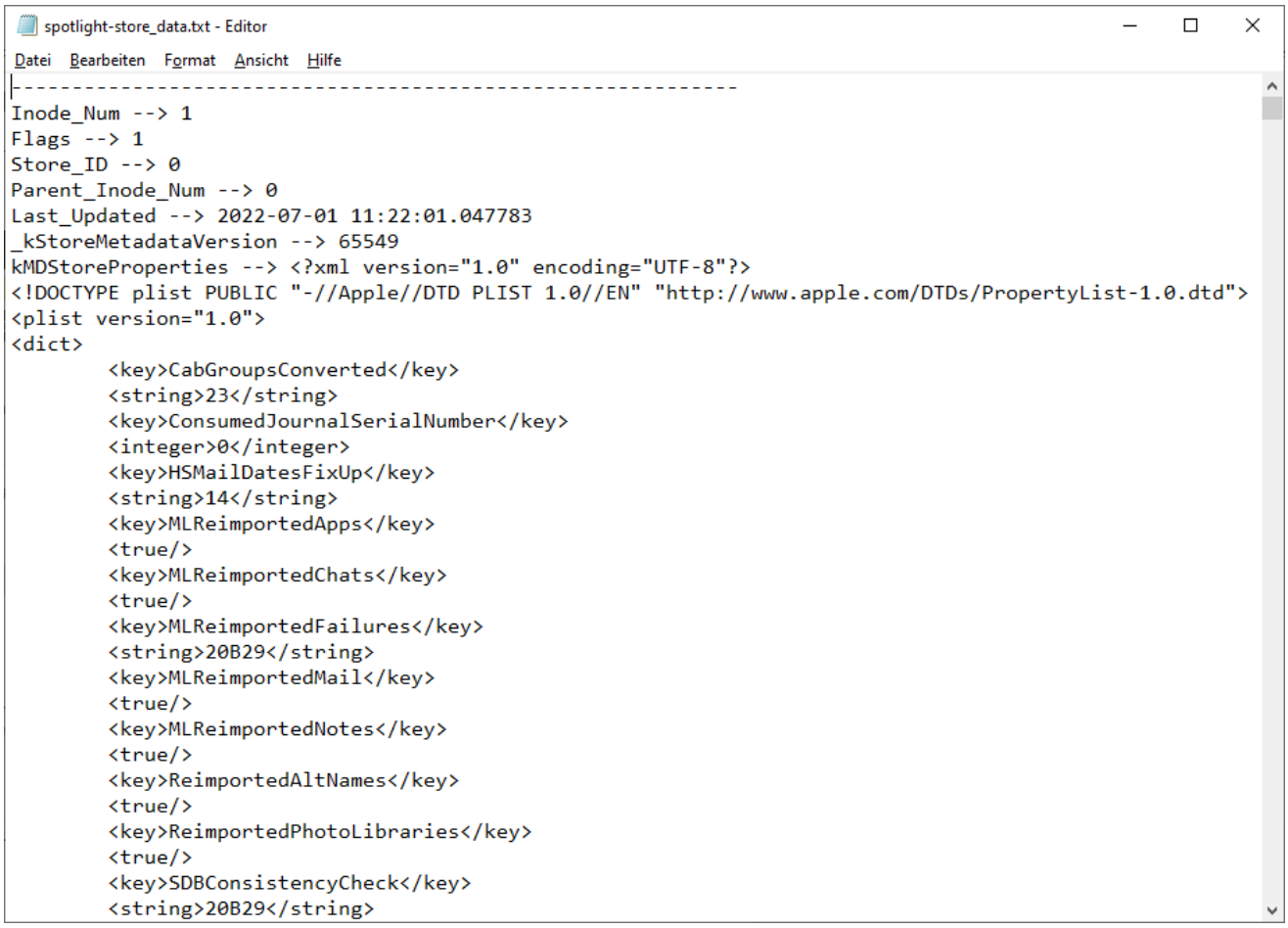




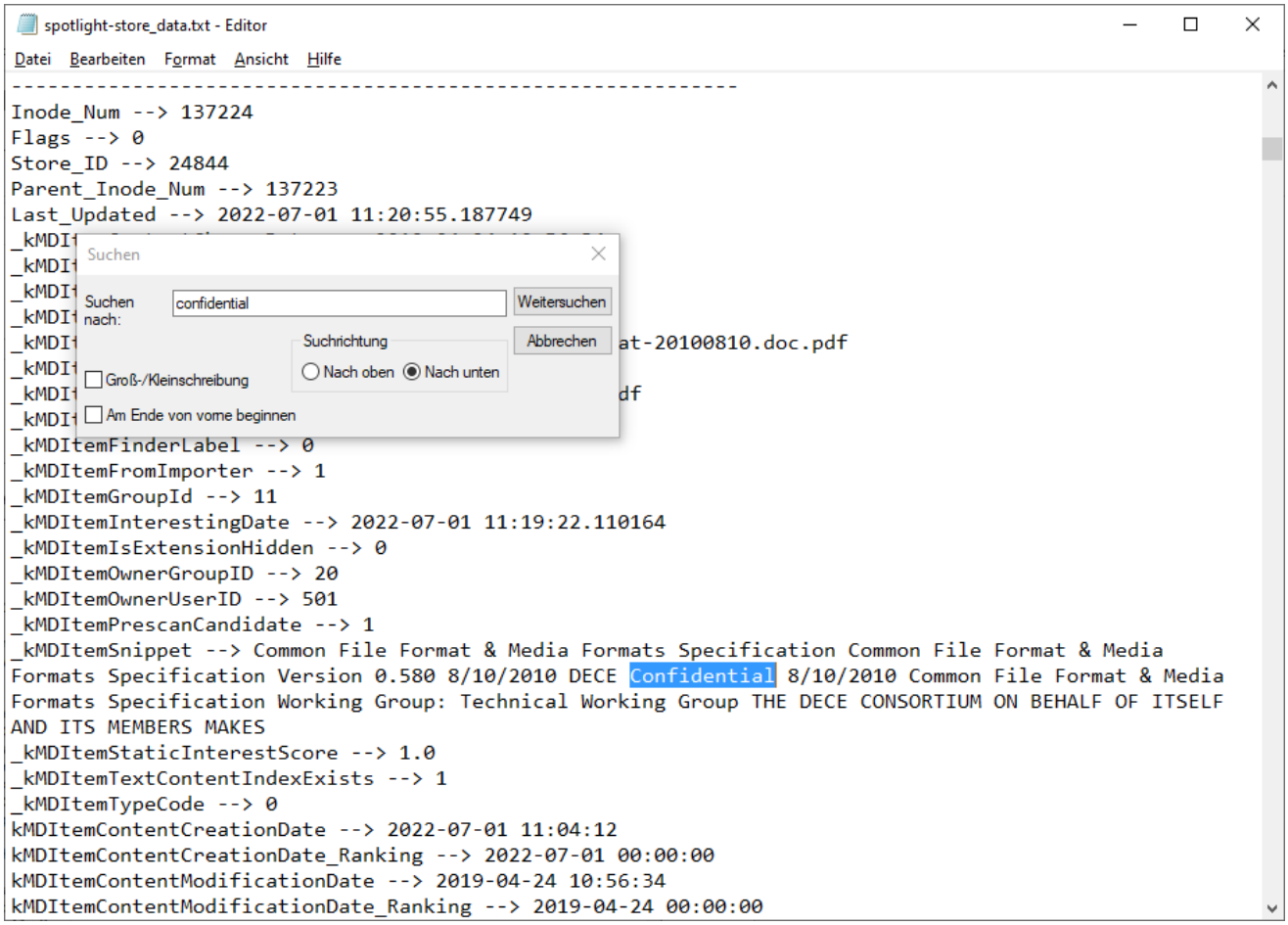
Im Ausgabeverzeichnis erstell der Parser eine Textdatei mit den aufbereiteten Spotlight Meta-Informationen.



Hier finden Sie alle ausgelesenen Daten der Spotlight Datenbank.



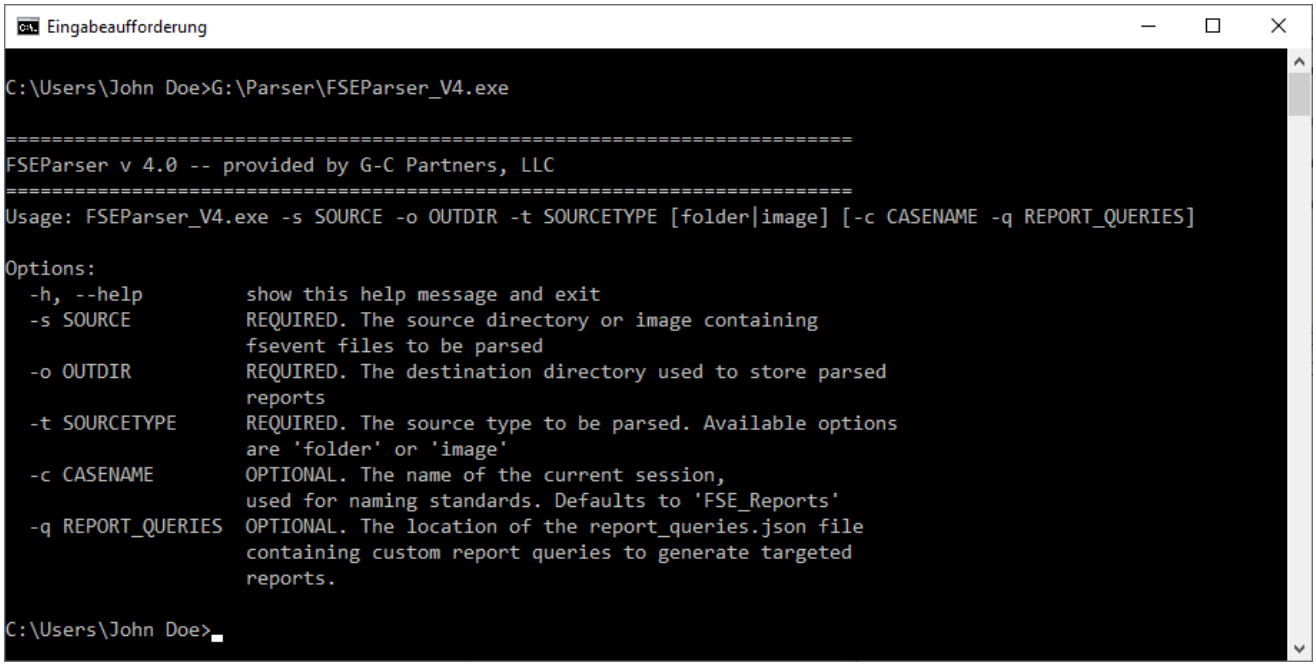
Suchen Sie nach dem Schlüsselwort **Confidential**!



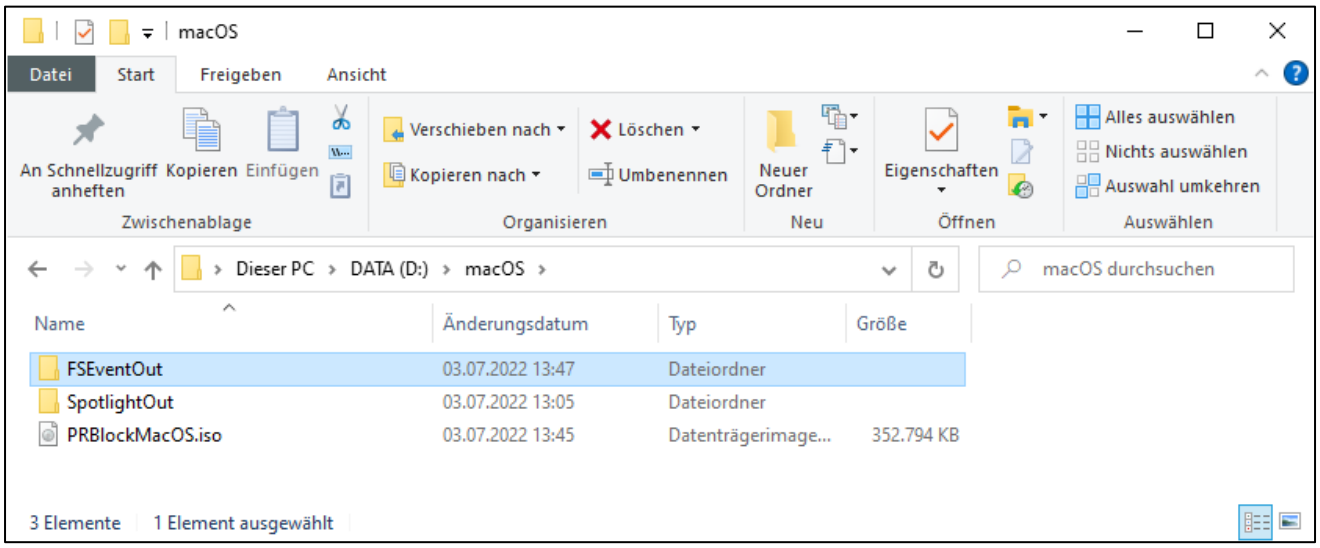
Sie erhalten sogar die indizierten Meta Informationen die aus der PDF Datei gelesen und indiziert wurden!

3.2. FSEVENT UNTERSUCHUNG MIT FSEVENT PARSER

Für die Untersuchung der FSEvent Daten wird der FSEvent Parser verwendet der als Executable im Verzeichnis Parser auf der CD vorhanden ist.

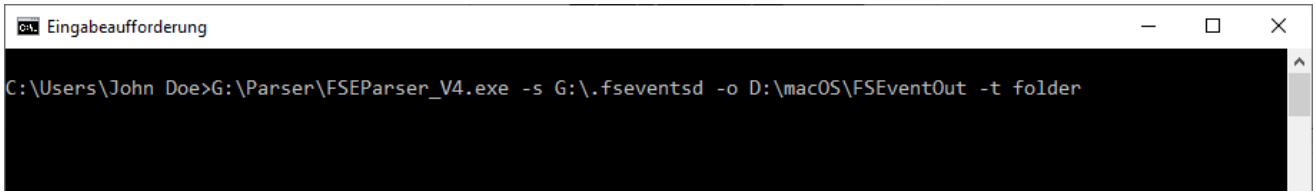


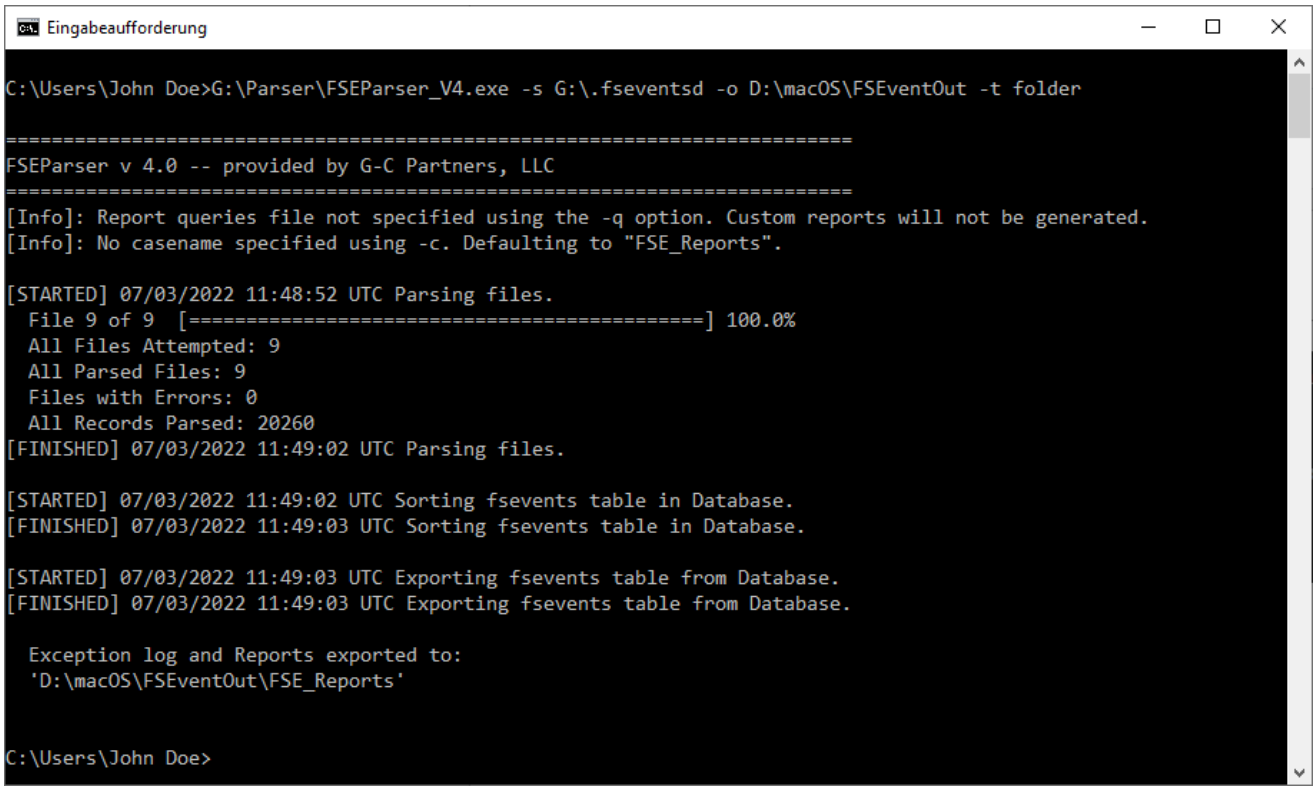
Der FSEventParser benötigt zur Ausgabe ein Verzeichnis, welches vor Nutzung angelegt werden muss.



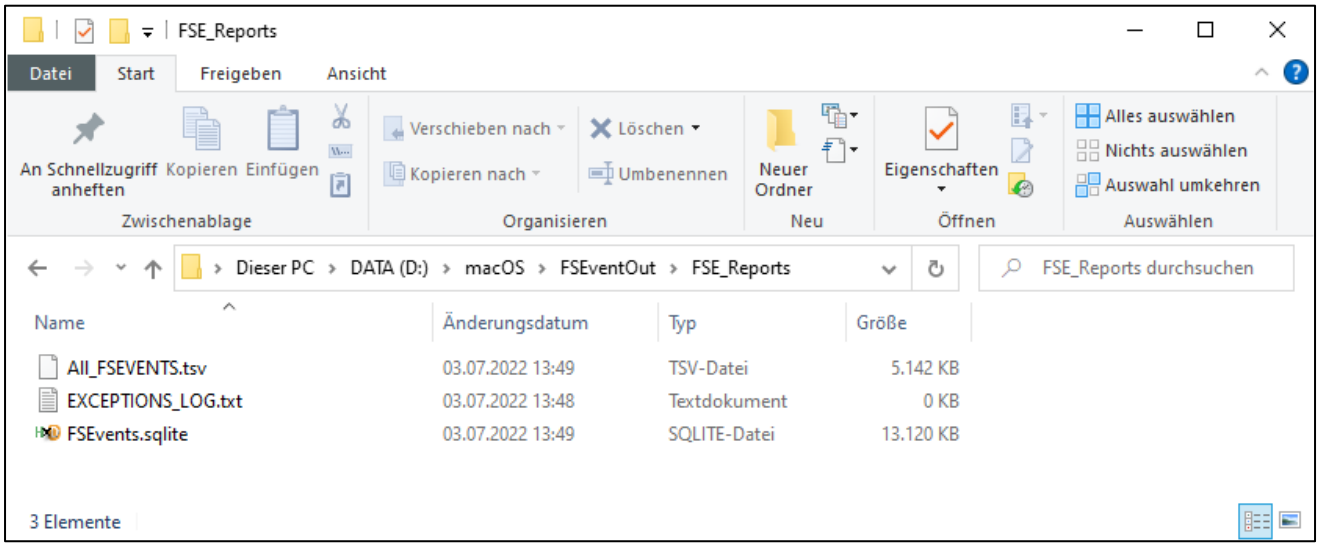
Mit folgendem Befehl kann der FSEvent Parser gestartet werden:

```
\Parser\FSEParser_V4.exe -s G:\.fseventsd -o D:\macOS\FSEventOut\FSE_Reports -t folder
```

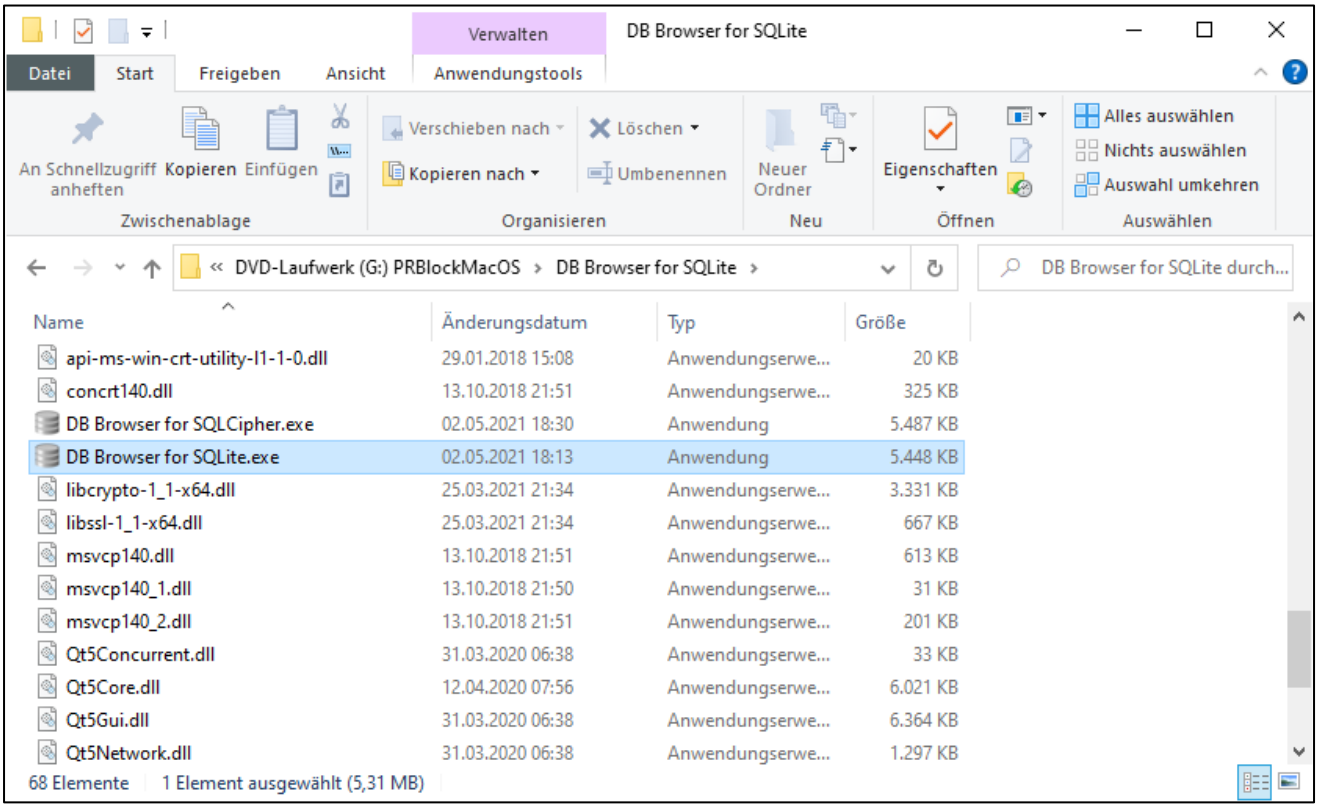


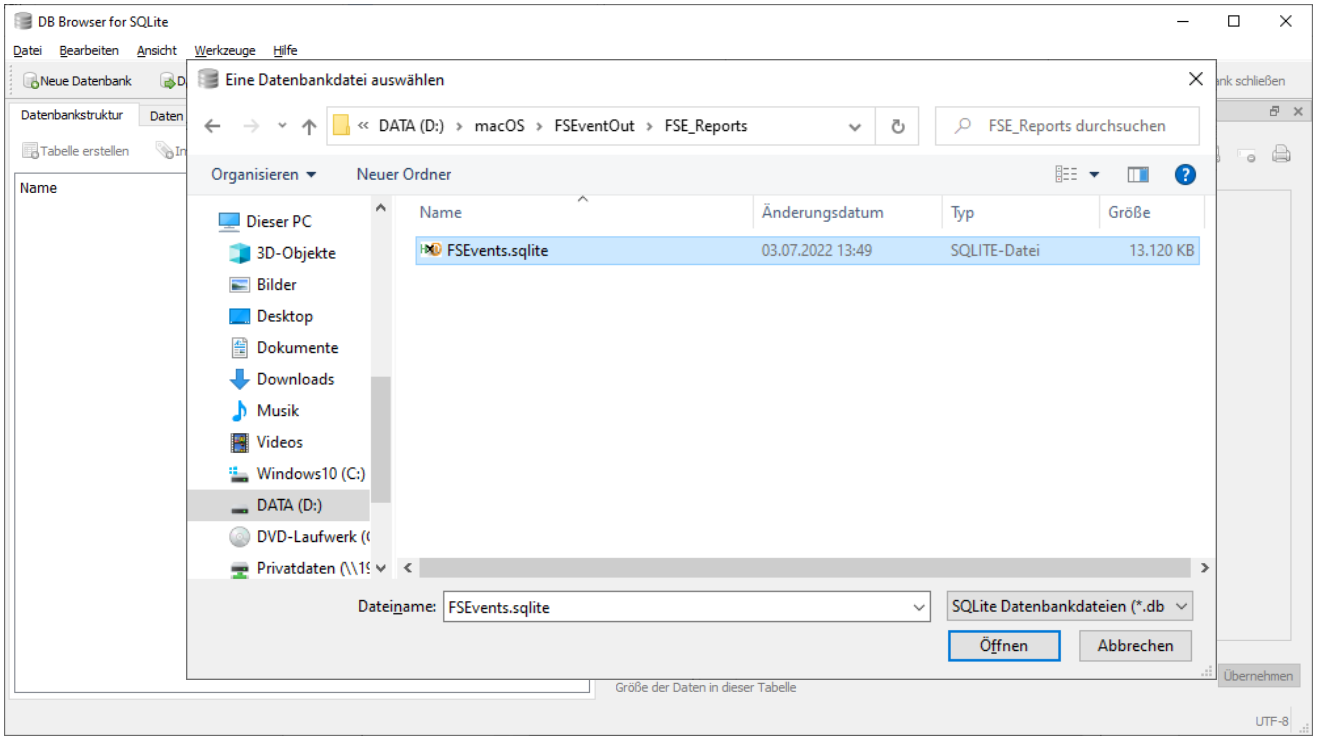


Im Ausgabeverzeichnis erstell der Parser drei Dateien. Ein Errorlog mit Fehleraufzeichnung während der Verarbeitung der Daten und eine CSV Datei sowie eine SQLite Datenbank mit den aufbereiteten FS-Events.

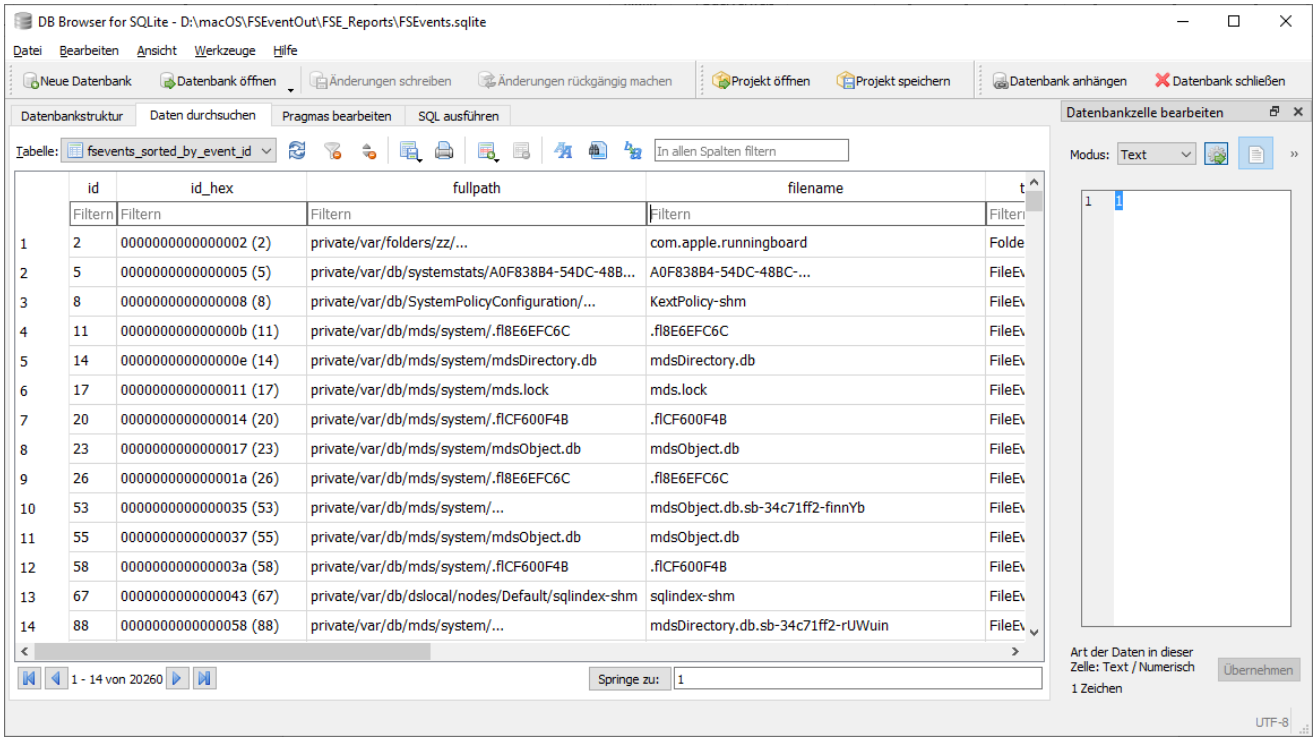


Zur Untersuchung der FSEvent Eintragungen kann nun die Datei **FSEvents.sqlite** herangezogen werden. Diese kann im **DB Browser for SQLite** geöffnet und eingesehen werden.

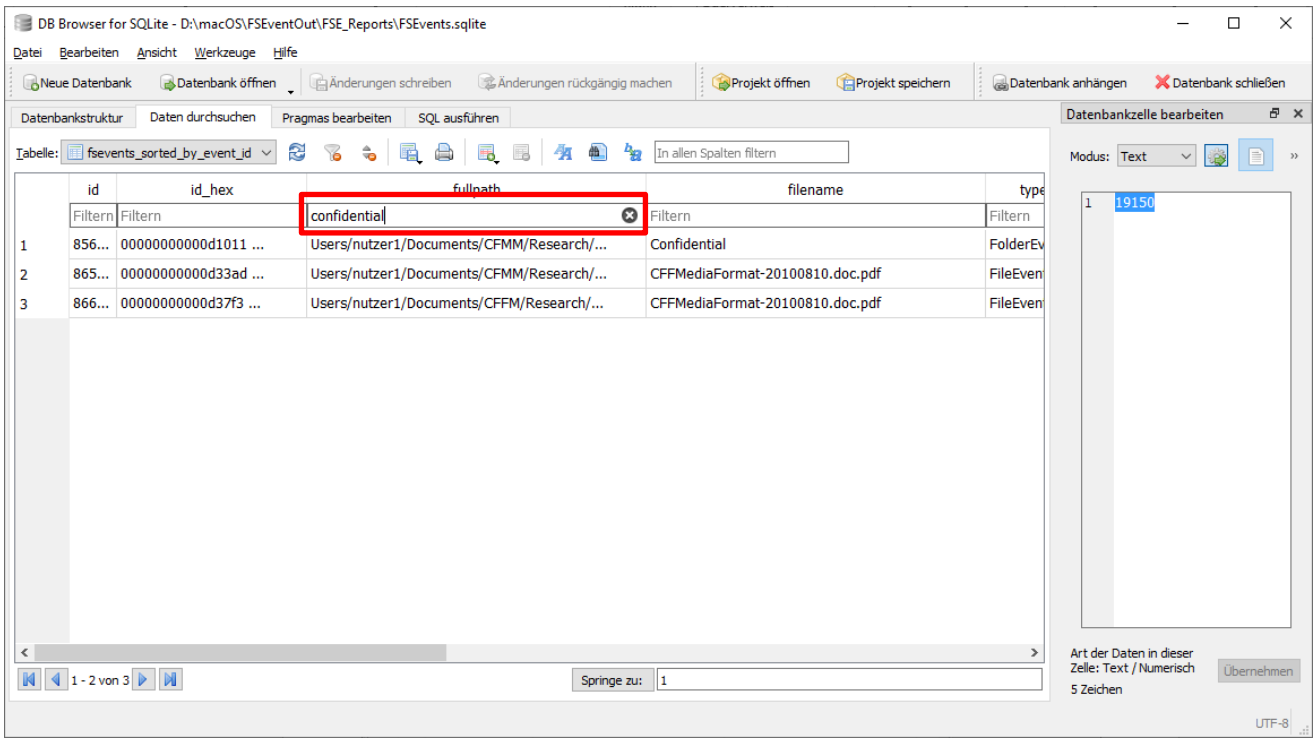




Hier können alle aufgezeichneten Dateisystem Events nachverfolgt werden.

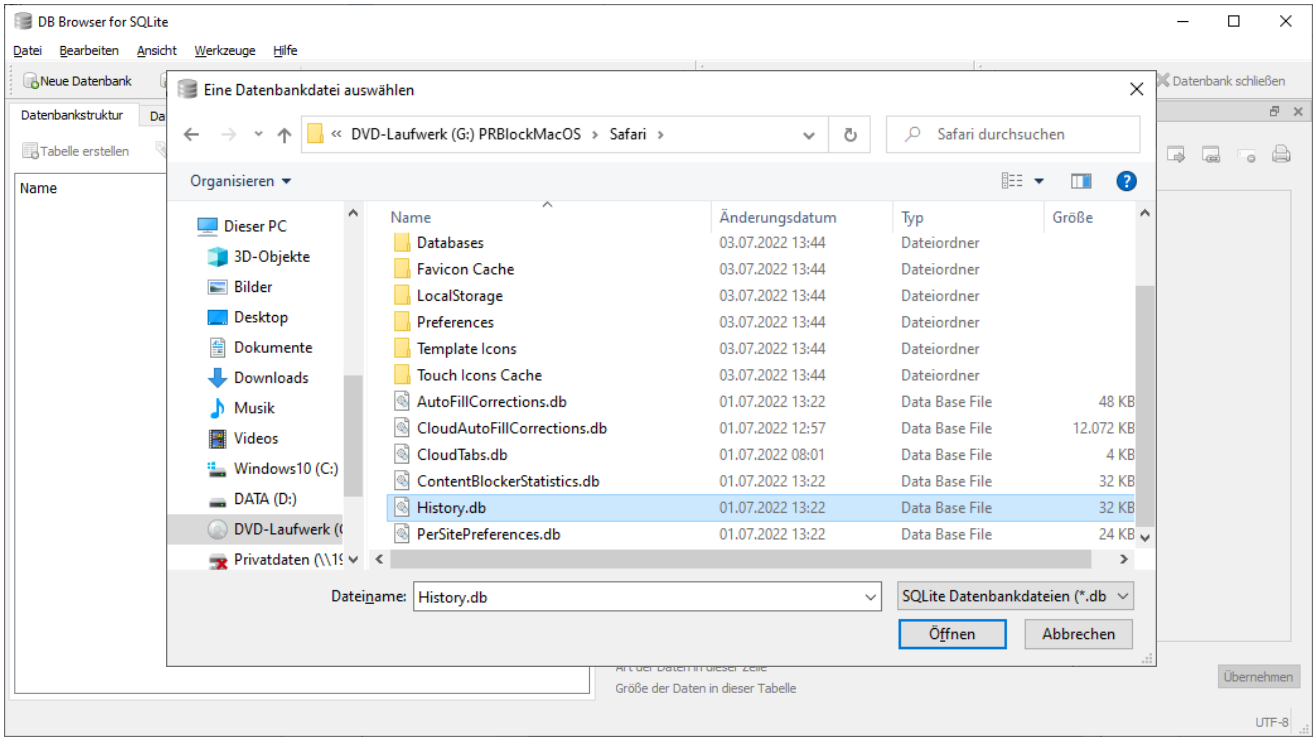


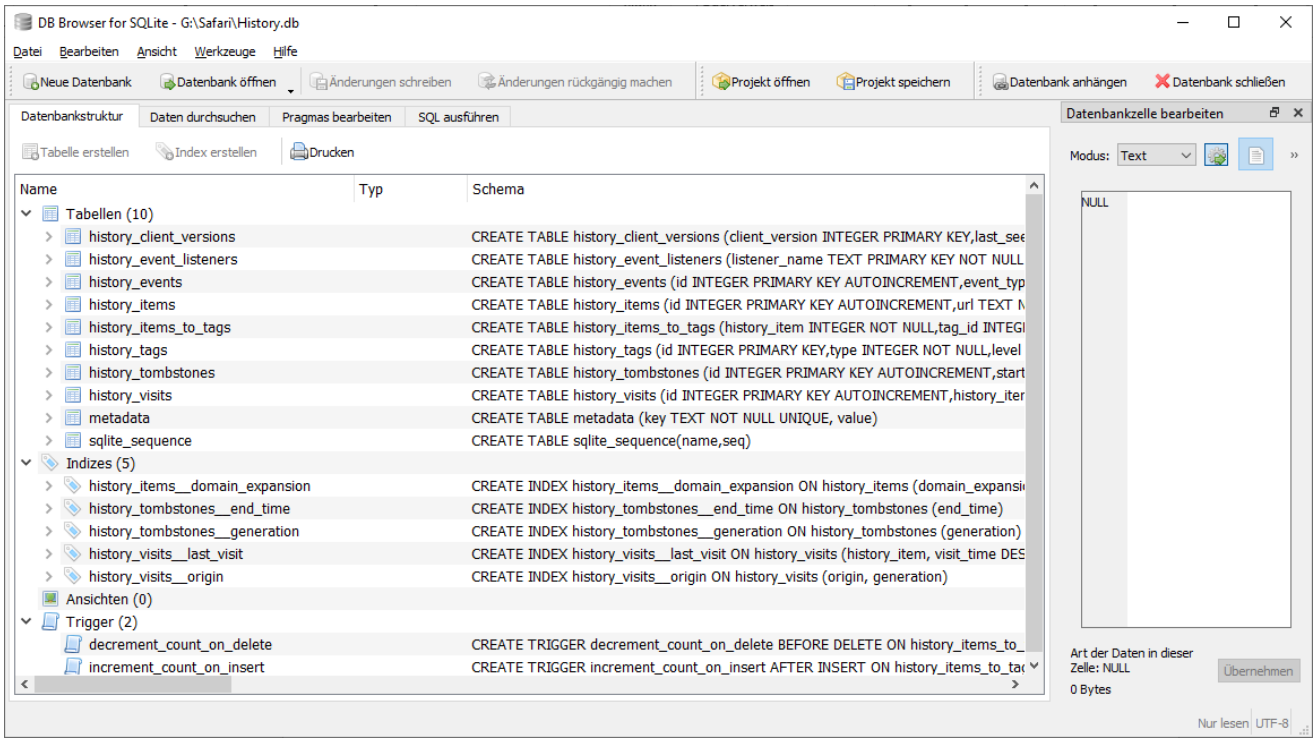
Es gibt sogar die Möglichkeit zu filtern, wie im Beispiel nach **Confidential**.



3.3. UNTERSUCHUNG DER SAFARI HISTORY MIT SQLITE

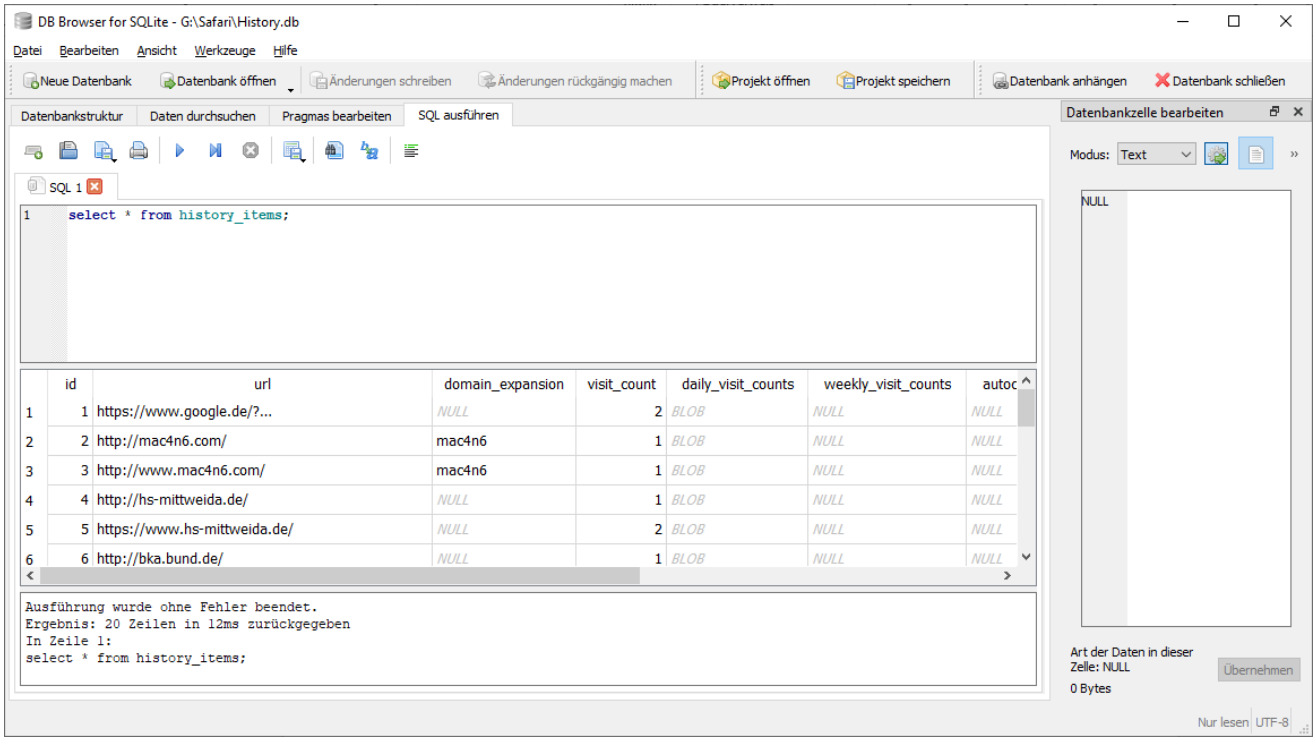
Zur Untersuchung des Safari Browserverlaufs kann die Datei **History.db** herangezogen werden. Diese kann im **DB Browser for SQLite** geöffnet und eingesehen werden.





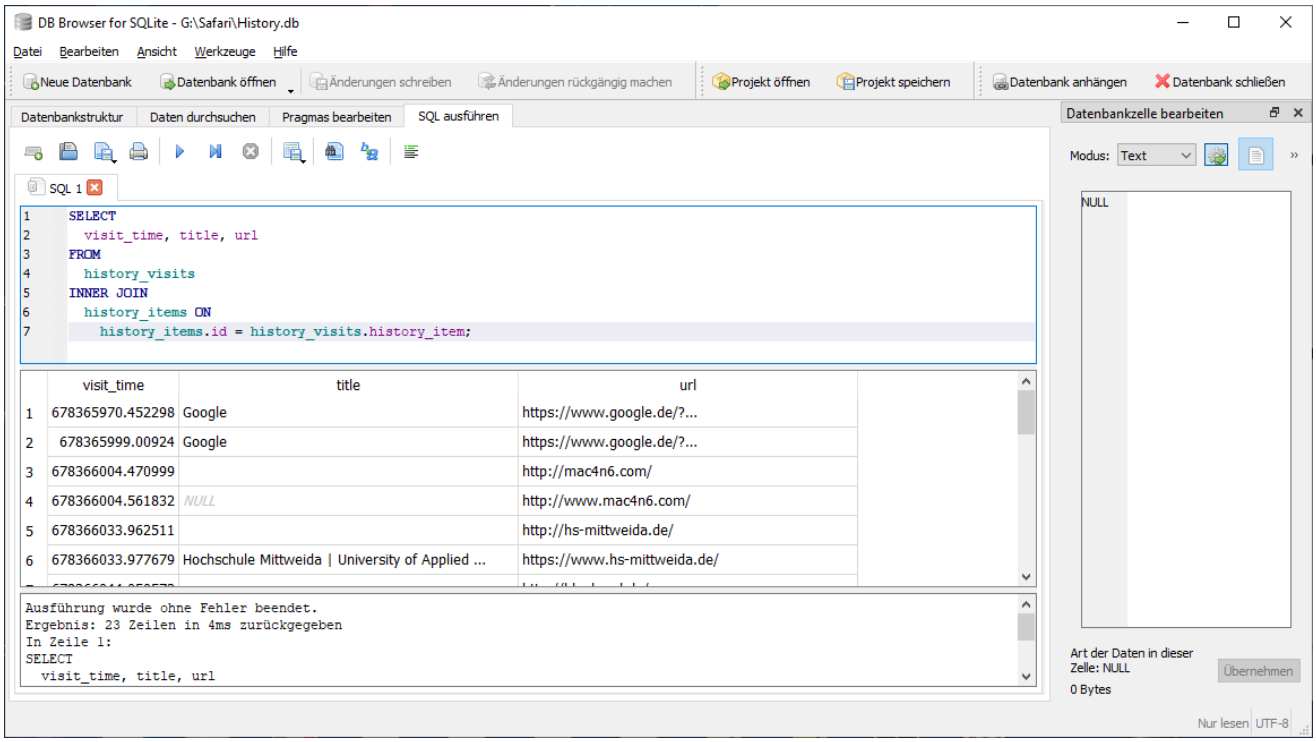
Ausgabe der Tabellen Einträge mit **SELECT** mit wenig verwertbaren forensischen Inhalten.

```
select * from history_items;
```



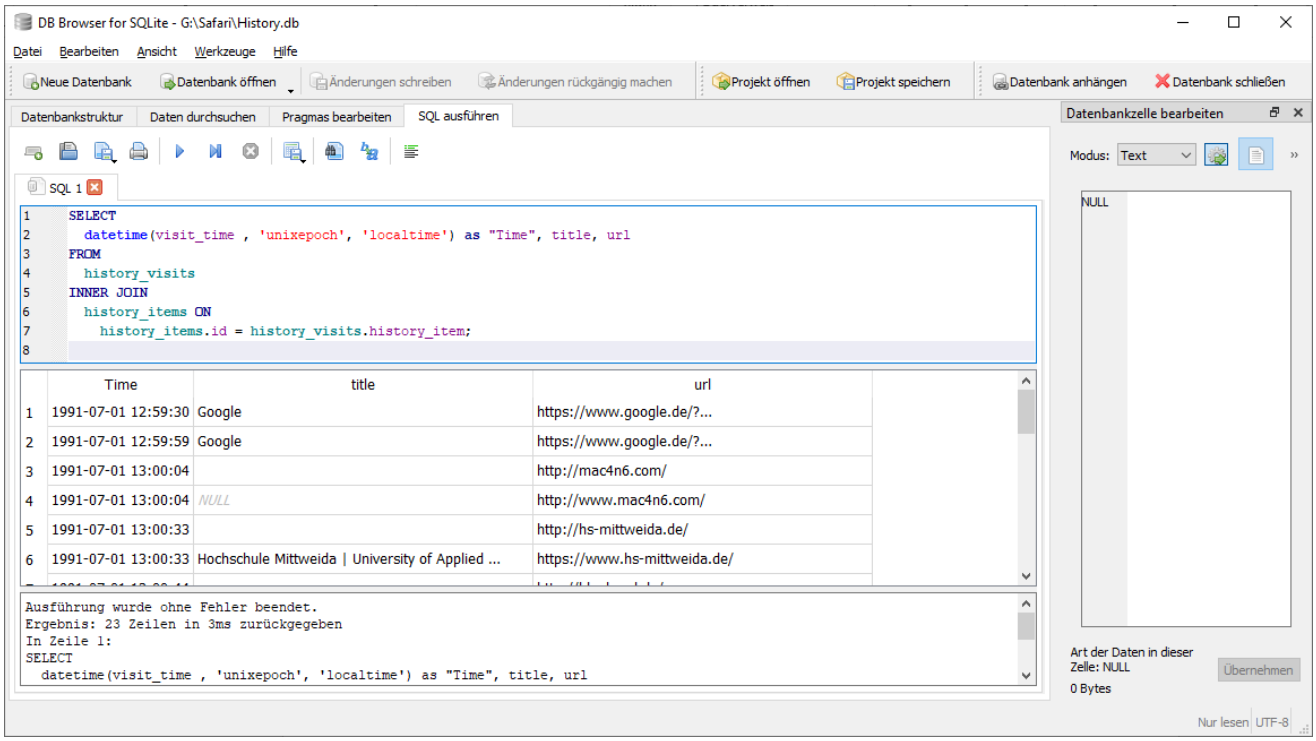
Eine Ausgabe die mehrere Tabellen zusammengefasst (URL, Titel und Abrufdatum) erhält man mit **INNER JOIN**.

```
SELECT   visit_time, title, url

FROM

  history_visits

INNER JOIN

  history_items ON

    history_items.id = history_visits.history_item;
```



Eine Ausgabe der Datumsformate erreicht man mittels d**atetime()** Funktion.

```
SELECT
  datetime(visit_time , 'unixepoch', 'localtime') as "Time", title, url
FROM
  history_visits
INNER JOIN
  history_items ON
    history_items.id = history_visits.history_item;
```



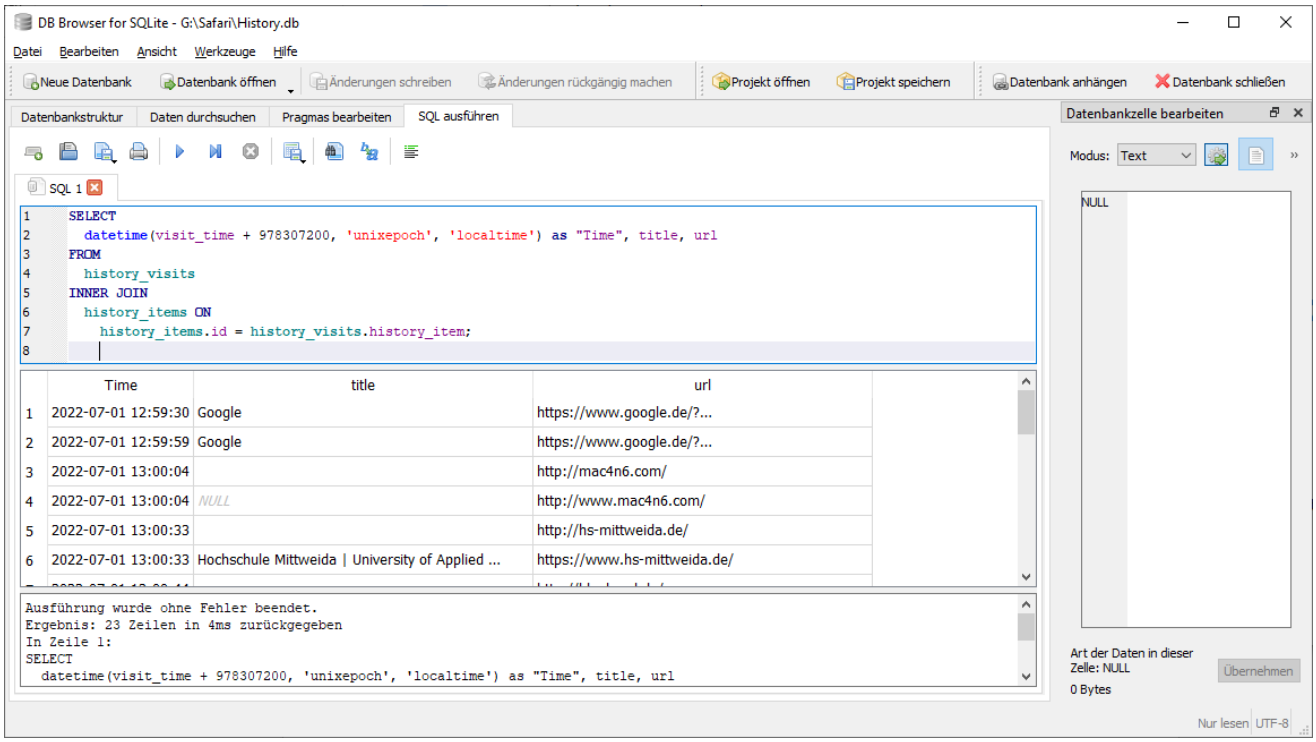
Die Zeitstempel scheinen nicht ganz zu stimmen, betrachtet man das Erscheinungsdatum von macOS BigSur.

Datetime liefert eine **unixepoch Zeit** als Sekunden seit dem 01.01.1970. Die **macepoch Zeit** basiert auf dem 01.01.2001 sozusagen **978.307.200** Sekunden später als die unixepoch Zeit.

Daher lässt sich der korrekte Zeitstempel leicht berechnen:

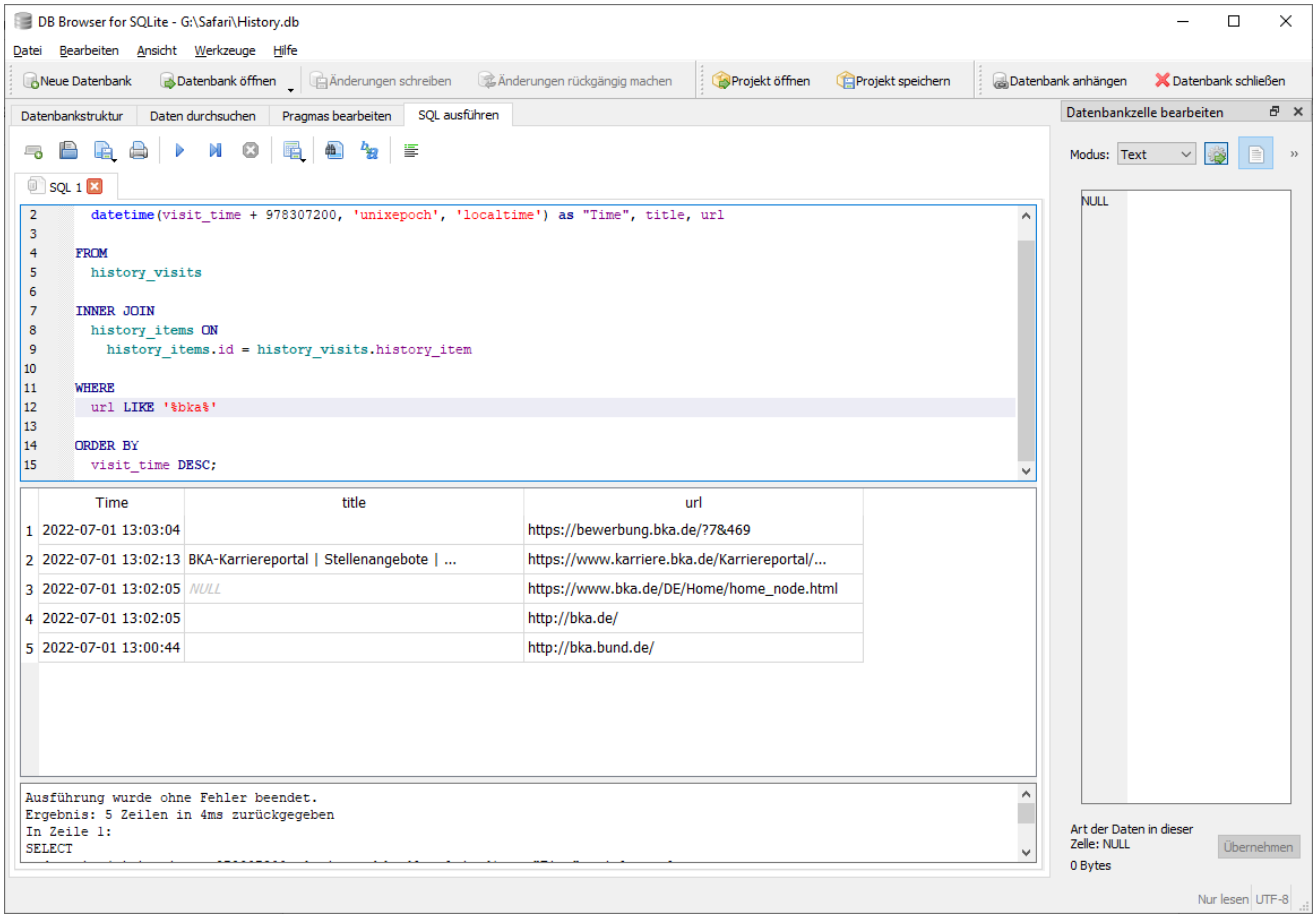
macepoch (cocoa touch / apple base time) **= 'unixepoch' + 978307200**

```
SELECT
  datetime(visit_time + 978307200, 'unixepoch', 'localtime') as "Time", title, url
FROM
  history_visits
INNER JOIN
  history_items ON
    history_items.id = history_visits.history_item;
```

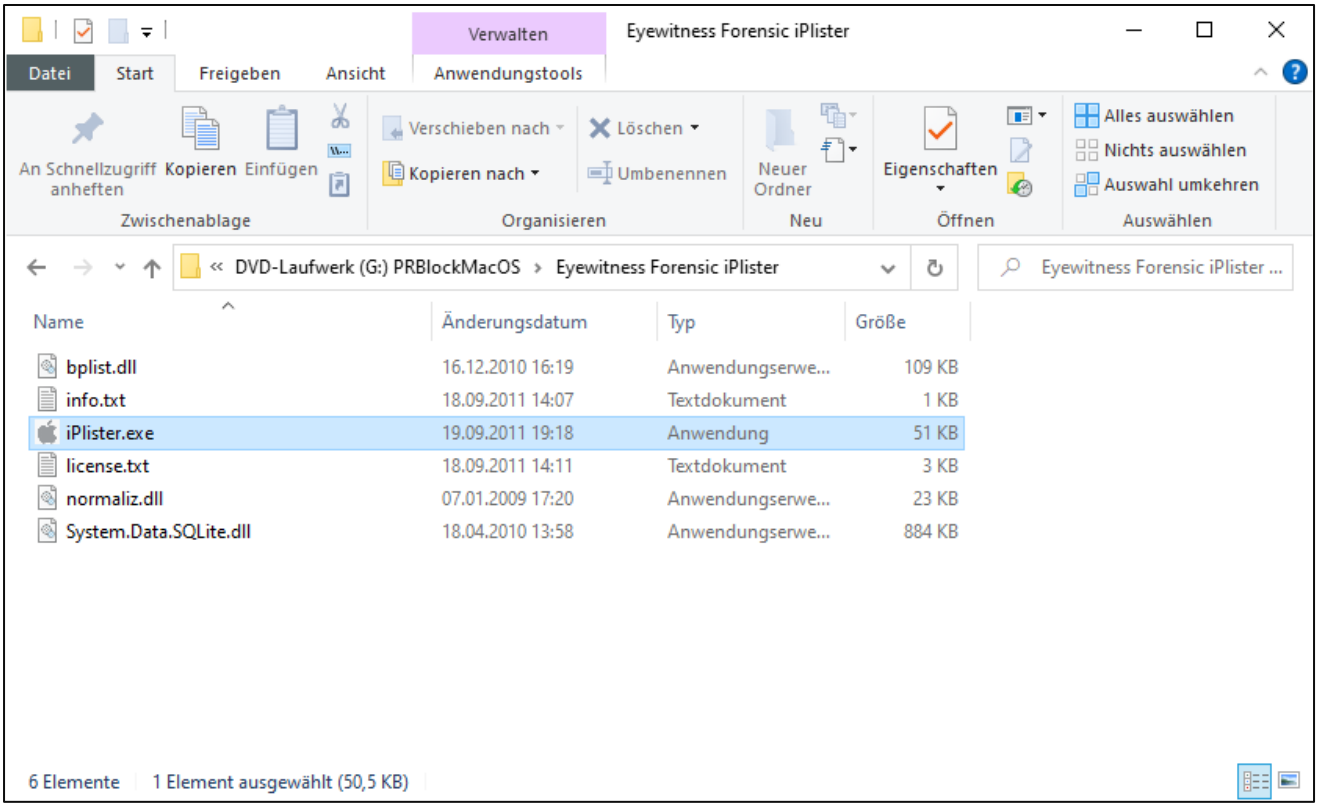


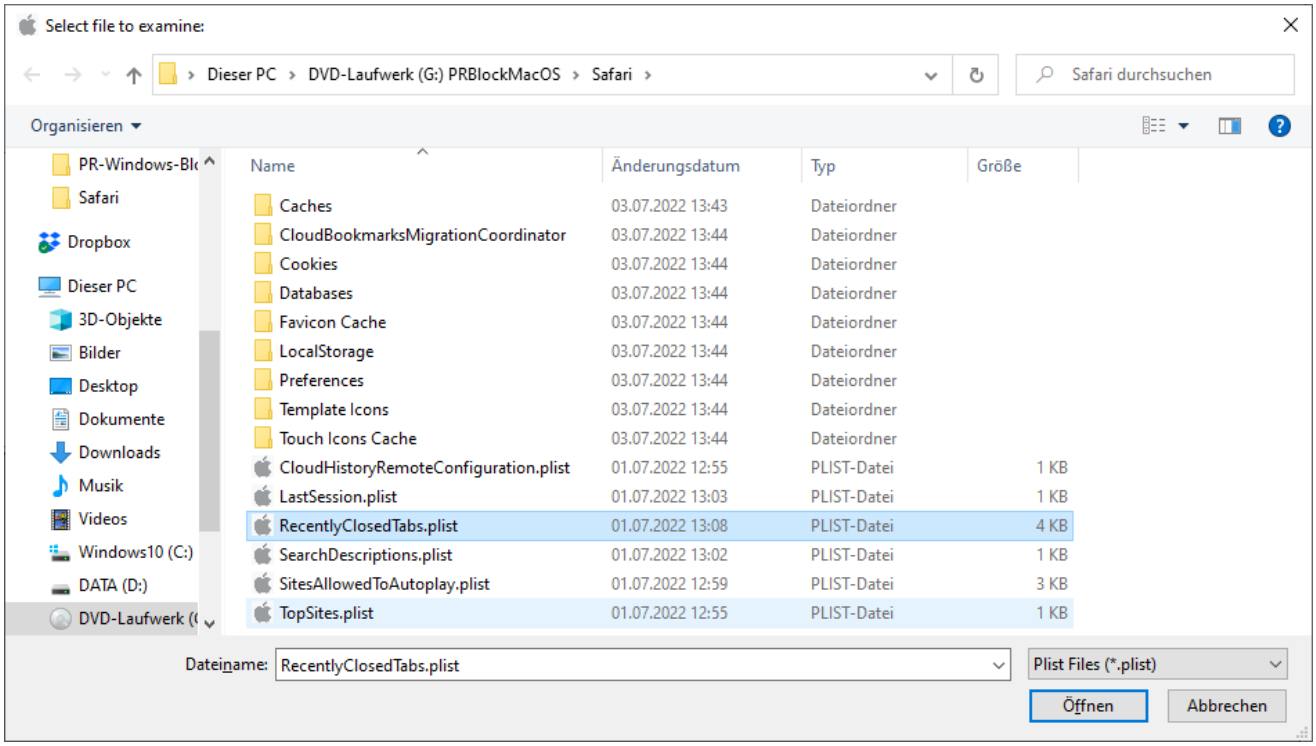
Mit den Abfragen ist auch eine **gezielte Suche** nach Inhalten möglich, im Beispiel **nach BKA** zeitlich geordnet:

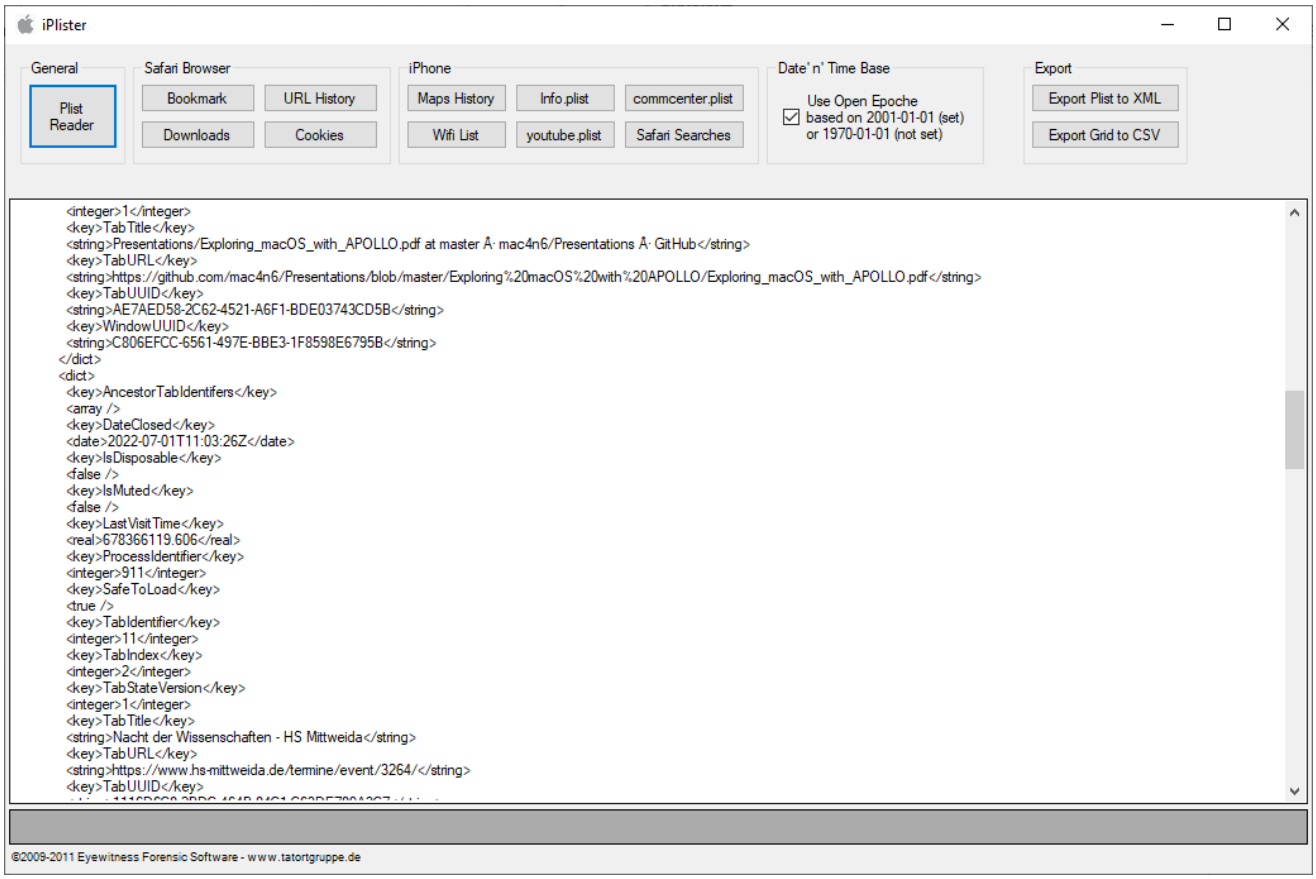
```
SELECT
  datetime(visit_time + 978307200, 'unixepoch', 'localtime') as "Time", title, url
FROM
  history_visits
INNER JOIN
  history_items ON
    history_items.id = history_visits.history_item
WHERE
  url LIKE '%bka%'
ORDER BY
  visit_time DESC;
```



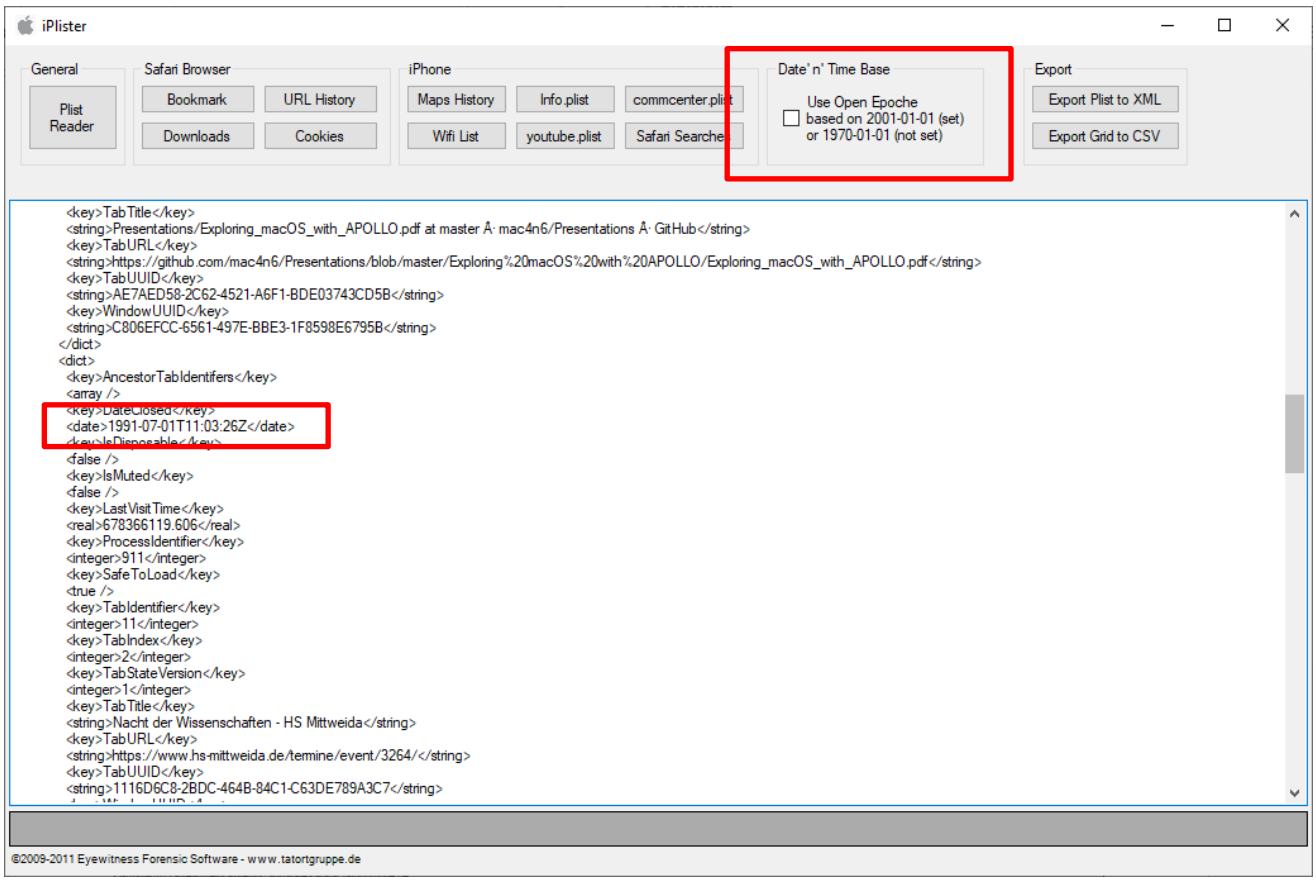
Zudem können mit dem iPlister die Binary Plist Dateien im Safari Verzeichnis ebenfalls noch eingesehen werden:





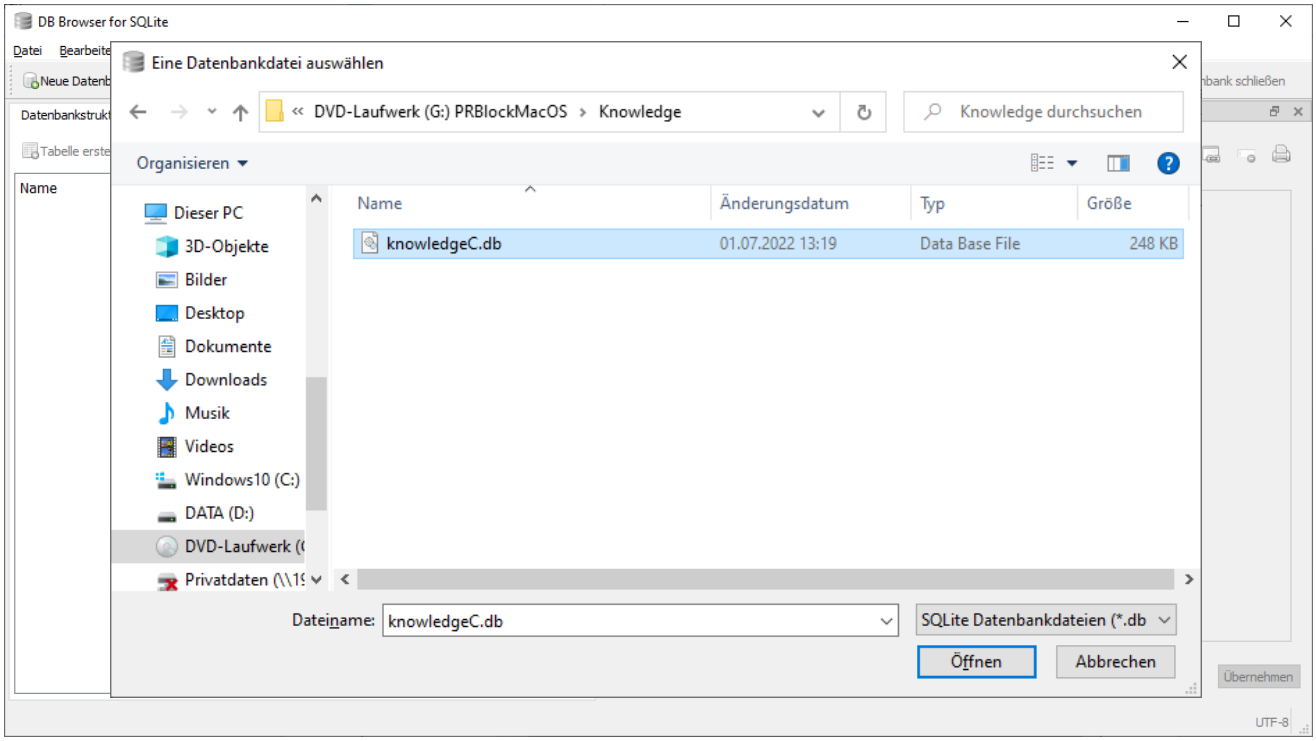


Eine Umschaltung der Datumsformate zwischen Unix Zeit und Mac Base Zeit ist möglich (Datei erneut einlesen erforderlich).

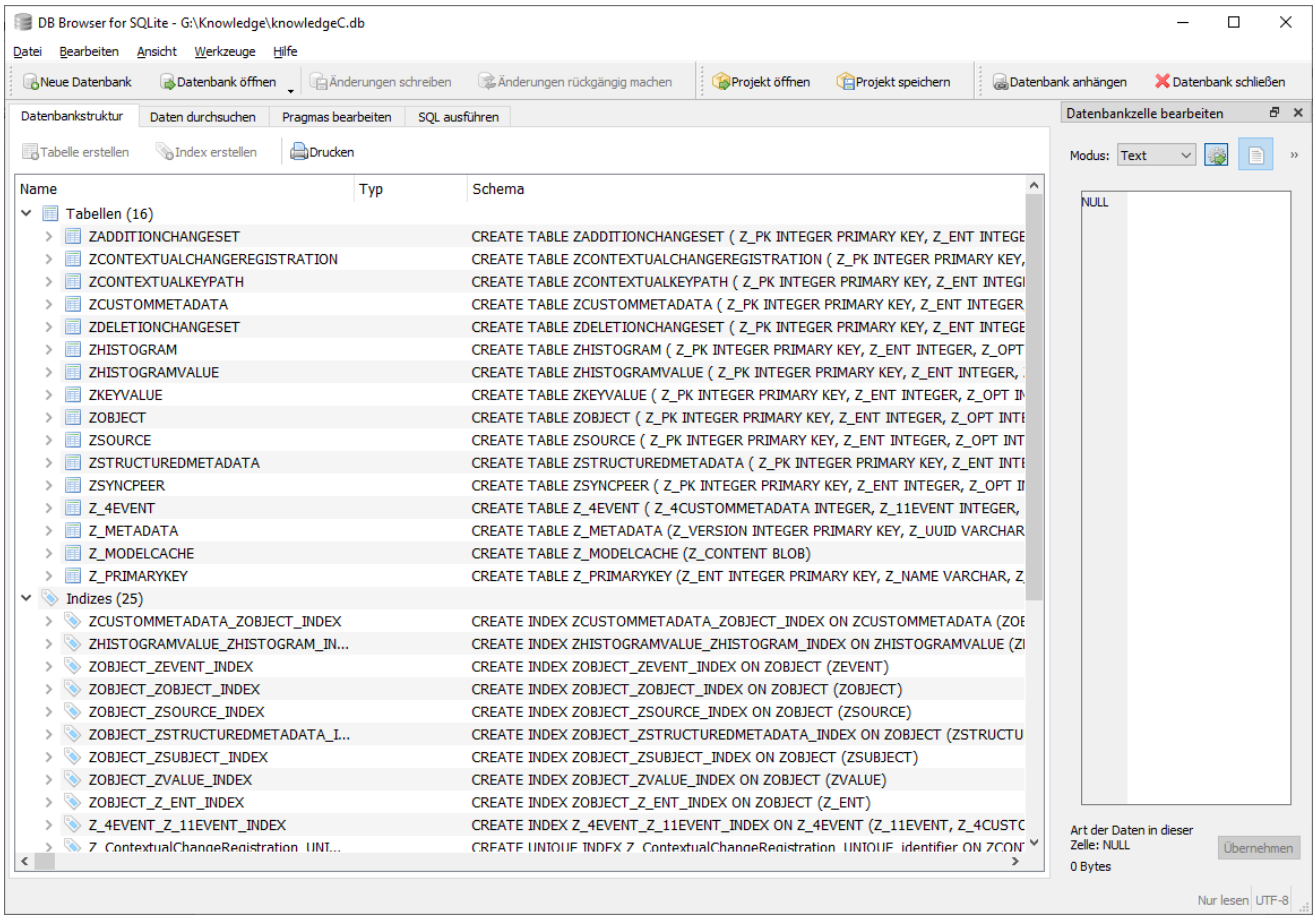


3.4. UNTERSUCHUNG DER DATENBANKDATEI KNOWLEDGEC.DB MIT SQLITE

Zur Untersuchung der Pattern of Life Informationen kann die Datei **KnowledgeC.db** herangezogen werden. Diese kann im **DB Browser for SQLite** geöffnet und eingesehen werden.

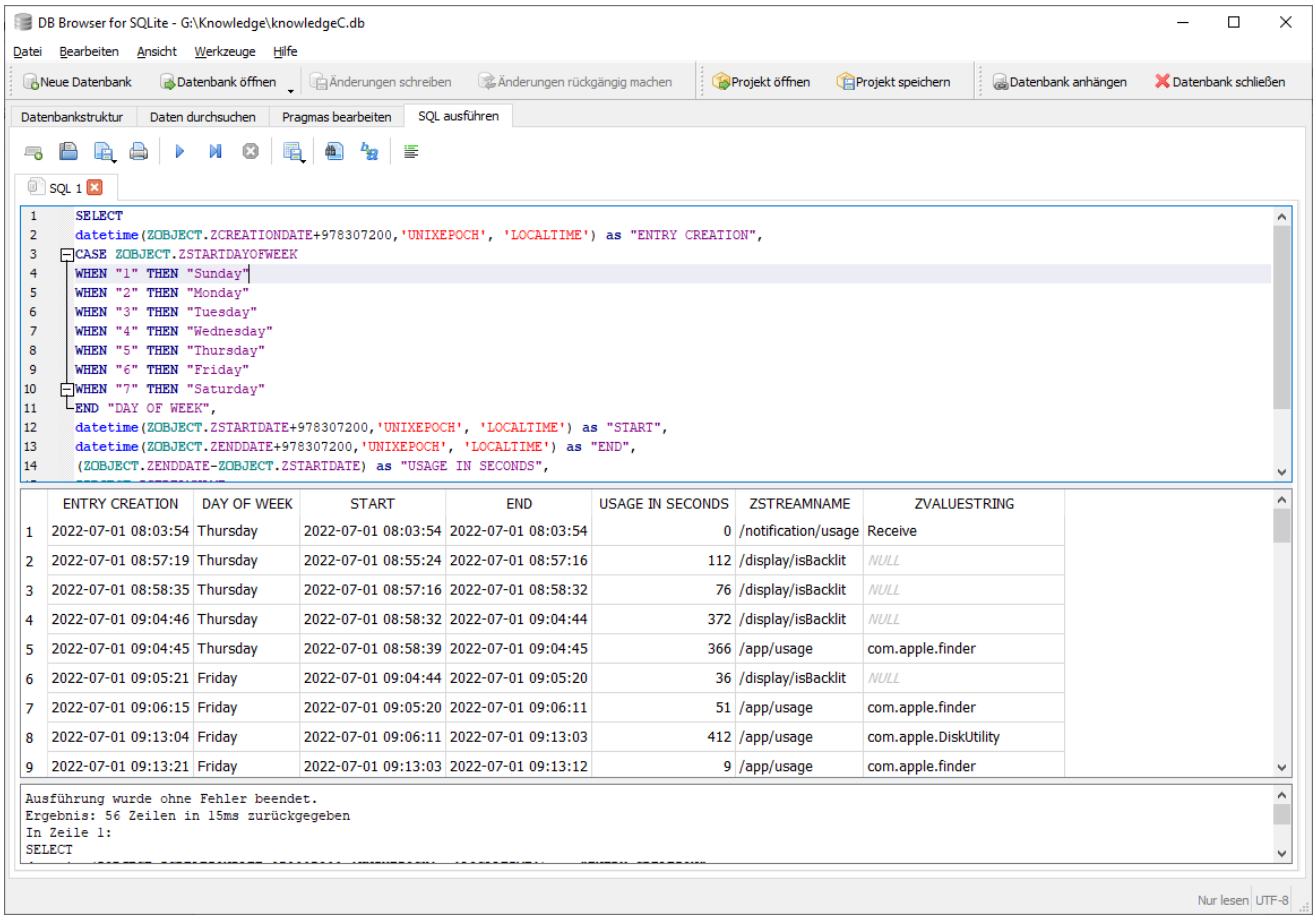


Die Datenbank beinhaltet sehr viele zusammenzuführende Tabellen.



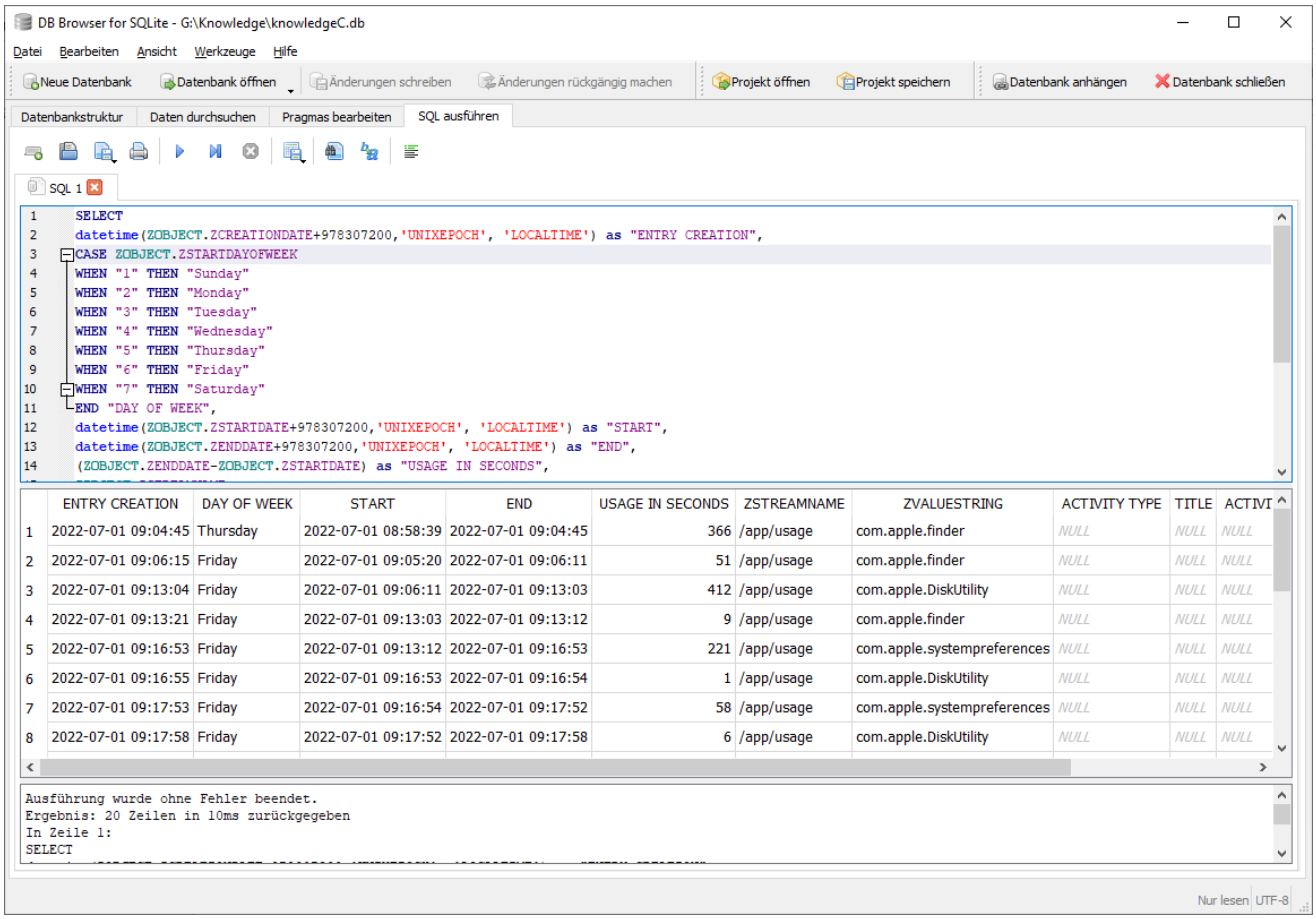
Folgender SQL Befehl stellt die **wichtigsten Eintragungen im Überblick** dar:

```
SELECT
datetime(ZOBJECT.ZCREATIONDATE+978307200,'UNIXEPOCH', 'LOCALTIME') as "ENTRY
CREATION",
CASE ZOBJECT.ZSTARTDAYOFWEEK
WHEN "1" THEN "Sunday"
WHEN "2" THEN "Monday"
WHEN "3" THEN "Tuesday"
WHEN "4" THEN "Wednesday"
WHEN "5" THEN "Thursday"
WHEN "6" THEN "Friday"
WHEN "7" THEN "Saturday"
END "DAY OF WEEK",
datetime(ZOBJECT.ZSTARTDATE+978307200,'UNIXEPOCH', 'LOCALTIME') as "START",
datetime(ZOBJECT.ZENDDATE+978307200,'UNIXEPOCH', 'LOCALTIME') as "END",
(ZOBJECT.ZENDDATE-ZOBJECT.ZSTARTDATE) as "USAGE IN SECONDS",
ZOBJECT.ZSTREAMNAME,
ZOBJECT.ZVALUESTRING
FROM ZOBJECT
ORDER BY "START"
```



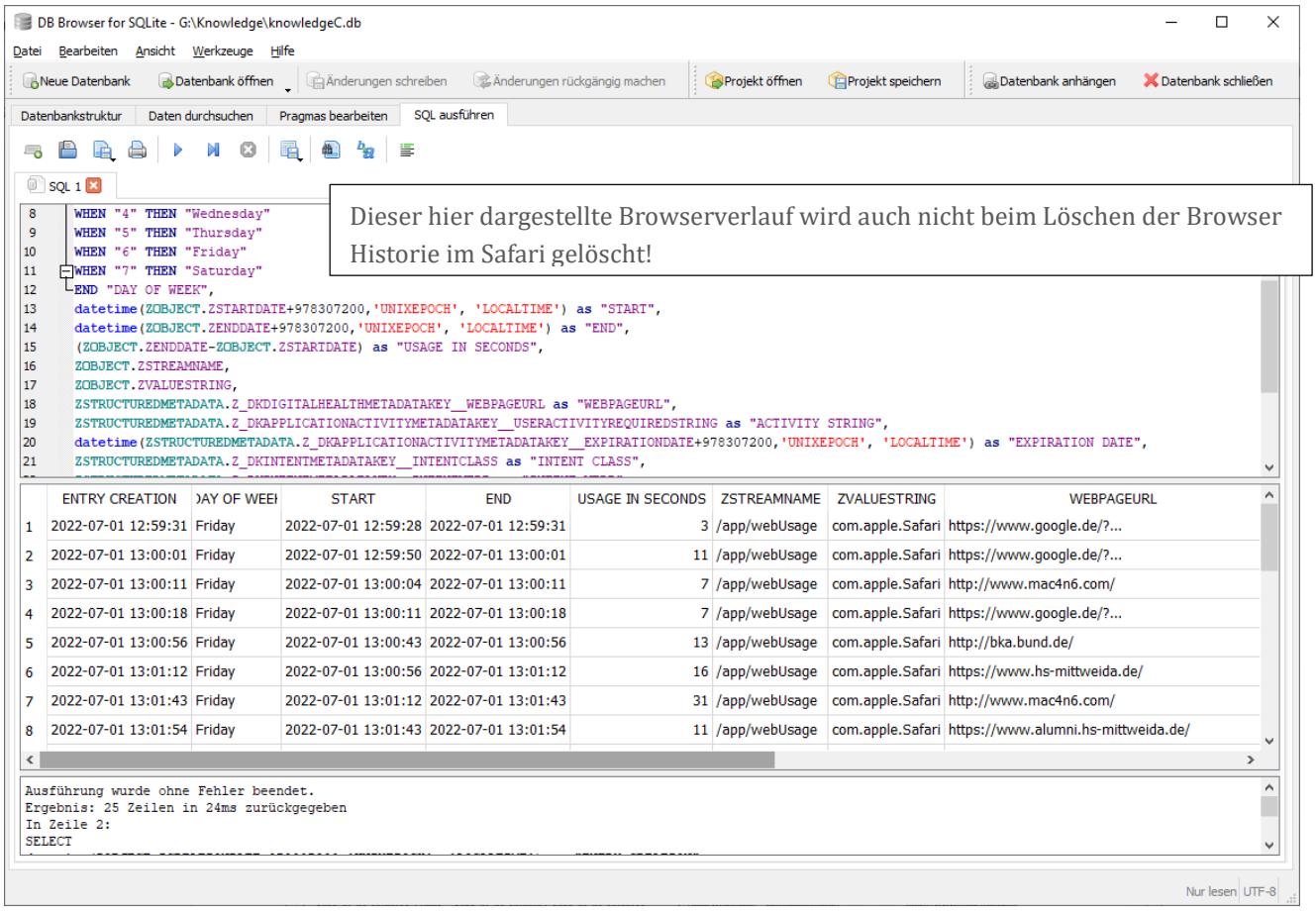
Folgender SQL Befehl zeigt die **Nutzung der Apps** an:

```
SELECT
datetime(ZOBJECT.ZCREATIONDATE+978307200,'UNIXEPOCH', 'LOCALTIME') as "ENTRY
CREATION",
CASE ZOBJECT.ZSTARTDAYOFWEEK
WHEN "1" THEN "Sunday"
WHEN "2" THEN "Monday"
WHEN "3" THEN "Tuesday"
WHEN "4" THEN "Wednesday"
WHEN "5" THEN "Thursday"
WHEN "6" THEN "Friday"
WHEN "7" THEN "Saturday"
END "DAY OF WEEK",
datetime(ZOBJECT.ZSTARTDATE+978307200,'UNIXEPOCH', 'LOCALTIME') as "START",
datetime(ZOBJECT.ZENDDATE+978307200,'UNIXEPOCH', 'LOCALTIME') as "END",
(ZOBJECT.ZENDDATE-ZOBJECT.ZSTARTDATE) as "USAGE IN SECONDS",
ZOBJECT.ZSTREAMNAME,
ZOBJECT.ZVALUESTRING,
ZSTRUCTUREDMETADATA.Z_DKAPPLICATIONACTIVITYMETADATAKEY__ACTIVITYTYPE AS "ACTIVITY
TYPE",
ZSTRUCTUREDMETADATA.Z_DKAPPLICATIONACTIVITYMETADATAKEY__TITLE as "TITLE",
ZSTRUCTUREDMETADATA.Z_DKAPPLICATIONACTIVITYMETADATAKEY__USERACTIVITYREQUIREDSTRING as
"ACTIVITY STRING",
datetime(ZSTRUCTUREDMETADATA.Z_DKAPPLICATIONACTIVITYMETADATAKEY__EXPIRATIONDATE+978307
200,'UNIXEPOCH', 'LOCALTIME') as "EXPIRATION DATE"
FROM ZOBJECT
left join ZSTRUCTUREDMETADATA on ZOBJECT.ZSTRUCTUREDMETADATA =
ZSTRUCTUREDMETADATA.Z_PK
WHERE ZSTREAMNAME is "/app/usage"
ORDER BY "START"
```



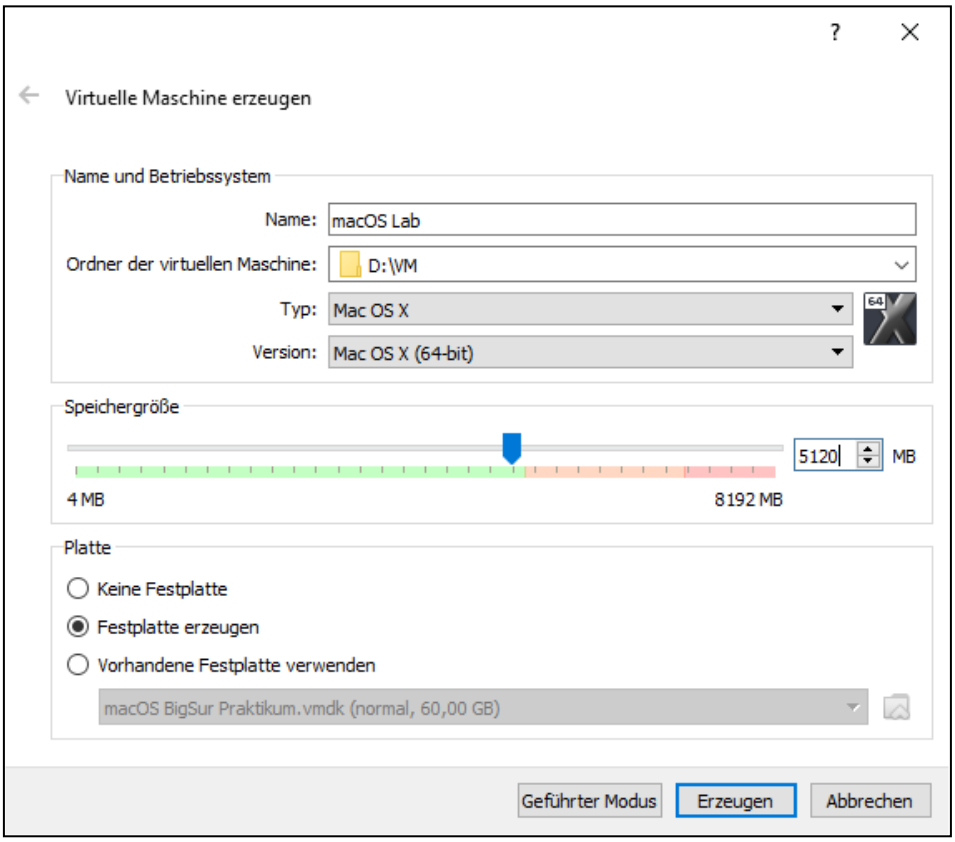
Folgender SQL Befehl zeigt die **Nutzung des Safari Browsers** und deren **aufgerufener URL** an:

```
SELECT
datetime(ZOBJECT.ZCREATIONDATE+978307200,'UNIXEPOCH', 'LOCALTIME') as "ENTRY
CREATION",
CASE ZOBJECT.ZSTARTDAYOFWEEK
WHEN "1" THEN "Sunday"
WHEN "2" THEN "Monday"
WHEN "3" THEN "Tuesday"
WHEN "4" THEN "Wednesday"
WHEN "5" THEN "Thursday"
WHEN "6" THEN "Friday"
WHEN "7" THEN "Saturday"
END "DAY OF WEEK",
datetime(ZOBJECT.ZSTARTDATE+978307200,'UNIXEPOCH', 'LOCALTIME') as "START",
datetime(ZOBJECT.ZENDDATE+978307200,'UNIXEPOCH', 'LOCALTIME') as "END",
(ZOBJECT.ZENDDATE-ZOBJECT.ZSTARTDATE) as "USAGE IN SECONDS",
ZOBJECT.ZSTREAMNAME,
ZOBJECT.ZVALUESTRING,
ZSTRUCTUREDMETADATA.Z_DKDIGITALHEALTHMETADATAKEY__WEBPAGEURL as "WEBPAGEURL",
ZSTRUCTUREDMETADATA.Z_DKAPPLICATIONACTIVITYMETADATAKEY__USERACTIVITYREQUIREDSTRING as
"ACTIVITY STRING",
datetime(ZSTRUCTUREDMETADATA.Z_DKAPPLICATIONACTIVITYMETADATAKEY__EXPIRATIONDATE+978307
200,'UNIXEPOCH', 'LOCALTIME') as "EXPIRATION DATE",
ZSTRUCTUREDMETADATA.Z_DKINTENTMETADATAKEY__INTENTCLASS as "INTENT CLASS",
ZSTRUCTUREDMETADATA.Z_DKINTENTMETADATAKEY__INTENTVERB as "INTENT VERB",
ZSTRUCTUREDMETADATA.Z_DKINTENTMETADATAKEY__SERIALIZEDINTERACTION as "SERIALIZED
INTERACTION",
ZSOURCE.ZBUNDLEID
FROM ZOBJECT
left join ZSTRUCTUREDMETADATA on ZOBJECT.ZSTRUCTUREDMETADATA =
ZSTRUCTUREDMETADATA.Z_PK
left join ZSOURCE on ZOBJECT.ZSOURCE = ZSOURCE.Z_PK
WHERE ZSTREAMNAME is "/app/webUsage"
ORDER BY "START"
```

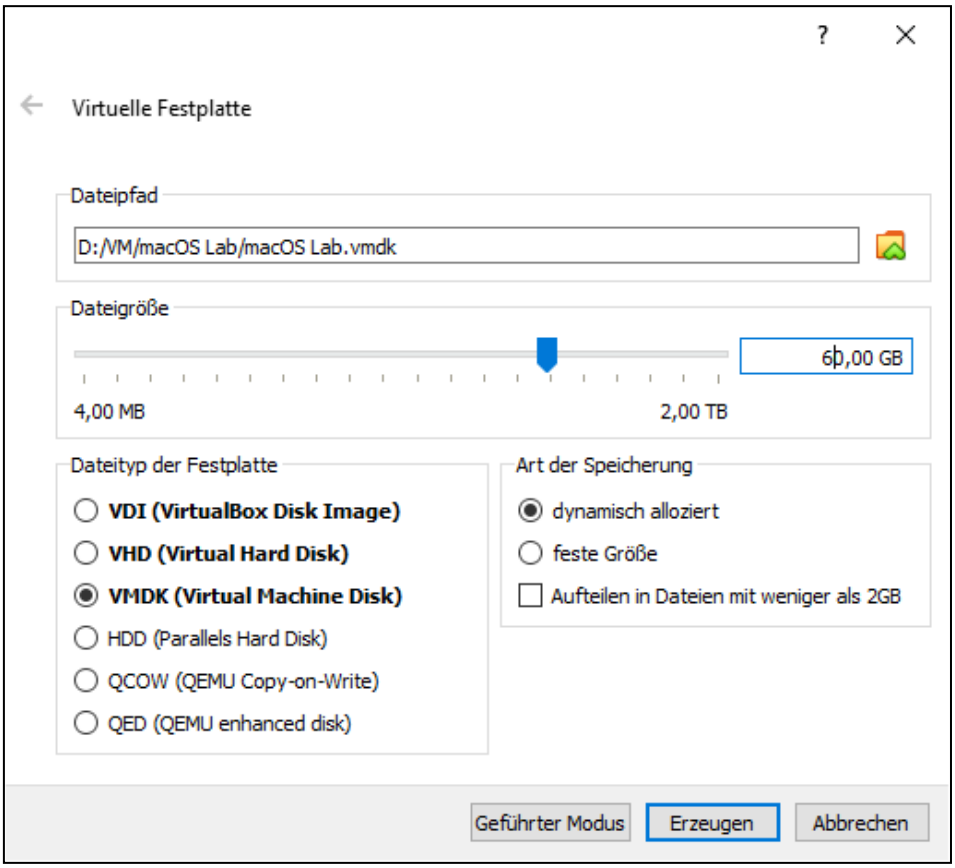


4. ERSTELLUNG EINER MACOS LAB VM IN VIRTUALBOX (UNTER WINDOWS)

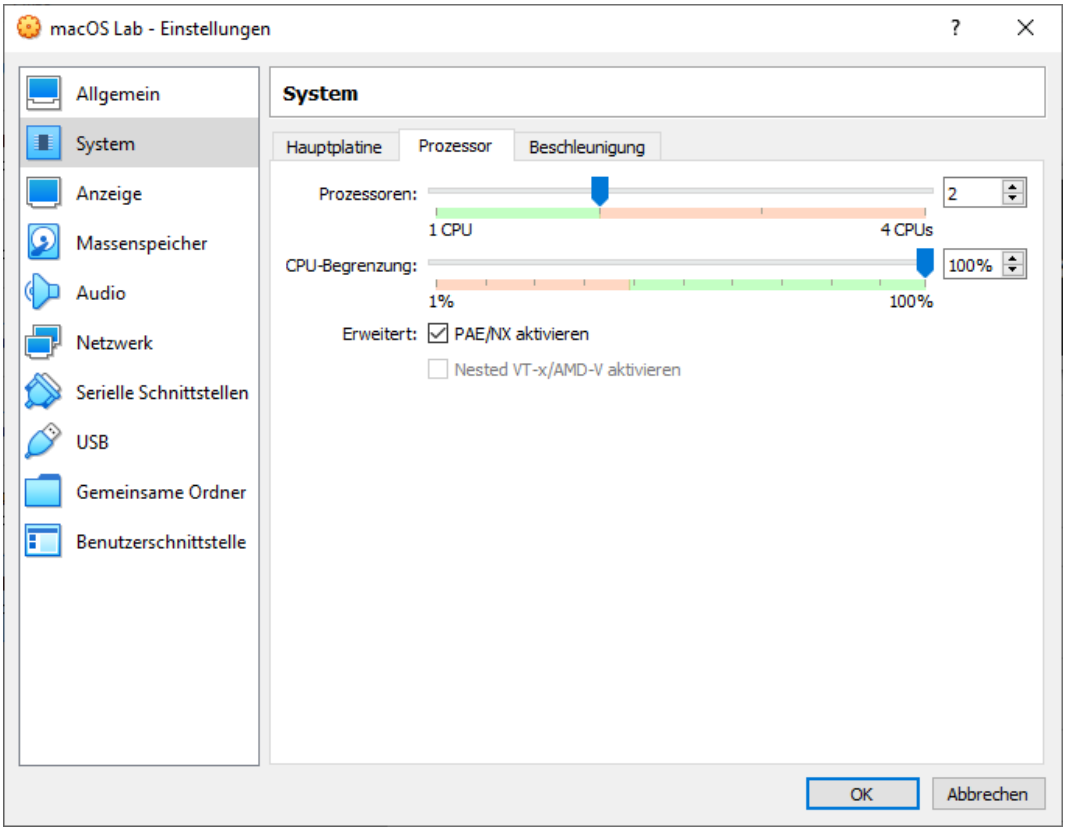
In VirtualBox **Neu** wählen und folgende Einstellungen vornehmen (wichtig mindestens 4GB RAM).



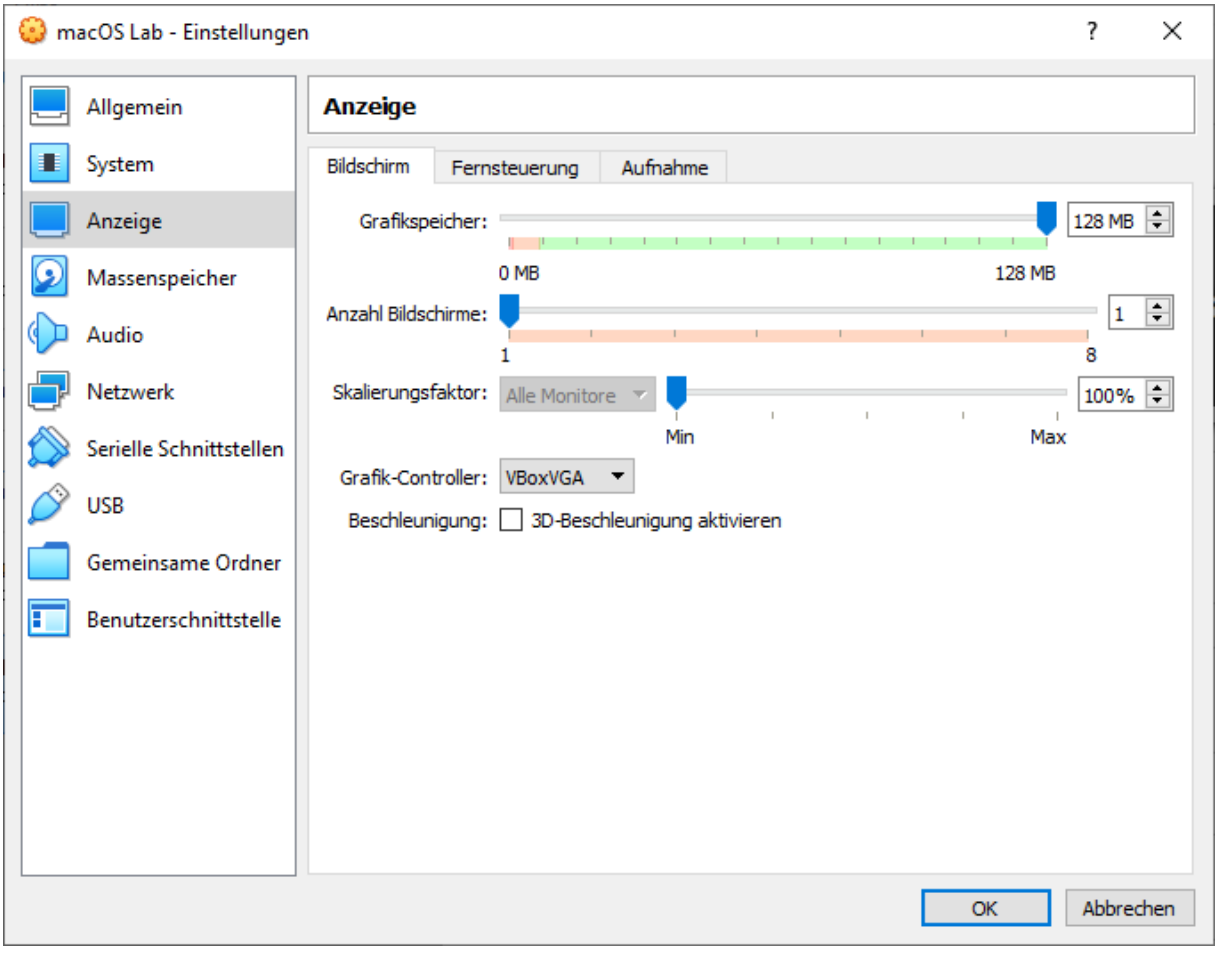
Festplatte erzeugen als VMDK und dynamische Größe mindestens 60 GB.



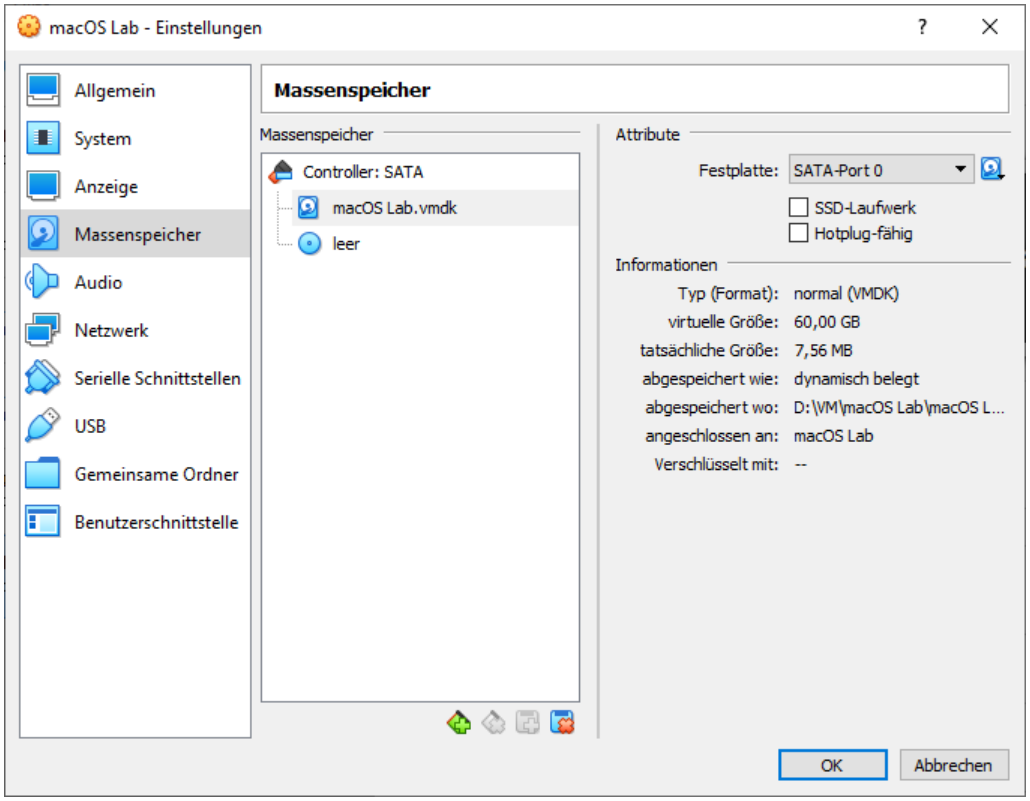
System Einstellung mininmal 2 CPUs

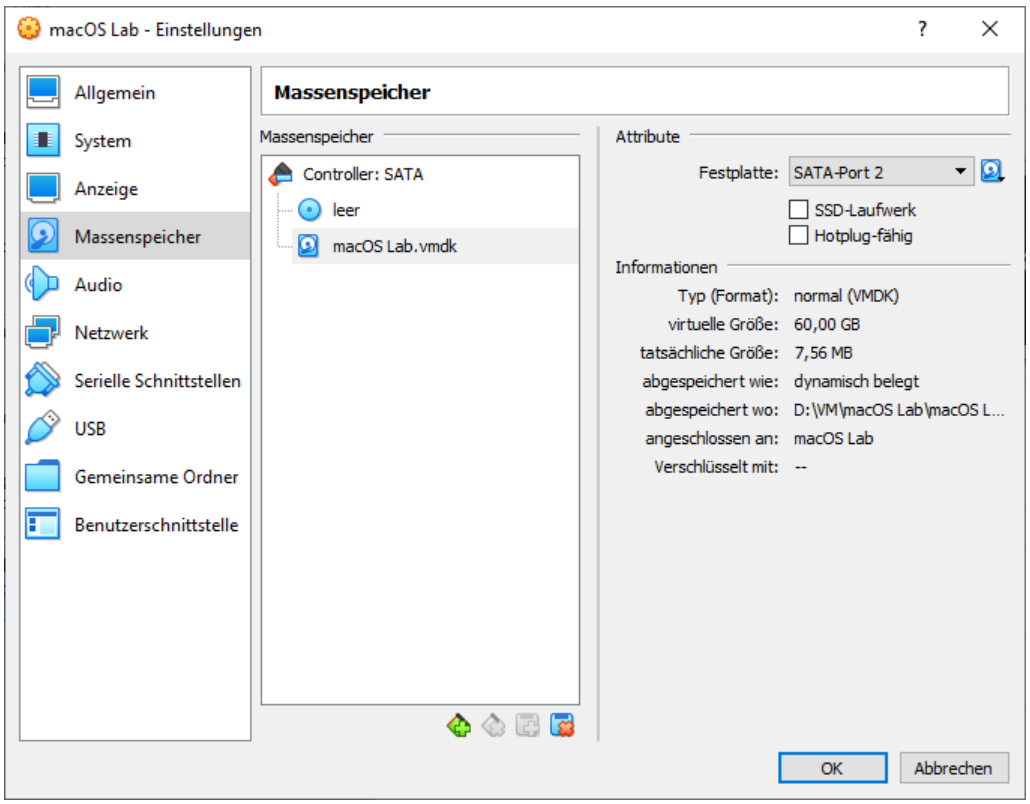


Anzeige Einstellunge Grphik Speicher 128 MB.

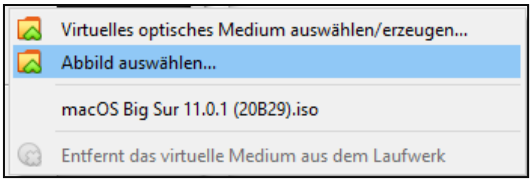


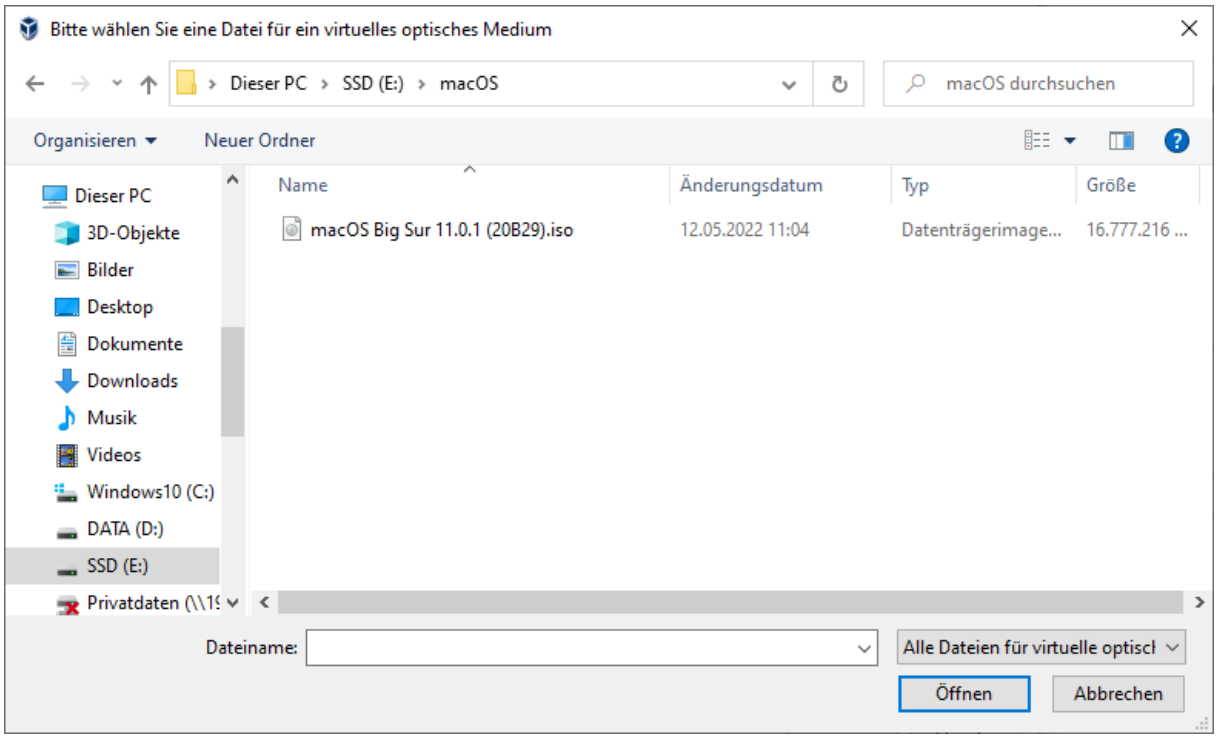
Massenspeicher **macOS Lab.vmdk** von **SATA-Port 0** auf 2 oder 3 ändern.

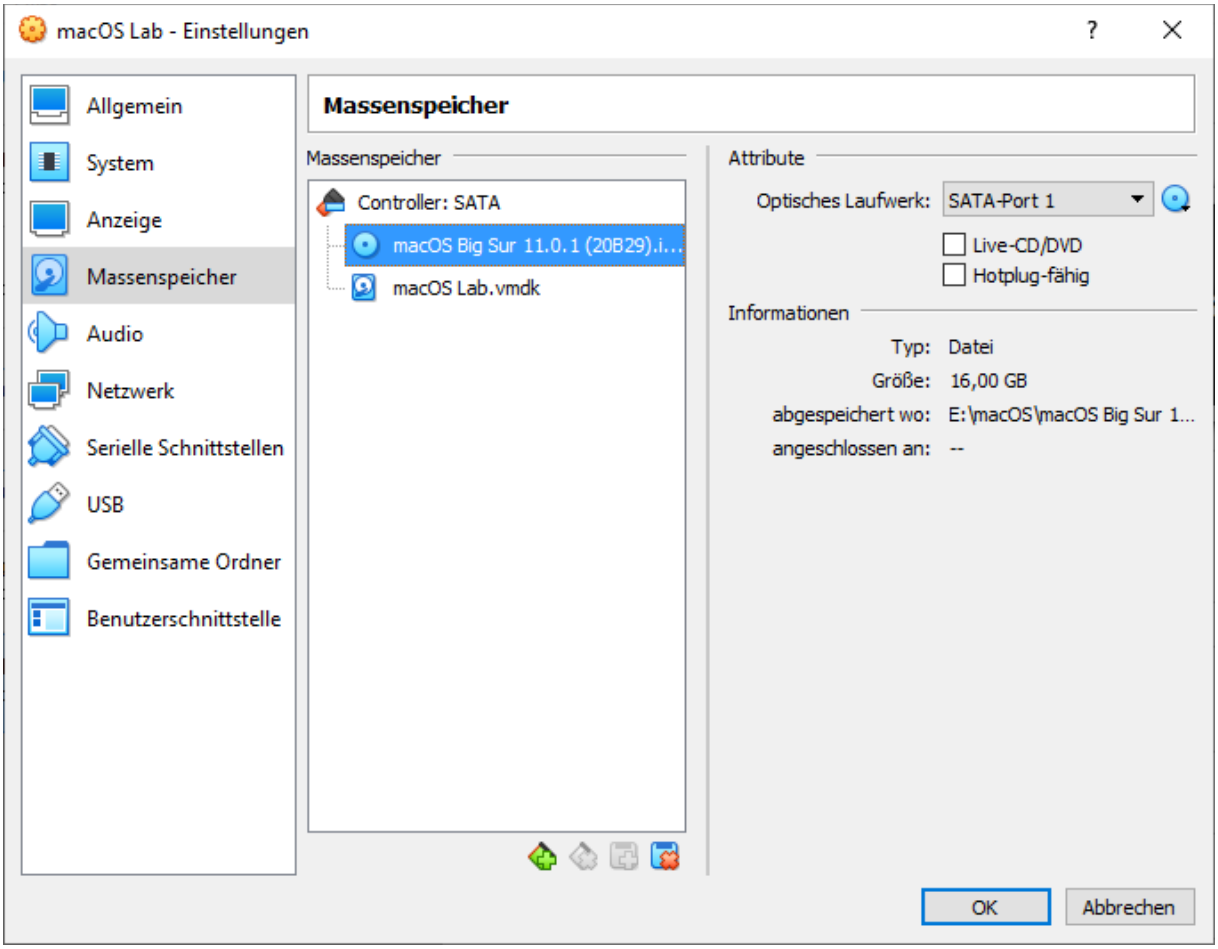




CD Image **macOS Big Sur....ISO** oder neuer auswählen für die CD.




Bitte wählen Sie eine Datei für ein virtuelles optisches Medium
Dieser PC › SSD (E:) › macOS
macOS durchsuchen
Organisieren
Neuer Ordner
Dieser PC
3D-Objekte
Bilder
Desktop
Dokumente
Downloads
Musik
Videos
Windows10 (C:)
DATA (D:)
SSD (E:)
Privatdaten (\\1
Name
Änderungsdatum
Typ
Größe
macOS Big Sur 11.0.1 (20B29).iso
12.05.2022 11:04
Datenträgerimage...
16.777.216 ...
Dateiname:
Alle Dateien für virtuelle optisch
Öffnen
Abbrechen


macOS Lab - Einstellungen
Allgemein
System
Anzeige
Massenspeicher
Audio
Netzwerk
Serielle Schnittstellen
USB
Gemeinsame Ordner
Benutzerschnittstelle
Massenspeicher
Massenspeicher
Controller: SATA
macOS Big Sur 11.0.1 (20B29).i...
macOS Lab.vmdk
Attribute
Optisches Laufwerk:
SATA-Port 1
Live-CD/DVD
Hotplug-fähig
Informationen
Typ: Datei
Größe: 16,00 GB
abgespeichert wo: E:\macOS\macOS Big Sur 1...
angeschlossen an: --
OK
Abbrechen

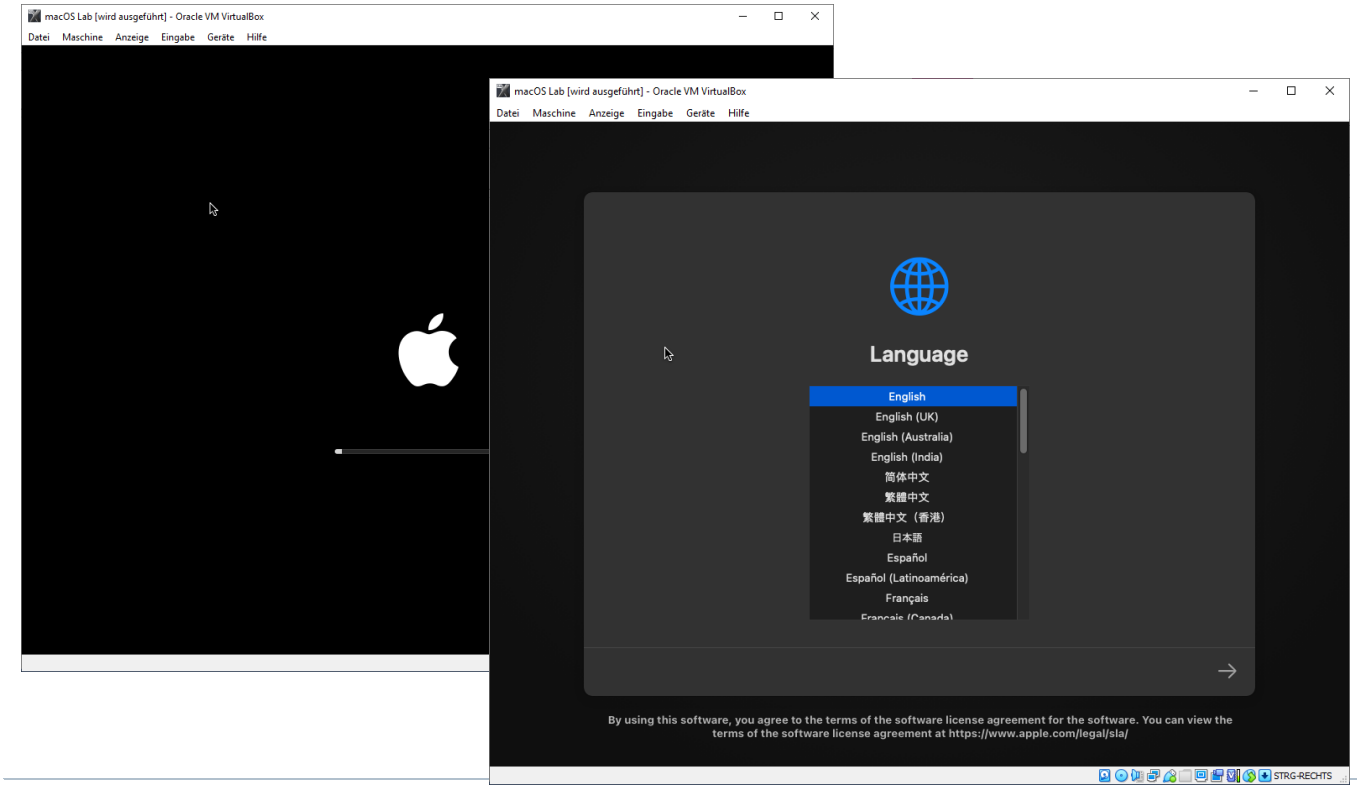
Danach Öffnen einer Eingabeaufforderung (auch ohne Admin Rechte) und Ausführung folgender Befehle mit angepasstem VM Name „macOS Lab“ in einer Kommandozeile.

```
cd "C:\Program Files\Oracle\VirtualBox\"
VBoxManage.exe modifyvm "macOS Lab" --cpuidset 00000001 000106e5 00100800
0098e3fd bfebfbff
VBoxManage setextradata "macOS Lab"
"VBoxInternal/Devices/efi/0/Config/DmiSystemProduct" "iMac19,1"
VBoxManage setextradata "macOS Lab"
"VBoxInternal/Devices/efi/0/Config/DmiSystemVersion" "1.0"
VBoxManage setextradata "macOS Lab"
"VBoxInternal/Devices/efi/0/Config/DmiBoardProduct" "Mac-AA95B1DDAB278B95"
VBoxManage setextradata "macOS Lab" "VBoxInternal/Devices/smc/0/Config/DeviceKey"
"ourhardworkbythesewordsguardedpleasedontsteal(c)AppleComputerInc"
VBoxManage setextradata "macOS Lab"
"VBoxInternal/Devices/smc/0/Config/GetKeyFromRealSMC" 1
```

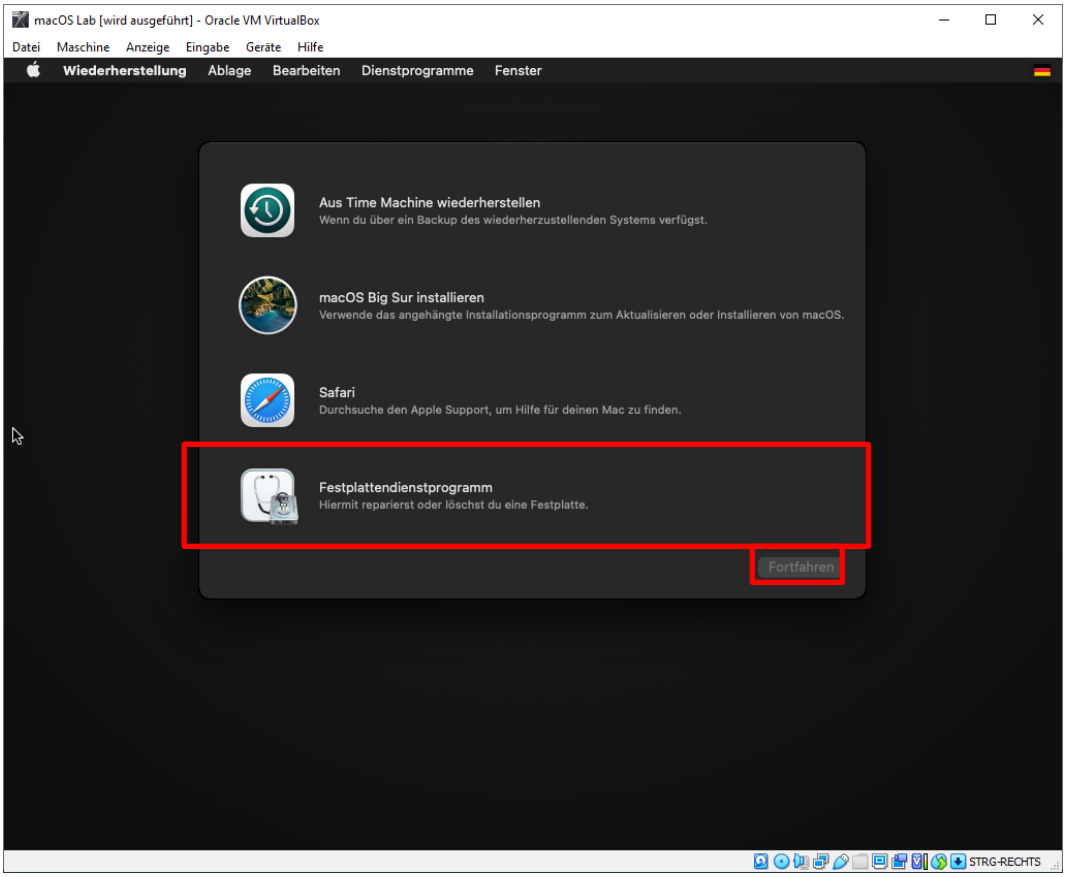
Eine vorgefertigte und eingerichtete VM finden Sie unter:

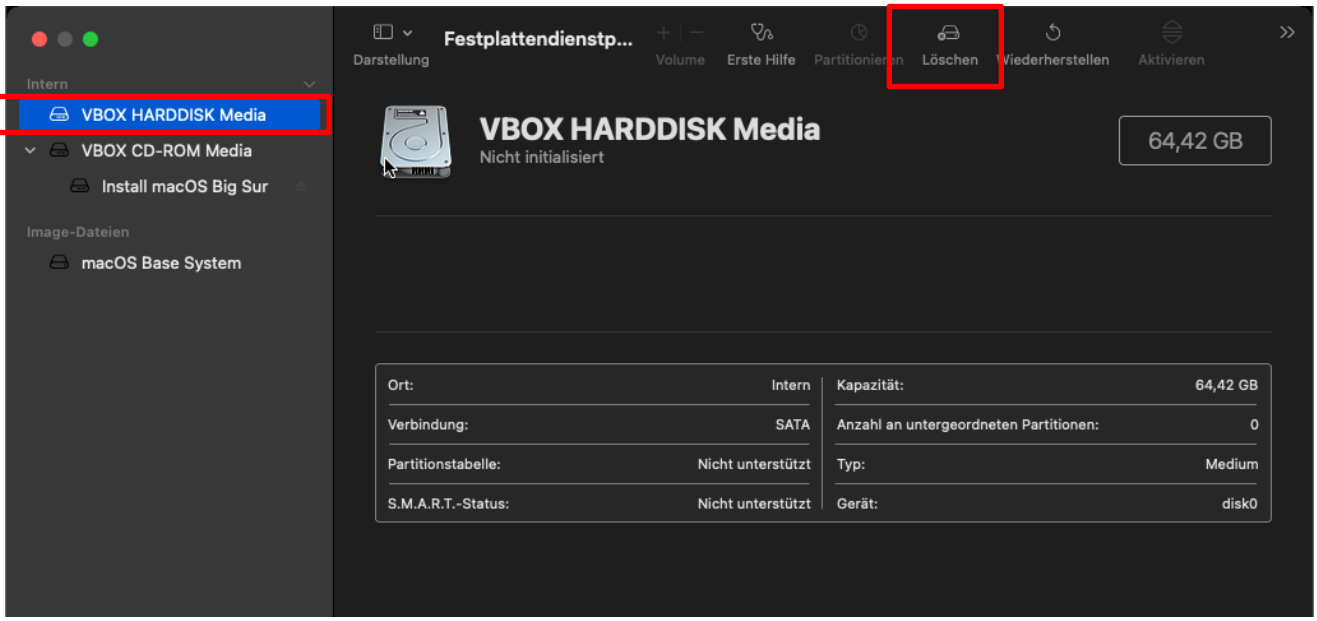
https://download.hs-mittweida.de/intranet/Lehre/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum%20Blockwochen/macOS/macOS Lab.ova

Danach Starten der VM und Boot Vorgang der macOS Installaltions CD abwarten. Jetzt kann macOS eingerichtet werden.

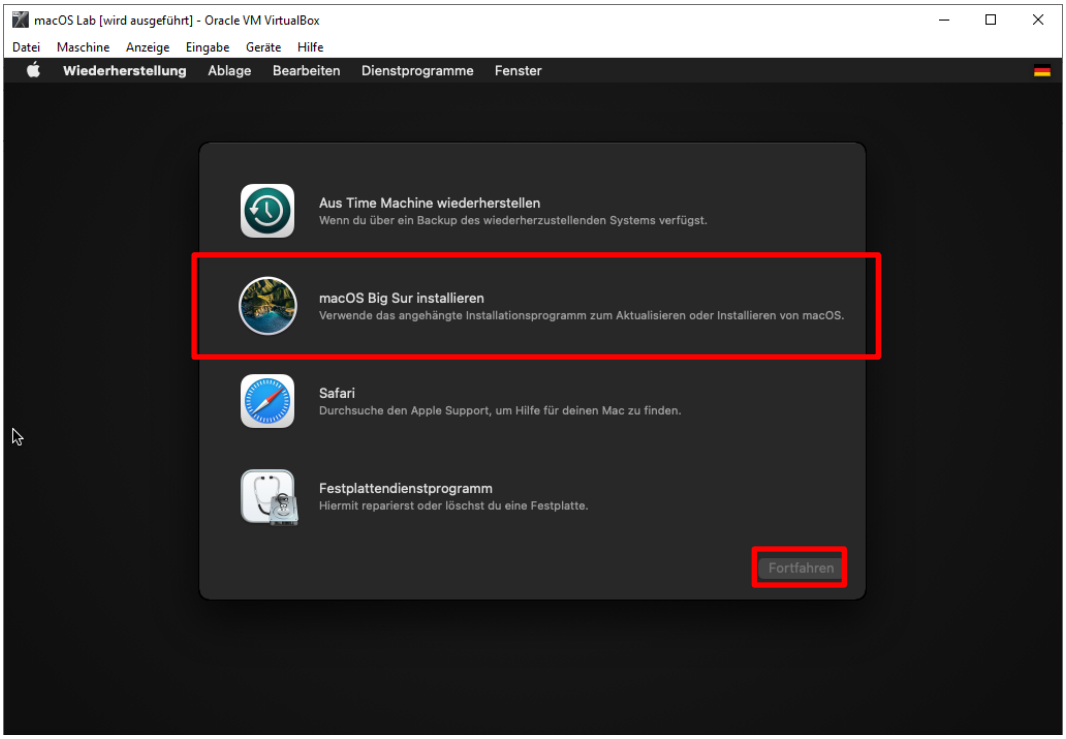


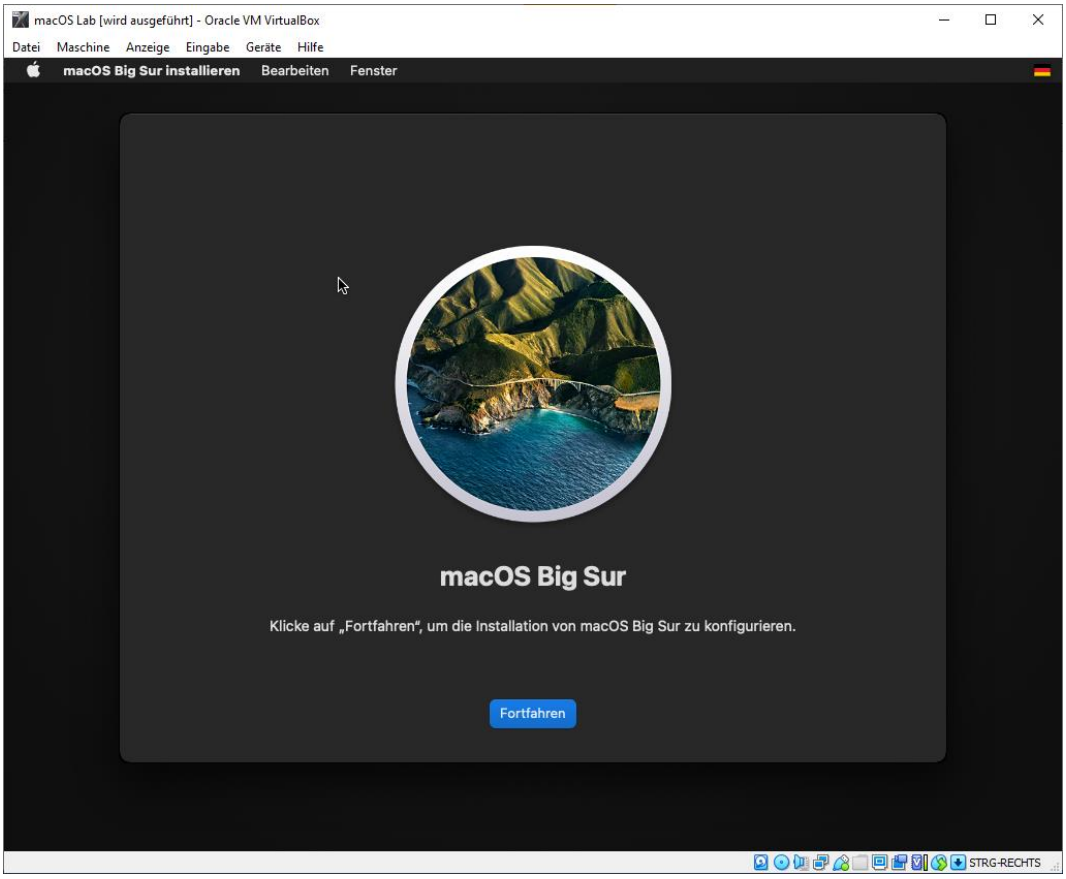
Für die Installation muss die HDD manuell formatiert (gelöscht) werden um macOS zu installieren.

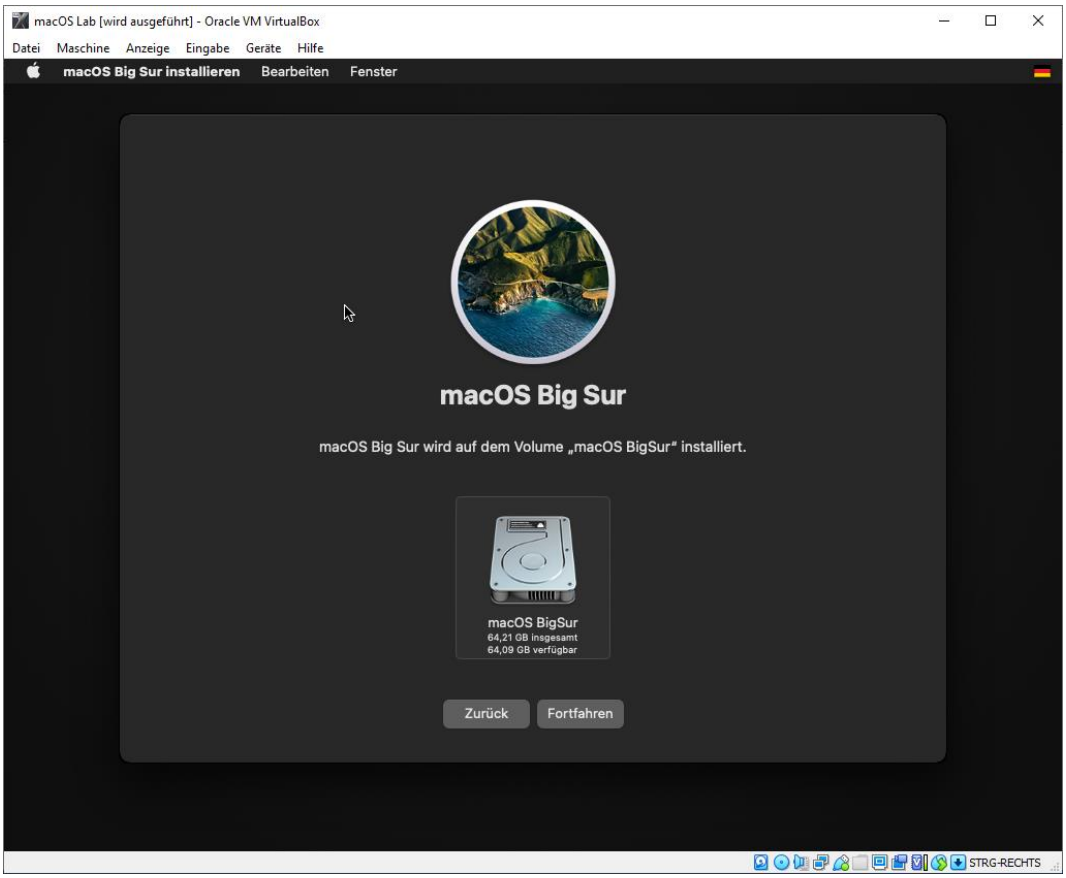





„VBOX HARDDISK Media“ wird gelöscht und „macOS BigSur“ wird erstellt
Warten, bis Partitionen aktiviert sind
Details einblenden
Fertig


macOS Lab [wird ausgeführt] - Oracle VM VirtualBox
Datei Maschine Anzeige Eingabe Geräte Hilfe
Wiederherstellung Ablage Bearbeiten Dienstprogramme Fenster
Aus Time Machine wiederherstellen
Wenn du über ein Backup des wiederherzustellenden Systems verfügst.
macOS Big Sur installieren
Verwende das angehängte Installationsprogramm zum Aktualisieren oder Installieren von macOS.
Safari
Durchsuche den Apple Support, um Hilfe für deinen Mac zu finden.
Festplattendienstprogramm
Hiermit reparierst oder löschst du eine Festplatte.
Fortfahren


macOS Lab [wird ausgeführt] - Oracle VM VirtualBox
Datei Maschine Anzeige Eingabe Geräte Hilfe
macOS Big Sur installieren Bearbeiten Fenster
macOS Big Sur
Klicke auf „Fortfahren“, um die Installation von macOS Big Sur zu konfigurieren.
Fortfahren
STRG-RECHTS

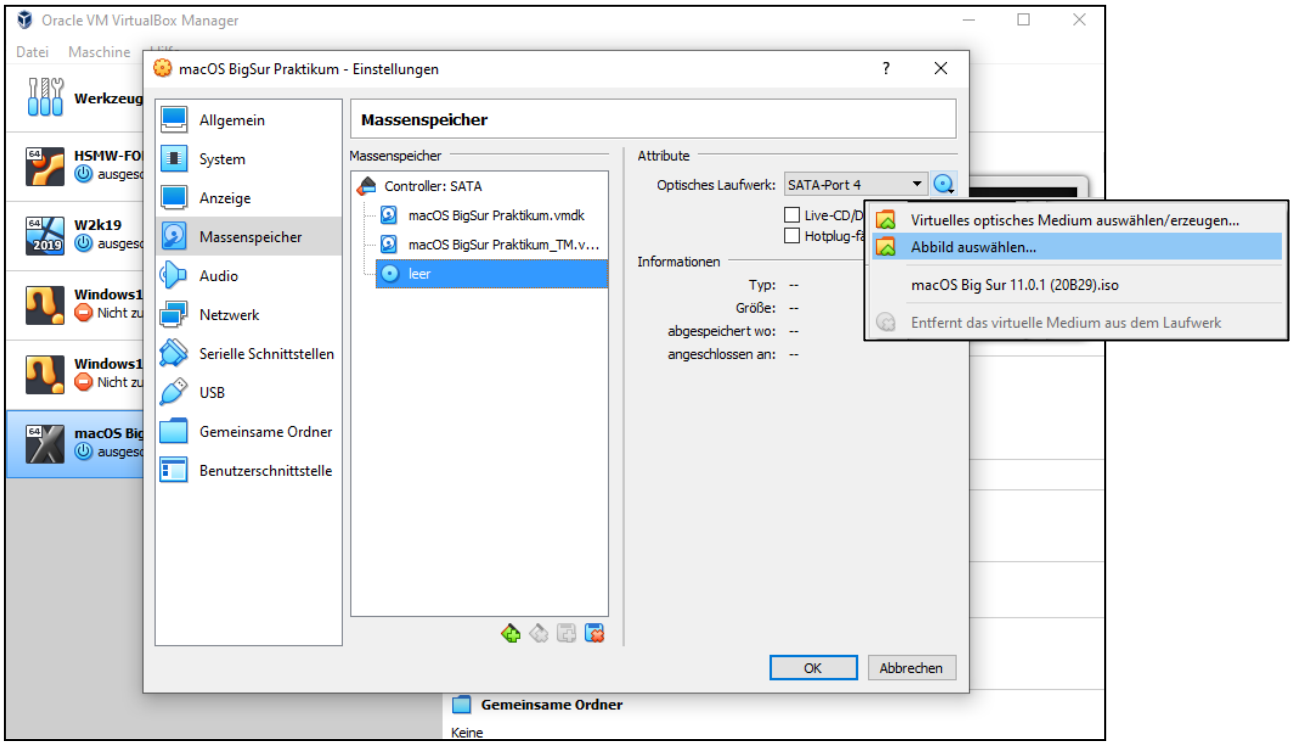


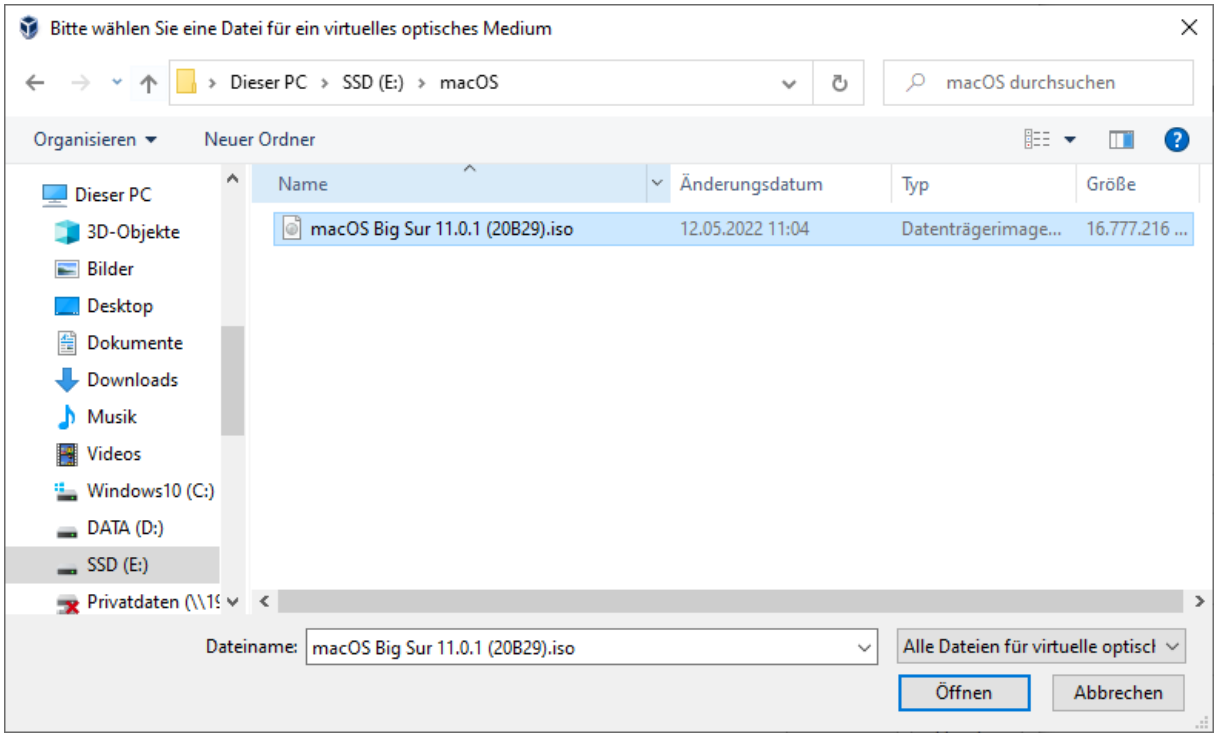
Jetzt kann die weitere Installation erfolgen, was bis zu 1h andauern kann.

5. DEAKTIVIERUNG DER SIP IN VIRTUALBOX

Konfiguration der VM aufrufen über Ändern.

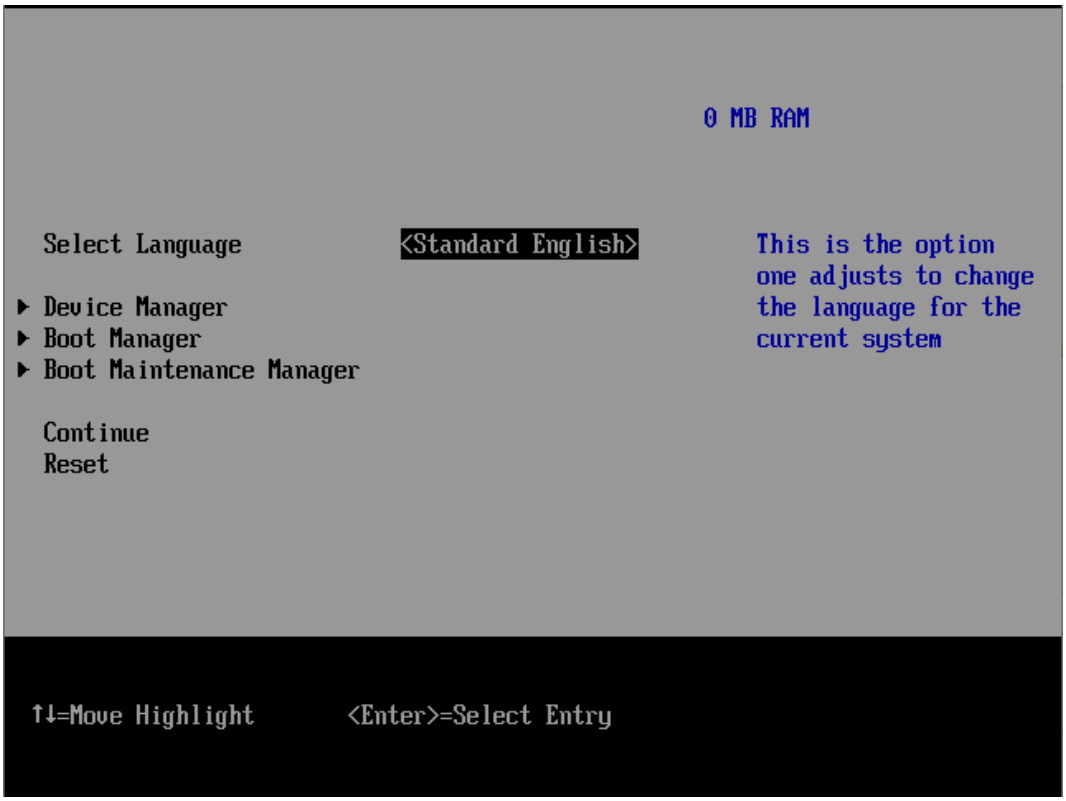
Massenspeicher auswählen und der leeren CD ein Abbild der **macOS Big Sur 11.0.1 (20B29).iso** Image Datei hinzufügen.





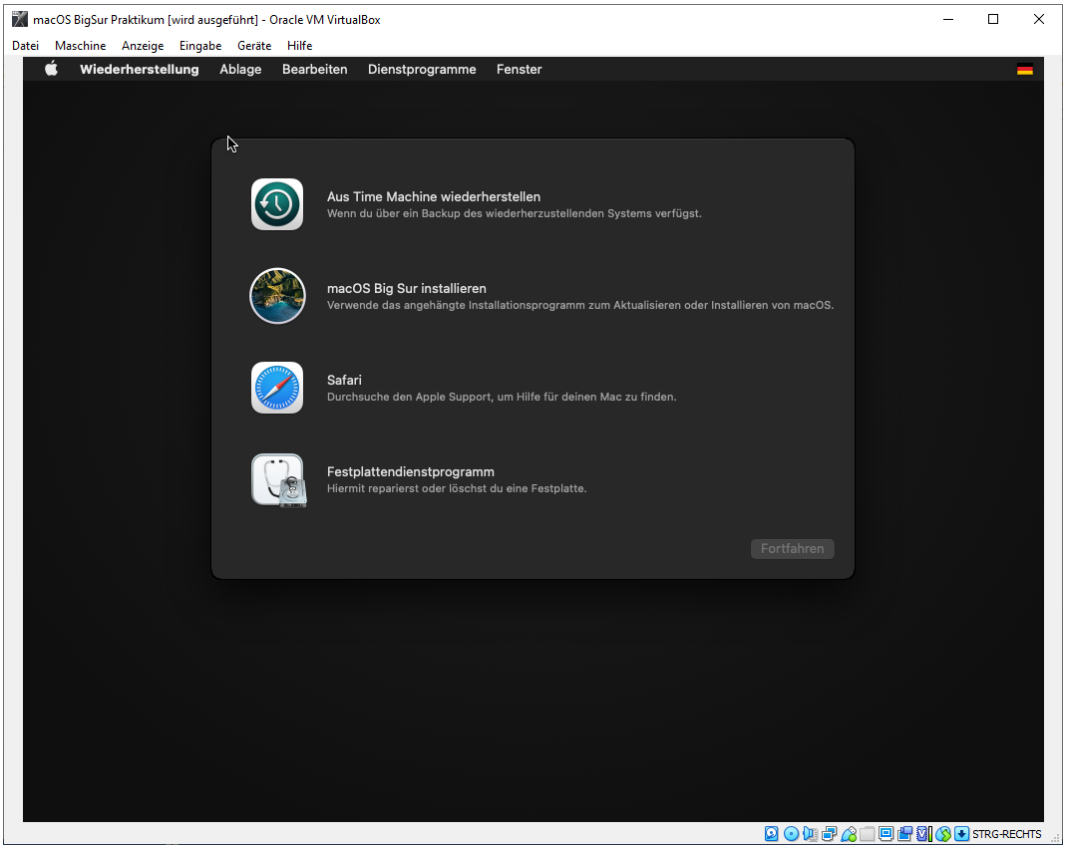
Danach Starten Sie die VM mit eingelegter macOS BigSur Installations CD / ISO Datei.

Direkt beim Starten F8/F12/**ESC** drücken (neueste VBox Version ESC ältere F8 oder F12!)

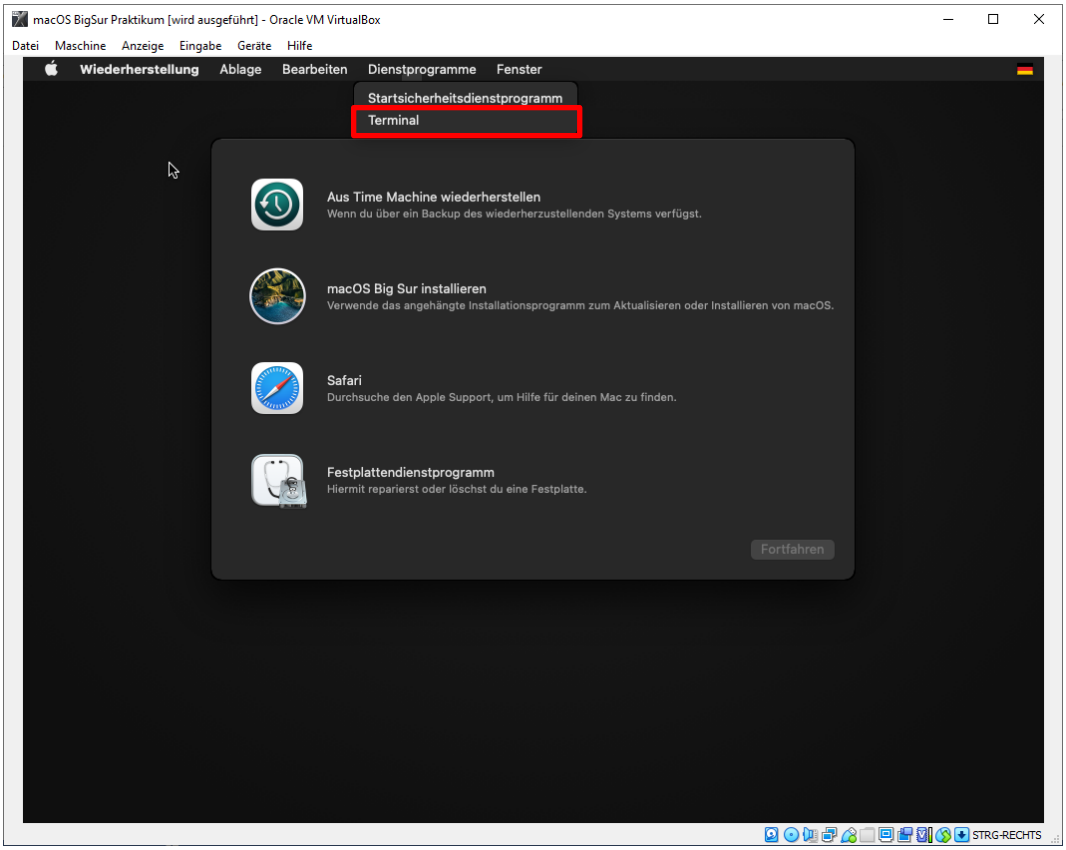


Boot Manager auswählen und CD Booten.

Wiederherstellungskonsole wird gestartet.



Terminal aus der Menüleiste aufrufen.



Im Terminal SIP überprüfen:

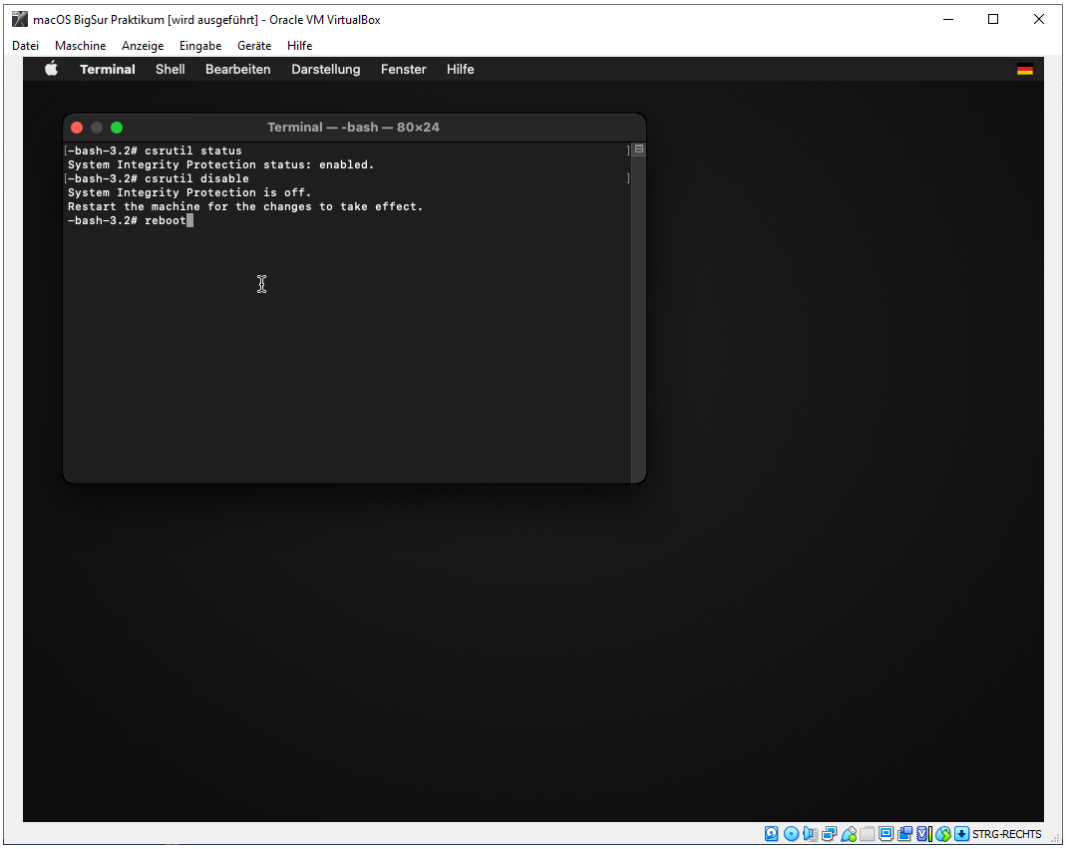
csrutil status

SIP deaktivieren mit:

csrutil disable

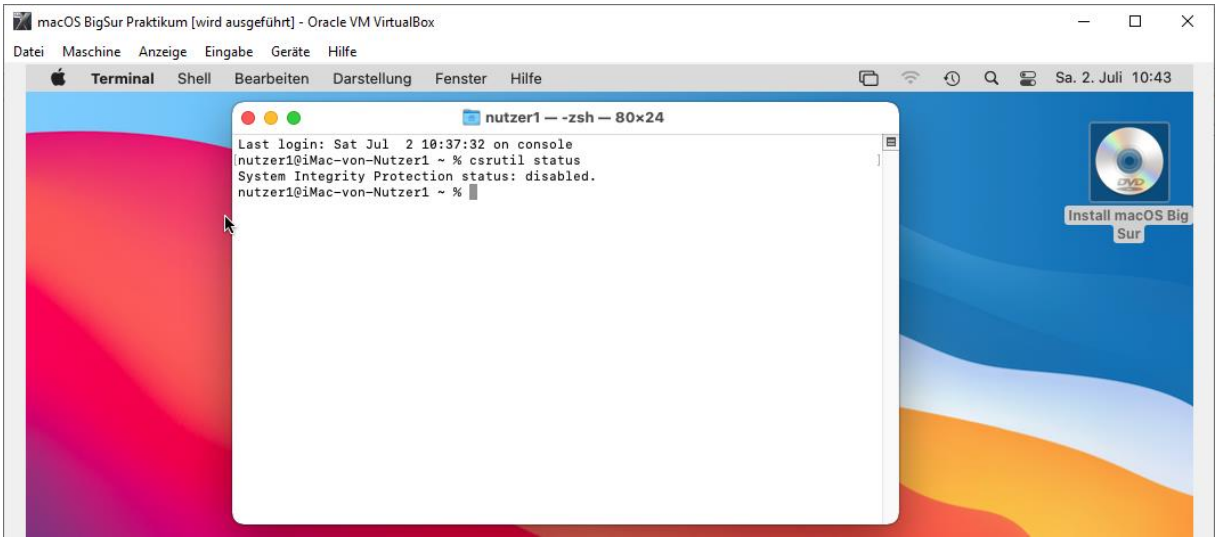
Die Deaktivierung erfolgt erst nach Neustart:

reboot



Im macOs Anmelden und das Terminal aufrufen und die Deaktivierung überprüfen mit:

csrutil status



Der System Integritätsschutz SIP ist deaktiviert.