HOCHSCHULE MITTWEIDA
University of Applied Sciences

Fraunhofer SIT

Bundeskriminalamt

Betriebssysteme

macOS - Teil2

Autor: Prof. Ronny Bodach

macOS Agenda

1. Einführung in macOS
2. macOS Bedienung
3. macOS Lab & Image Einbindung
4. Bootcamp Besonderheiten (& Parallels)
5. Mac FHS und Speicherstrukturen
6. Datenformate SQLite und Plist
7. Zuletzt genutzte Elemente & Nutzeraktivitäten
8. Spotlight und erweiterte Metadaten
9. Gelöschte Dateien
10. Schlüsselbund
11. Logdateien
12. Mac Disk Images
13. Time Machine und lokale Backups
14. Kommunikations-Apps
15. Browser Artefakte
16. Cloud
17. iOS Backups

macOS Agenda

2. macOS Bedienung
3. macOS Lab & Image Einbindung
4. Bootcamp Besonderheiten (& Parallels)

BETRIEBSSYSTEM macOS

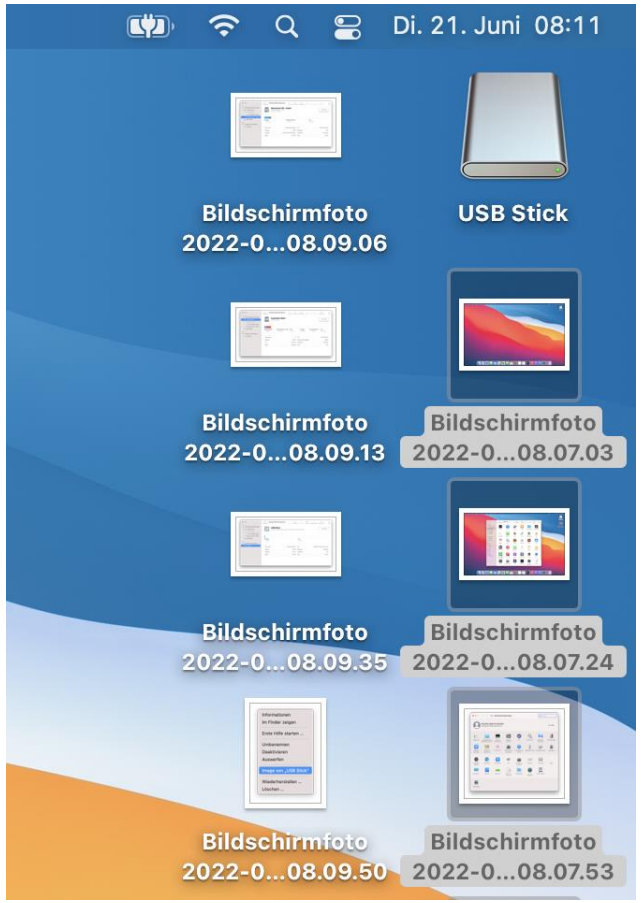
Bedienung

macOS Bedienung

macOS Bedienung

Schreibtisch/Desktop

- der Schreibtisch ist der Hintergrundbereich der Bildschirmanzeige
- auf dem Schreibtisch sind Symbole für Festplatten, CDs und Server, die an den Mac angeschlossen sind
- es können Dateien und Ordner direkt auf dem Schreibtisch abgelegt werden, um schnell darauf zuzugreifen



macOS Bedienung

Dock

- Das Dock wird zum Öffnen von Programmen, Dokumenten, Ordnern und anderen Objekten verwendet. Es wird standardmäßig am unteren Bildschirmrand angezeigt.
- Wenn ein Fenster minimiert oder ein Programm geöffnet wird, das nicht im Dock enthalten ist, wird das zugehörige Symbol im Dock angezeigt.
- Jedes Objekt im Dock besitzt ein Kontextmenü, das einen schnellen Zugriff auf die Befehle ermöglicht, die für das betreffende Objekt verfügbar sind.

macOS Bedienung

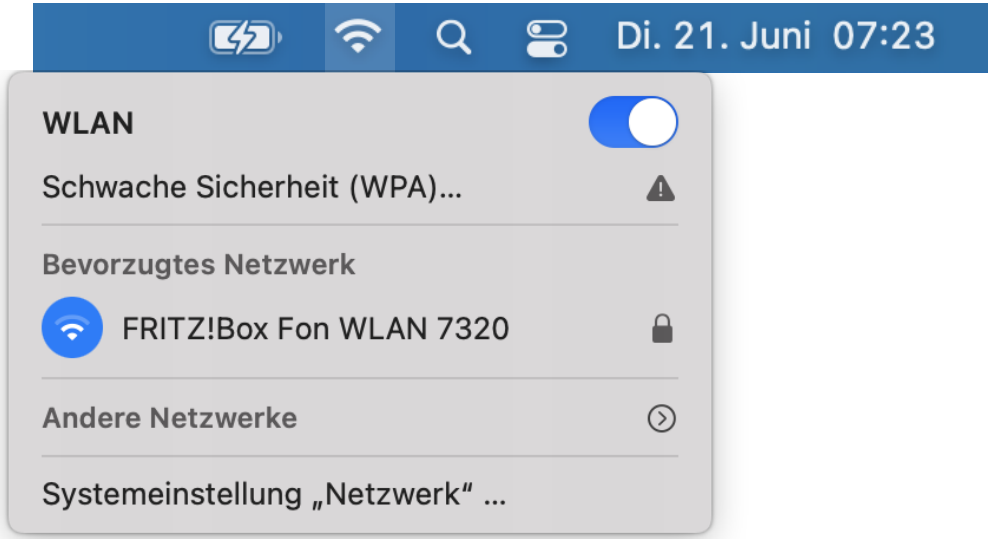
Menüleiste

- Am oberen Rand des Bildschirms befindet sich die Menüleiste.
- Diese ist, mit Ausnahme des Apple-Menüs ganz links sowie der Uhrzeit und dem Kontrollzentrum ganz rechts programmspezifisch und ändert sich, wenn man von einem Programm zum anderen wechselt.
- Wie das Dock lässt sich die Menüleiste ausblenden und erscheint dann nur, wenn man den Mauszeiger dorthin bewegt.

macOS Bedienung

Menüleiste

- Außerdem lassen sich für verschiedene Systemfunktionen und manche Anwendungen Symbole der Menüleiste hinzufügen (Menü-Extras), beispielsweise für Spotlight, das WLAN, Time Machine, 1Password oder Carbon Copy Cloner.
- Auch diese Symbole werden immer angezeigt, egal mit welcher Anwendung man gerade arbeitet.



macOS Bedienung

Das Apple-Menü

- Das Apple-Menü ganz links mit dem Apfelsymbol dient dazu, immer Zugriff auf bestimmte Funktionen zu haben, egal, in welcher Anwendung man sich gerade befindet.
- Hier ist die Systemeinstellungen, der App Store und unter „Benutzte Objekte“die zuletzt verwendeten Programme, Dokumente und Server aufgelistet
- Hält man die Taste Command (⌘) gedrückt, kann man sich die Objekte im Finder anzeigen lassen.

macOS Bedienung

Das Apple-Menü

- Über den Befehl „Sofort beenden“ lässt sich ein hängengebliebenes Programm zur Aufgabe bewegen.
- Mit „Ruhezustand“ schickt man den Mac in den Schlafmodus, zum Aufwachen genügt es, eine Taste auf der Tastatur oder die Maustaste zu drücken beziehungsweise auf das Trackpad zu tippen. D
- ann folgen die Befehle zum Neustart des Rechners und zum Ausschalten. Das System fragt vorsichtshalber jeweils nach, ob man dies auch wirklich möchte. Um die Nachfrage zu umgehen, hält man die Taste Option (⌥) gedrückt, wenn man den Befehl auswählt.
- Mit den beiden letzten Optionen im Apple-Menü lässt sich der Bildschirm sperren oder der momentan aktive Benutzer am System abmelden.

macOS Bedienung

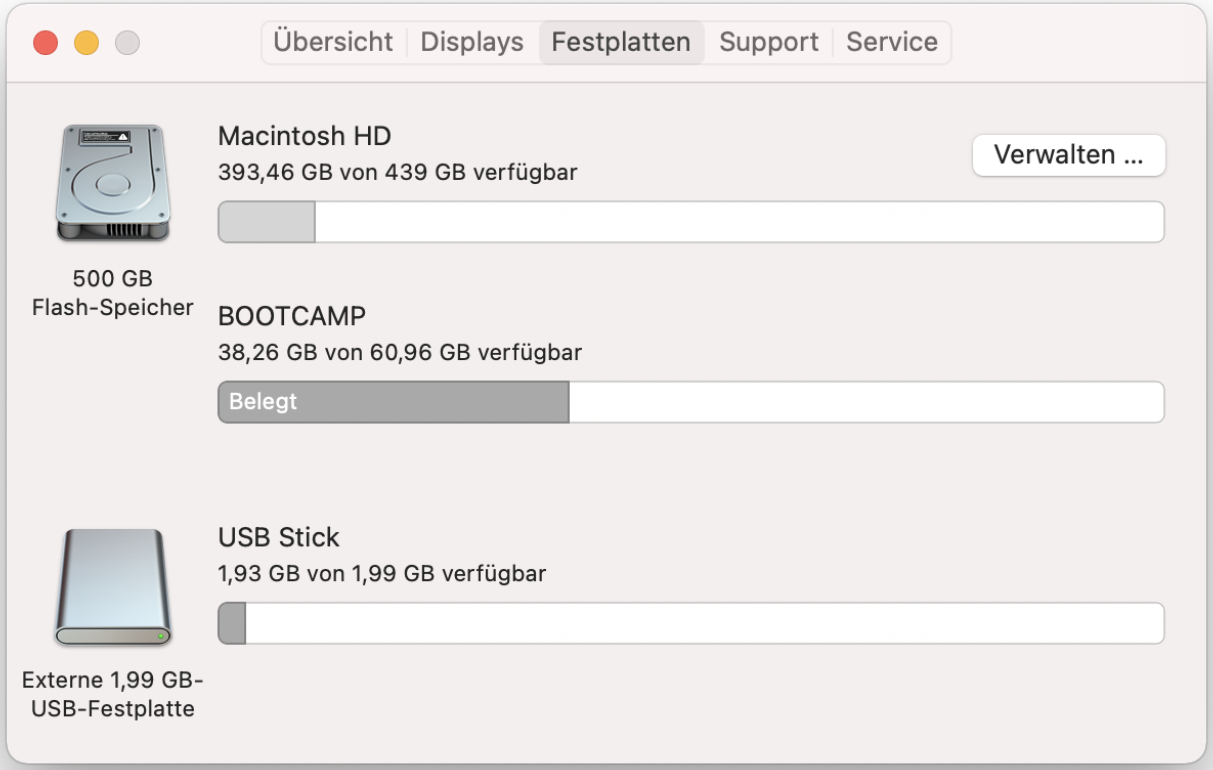
Das Apple-Menü

- An oberster Stelle im Apple-Menü befindet sich der Eintrag „Über diesen Mac“, mit dem sich ein Informationsfenster öffnet.
- Es zeigt die Version des Systems an, den Rechnertyp, den Prozessortyp, die Größe des eingebauten Arbeitsspeichers, von welchem Volume der Mac gestartet ist sowie die Seriennummer.

macOS Bedienung

Das Apple-Menü

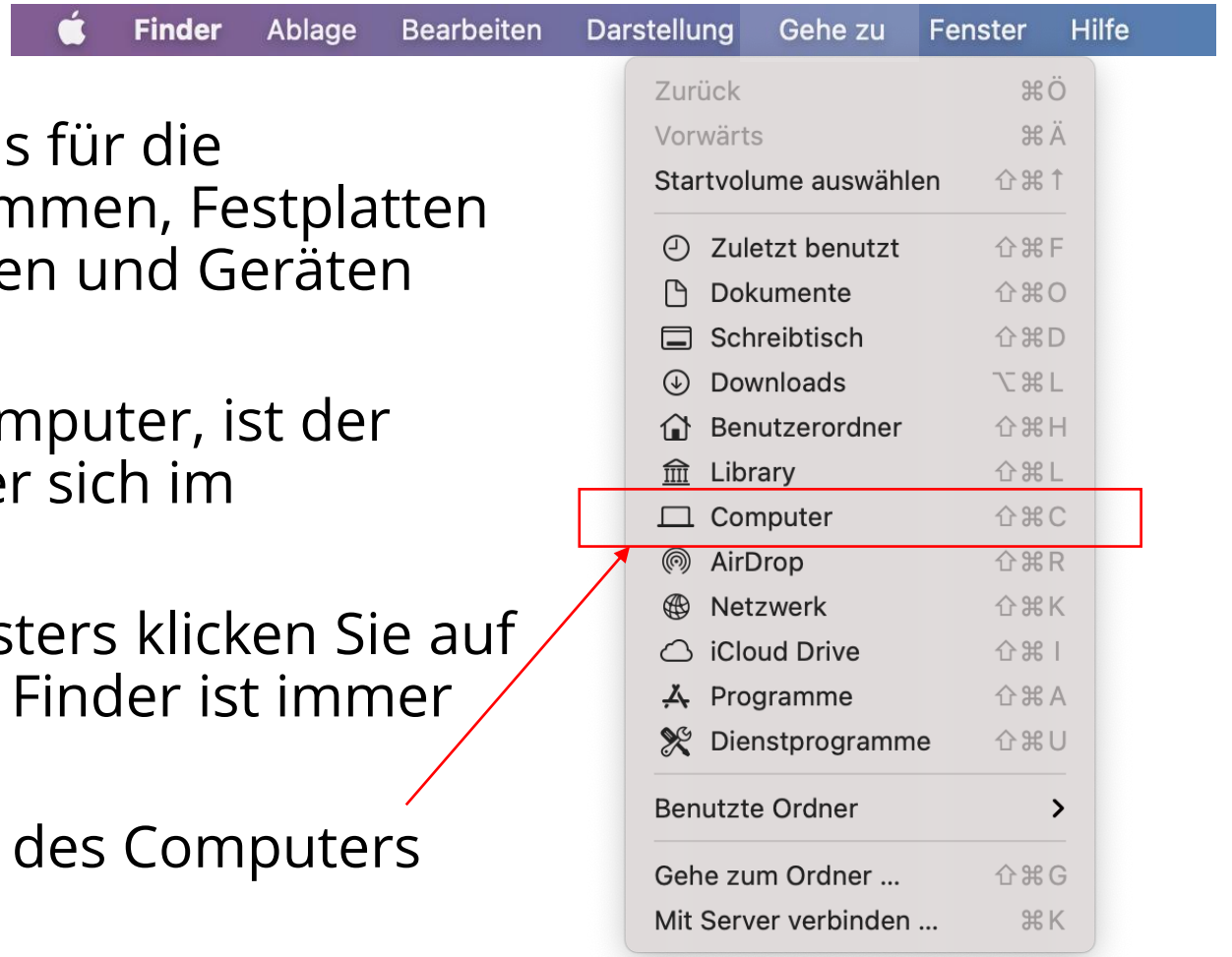
- An oberster Stelle im Apple-Menü befindet sich der Eintrag „Über diesen Mac“, mit dem sich ein Informationsfenster öffnet.
- Unter „Festplatten“ findet man Informationen über die verfügbaren Datenträger angezeigt.



macOS Bedienung

Der Finder

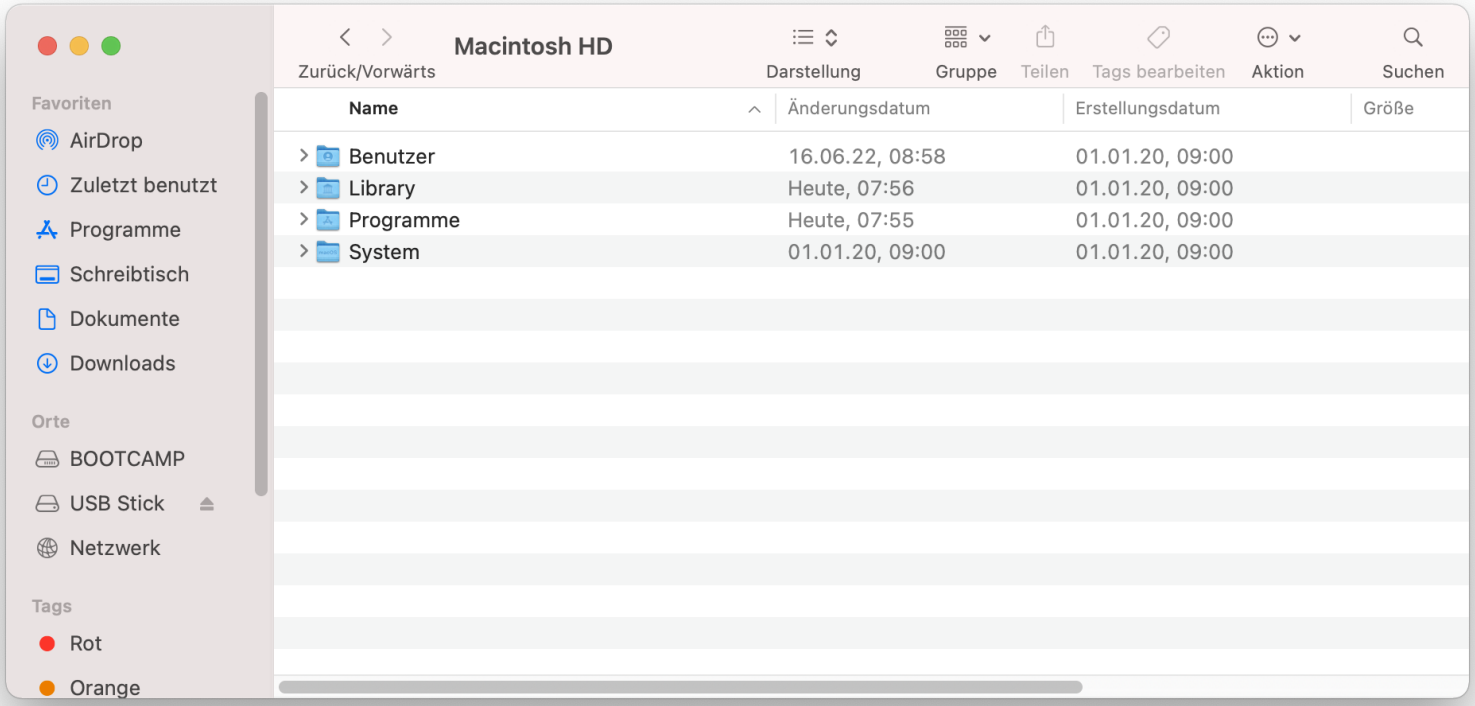
- Der Finder ist das Programm, das für die Verwaltung von Dateien, Programmen, Festplatten (Volumes), Netzwerkverbindungen und Geräten (wie Drucker) zuständig ist.
- Während der Arbeit mit dem Computer, ist der Finder immer aktiv, auch wenn er sich im Hintergrund befindet
- Zum Einblenden des Finder-Fensters klicken Sie auf das Finder-Symbol im Dock. Der Finder ist immer das erste Symbol im Dock.
- Über den Finder kann der Inhalt des Computers aufgelistet werden (Computer).



macOS Bedienung

Der Finder

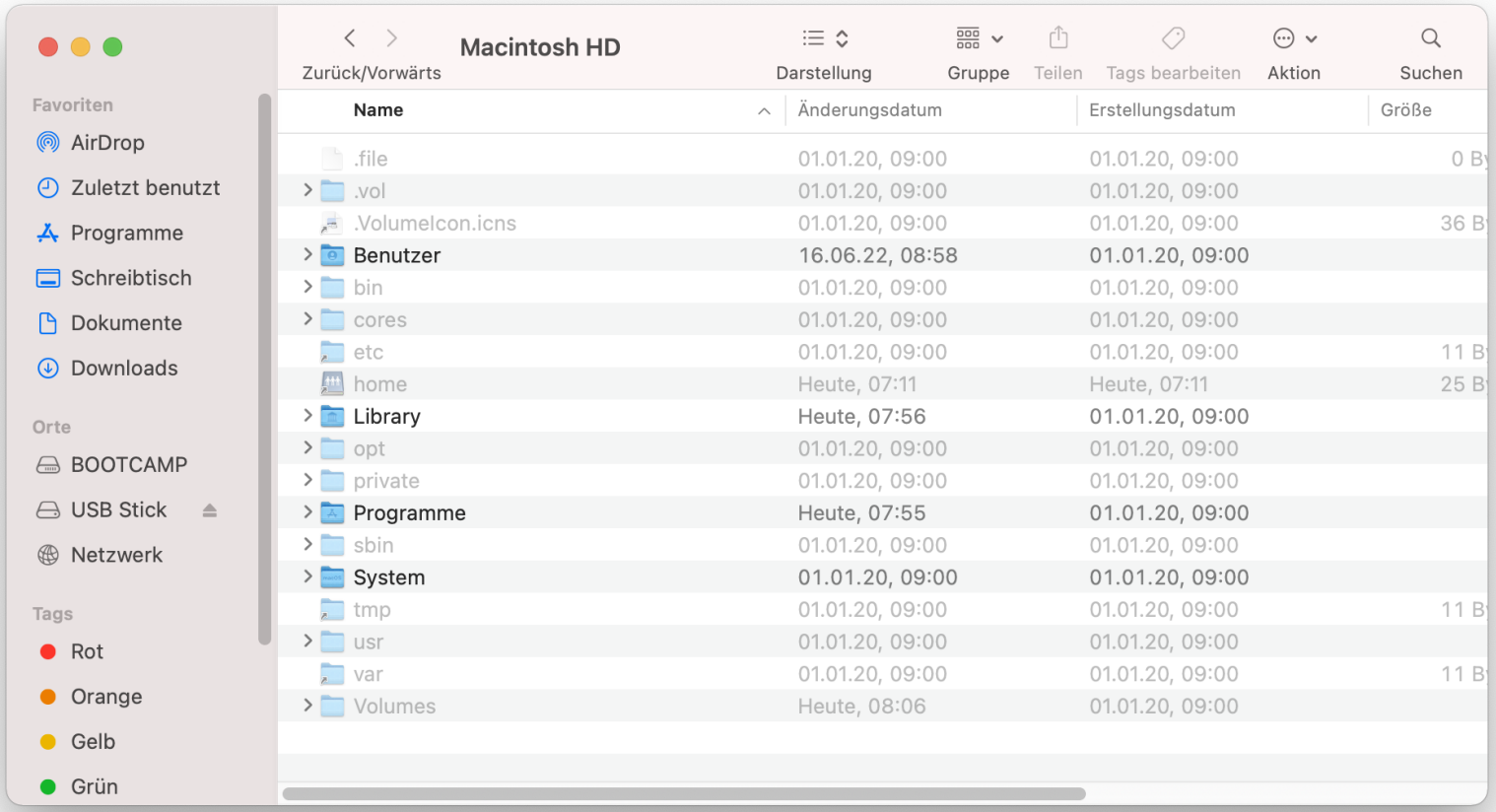
Die Standard Ansicht zeigt dabei leider nur sehr wenig Daten an:



macOS Bedienung

Der Finder

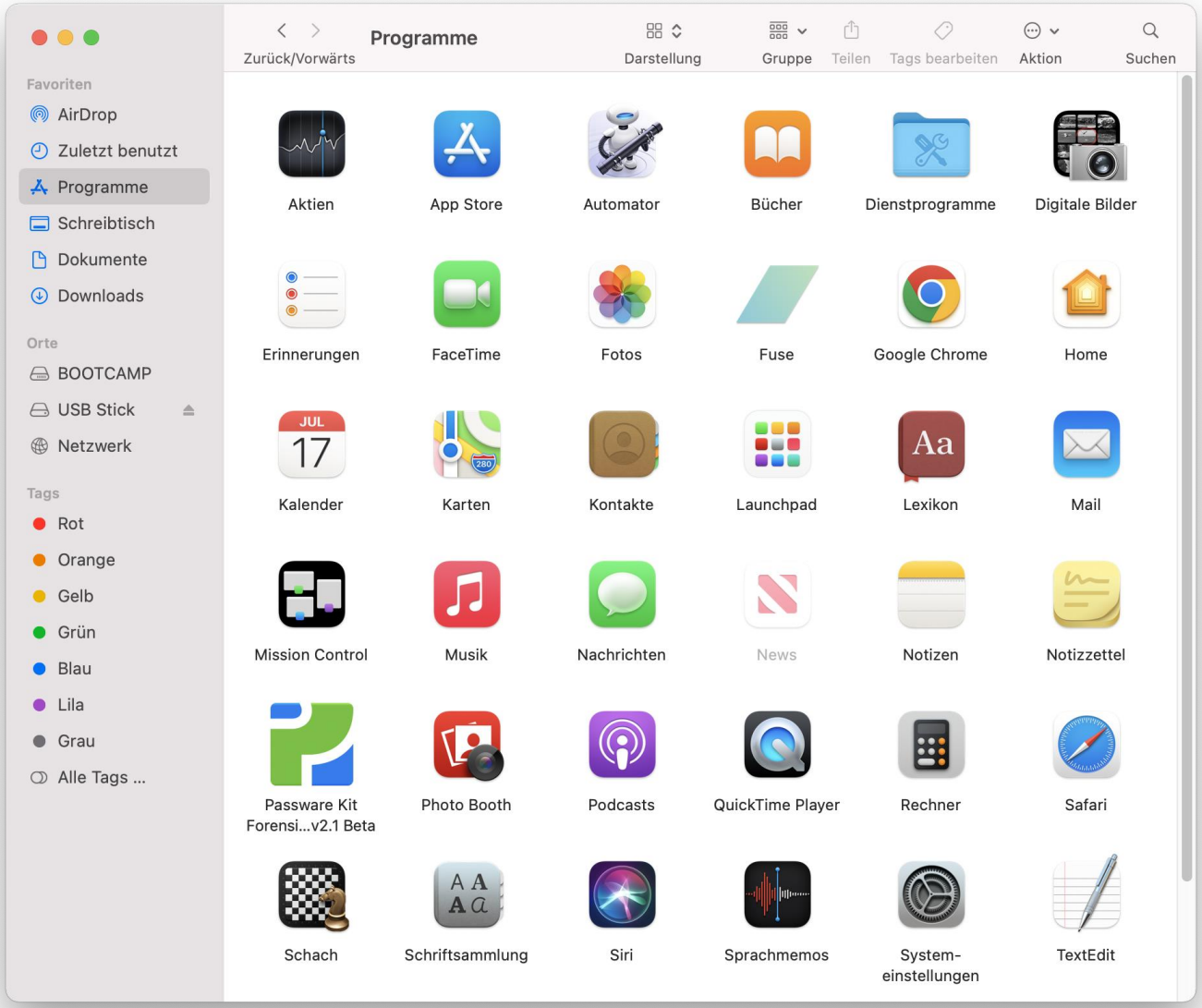
Die Vollansicht (**Shift** + Befehlstaste/**Command** (⌘) + **.**) offenbart weitere Daten:



macOS Bedienung

Programme

- Die installierten Anwendungen befinden sich unter Progrmme abgelegt.
- macOS hat viele davon als Standard on Board
- Installations DVD macOS ca. 20 GB!
- Wichtige Punkt sind hier Dienstprogramme und Systemeinstellungen

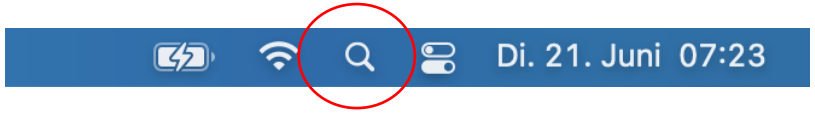


macOS Bedienung

Programme

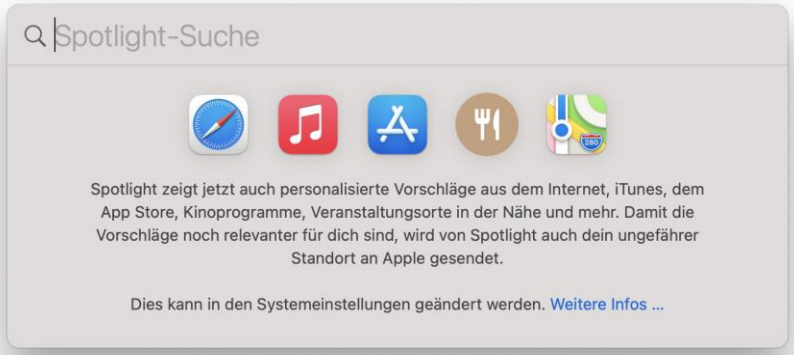
- Anwendungen werden durch Drag & Drop installiert.

macOS Bedienung



Spotlight

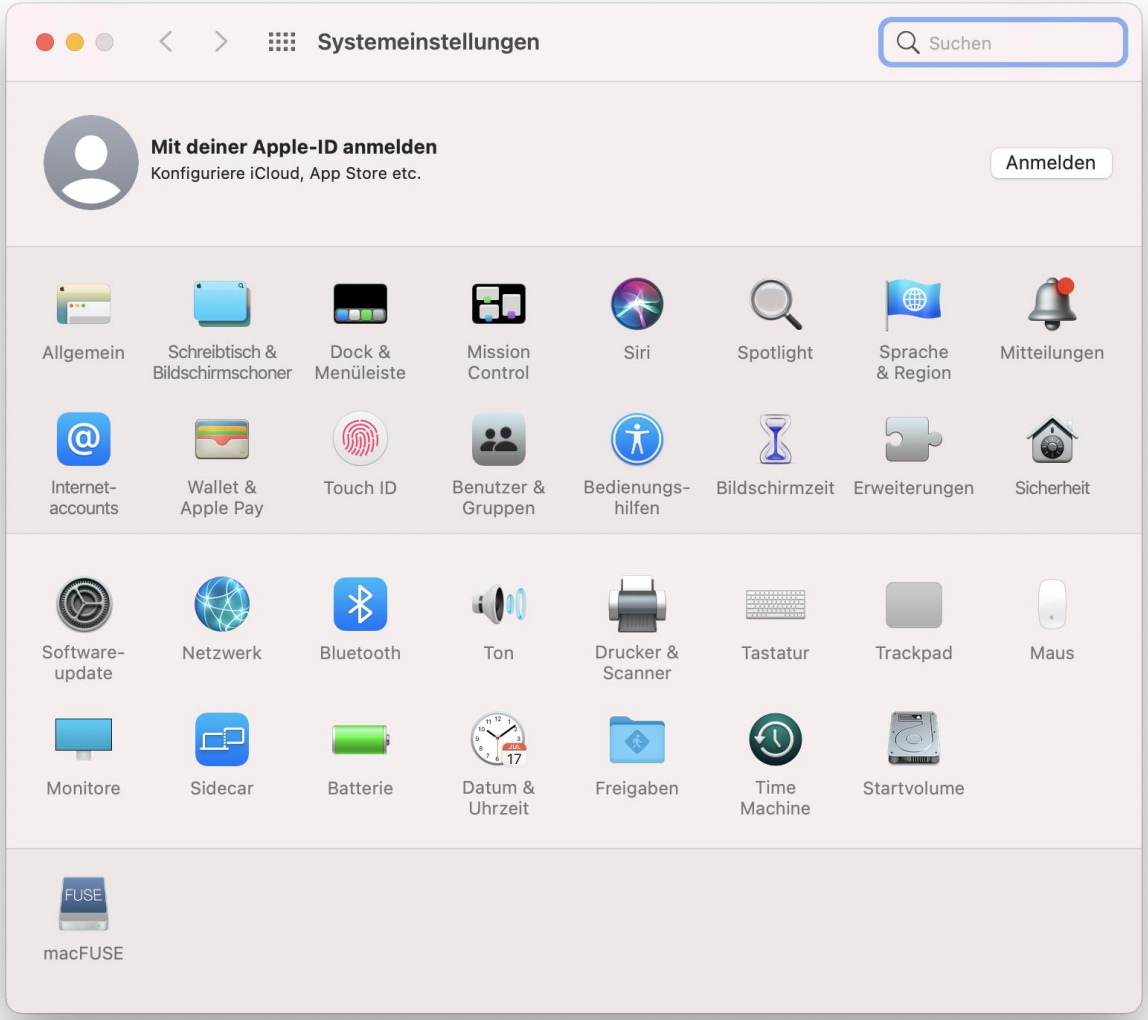
- Mit Spotlight können Sie Informationen auf Ihrem Computer ganz einfach finden.
- Spotlight ist der Index zum macOS System.
- In vielen Fällen ist es einfacher, Dateien, Ordner und Programme mit Spotlight zu öffnen, anstatt den Finder zu verwenden.
- Sobald Sie beginnen, Text in das Suchfeld von Spotlight einzugeben, werden die Suchergebnisse sofort in einem Menü unterhalb des Suchfelds angezeigt.



macOS Bedienung

Systemeinstellungen

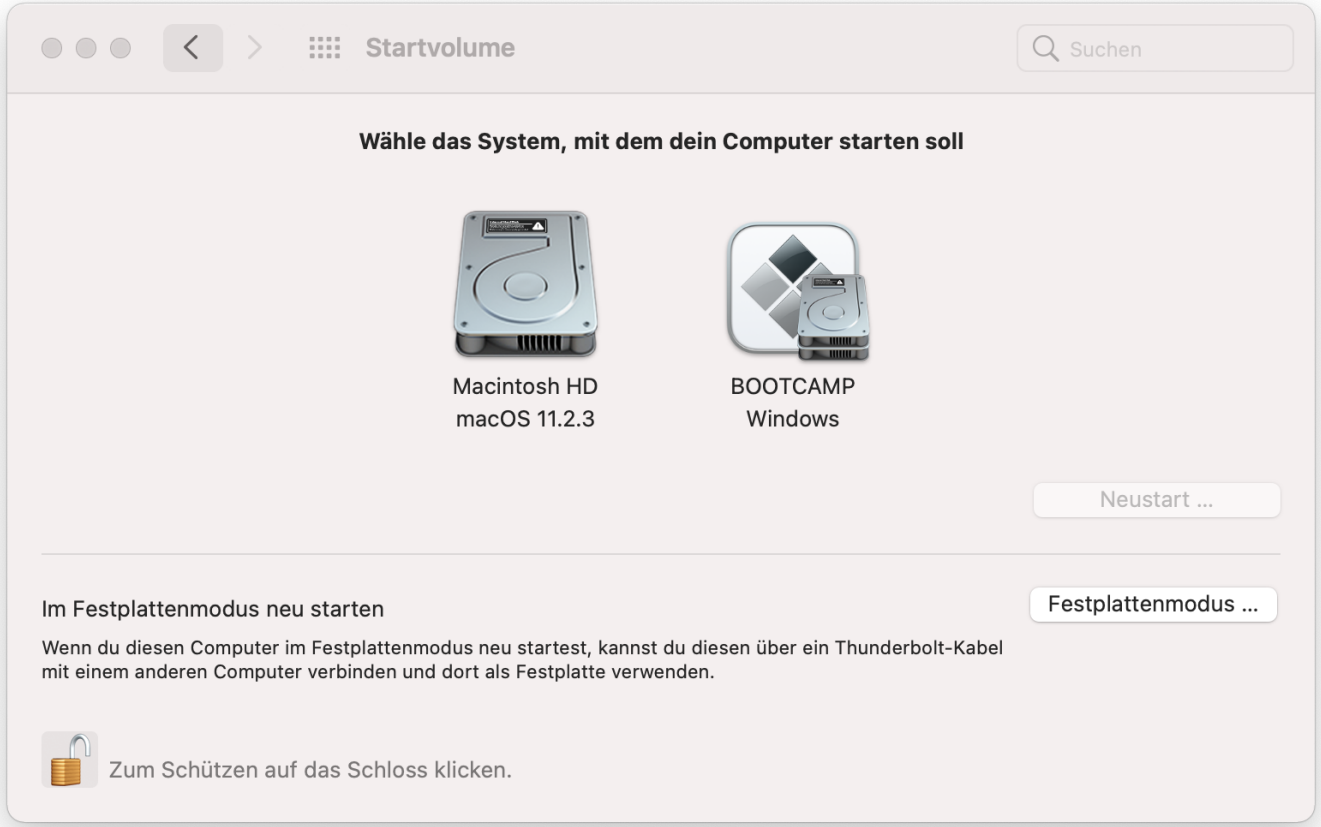
- Mithilfe der Systemeinstellungen kann das macOS verwaltet werden.
- Die Systemeinstellungen befinden sich im Menü "Apple" und im Dock.
- Wichtige forensische Bestandteile sind:
  - Internet Accounts
  - Wallet
  - Benutzer & Gruppen
  - Erweiterungen
  - Time Maschine
  - Startvolume



macOS Bedienung

Systemeinstellungen

Systemeinstellung „Startvolume"



macOS Bedienung

Systemeinstellungen

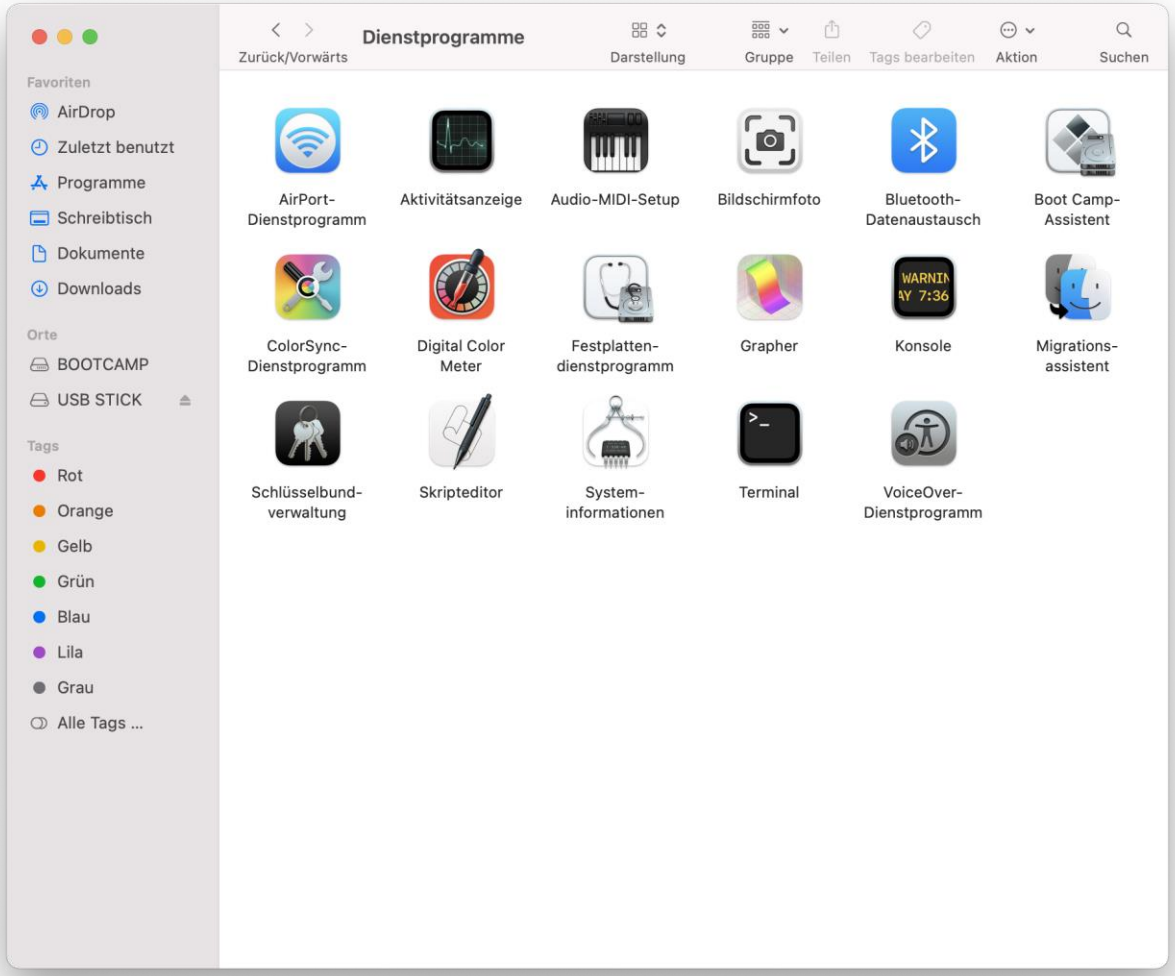
Systemeinstellung „Time Maschine"

macOS Bedienung

Dienstprogramme

Dienstprogramme enthält eine Reihe wichtiger Inforamtionsquellen für eine Untersuchung:

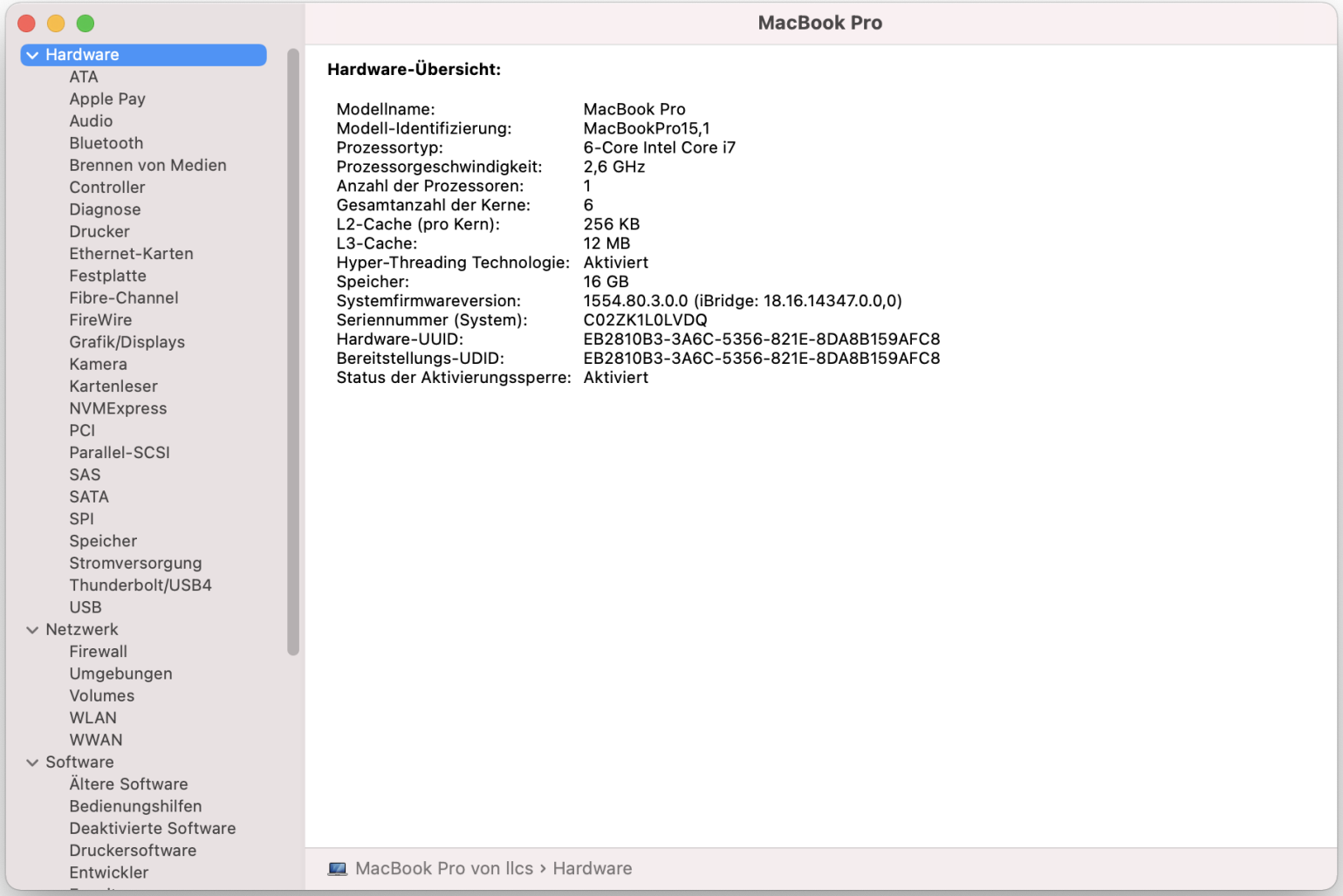
- Festplattendienstprogramm
- Schlüsselbundverwaltung
- Systeminformationen
- Terminal
- Bootcamp Assistent



macOS Bedienung

Dienstprogramme

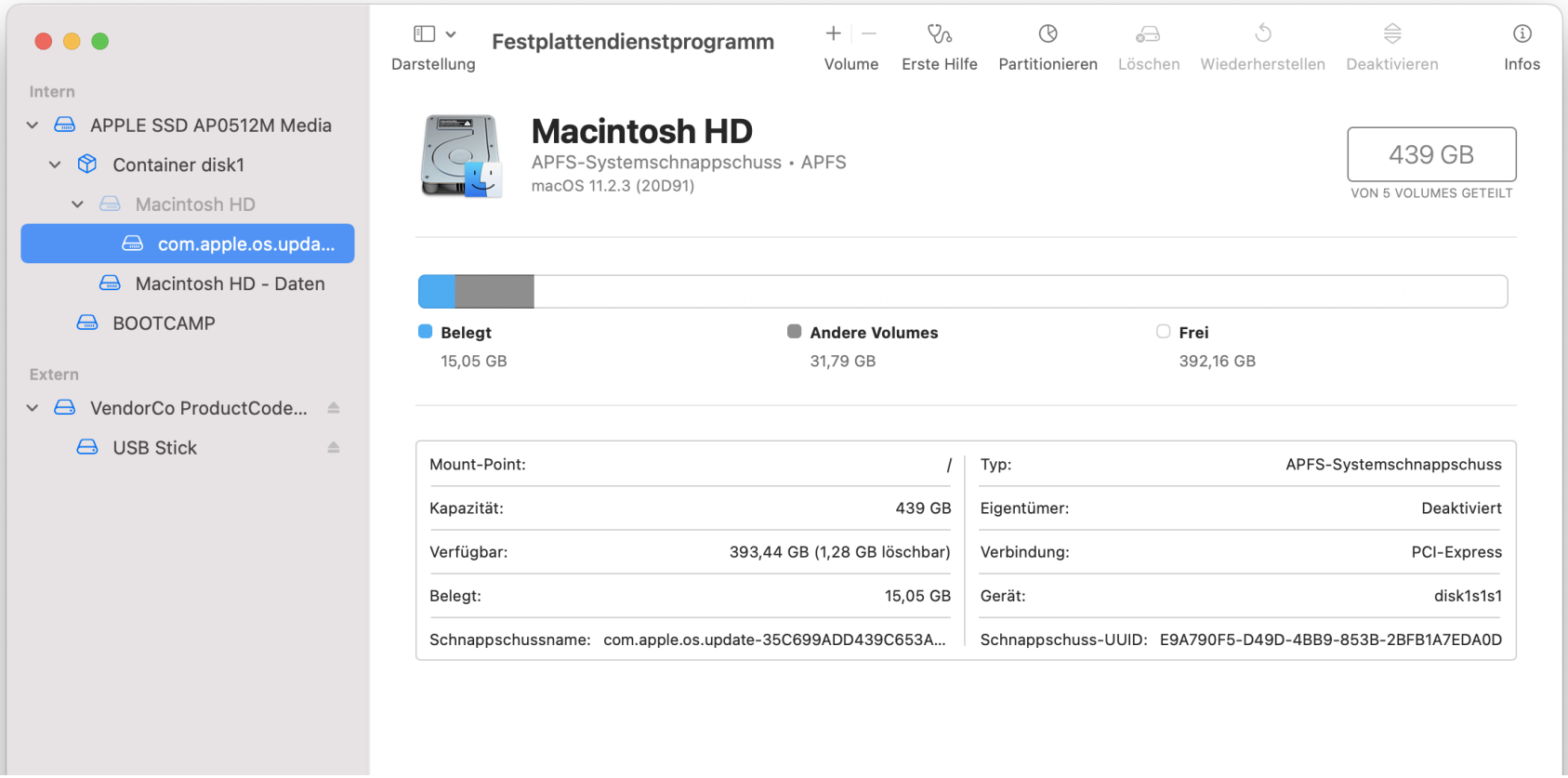
Systeminformationen



macOS Bedienung

Dienstprogramme

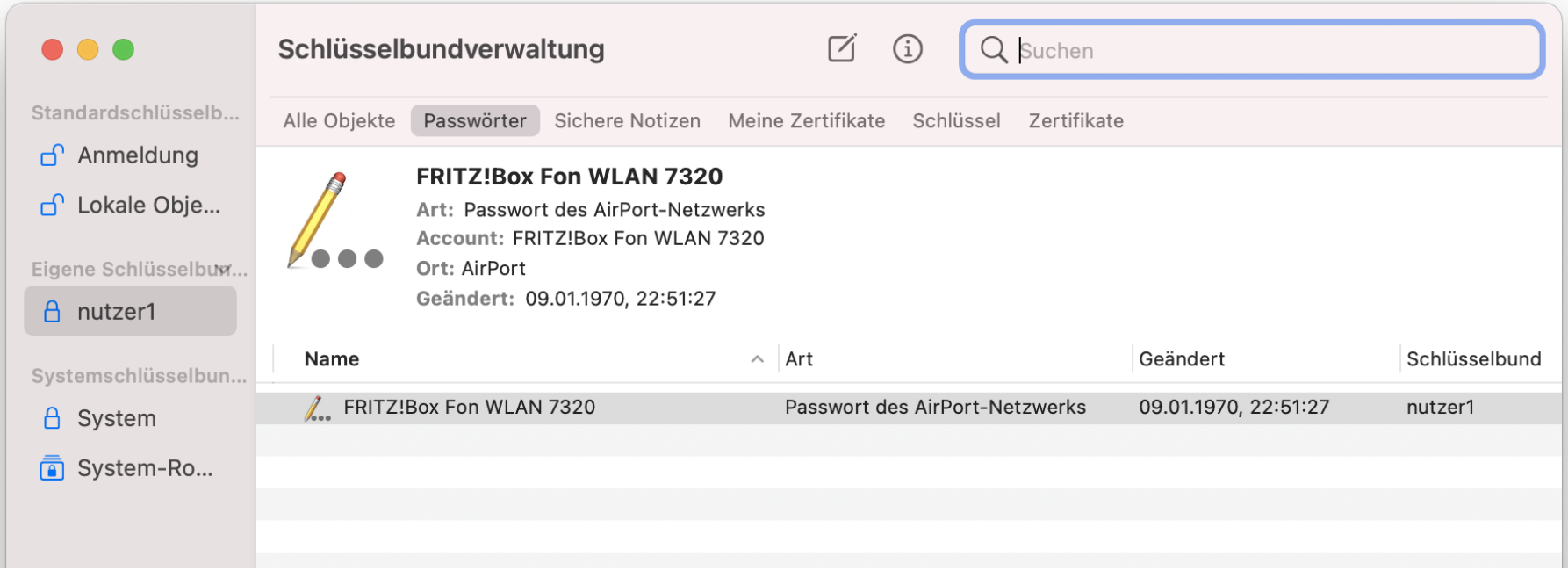
Fesplattendienstprogramm



macOS Bedienung

Dienstprogramme

Schlüsselbundverwaltung / Keychain



macOS Bedienung

Terminal

Zsh – die Z shell ist eine UNIX Shell und basiert auf der bash ist mittlwerweile die Standard Shell auf MacOS.

BETRIEBSSYSTEM macOS

macOS Lab & Image Einbindung

macOS Lab & Image Einbindung

Herausforderungen bei der Datensicherung von macOS Systemen:

- Verschlüsselung mit Hardwareeinbindung T2 & M1 Chipsätze
- fest verbaute Datenträger (SSD on Board)
- fehlende Zugriffsmöglichkeiten auf Hardware, wie etwa PCB

macOS Lab & Image Einbindung

Herausforderungen bei der Analyse von macOS Systemen:

- Log Formate mit speziellen Binärcodierungen (ähnlich evtx)
- Datenspeicherformate mit Binärcodierungen
- Schlüsselbund/Keychain Informationen mit Hardwareeinbindung T2 & M1

macOS Lab & Image Einbindung

Die Datensicherung wie auch Untersuchung eines macOS Systems lässt sich nur bedingt auf externen Geräten ohne macOS durchführen.

Daher empfiehlt es sich ein **macOS System** als **macOS Lab** vorzuhalten, um auf Probleme im Umgang mit macOS spezifischen Besonderheiten einzugehen!

macOS Lab & Image Einbindung

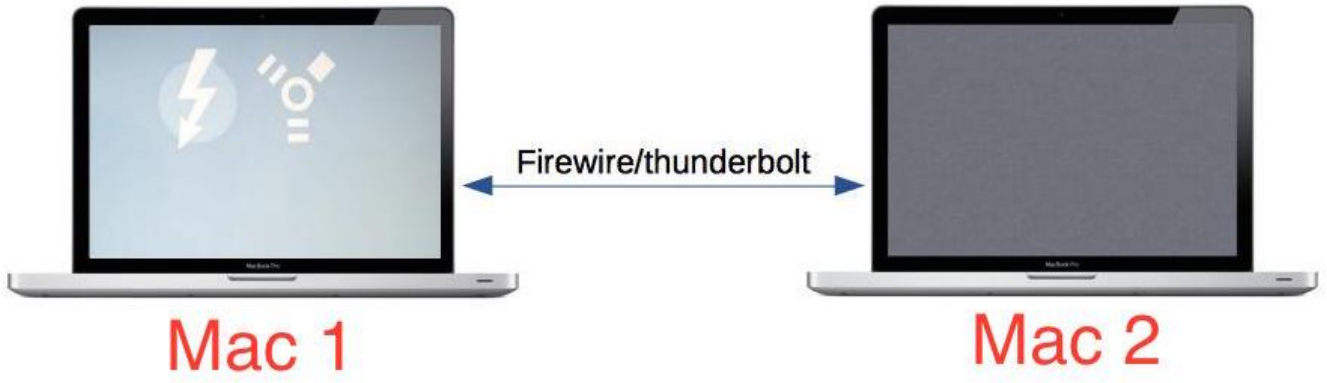
Vorbereitung macOS Lab zur Nutzung als Forensic Lab Station

- Deaktivierung der System Integrity Protection SIP
- Installation Homebrew (Paketmanager)
- Installation Xcode Umgebung
- Installation libewf
- Installation xmount

macOS Lab & Image Einbindung

Anschluss von macOS Asservaten an die Forensic Lab Station

- Nutzung des **Target Disk Mode TDM** beim booten durch drücken von **T**
- danach wird der TDM gestartet am Asservat und das Asservat verhält sich wie eine externe Festplatte (Firewire/Thunderbold)



macOS Lab & Image Einbindung

Anschluss von macOS Asservaten an die Forensic Lab Station

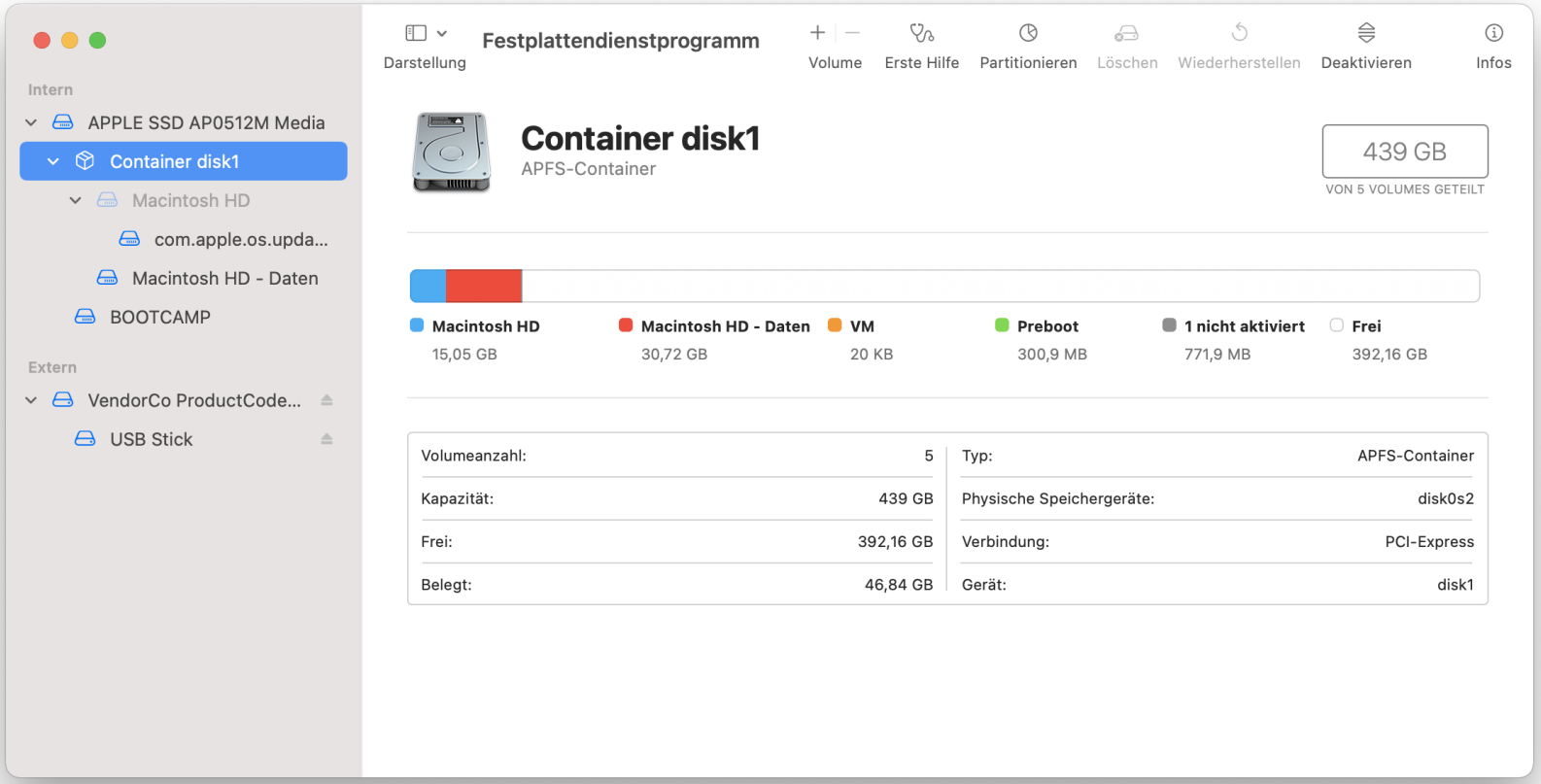
Einschränkungen:

- im TDM Mode wird nur die erste Festplatte durchgegeben
- mit gesetztem Firmewarepasswort lässt sich der TDM Mode nicht starten
- ein Benutzerpassswort mit Admin Berechtigungen ist zum Freischalten der Verschlüsselungen notwendig
- Beim Anschluss wird die Festplatte automatisch im Read-Write Mode eingebunden!
  - ➢ Nutzung eines Hardware Schreibblockers unverzichtbar!

macOS Lab & Image Einbindung

Verhinderung eines Auto Mount an der Forensic Lab Station

Die Auflistung der angeschlossenen Datenträger kann im Festplattendienstprogramm eingesehen werden oder mit dem Terminal Programm diskutil:

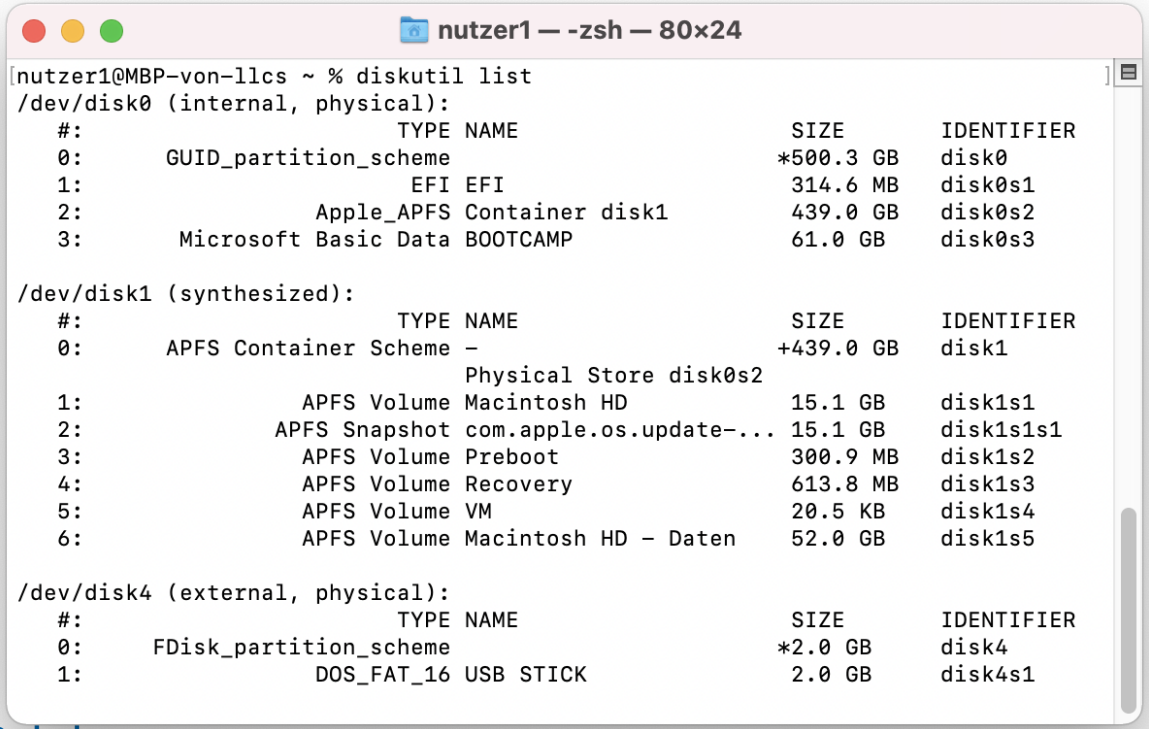


macOS Lab & Image Einbindung

Verhinderung eines Auto Mount an der Forensic Lab Station

Die Auflistung der angeschlossenen Datenträger kann im Festplattendienstprogramm eingesehen werden oder mit dem Terminal Programm diskutil:

diskutil list



macOS Lab & Image Einbindung

Verhinderung eines Auto Mount an der Forensic Lab Station

Beim Anschluss von externen Datenträgern wird durch den Disk Arbitrator jeder Datenträger automatisch im Read Write Mode eingebunden.

- dies kann durch externe Schreibblocker verhindert werden!
- eine weitere Möglichkeit dies zu verhindern ist es den Disk Arbitrator temporär abzuschalten:

  sudo launchctl unload */System/Library/LaunchDaemons/com.apple.diskarbitrationd.plist*

  danach kann der Datenträger ohne Automount angeschlossen und gesichert werden (im gestoppten Zustand kein diskutil verfügbar)
- Nach der Sicherung kann der Dienst wieder gestartet werden:

  sudo launchctl load */System/Library/LaunchDaemons/com.apple.diskarbitrationd.plist*

macOS Lab & Image Einbindung

Datensicherung in macOS Systemen

- Möglichkeit 1 – Live Betrieb/Target Disk Mode mit hdutil
- Möglichkeit 2 – Live Betrieb/Target Disk Mode mit asr
- Möglichkeit 3 – kommerzieller Fremdboot mit Cellebrite Macquisition/Digital Collector
- Möglichkeit 4 – kommerzieller Fremdboot mit Sumuri Recon Imager / Recon ITR
- Möglichkeit 5 – Datensicherung im macOS Lab mit DD bzw. ewfacquire
- Möglichkeit 6 – Datensicherung mittels Bildschirmfotos

macOS Lab & Image Einbindung

Datensicherung Möglichkeit 1 – Live Betrieb/Target Disk Mode mit hdutil

- mit dem Tool hdiutil können Images erstellt und auch eingebunden werden
- Der Befehl lässt sich auf einzelnen Verzeichnisse anwenden und erstellt ein DMG Container Image

hdiutil create *-srcfolder* /Verzeichnisangabe *-volname* DMGNAME /mountpoint/folder/DMGNAME.dmg

- Der erstellte DMG Container ist ein Image welches nicht veränderbar ist und für die weitere Verarbeitung wie eine Festplatte aufgebaut ist.

macOS Lab & Image Einbindung

Datensicherung Möglichkeit 1 – Live Betrieb/Target Disk Mode mit hdutil

- mit dem Tool hdiutil können Images erstellt und auch eingebunden werden
- Der Befehl lässt sich auf einzelnen Verzeichnisse anwenden und erstellt ein DMG Container Image

hdiutil create *-srcfolder* /Verzeichnisangabe *-volname* DMGNAME /mountpoint/folder/DMGNAME.dmg

- Der erstellte DMG Container ist ein Image welches nicht veränderbar ist und für die weitere Verarbeitung wie eine Festplatte aufgebaut ist.

macOS Lab & Image Einbindung

Datensicherung Möglichkeit 2 – Live Betrieb/Target Disk Mode mit asr

- mit dem Tool asr können Images von Disks und Snapshots erstellt werden
- der Befehl lässt sich auf einzelnen Disks anwenden und erstellt eine Kopie auf ein zweites Volume

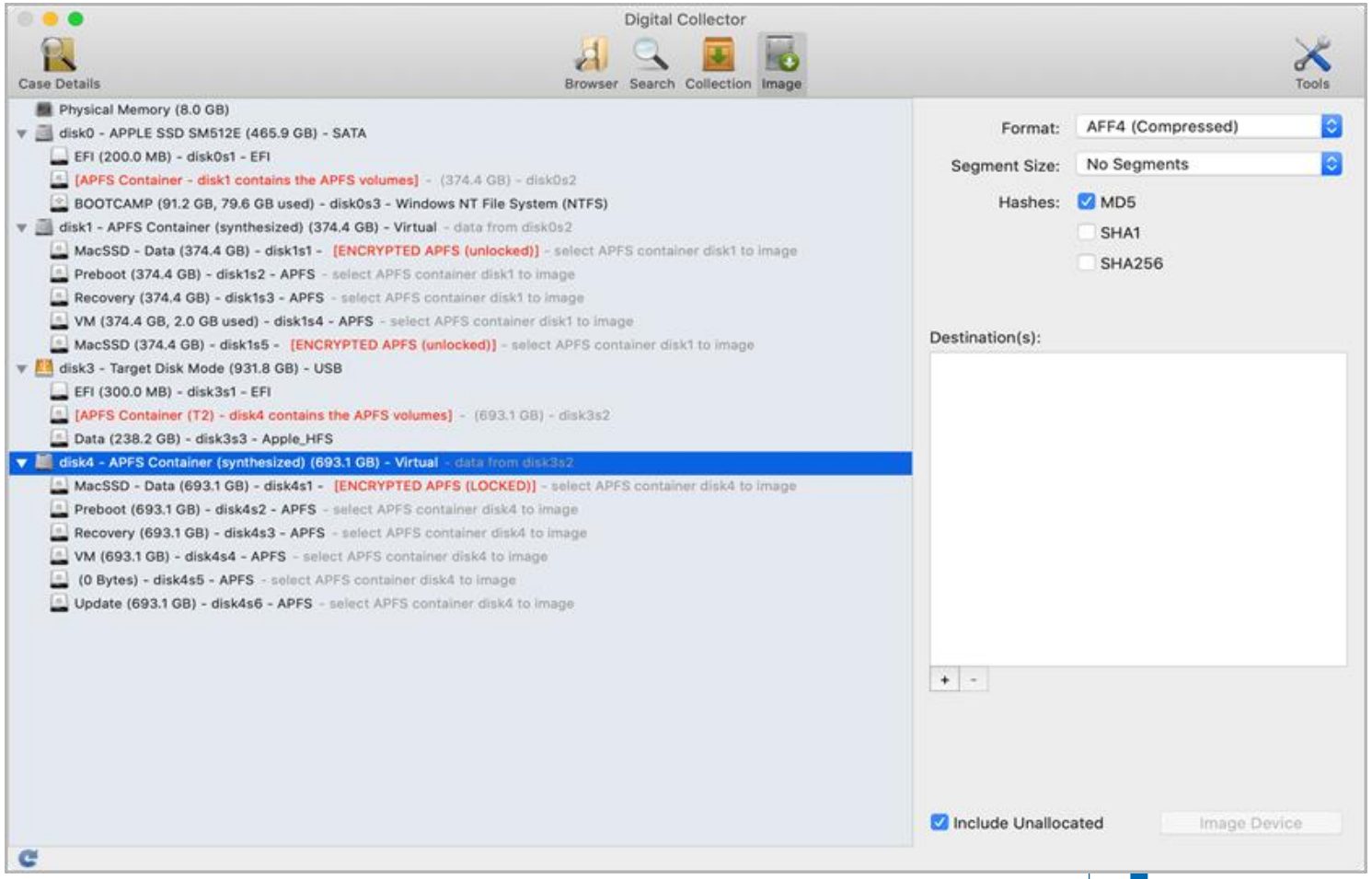
asr restore *--source* /dev/diskx *--target* /dev/diskx
(*--toSnapshot* SnapshotUUID)

- damit kann auch option von einem Snapshot des Systems eine Kopie erstellt werden
- diese Option kann etwa bei Seal Broken Volumes auf den Snapshoot angewendet werden

macOS Lab & Image Einbindung

Datensicherung - Möglichkeit 3 – Cellebrite Macquisition/Digital Collector

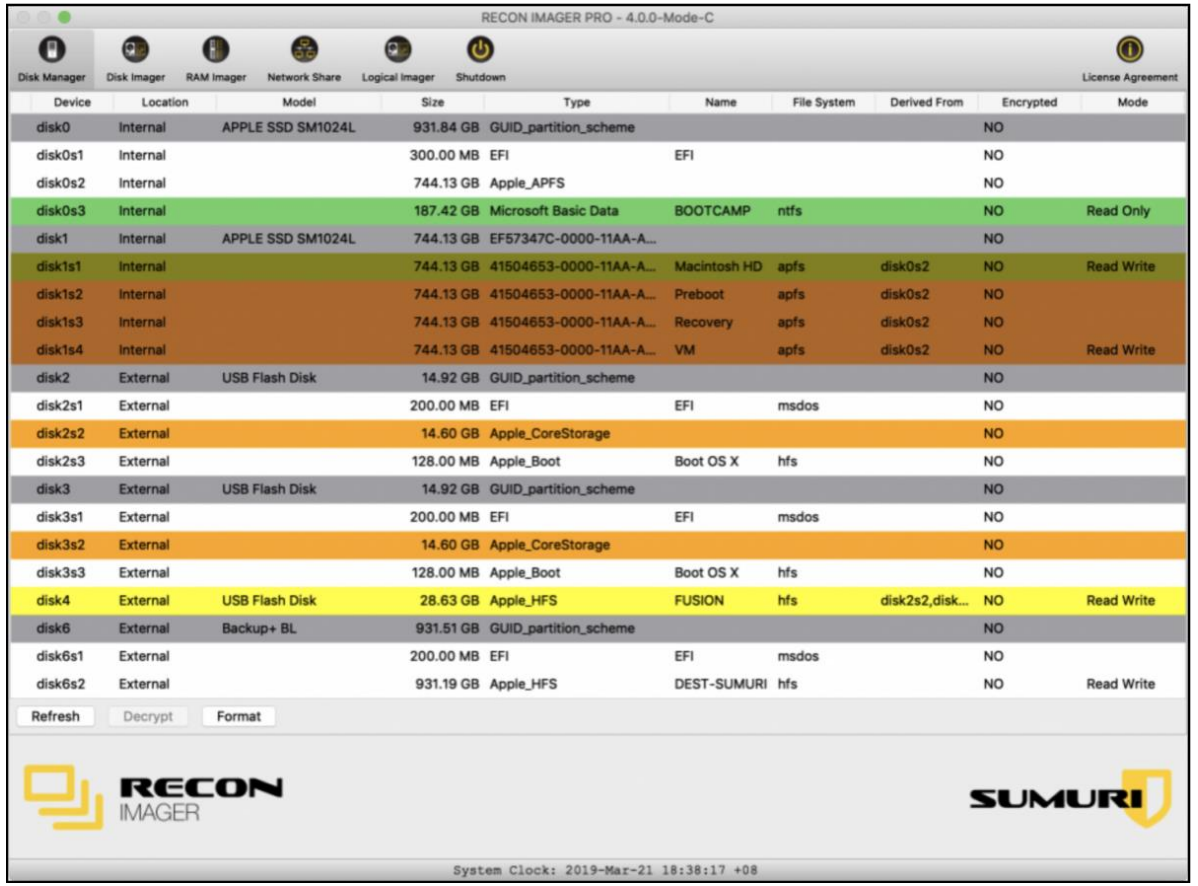
- Kommerzielles Tool welches Dateien einzeln oder ganze Images sichern kann
- Entschlüsselt sowohl T2&M1 Hardware Keys wie auch Filevault2 automatisch
- Passwörter notwendig!



macOS Lab & Image Einbindung

Datensicherung - Möglichkeit 4 – Sumuri Recon Imager / Recon ITR

- Kommerzielles Tool welches Dateien einzeln oder ganze Images sichern kann
- Entschlüsselt sowohl T2&M1 Hardware Keys wie auch Filevault2 automatisch
- Passwörter notwendig!



macOS Lab & Image Einbindung

Datensicherung - Möglichkeit 5 – mit DD bzw. ewfacquire

- mit dem Tool dd können RAW Images von Disks erstellt werden, wie auch unter Linux

  dd *if*=/dev/diskx *of*=/ImageDateiname.dmg (*--bs=512*)

- bei installierter libewf kann auch das Tool ewfacquire genutzt werden

  ewfacquire /dev/diskx

  um *.E01 Images anzulegen
- Mit beiden Tools können von externen Datenträgern Datenträgerkopien erstellt werden, nicht von den internen verschlüsselten Systemen!

macOS Lab & Image Einbindung

Datensicherung - Möglichkeit 6 – mittels Bildschirmfotos

- Oft wird es notwendig zusätzliche Information bei live Datensicherungen zu erheben. Hier haben sich auch Bildschirmfotos bewährt.
- Bildschirmfotos vom kompletten Bildschirm können mit der Tasten-Kombination:

  Shift + Befehlstaste/**Command** (⌘) + **3**

  aufgenommen werden.
- Standard Ablageort ist der Desktop des Benutzers!

macOS Lab & Image Einbindung

Datensicherung - Möglichkeit 6 – mittels Bildschirmfotos

- Oft wird es notwendig zusätzliche Information bei live Datensicherungen zu erhaben. Hier haben sich auch Bildschirmfotos bewährt.
- Bildschirmfotos von Bildschirmfenstern können mit der Tasten-Kombination:

Shift + Befehlstaste/**Command** (⌘) + **5**

aufgenommen werden.

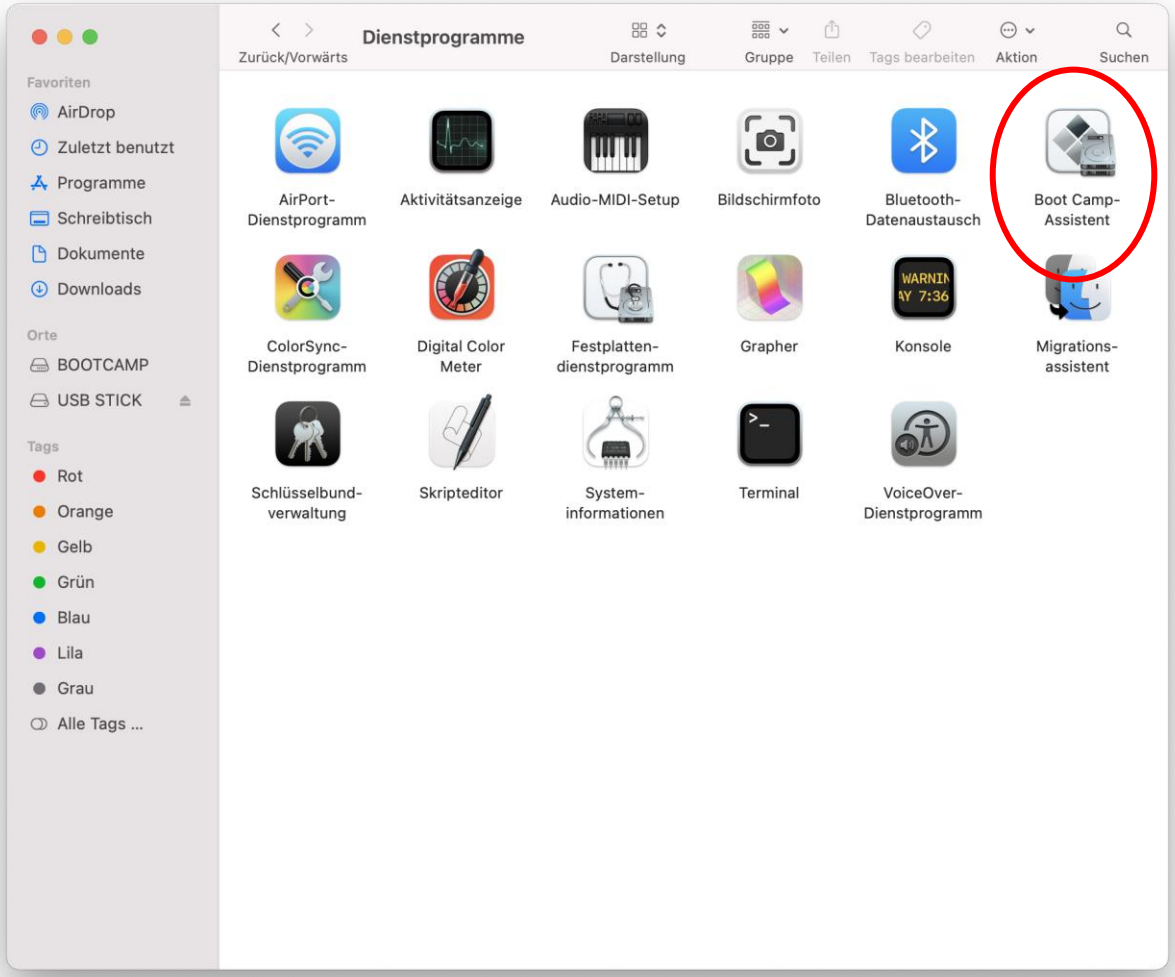
- Hierbei kann auch der Speicherort unter Optionen angegeben werden

BETRIEBSSYSTEM macOS

Bootcamp Besonderheiten (& Parallels)

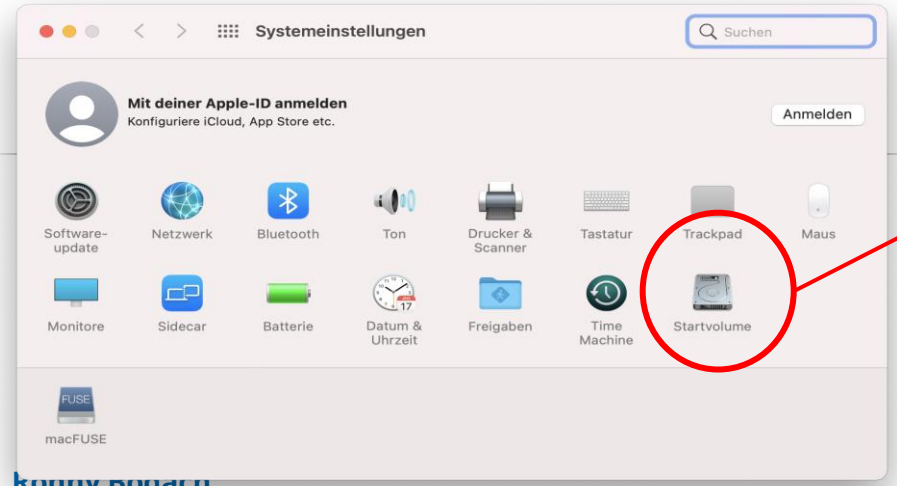
Bootcamp Besonderheiten

- Auf macOS System mit Intel Architektur lässt sich per Einrichtungsdialog ein Windows System installieren
- Die genutzte Technik heißt Bootcamp und erzeugt ein Volume im System für die Installation von Windows
- Auf Silicon Mac Systemen mit M1 Architektur geht dies nicht mehr!



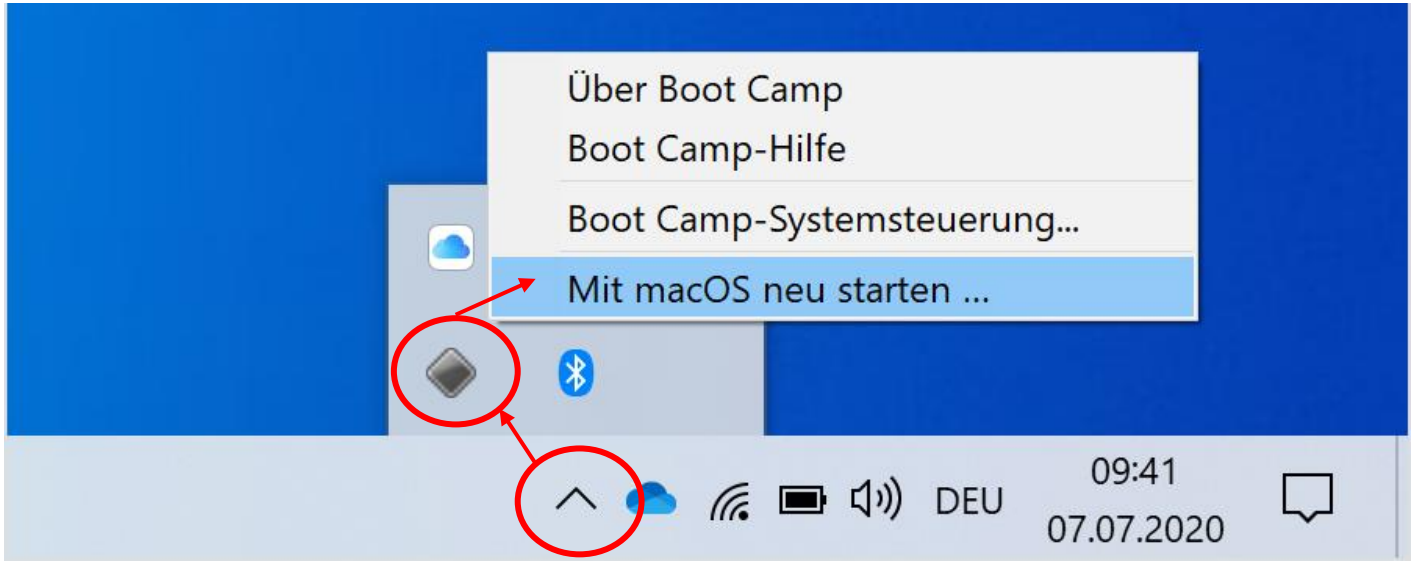
Bootcamp Besonderheiten

- das Startvolume kann entweder im Start Manager (Wahltaste/Option (⌥)) oder
- im macOS Systemeinstellungen > Startvolume (schneller Spotlight > Startvolume) ausgewählt werden



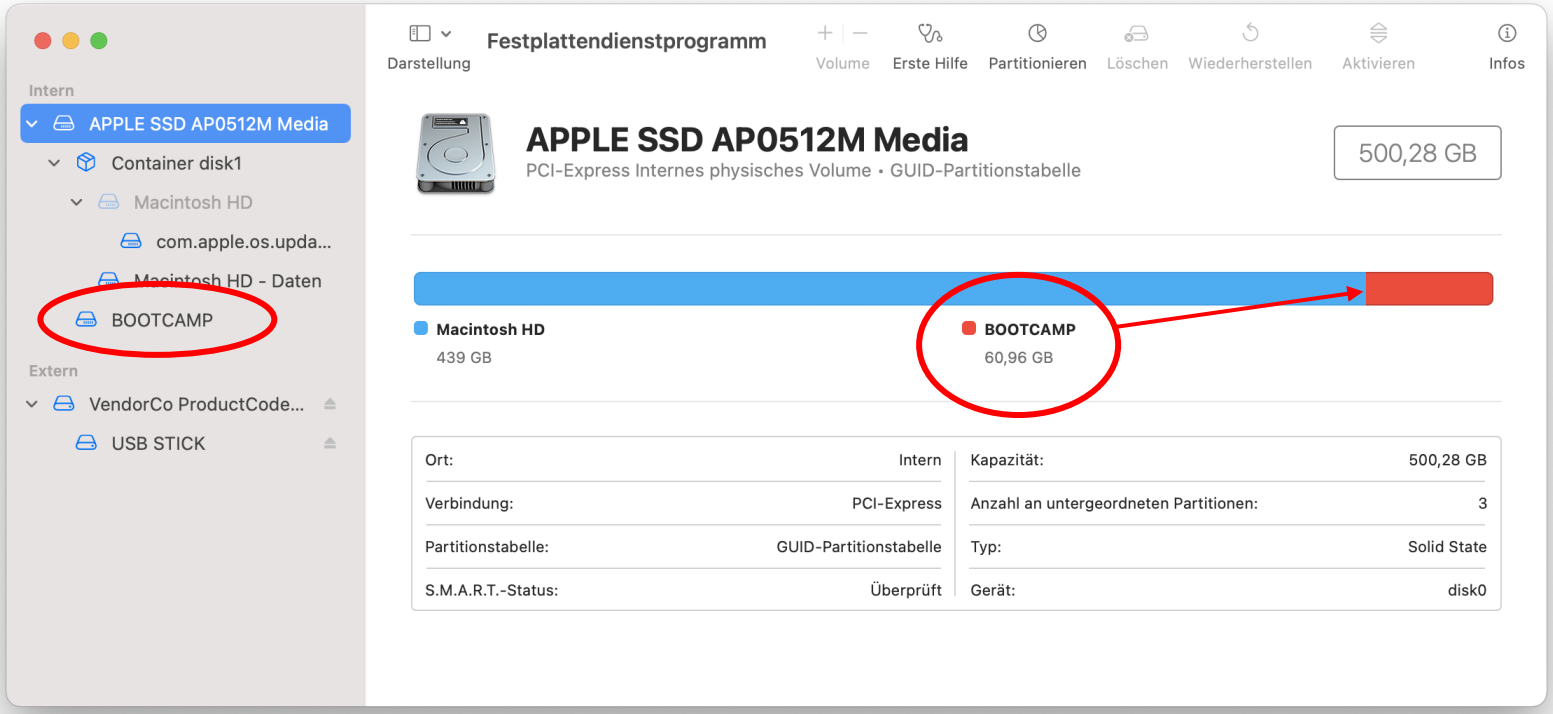
Bootcamp Besonderheiten

- Ein Bootcamp Icon in der Windows Taskbar zeigt an das Bootcamp installiert ist und kann genutzt werden um zurück zu macOS zu booten



Bootcamp Besonderheiten

- das Bootcamp Volume gehört nicht zum APFS Container und ist eine separate Partition!
- es kann wie jede normale Windows Partition untersucht werden



Parallels Besonderheiten

Parallels Desktop

- Virtualisierungslösung als Alternative zu Bootcamp
- Bewährte Desktop-Virtualisierungs-software seit 15 Jahren
- Installation von Windows und Linux auf Intel- oder Apple M1-Mac (derzeit einziger Anbieter)
- Flüssige Reaktionszeit der Windows-Benutzeroberfläche und Videowiedergabe
- Optimiert für macOS Monterey und Windows 11
- Konkurrent zum VMWare Fusion (kein Windows Support auf Silicon M1 mac‘s)

Vielen Dank

Prof. Ronny Bodach

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

T +49 (0) 3727 58-1011
F +49 (0) 3727 58-21011
bodach@hs-mittweida.de
www.cb.hs-mittweida.de

Haus 8 | Richard-Stücklen Bau | Raum 8-205
Am Schwanenteich 6b | 09648 Mittweida

HOCHSCHULE MITTWEIDA
University of Applied Sciences

hs-mittweida.de