

# Betriebssysteme

## macOS - Teil4

Autor: Prof. Ronny Bodach



**HOCHSCHULE  
MITTWEIDA**  
University of Applied Sciences



**Fraunhofer**  
SIT



Bundeskriminalamt

# 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

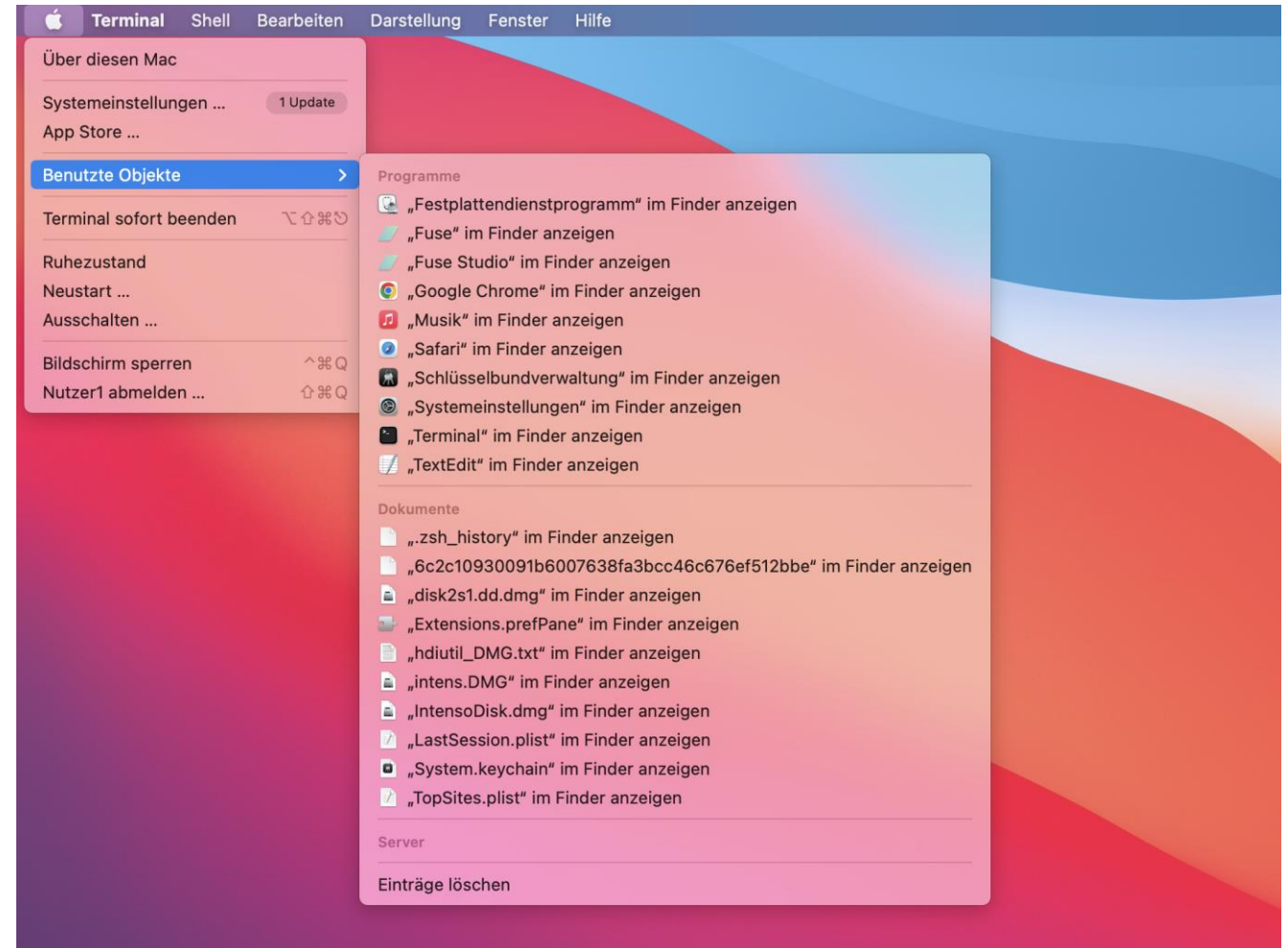
7. Zuletzt genutzte Elemente & Nutzeraktivitäten
8. Spotlight und erweiterte Metadaten
9. Gelöschte Dateien
10. Schlüsselbund

# **BETRIEBSSYSTEM macOS**

**Zuletzt genutzte Elemente & Nutzeraktivitäten**

# Zuletzt genutzte Elemente & Nutzeraktivitäten

Recent/Verlaufseinträge  
Können für den Benutzer über  
das Apfel Symbol unter  
„Benutzte Objekte“ angezeigt  
werden.



# Zuletzt genutzte Elemente & Nutzeraktivitäten

In macOS Versionen vor Big Sure werden diese unter folgenden Einträgen in Plist Dateien erfasst:

- Recent Einträge:

`%%users.homedir%%/Library/Preferences/com.apple.recentitems.plist`

- Recent Einträge pro Anwendung:

`%%users.homedir%%/Library/Preferences/*LSSharedFileList.plist`

# Zuletzt genutzte Elemente & Nutzeraktivitäten

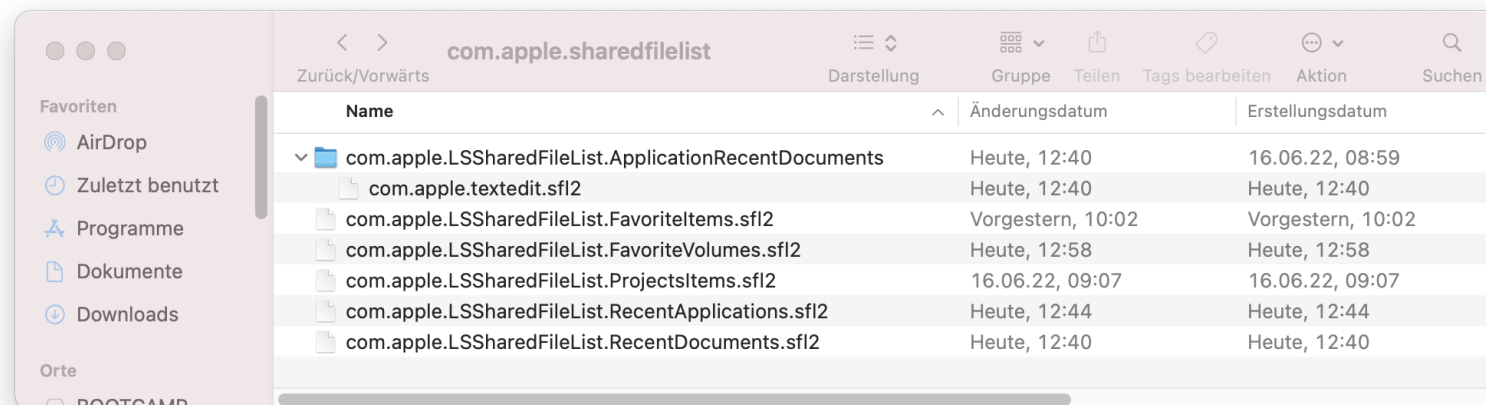
In macOS Versionen ab Big Sure werden diese unter folgenden Einträgen in \*.sif2 (Bplist) Dateien erfasst:

- Recent Einträge:

~/Library/Application\ Support/com.apple.sharedfilelist/\*.sif2

- Recent Einträge pro Anwendung:

com.apple.LSSharedFileList.ApplicationRecentDocuments/\*.sif2



# Zuletzt genutzte Elemente & Nutzeraktivitäten

In macOS Versionen ab Big Sure werden diese unter folgenden Einträgen in \*.sif2 (Bplist) Dateien erfasst:

```

com.apple.LSSharedFileList.RecentDocuments.sif2
393 <dict>
394   <key>NS.keys</key>
395   <array>
396   </array>
397   <key>NS.objects</key>
398   <array>
399   </array>
400   <key>$class</key>
401   <dict>
402     <key>CF$UID</key>
403     <integer>12</integer>
404   </dict>
405 </dict>
406 <string>disk2s1.dd.dmg</string>
407 <data>
408 Ym9va7QCAAAAAAAAQMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEA
409 AAQAAAAADwAAAAAAAAIAUAAAAAQAQAVXN1cnMAAAAHAAAAQEAAAG5ldHp1cjEADgAAAAEB
410 AABkaXNrMnMxLmRkLmRtZWAAADAAAAEGAAQAQAAAIATAAADAAAAIAAAABAMAAKXgAAAA
411 AAAACAAAAQDAAC2wwIAAAAAAagAAAAEAAAC9MFAAAAAAMAAAAQYAAFWAAABsAAAA
412 fAAAAAgAAAAABAAQcQw2Xc4jqEYAAAAQIAAAEAAAAAAAAAHwIAAAAAAAaAgAAAAAA
413 AAgAAAAEAWAAQAAAAAAAAAAAAAAwMAAPYBAAAIATAAAQkAAGZpbGU6Ly8vDAAAAEB
414 AABNYWNpbnRvc2ggSEQIAAAABAMAAACgfhZmAAAACAAAAAEAABBwd5EgAAAAACQAAAAA
415 AQAAQTQ0OURFjAtQjMwMy00QzVELUxFFMkQtNkQyNTRCRTCVCOTBFGAAAAEAACAABAAAA
416 AQAAAO8TAAABAAAAAAAAAAAAAAAAAAAAAAQEAAC8AAAAAAAAAAQUAAAAAAAAABQAA5AAA
417 AP7///8BAAAAAAAAABIAAAAEFAAAASAAAAAAAAAAFEAAAjAAAAAAAAAAQEAASAAAAAAA
418 AABAEAAAoAAAAAAAAAACIAAAfEAAAAAAAAAFIAAA7AAAAAAAAAQIAAA/AAAAAAAAAR
419 IAAMAEAAAAAAAAASIAAAEFAAAAAAAAAATIAAAIAEAAAAAAAAAgIAAAAEAAAAAAAAAwIAAA
  
```

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000A60	A0	A0	80	0C	5E	64	69	73	6B	32	73	31	2E	64	64	2E	e.^disk2s1.dd.
00000A70	64	6D	67	4F	11	02	B4	62	6F	6F	6B	B4	02	00	00	00	dmgO..'book'....
00000A80	00	04	10	30	00	00	00	00	00	00	00	00	00	00	00	00	...0.....
00000A90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000AA0	00	00	00	00	00	00	00	98	01	00	00	04	00	00	00	03	.....~.....
00000AB0	03	00	00	00	00	00	20	05	00	00	00	01	01	00	00	55	.....U
00000AC0	73	65	72	73	00	00	07	00	00	00	01	01	00	00	00	6E	sers.....n
00000AD0	75	74	7A	65	72	31	00	0E	00	00	00	01	01	00	00	64	utzer1.....d
00000AE0	69	73	6B	32	73	31	2E	64	64	2E	64	6D	67	00	00	0C	isk2s1.dd.dmg...
00000AF0	00	00	00	01	06	00	00	10	00	00	00	20	00	00	00	30	.....0
00000B00	00	00	00	08	00	00	00	04	03	00	00	AC	60	00	00	00	.....~`...
00000B10	00	00	00	08	00	00	00	04	03	00	00	B6	C3	02	00	00	.....Ä...
00000B20	00	00	00	08	00	00	00	04	03	00	00	0B	D3	05	00	00	.....Ö...
00000B30	00	00	00	0C	00	00	00	01	06	00	00	5C	00	00	00	6C	.....\...l
00000B40	00	00	00	7C	00	00	00	08	00	00	00	00	04	00	00	41	... .....A
00000B50	C4	30	D9	77	38	8E	A1	18	00	00	00	01	02	00	00	01	Ä0Ûw8žj.....
00000B60	00	00	00	00	00	00	00	1F	02	00	00	00	00	00	00	1A	.....
00000B70	02	00	00	00	00	00	00	08	00	00	00	04	03	00	00	01	.....
00000B80	00	00	00	00	00	00	00	04	00	00	00	03	03	00	00	F6	.....ö
00000B90	01	00	00	08	00	00	00	01	09	00	00	66	69	6C	65	3A	.....file:
00000BA0	2F	2F	2F	0C	00	00	00	01	01	00	00	4D	61	63	69	6E	///.....Macin
00000BB0	74	6F	73	68	20	48	44	08	00	00	00	04	03	00	00	00	tosh HD.....



# Zuletzt genutzte Elemente & Nutzeraktivitäten

Terminal Kommando Historie

- mit Bash Shell:

```
%%users.homedir%%/.bash_history
```

- mit Z-Shell:

```
%%users.homedir%%/.zsh_history
```

# Zuletzt genutzte Elemente & Nutzeraktivitäten

## Knowledge is Power!

- **pattern-of-life** Daten gehören zu den nützlichsten Informationen auf einem Gerät – sie erzählen die tatsächliche Geschichte über die Nutzung eines Gerätes durch den Benutzer
- **knowledgeC.db** – Datenbank
- auch auf **iOS Geräten** vorhanden
- **SQLite Datenbank** mit Eintragungen zur genauen Benutzer- und Anwendungsnutzung

# Zuletzt genutzte Elemente & Nutzeraktivitäten

## KnowledgeC.db

- beinhaltet:
  - Application Usage
  - Application Activities
  - Safari Browser History
  - Device Power Status
  - Lock Status (iOS Only)
  - Battery Usage (iOS Only)
  - App Installations (iOS Only)
  - Audio Status (iOS Only)

# Zuletzt genutzte Elemente & Nutzeraktivitäten

## KnowledgeC.db

- Fundstellen:
  - System Kontext Datenbank

/private/var/db/CoreDuet/Knowledge/**KnowledgeC.db**

- Benutzer Datenbank

%%users.homedir%%/Library/Application  
Support/Knowledge/**KnowledgeC.db**

# Zuletzt genutzte Elemente & Nutzeraktivitäten

## KnowledgeC.db

- Folgende Eintragungen werden als Inhalt erfasst:
  - "/activity/level"
  - "/app/activity"
  - "/app/inFocus"
  - "/app/intents"
  - "/app/usage"
  - "/app/WebUsage"
  - "/device/isPluggedIn"
  - "/display/isBacklit"
  - "/safari/history"

# Zuletzt genutzte Elemente & Nutzeraktivitäten

## KnowledgeC.db

- Aufbau:
  - die Datenbank hat viele Tabellen mit multiplen Spalten
  - Tabelle ZOBJECT – Enthält potenziell Nutzungseinträge für etwa 4 Wochen
  - Andere Tabellen, auf die ZOBJECT-Einträge verweisen können, befinden sich in diesen Tabellen:
    - ZSOURCE – Quelle der ZOBJECT-Einträge
    - ZSTRUCTUREDMETADATA – Zusätzliche Metadaten, die ZOBJECT-Einträgen zugeordnet sind
  - Zeitstempel in dieser Datenbank verwenden die Mac-Epochenzeit (01.01.2001 00:00:00 UTC)

# Zuletzt genutzte Elemente & Nutzeraktivitäten

## KnowledgeC.db

The screenshot shows the DB Browser for SQLite interface. The title bar indicates the database path: E:\Knowledge\knowledgeC.db. The menu bar includes Datei, Bearbeiten, Ansicht, Werkzeuge, and Hilfe. The toolbar contains icons for opening a new database, opening an existing database, saving changes, undoing changes, opening a project, and attaching a database.

The main window has tabs for Datenbankstruktur, Daten durchsuchen, Pragmas bearbeiten, and SQL ausführen. The SQL editor shows the following query:

```
SQL 1
1 SELECT
2 datetime(ZOBJECT.ZCREATIONDATE+978307200,'UNIXEPOCH', 'LOCALTIME') as "ENTRY CREATION",
3 CASE ZOBJECT.ZSTARTDAYOFWEEK
4 WHEN "1" THEN "Sunday"
5 WHEN "2" THEN "Monday"
6 WHEN "3" THEN "Tuesday"
7 WHEN "4" THEN "Wednesday"
8 WHEN "5" THEN "Thursday"
9 WHEN "6" THEN "Friday"
```

The results table displays the following data:

	ENTRY CREATION	DAY OF WEEK	START	END	USAGE IN SECONDS	ZSTREAMNAME	ZVALUESTRING
324	2022-06-23 12:50:56	Thursday	2022-06-23 12:50:53	2022-06-23 12:50:56	3	/app/usage	com.apple.Terminal
325	2022-06-23 12:55:56	Thursday	2022-06-23 12:50:56	2022-06-23 12:55:56	300	/app/usage	com.apple.finder
326	2022-06-23 13:02:04	Thursday	2022-06-23 12:58:32	2022-06-23 13:02:04	212	/app/usage	com.apple.finder
327	2022-06-23 13:02:08	Thursday	2022-06-23 13:02:04	2022-06-23 13:02:08	4	/app/usage	com.apple.TextEdit
328	2022-06-23 13:07:34	Thursday	2022-06-23 13:02:08	2022-06-23 13:07:34	326	/app/usage	com.apple.finder
329	2022-06-23 13:21:42	Thursday	2022-06-23 13:14:37	2022-06-23 13:21:42	425	/app/usage	com.apple.finder

The status bar at the bottom indicates: Ergebnis: 329 Zeilen in 863ms zurückgegeben. In Zeile 1: 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"

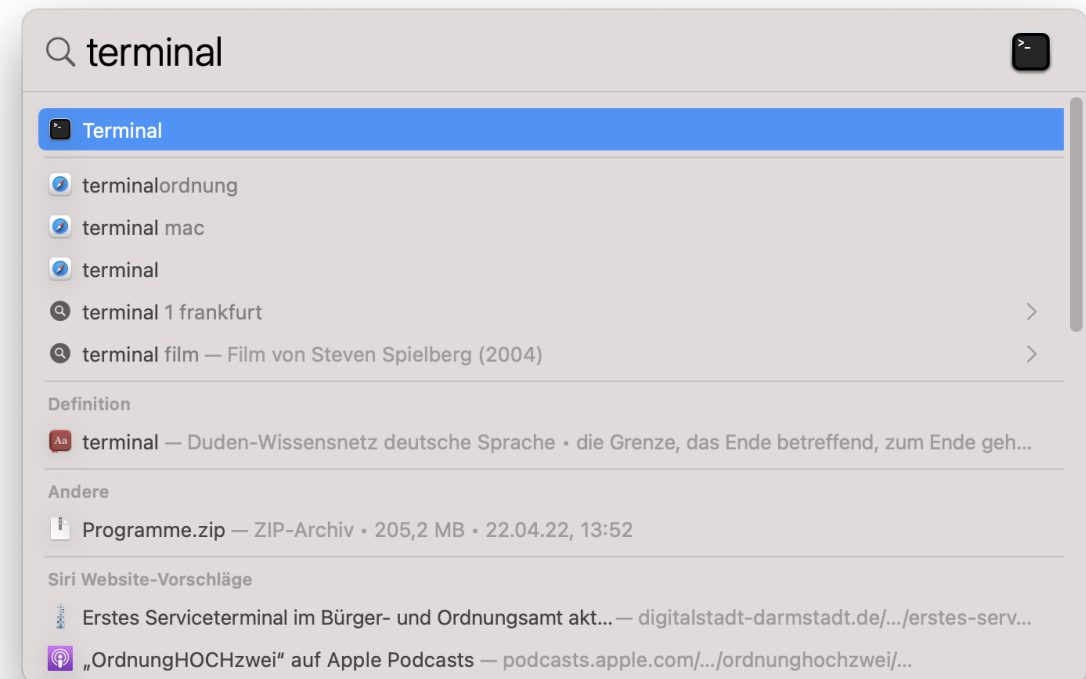
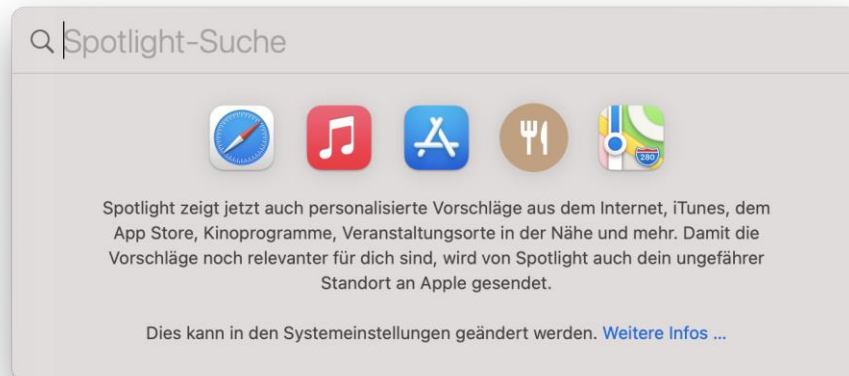
# BETRIEBSSYSTEM macOS

Spotlight und erweiterte Metadaten



# Spotlight und erweiterte Metadaten

- Spotlight ist der Name des Indexierungssystems, das in macOS integriert ist.
- Aufrufbar mit Befehlstaste/Command (⌘) + Leertaste



# Spotlight und erweiterte Metadaten

Spotlight ist aber auch:

- für die kontinuierliche Indizierung von Dateien und Ordnern auf allen angeschlossenen Volumes verantwortlich
- bewahrt eine Kopie aller Metadaten für fast jede einzelne Datei und jeden Ordner auf der Festplatte auf
- kann einige hervorragende Daten für Ihre Untersuchung liefern
  - Während viele der gleichen Informationen erhalten werden können, wenn Sie Zugriff auf das vollständige Disk-Image haben, ist bekannt, dass diese Datenbank Informationen enthält, die anderswo nicht verfügbar sind.
  - Details wie das/die Datum(e) des letzten Öffnens oder wie oft (eine Anwendung oder Datei) geöffnet/verwendet wurde, sind nirgendwo anders im Dateisystem verfügbar

# Spotlight und erweiterte Metadaten

- die Meta Daten einer Datei können zudem auch über den Befehl

**mdls ./DATEI**

im Terminal pro Datei abgerufen werden:

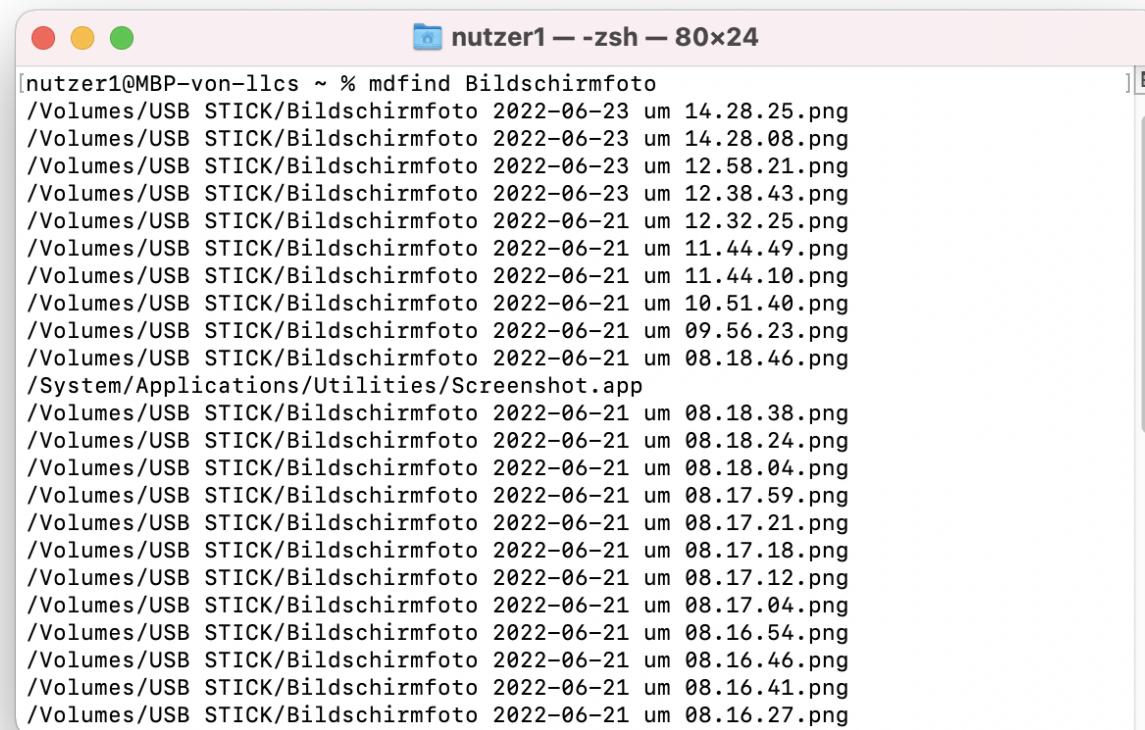
```
nutzer1@MBP-von-llcs ~ % mdls /Volumes/USB\ STICK/Bildschirmfoto\ 2022-06-23\ um
\ 12.58.21.png
_kMDItemDisplayNameWithExtensions = "Bildschirmfoto 2022-06-23 um 12.58.21.
png"
kMDItemAlternateNames = (
    "Bildschirmfoto 2022-06-23 um 12.58.21.png"
)
kMDItemBitsPerSample = 32
kMDItemColorSpace = "RGB"
kMDItemComment = "Screenshot"
kMDItemContentCreationDate = 2022-06-23 10:58:26 +0000
kMDItemContentCreationDate_Ranking = 2022-06-23 00:00:00 +0000
kMDItemContentModificationDate = 2022-06-23 10:58:26 +0000
kMDItemContentModificationDate_Ranking = 2022-06-23 00:00:00 +0000
kMDItemContentType = "public.png"
kMDItemContentTypeTree = (
    "public.png",
    "public.image",
    "public.data",
    "public.item",
    "public.content"
)
```

```
nutzer1@MBP-von-llcs ~ % mdls /Volumes/USB\ STICK/Bildschirmfoto\ 2022-06-23\ um
\ 12.58.21.png
kMDItemLastUsedDate_Ranking = 2022-06-23 00:00:00 +0000
kMDItemLogicalSize = 291961
kMDItemOrientation = 0
kMDItemPhysicalSize = 294912
kMDItemPixelCount = 1364480
kMDItemPixelHeight = 656
kMDItemPixelWidth = 2080
kMDItemProfileName = "Farb-LCD"
kMDItemResolutionHeightDPI = 144
kMDItemResolutionWidthDPI = 144
kMDItemScreenCaptureGlobalRect = (
    285,
    372,
    1040,
    328
)
kMDItemScreenCaptureType = "window"
kMDItemUseCount = 1
kMDItemUsedDates = (
    "2022-06-22 22:00:00 +0000"
)
nutzer1@MBP-von-llcs ~ %
```

# Spotlight und erweiterte Metadaten

- Die Suche nach Dateien kann über den Befehl **mdfind** im Terminal gestartet werden:

## mdfind Suchbegriff



```
nutzer1@MBP-von-llcs ~ % mdfind Bildschirmfoto
/Volumes/USB STICK/Bildschirmfoto 2022-06-23 um 14.28.25.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-23 um 14.28.08.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-23 um 12.58.21.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-23 um 12.38.43.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 12.32.25.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 11.44.49.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 11.44.10.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 10.51.40.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 09.56.23.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 08.18.46.png
/System/Applications/Utilities/Screenshot.app
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 08.18.38.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 08.18.24.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 08.18.04.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 08.17.59.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 08.17.21.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 08.17.18.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 08.17.12.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 08.17.04.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 08.16.54.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 08.16.46.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 08.16.41.png
/Volumes/USB STICK/Bildschirmfoto 2022-06-21 um 08.16.27.png
```

# Spotlight und erweiterte Metadaten

- die Informationen die Spotlight dabei nutzt befinden sich in Datenbank Dateien **store** bzw. **.store**
- zu finden im jeweiligen Datenträger unter:

`/.Spotlight-V100/Store-V2/<UUID>/.store`

- seit macOS 10.13, existiert zudem eine Datenbank für jeden Nutzer unter:

`~/Library/Metadata/CoreSpotlight/index.spotlightV3/.store`

# Spotlight und erweiterte Metadaten

- leider verwendet es ein proprietäres, undokumentiertes Format, und es gibt keinen öffentlich verfügbaren Code von Apple, um es zu lesen
- es existiert jedoch ein Spotlight parser für Python der hier genutzt werden kann:

[https://github.com/ydkhatri/spotlight\\_parser](https://github.com/ydkhatri/spotlight_parser)

```
C:\spotlight_parser>c:\Python27\python.exe spotlight_parser.py g:\ElCapitan\store.db c:\output\elcap
INFO - Output folder 'c:\output\elcap' does not exist! Creating it for you.
INFO - Processing g:\ElCapitan\store.db
INFO - Creating output file c:\output\elcap\spotlight-store_data.txt
INFO - Creating output file c:\output\elcap\spotlight-store_fullpaths.csv
DEBUG - Trying to decompress compressed block @ 19014
DEBUG - Trying to decompress compressed block @ 7D014
DEBUG - Trying to decompress compressed block @ 71014
DEBUG - Trying to decompress compressed block @ A5014

... output snipped ...

DEBUG - Trying to decompress compressed block @ 7F9014
DEBUG - Trying to decompress compressed block @ 801014
...
DEBUG - Err, could not find path for id 956655
DEBUG - Err, could not find path for id 957257
DEBUG - Err, could not find path for id 963495
INFO - Finished in time = 00:00:48
```

# Spotlight und erweiterte Metadaten

[https://github.com/ydkhatri/spotlight\\_parser](https://github.com/ydkhatri/spotlight_parser)

```
Inode_Num --> 100
Flags --> 0
Store_ID --> 5824
Parent_Inode_Num --> 0
Last_Updated --> 2018-02-20 00:10:56
_kMDItemContentChangeDate --> 2017-11-09 22:57:58
_kMDItemCreationDate --> 2017-11-09 23:03:35
_kMDItemCreatorCode --> 0
_kMDItemFileName --> 96206759_099496705b_b.jpg
_kMDItemFinderFlags --> 0
_kMDItemFinderLabel --> 0
_kMDItemGroupId --> 13
_kMDItemIsExtensionHidden --> 0
_kMDItemOwnerGroupID --> 99
_kMDItemOwnerUserID --> 99
_kMDItemTextContentIndexExists --> 0
_kMDItemTypeCode --> 0
kMDItemBitsPerSample --> 32
```

```
kMDItemInterestingDate_Ranking --> 2017-11-09 00:00:00
kMDItemKind --> JPEG image
kMDItemLastUsedDate --> 2017-11-09 23:13:43.323351
kMDItemLastUsedDate_Ranking --> 2017-11-09 00:00:00
kMDItemLogicalSize --> 763434
kMDItemOrientation --> 0
kMDItemPhysicalSize --> 786432
kMDItemPixelCount --> 786432
kMDItemPixelHeight --> 768
kMDItemPixelWidth --> 1024
kMDItemResolutionHeightDPI --> 72
kMDItemResolutionWidthDPI --> 72
kMDItemUseCount --> 6
kMDItemUsedDates --> 2017-11-09 05:00:00, 2018-02-19 05:00:00
```

- Rot sind Metadaten, die sich auf einen einzelnen Eintrag in der Datenbank beziehen, einschließlich Datum und Uhrzeit der letzten Aktualisierung.
- Danach folgen die Metadaten selbst.
- Die Elemente in Blau sind Informationen, die nur in der Spotlight-Datenbank verfügbar sind. Die letzten beiden können für einen Ermittler von besonderem Interesse sein.

# BETRIEBSSYSTEM macOS

Gelöschte Dateien



# Gelöschte Dateien

Der Papierkorb:

- auf jedem Laufwerk existiert ein Verzeichnis **.Trashes** welches die gelöschten Dateien in einem Unterverzeichnis beinhaltet
- die darin befindlichen Dateien haben ihren originalen Dateinamen behalten

Name ▲	Beschreibung	Erw.	Größe
.. = .Trashes (4)	existierend		611 KB
. = 502 (4)	existierend		611 KB
.DS_Store	existierend		6,0 KB
Bildschirmfoto 2022-06-23 um 16.17.42.png (2)	existierend	png	605 KB

- im **.Trashes** Verzeichnis befindet sich zudem eine Datei **.DS\_Store**, diese beinhaltet die notwendigen Pfadangaben der gelöschten Inhalte, um diese wiederherstellen zu können

# Gelöschte Dateien

Der Papierkorb:

- Die **.DS\_Store** Dateien enthalten neben den Dateinamen Informationen über die Ansichtseinstellungen, der Position von Icons, Sortiereinstellungen, Informationen über Fenstergröße und -position sowie andere Metadaten.
- **.DS\_Store** Dateien aus dem Papierkorb können Auskunft über Struktur und Ordnernamen eventuell bereits gelöschter Daten geben, auch wenn diese durch mehrfaches Überschreiben oder ähnliche Maßnahmen tatsächlich physikalisch nicht mehr nachweisbar sind.

# Gelöschte Dateien

**.DS\_Store** Dateien können mit einem speziellen Parser gelesen werden:

[https://github.com/hanwenzhu/.DS\\_Store-parser](https://github.com/hanwenzhu/.DS_Store-parser)

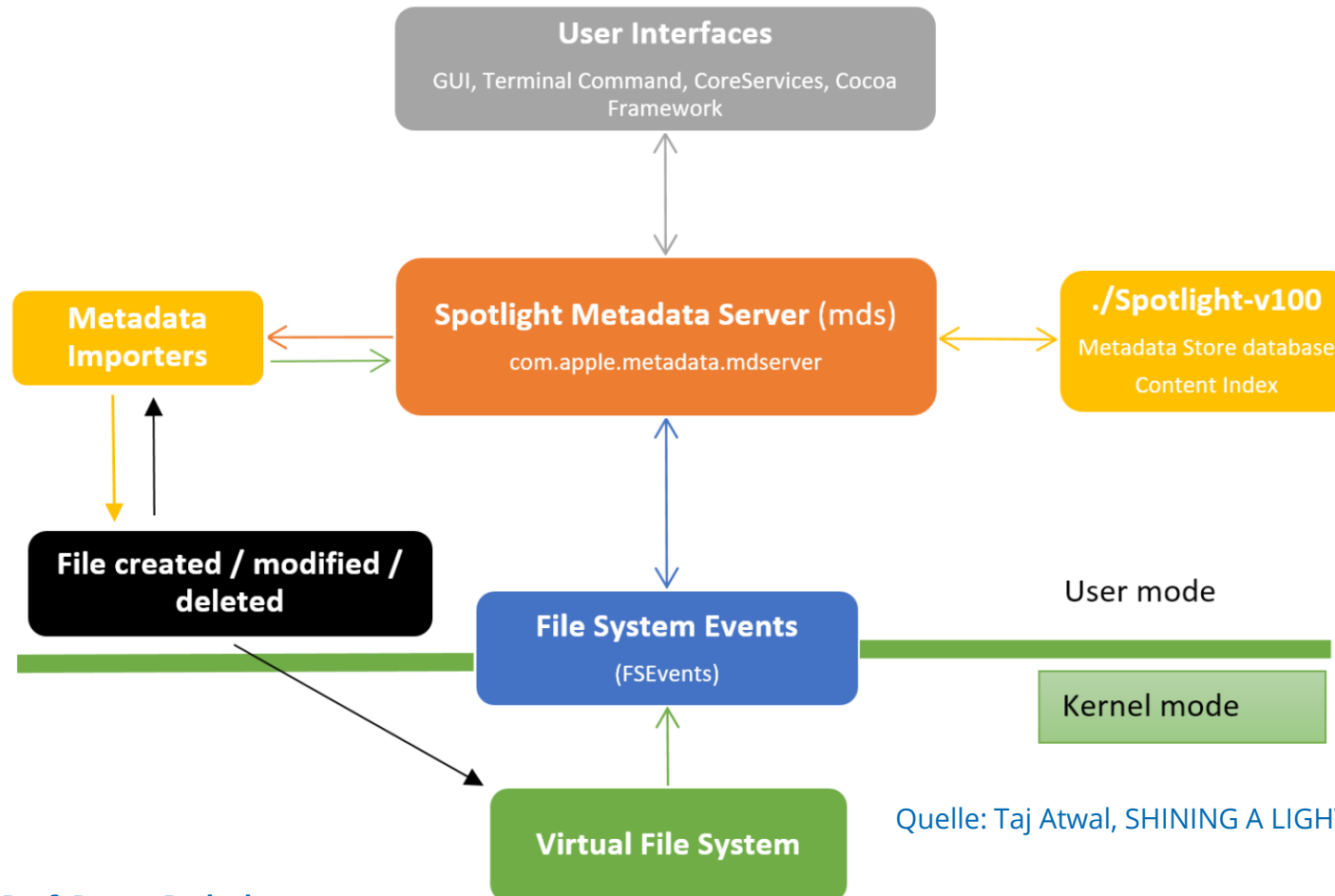
```
F:\>python F:\dsparse.py F:\.DS_Store
Bildschirmfoto 2022-06-23 um 16.17.42.png
  ptbL (unrecognized): '/'
  ptbN (unrecognized): 'Bildschirmfoto 2022-06-23 um 16.17.42.png'

F:\>
```

Im Beispiel ist die Bildschirmfoto 2022-06-23 um 16.17.42.png aus dem Verzeichnis / des Datenträgers gelöscht worden.

# Gelöschte Dateien

Dateisystem Artefakte und deren Zusammenspiel:



# Gelöschte Dateien

## FSEvents

- eingeführt mit macOS 10.7 Lion
- zu finden auf macOS Systemen und externen Datenträgern
- Registriert Dateisystemänderungen in FSEvent log Dateien (gzip):
  - Historische Ereignisse von Änderungen am Dateisystem
  - Protokolle können Tage bis Monate umfassen
  - Datensätze werden alphabetisch und nicht chronologisch gespeichert

# Gelöschte Dateien

## FSEvent logs

- Fundstelle in macOS (System oder Laufwerk):

**/.fseventsd/xxxxxxxxxxx**

- Gzip archive format
- Name ist letzte gespeicherte Event ID im FSevent log +1
- z.B. "000000000000a4b3e" oder 674,622 Dezimal

# Gelöschte Dateien

FSEvent logs können mit einem speziellen Parser gelesen werden:

<https://github.com/dlcowen/FSEventsParser>

```
C:\Users\John>F:\FSEParser_V4.exe -s F:\.fseventsd -o f:\fsout -t folder
=====
FSEParser v 4.0 -- provided by G-C Partners, LLC
=====
[Info]: Report queries file not specified using the -q option. Custom reports will not be generated.
[Info]: No casename specified using -c. Defaulting to "FSE_Reports".

[STARTED] 06/23/2022 14:29:25 UTC Parsing files.
  File 4 of 4  [=====] 100.0%
  All Files Attempted: 4
  All Parsed Files: 4
  Files with Errors: 0
  All Records Parsed: 22
[FINISHED] 06/23/2022 14:29:25 UTC Parsing files.

[STARTED] 06/23/2022 14:29:25 UTC Sorting fsevents table in Database.
[FINISHED] 06/23/2022 14:29:25 UTC Sorting fsevents table in Database.

[STARTED] 06/23/2022 14:29:25 UTC Exporting fsevents table from Database.
[FINISHED] 06/23/2022 14:29:25 UTC Exporting fsevents table from Database.

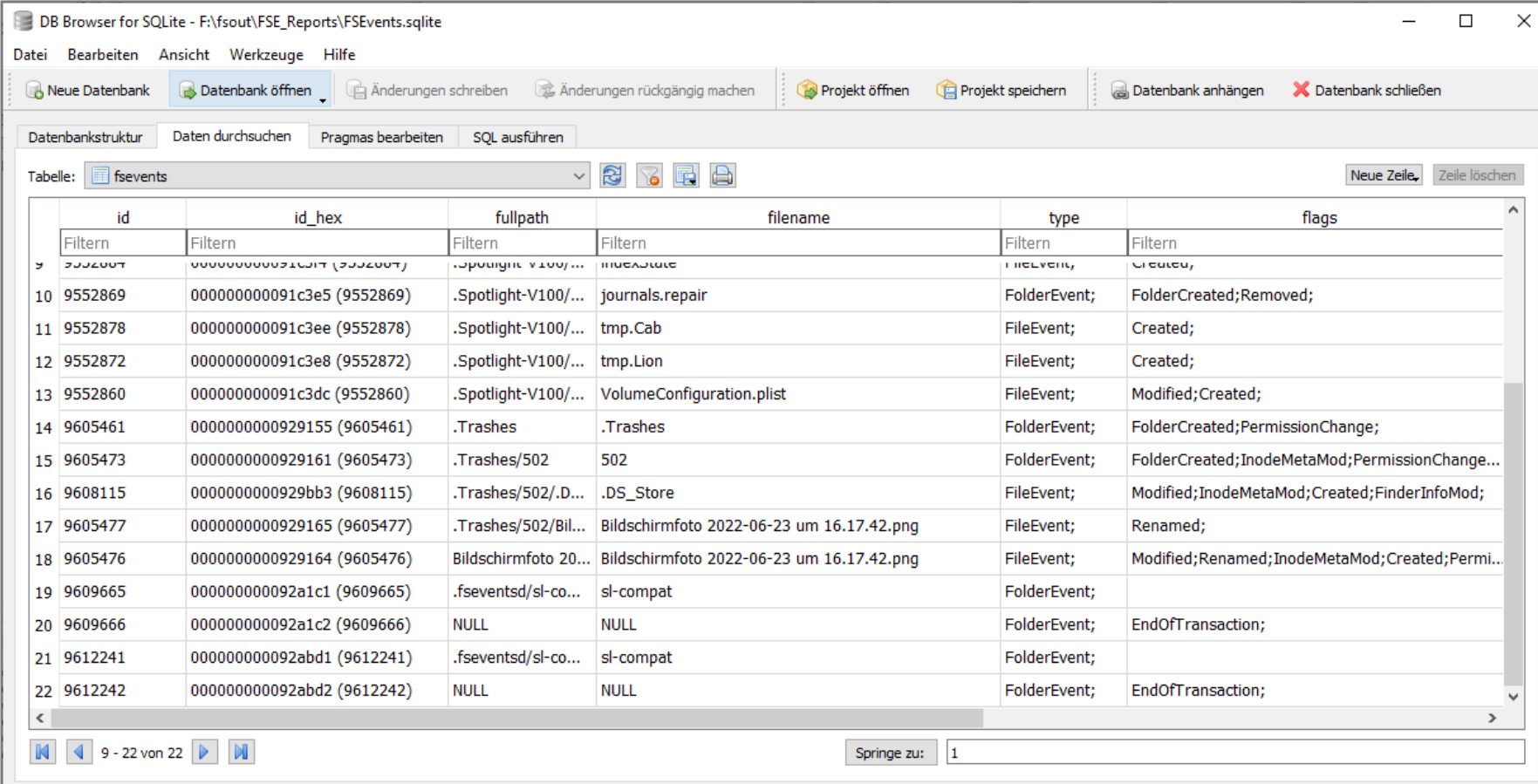
  Exception log and Reports exported to:
  'f:\fsout\FSE_Reports'

C:\Users\John>
```

# Gelöschte Dateien

FSEvent logs können mit einem speziellen Parser gelesen werden:

<https://github.com/dlcowen/FSEventsParser>



DB Browser for SQLite - F:\fsout\FSE\_Reports\FSEvents.sqlite

Neue Datenbank | Datenbank öffnen | Änderungen schreiben | Änderungen rückgängig machen | Projekt öffnen | Projekt speichern | Datenbank anhängen | Datenbank schließen

Datenbankstruktur | Daten durchsuchen | Pragmas bearbeiten | SQL ausführen

Tabelle: fsevents

	id	id_hex	fullpath	filename	type	flags
9	9552867	00000000091c3d7 (9552867)	.Spotlight-V100/...	INDEXSTATE	FileEvent;	Created;
10	9552869	00000000091c3e5 (9552869)	.Spotlight-V100/...	journals.repair	FolderEvent;	FolderCreated;Removed;
11	9552878	00000000091c3ee (9552878)	.Spotlight-V100/...	tmp.Cab	FileEvent;	Created;
12	9552872	00000000091c3e8 (9552872)	.Spotlight-V100/...	tmp.Lion	FileEvent;	Created;
13	9552860	00000000091c3dc (9552860)	.Spotlight-V100/...	VolumeConfiguration.plist	FileEvent;	Modified;Created;
14	9605461	000000000929155 (9605461)	.Trashes	.Trashes	FolderEvent;	FolderCreated;PermissionChange;
15	9605473	000000000929161 (9605473)	.Trashes/502	502	FolderEvent;	FolderCreated;InodeMetaMod;PermissionChange...
16	9608115	000000000929bb3 (9608115)	.Trashes/502/.D...	.DS_Store	FileEvent;	Modified;InodeMetaMod;Created;FinderInfoMod;
17	9605477	000000000929165 (9605477)	.Trashes/502/Bil...	Bildschirmfoto 2022-06-23 um 16.17.42.png	FileEvent;	Renamed;
18	9605476	000000000929164 (9605476)	Bildschirmfoto 20...	Bildschirmfoto 2022-06-23 um 16.17.42.png	FileEvent;	Modified;Renamed;InodeMetaMod;Created;Permi...
19	9609665	00000000092a1c1 (9609665)	.fseventsd/sl-co...	sl-compat	FolderEvent;	
20	9609666	00000000092a1c2 (9609666)	NULL	NULL	FolderEvent;	EndOfTransaction;
21	9612241	00000000092abd1 (9612241)	.fseventsd/sl-co...	sl-compat	FolderEvent;	
22	9612242	00000000092abd2 (9612242)	NULL	NULL	FolderEvent;	EndOfTransaction;

9 - 22 von 22 | Sprunge zu: 1



# BETRIEBSSYSTEM macOS

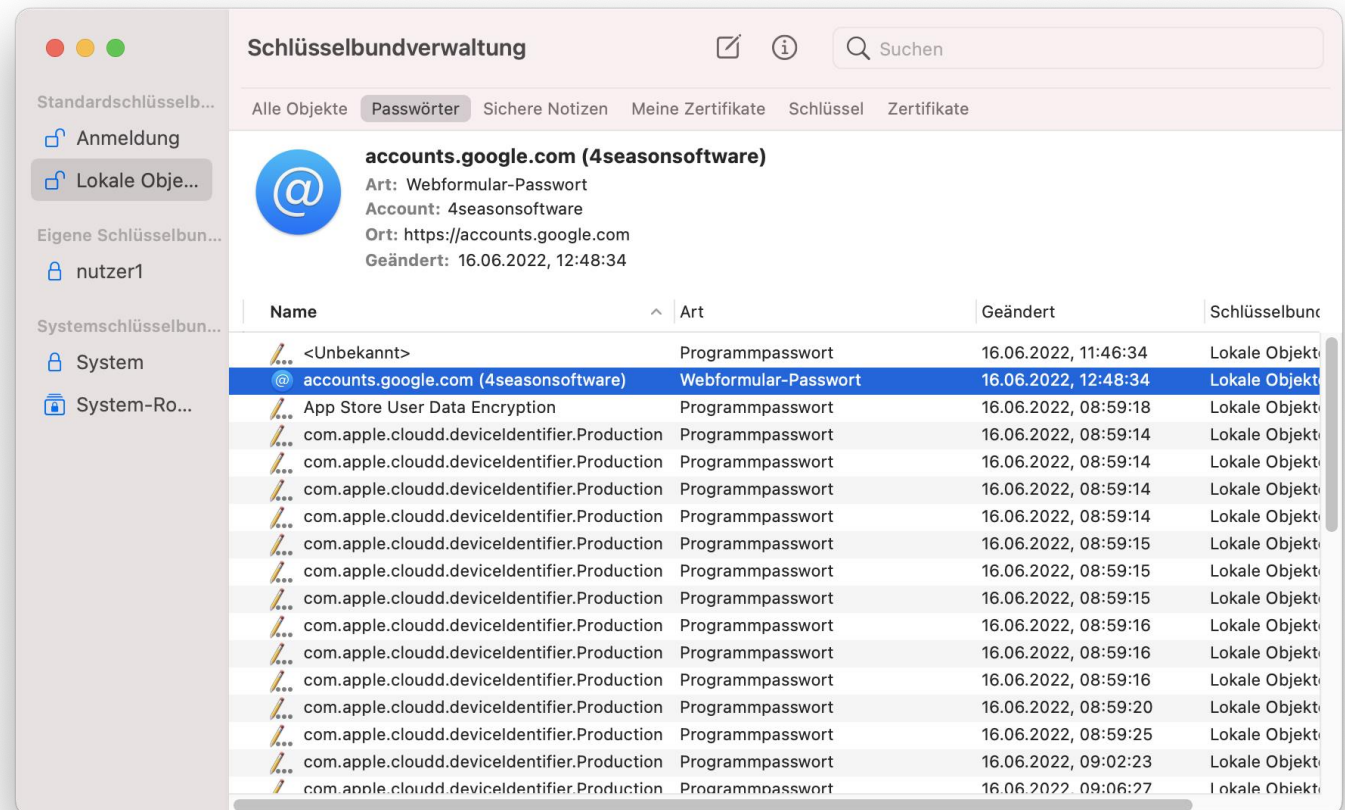
Schlüsselbund

# Schlüsselbund/Keychain

Passwörter (Zugänge, Web, etc.) und Zertifikate werden in macOS in der Schlüsselbundverwaltung / Keychain gespeichert und verwaltet.

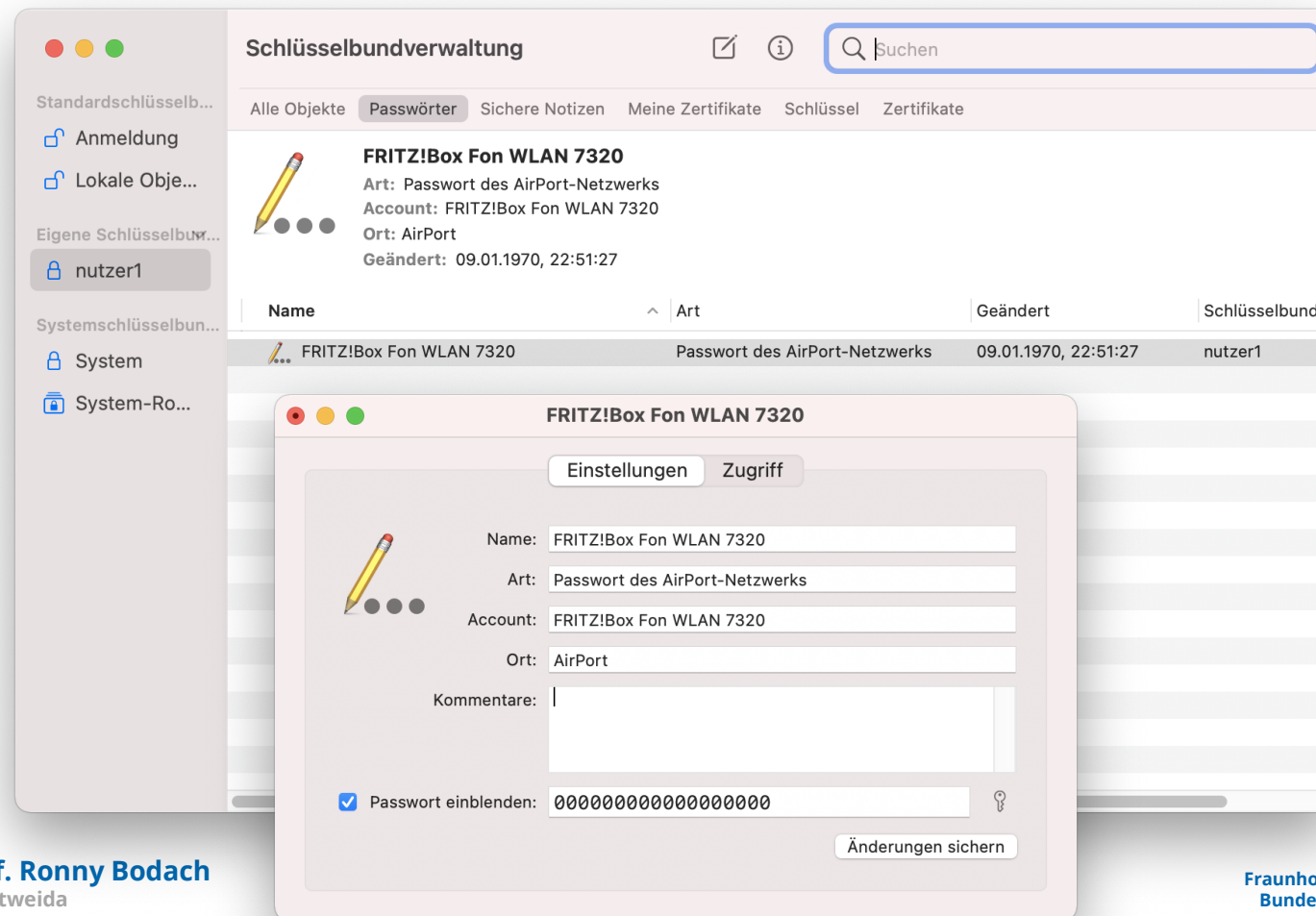
Auf neueren Geräten mit T2 und M1 Chipsatz sind die Passwörter zudem an den Hardwarekey HEK gebunden.

Passwörter können nur mit bekanntem Passwort des Benutzers angezeigt werden.



# Schlüsselbund/Keychain

Durch einen Doppelklick können die Elemente geöffnet werden und nach Eingabe des Kennworts des Benutzers angezeigt werden:



# Schlüsselbund/Keychain

## Keychain Directory

Die Passwörter werden in mehreren Keychain Dateien in einem Keychain Verzeichnis abgelegt und können damit auch kopiert werden.

```
%%users.homedir%%/Library/Keychains/*
```

Mit einem Python Toll kann dann die Keychain entschlüsselt werden:

```
https://github.com/n0fate/chainbreaker
```

# Schlüsselbund/Keychain

<https://github.com/n0fate/chainbreaker>

```
./chainbreaker.py --password=TestPassword -a test_keychain.keychain
2020-11-12 15:58:18,925 - INFO -

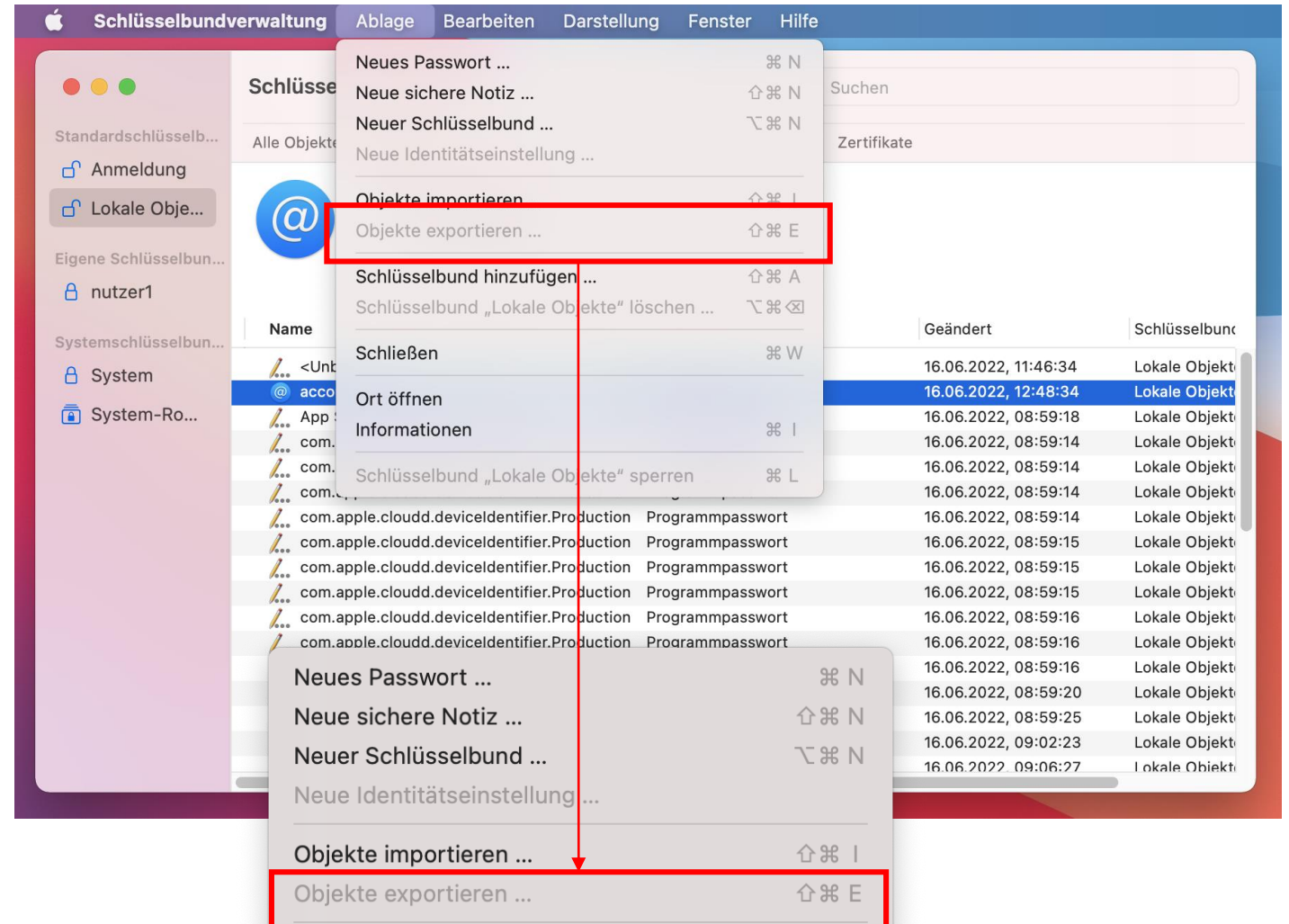
ChainBreaker 2 - https://github.com/gaddie-3/chainbreaker

2020-11-12 15:58:18,925 - INFO - Runtime Command: chainbreaker.py --password=TestPassword -a test_keychain.keychain
2020-11-12 15:58:18,925 - INFO - Keychain: test_keychain.keychain
2020-11-12 15:58:18,925 - INFO - Keychain MD5: eb3abc06c22afa388ca522ea5aa032fc
2020-11-12 15:58:18,925 - INFO - Keychain 256: 2d76f564ac24fa6a8a22adb6d5cb9b430032785b1ba3effa8ddea38222008441
2020-11-12 15:58:18,925 - INFO - Dump Start: 2020-11-12 15:58:18.925479
2020-11-12 15:58:19,245 - INFO - 1 Keychain Password Hash
2020-11-12 15:58:19,245 - INFO -
    $keychain$*7255a69abe21a28e1d2967265c9bba9c9bf4daf1*28dcfa41552db4eb*9dbb91712bb6a38f46e1b4335c334d444eb0c451e51fa02183eafe05c
35310d76014bc04b699d420d8487d4452d067e5
2020-11-12 15:58:19,245 - INFO -
2020-11-12 15:58:19,245 - INFO - 2 Generic Passwords
2020-11-12 15:58:20,306 - INFO -     [+] Generic Password Record
2020-11-12 15:58:20,306 - INFO -     [-] Create DateTime: 2020-10-13 23:01:17
2020-11-12 15:58:20,306 - INFO -     [-] Last Modified DateTime: 2020-10-13 23:01:17
2020-11-12 15:58:20,306 - INFO -     [-] Description: secure note
2020-11-12 15:58:20,306 - INFO -     [-] Creator:
2020-11-12 15:58:20,306 - INFO -     [-] Type: note
2020-11-12 15:58:20,307 - INFO -     [-] Print Name: Test Secure Note
2020-11-12 15:58:20,307 - INFO -     [-] Alias:
2020-11-12 15:58:20,307 - INFO -     [-] Account:
2020-11-12 15:58:20,307 - INFO -     [-] Service: Test Secure Note
2020-11-12 15:58:20,307 - INFO -     [-] Base64 Encoded Password:
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluc29iVVRGLTgiPz4KPCFET0NUWVBFIHBSaXN0IFBVQkxJQyAiLS8vQXBwbGUvL0RURCBQTElTVCAxLjAvL0VOIiAiaHR0cDovL3d3dy
5hcHBsZS5jb20vRFREcy9Qcm9wZXJ0eUxpc3QtMS4wLmR0ZCI
```

# Schlüsselbund/Keychain

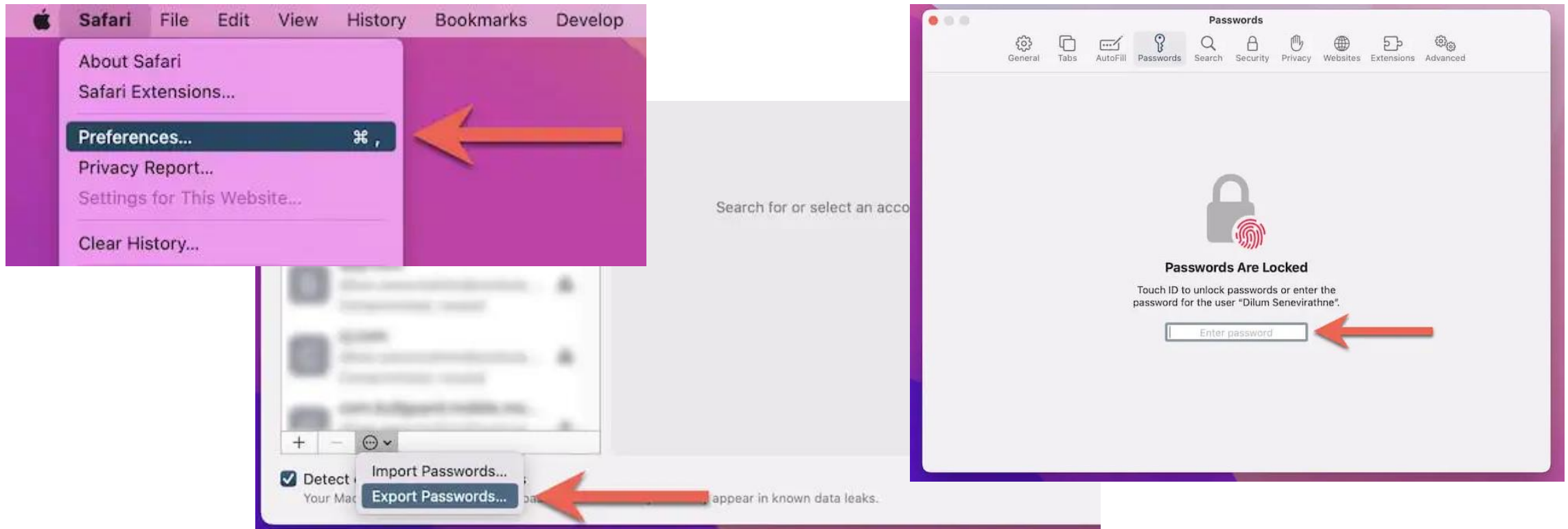
Auf macOS Geräten vor BigSure ist es möglich Passwörter zu exportieren.

- dazu wählt man die Objekte aus.
- unter Ablage existiert ein Punkt Objekte exportieren
- auf neueren Geräten ist diese Option ausgegraut und nicht verfügbar.



# Schlüsselbund/Keychain

Wenn auf dem Mac jedoch macOS Monterey oder höher ausgeführt wird, kann der integrierte Passwort-Manager von Safari verwendet werden, um Anmeldeinformationen im CSV-Dateiformat zu speichern.



# Vielen Dank



**HOCHSCHULE  
MITTWEIDA**  
University of Applied Sciences

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](mailto:bodach@hs-mittweida.de)

[www.cb.hs-mittweida.de](http://www.cb.hs-mittweida.de)

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

[hs-mittweida.de](http://hs-mittweida.de)