Hochschule Wismar
University of Applied Sciences
Technology, Business and Design
Fakultät für Ingenieurwissenschaften

Belegarbeit

Forensik in Betriebs- und Anwendungssystemen

Eingereicht am: 30. Juli 2024

von:

Betreuerin: Frau Prof. Dr. Antje Raab-Düsterhöft

Inhaltsverzeichnis

1 Beschreibung des Vorfalles

Das Landeskriminalamt führt gemäß §30a Abs.[1] 1 BtMG[2] ein Ermittlungsverfahren gegen eine Personengruppe wegen des bandenmäßigen Umgangs mit Betäubungsmitteln in nicht geringer Menge. Den Beschuldigten wird vorgeworfen den Anbau, die Herstellung, das Handeltreiben sowie die Ein- und Ausfuhr verschiedener Betäubungsmittel ausgeübt zu haben bzw.[3] auszuüben. Polizeiliche Maßnahmen haben diverse Beweise und Indizien liefern können. So ist eine erneute Lieferung aus einem Drittland an die Personengruppe geplant. Zu dieser Übergabe wird die Polizei und Staatsanwaltschaft in Erscheinung treten. Den beschuldigten Personen wird der Tatvorwurf eröffnet und die Belehrung zu deren Rechten im Strafverfahren verlesen. Anschließend erfolgt durch die Einsatzunterstützung der Bereitschaftspolizei und der Kriminalbeamten des Landeskriminalamts die Durchsuchungsmaßnahme. Neben den Beweisen und Spuren aus dem Bereich des BtMG ist mit elektronischen Datenträgern zu rechnen. Eine Telefonüberwachung ergab, dass es eine Tabelle mit dem Kundenkreis und dem Umsatz an verkauften Betäubungsmitteln geben soll. Hier ist mit antiforensischen Maßnahmen zu rechnen. Es gibt Hinweise, dass zur Dokumentation der innerbetrieblichen Abläufe mit einer Kamera Lichtbilder von der Anbaustätte gefertigt worden sein sollen. Weiter ist bekannt, dass es Absprachen über Kommunikationsmittel gegeben haben soll. Hier sind auf forensischen Datensicherungen gezielte Analysen durchzuführen.

[1] Absatz
[2] Betäubungsmittelgesetz
[3] beziehungsweise

2 Erstellung des Vorfalles

Für die folgende IT[1]-forensische Analyse von Datenträgern sind drei Speichermedien mit einer gewissen Spurenlage versehen worden. Es wurde entschieden, auf einen USB[2]-Stick eine Excel-Tabelle der Kundschaft abzulegen. Auf einem Desktop-PC[3] ist eine PDF[4]-Datei mit Angaben der Herstellung von Amphetaminen abgelegt. Diese wurde über den Messengerdienst 'Signal' an eine andere Person übertragen. Eine aus einer Kamera stammende SD-Card[5]-Karte ist mit Bilddateien der hergestellten Güter versehen. Diese wurden zum Schutz der Beschuldigten vor der Einsichtnahme Dritter mittels eines symmetrischen Schlüssels verschlüsselt.

2.1 Spurenlegung PC mit integrierter SSD

Auf einem Windows 10 PC mit einer 256 GB[6] SSD[7] wurde ein neues Benutzerkonto für den BTM[8]-Dealer Mad Max eingerichtet. Für den konstruierten Fall wird angenommen, dass es sich bei dem neu eingerichteten Konto um das einzige auf dem PC handelt, daher wird bei der späteren Analyse des PCs auf Ergebnisse aus den anderen vorhandenen Benutzerkonten nicht weiter eingegangen. Eine Anmeldung am Benutzerkonto erfolgt mittels Benutzernamen und Passwort. Das System ist nicht verschlüsselt.

Die Nutzung des PCs erfolgte im Zeitraum zwischen dem 17.05. und 27.05.2024. Während dieses Zeitraums suchte der Verdächtige nach Begriffen, wie 'Lieferdrohne', 'Schließfächer FFM Hauptbahnhof', 'Signal Desktop' und 'Bitcoin' (Abbildung 1).

[1] Informationstechnik
[2] Universal Serial Bus
[3] Personal Computer
[4] Portable Document Format
[5] Secure Digital Memory Card
[6] Gigabit
[7] Solid-State-Drive
[8] Betäubungsmittel

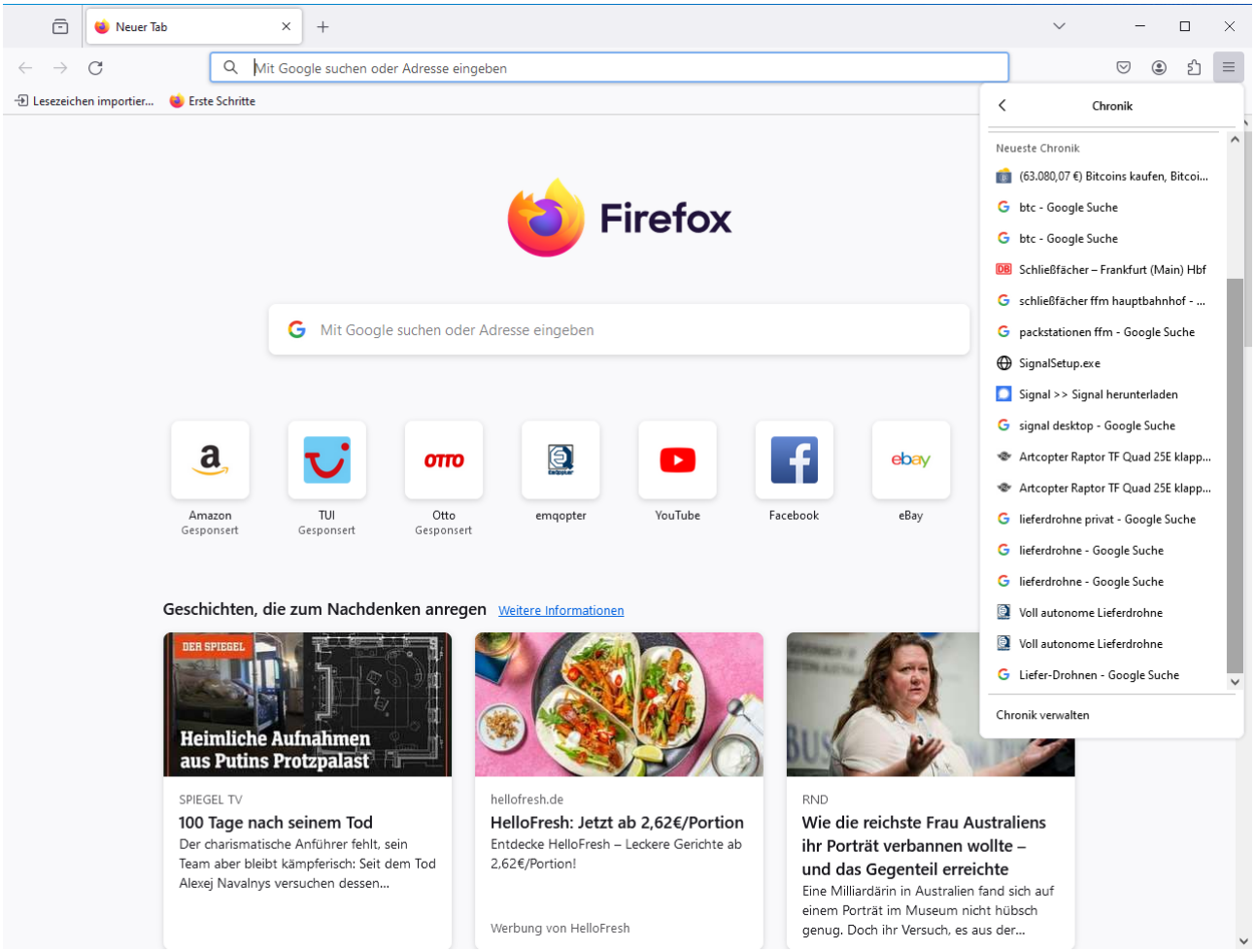


Abbildung 1: Firefox-Chronik

Der Verdächtige besuchte die Web-Seite des Signal-Messengers und lud die App 'Signal-Desktop' für Windows herunter. Diese wurde anschließend installiert und zur Kommunikation mit zwei weiteren Verdächtigen genutzt (Abbildung 2).

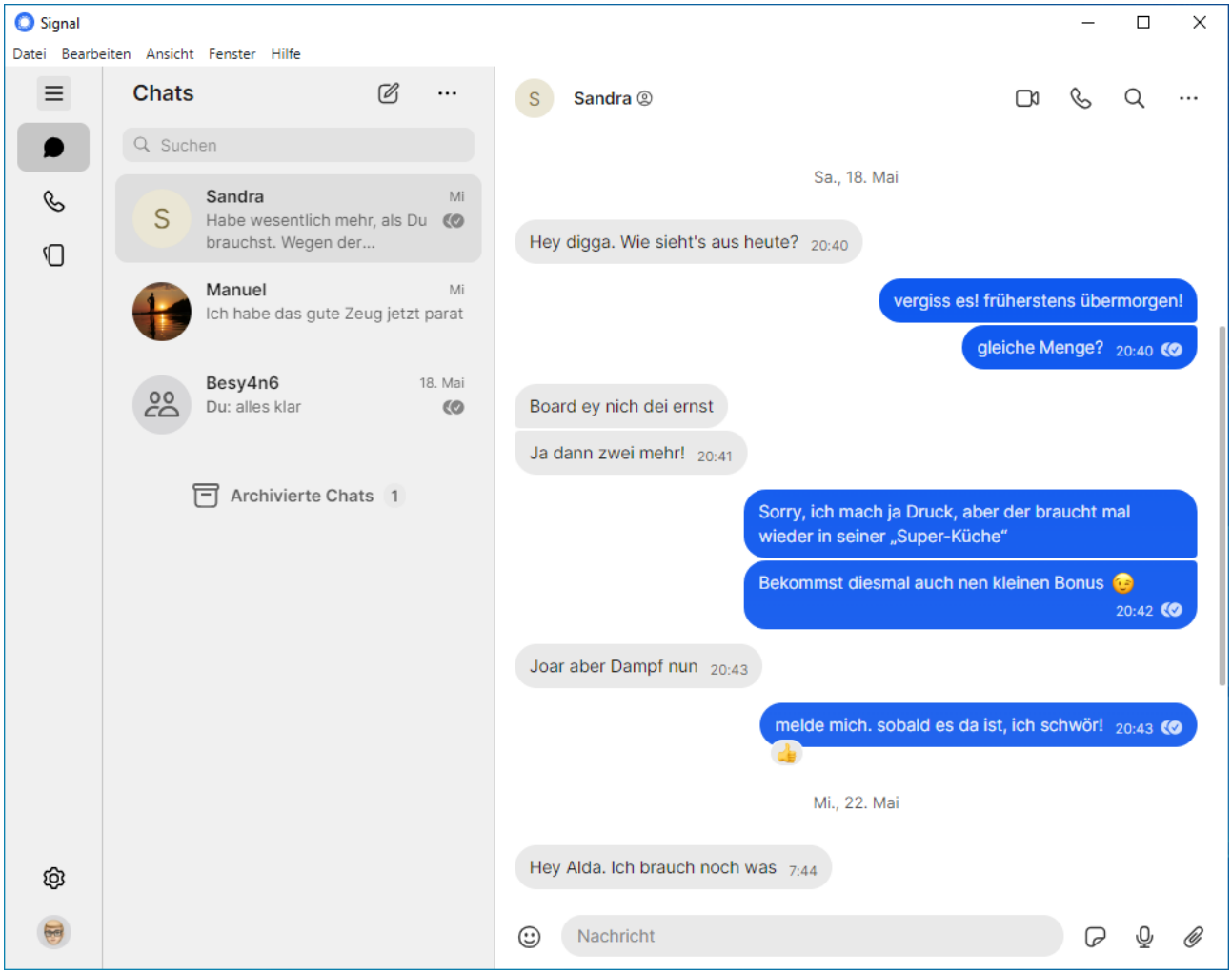


Abbildung 2: Auszug aus dem Signal-Chat

Aus dem Chat wurden eine JPEG[9]-Datei ('signal-2024-05-18-203244'), ein Word-Dokument ('Wuscha') und eine TXT[10]-Datei ('Herstellung') herunter geladen. Diese befinden sich zusammen mit der Installations-Anwendung für 'SignalDesktop' im Download-Ordner des PCs (Abbildung 3).

[9] Joint Photographic Experts Group
[10] Text

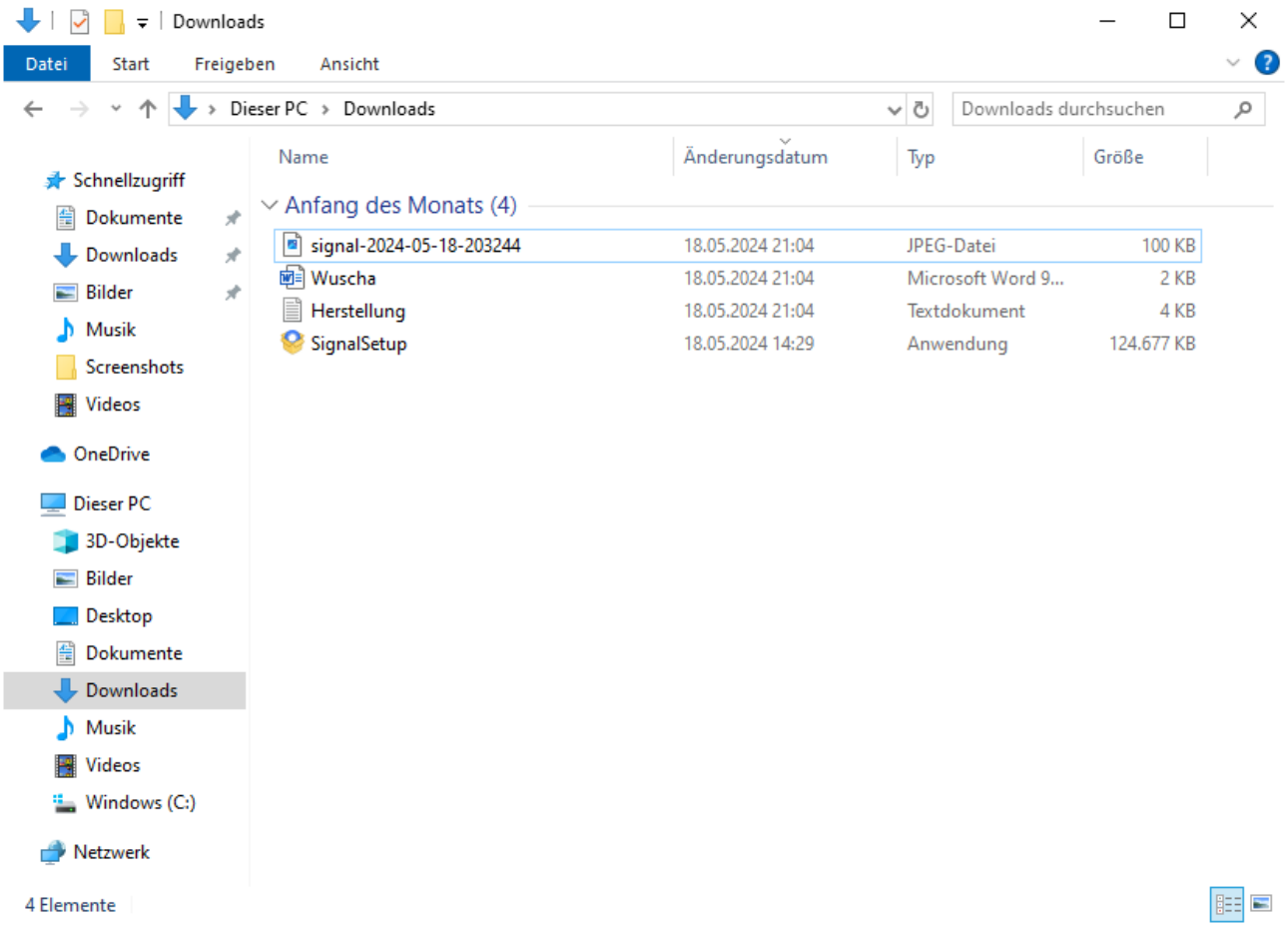


Abbildung 3: Download-Ordner

Nach der Benutzung wurde der PC herunter gefahren.

Der PC mit integrierten SSD Speichermodul wird im weiterführenden Sachverhalt als Spur K1/1 bezeichnet.

2.2 Spurenlegung USB-Datenspeicher

Auf einem USB-Datenspeicher befindet sich eine Datensammlung diverser Datenformate.

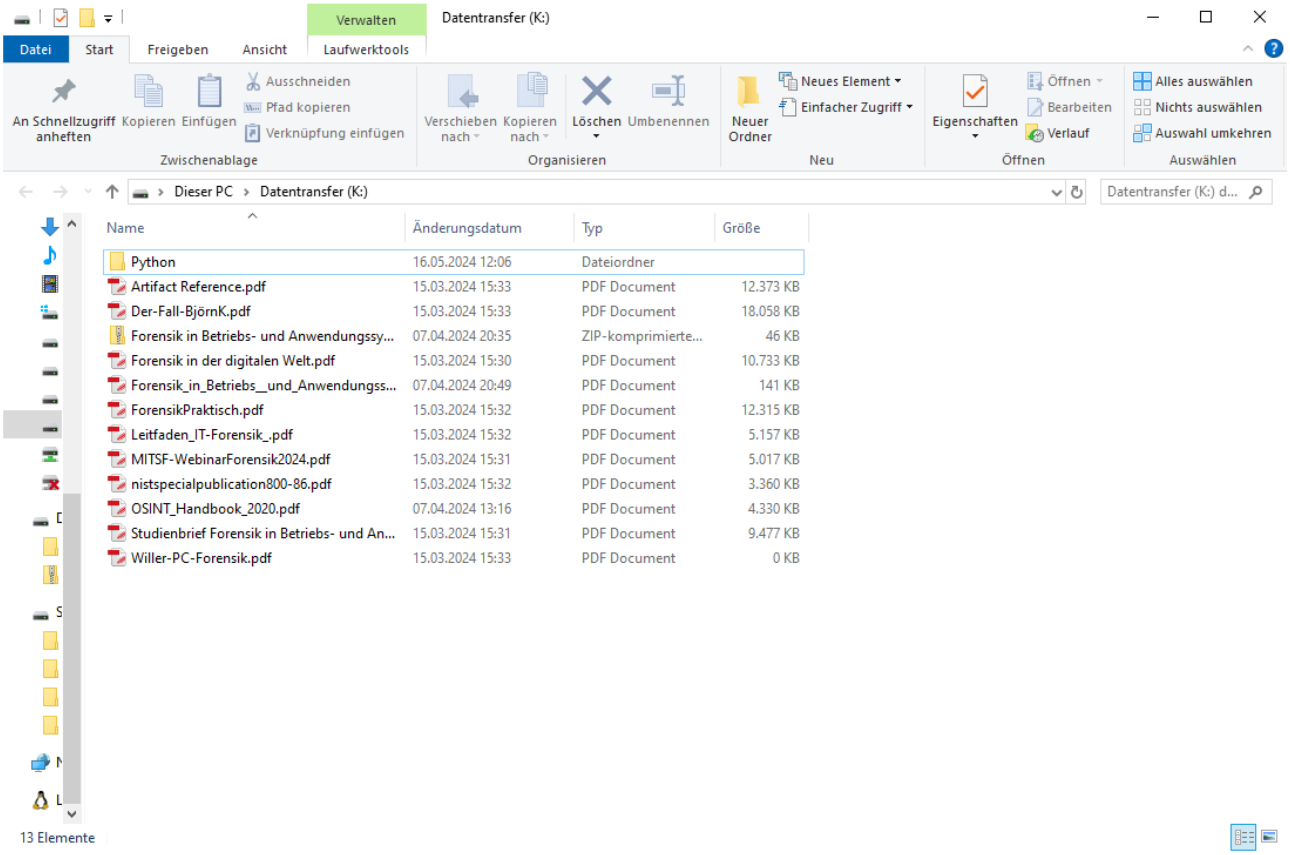


Abbildung 4: Logische Übersicht USB Datenträger

In Abbildung 4 können neben PDF Dokumenten auch ZIP-Dateien, Tabellenkalkulationsdateien sowie Videodateien unterschiedlichster Thematiken aufgefunden werden. Für den Sachverhalt wurde der Gedanke geschaffen, die Drogenverkaufstabelle eines Drogendealers in einem Speichermedium zu verstecken um diese so vor unbefugten Blicken Dritter verborgen zu halten. Es besteht die Frage warum ein Dealer solch eine Liste führen sollte. So können die Begründungen vielfältig sein. Von der Übersicht der Verkaufsaktivitäten, da diese selbst in Auftrag ausgeführt werden oder weil der Dealer selbst durch eigen durchgeführten Drogenkonsum selbst an Gehirnsubstanz minimiert und sich in der Vergesslichkeit verliert. So könnte diese Tabelle ein Gedankenanstoß sein an noch offene Verkaufstransaktionen von 'Kunden' erinnert zu werden, welche zum momentanen Zeitpunkt nicht die ausreichende Liquidität besaßen und das Geld im Nachgang mit einschließlich berechneten Zinsen einzufordern. Mit der erstellten Liste stellt sich die Frage wie solch eine auf einem Datenträger versteckt werden könnte. Es gibt verschiedene Möglichkeiten diese zu verbergen, auch Verschlüsselung wäre eine Option, im Falle der Vergesslichkeit für den Anwender jedoch kontraproduktiv. Das Verstecken kann mittels

spezieller Softwaretools, aber auch durch selbst erstellte Programmentwicklungen, in den freien Speicherbereich eingebettet werden. Für den Sachverhalt wurde das USB-Speichermedium nach gewisser Nutzungsdauer an der Gesamtdatengröße um einen Gigabyte Speicherbereich verringert (Abbildung 7).

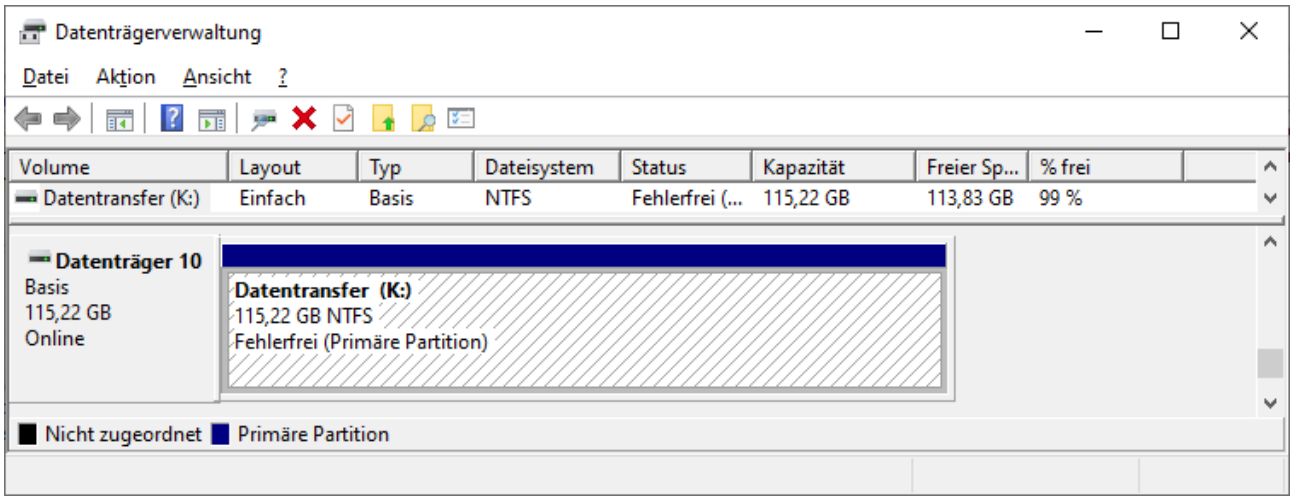


Abbildung 5: Datenträger unmanipuliert

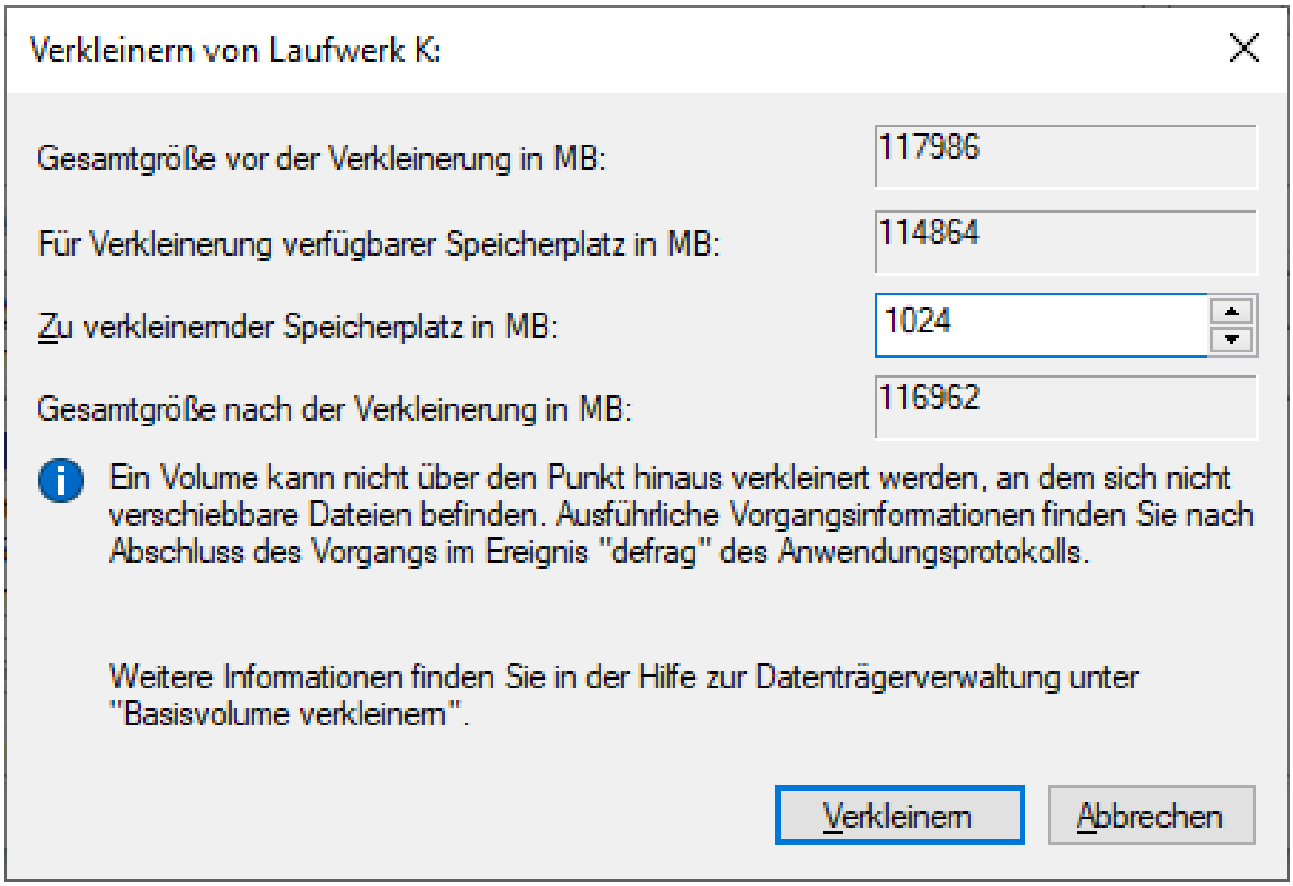


Abbildung 6: Verkeinerung Datenträger

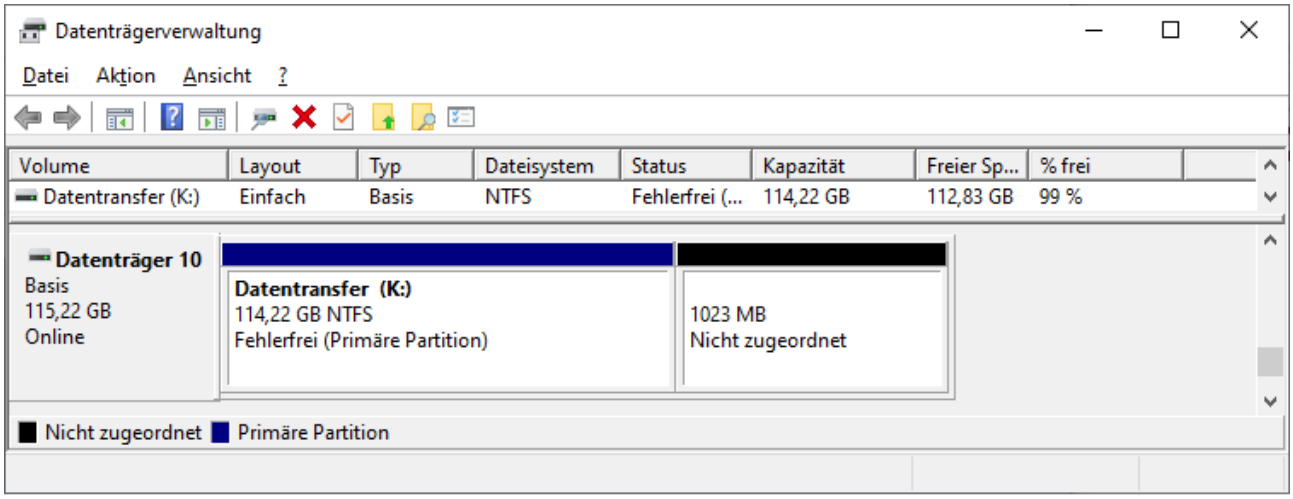


Abbildung 7: Datenträger manipuliert

Ein unpartitionierter Speicherbereich ist entstanden, welcher nicht weiter zugewiesen wurde und bei der Analyse der Datengröße leicht übersehen werden könnte. In diesem freien unpartitionierten Speicher wurde der Hexcode (Abbildung 8, 16) der zu versteckenden Datei eingebettet und mittels spezieller Software (Abbildung 9) mithilfe Schreibprozesses (Abbildung 15) persistent auf den Datenspeicher abgelegt.

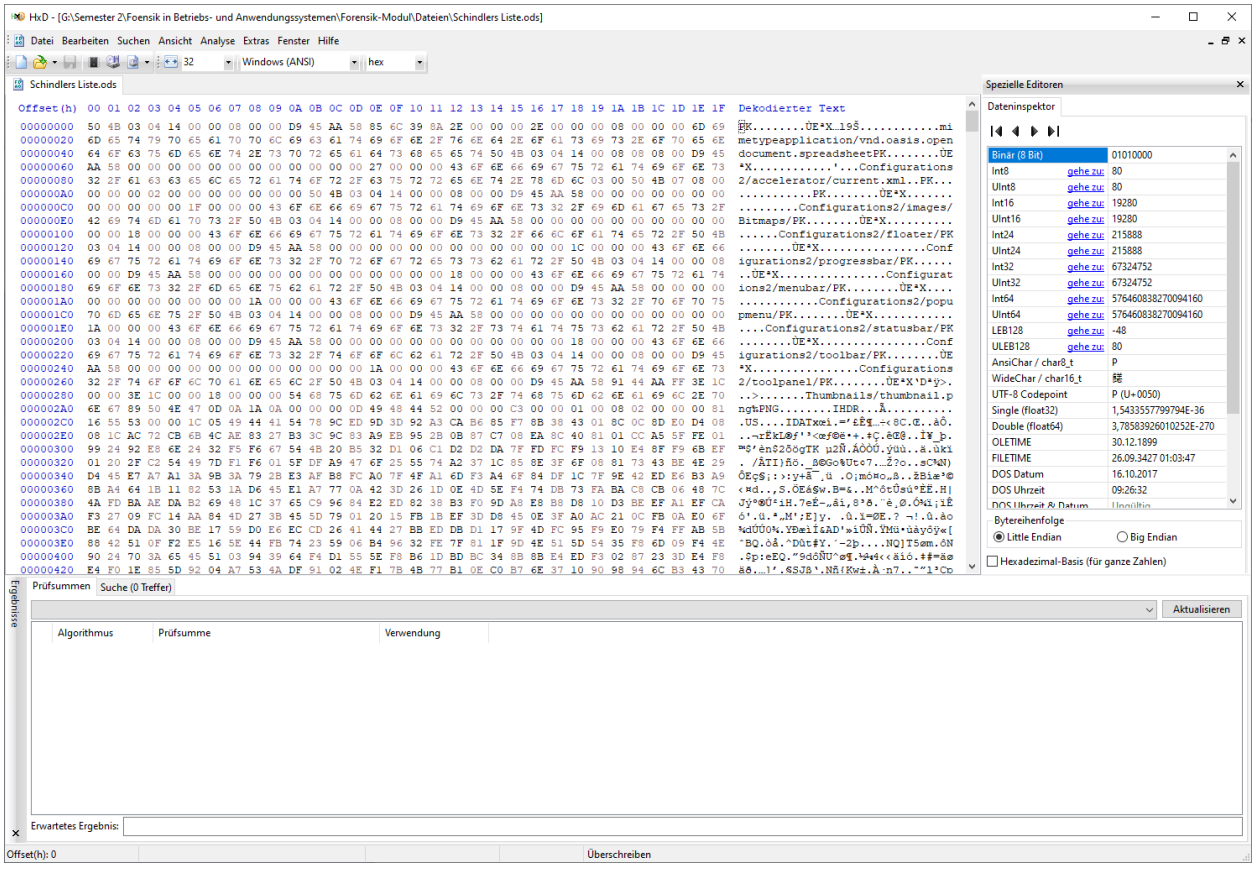


Abbildung 8: Hex Ansicht zu versteckende Datei

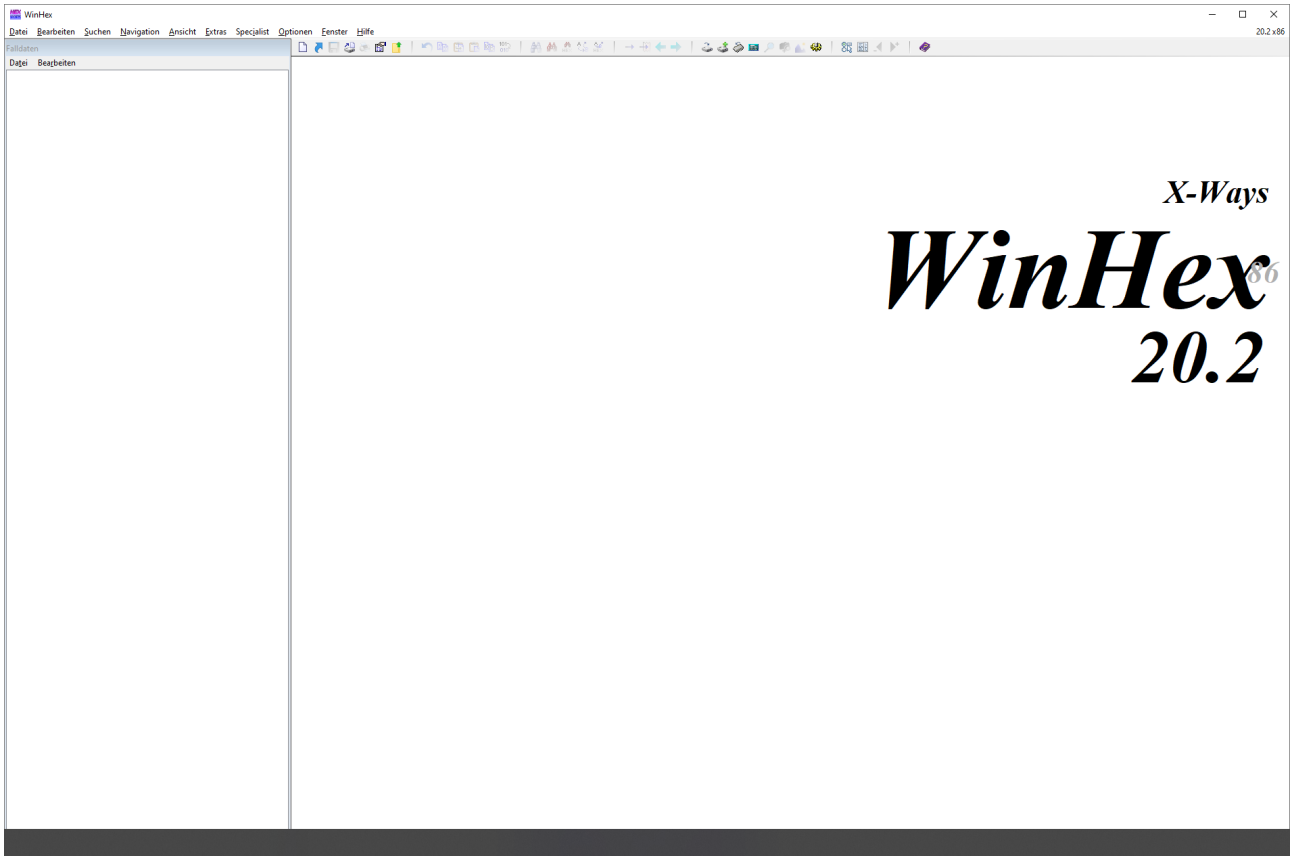


Abbildung 9: Programm zum Verstecken von Datenbasis

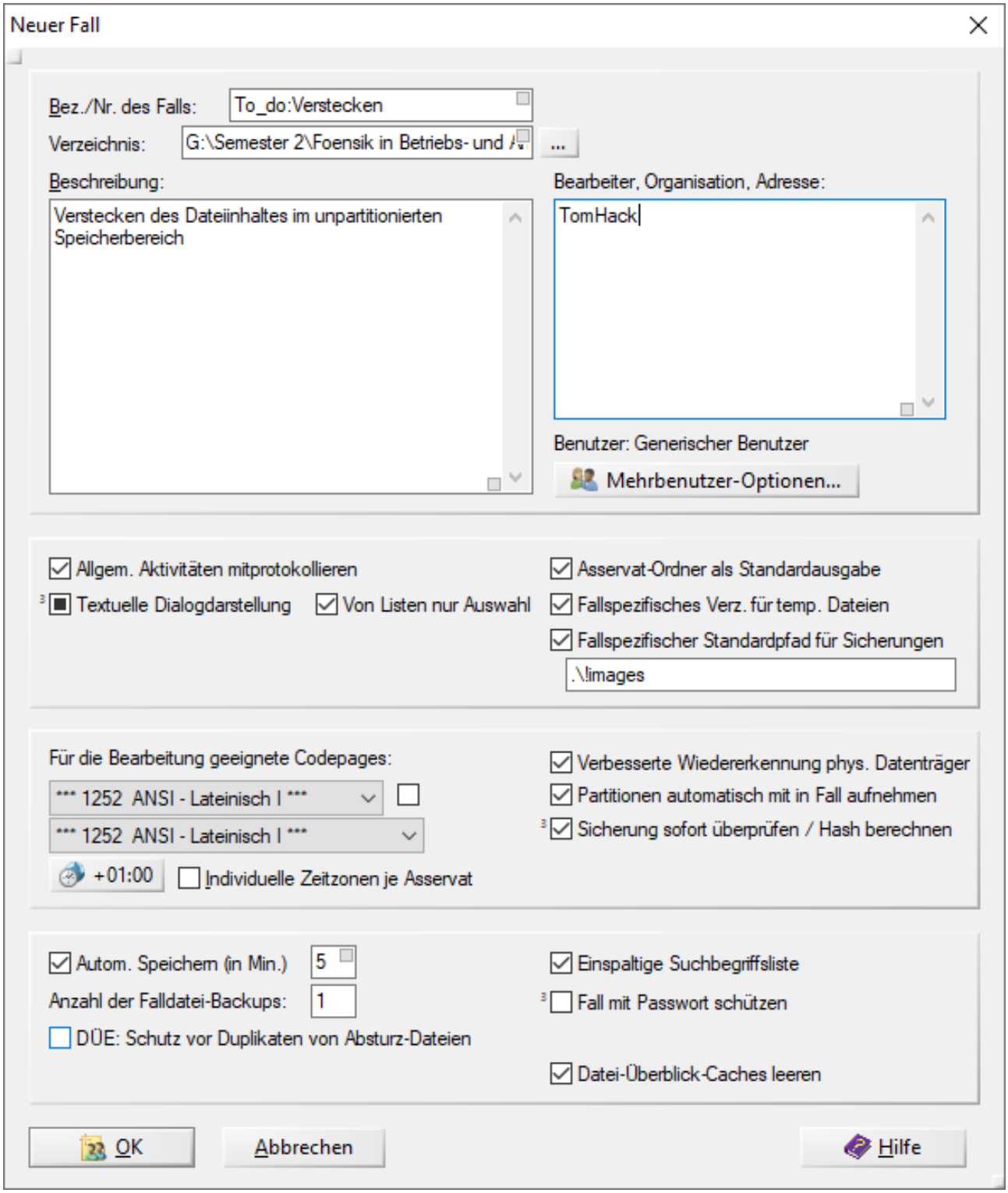


Abbildung 10: Anlegen eines neuen Falles

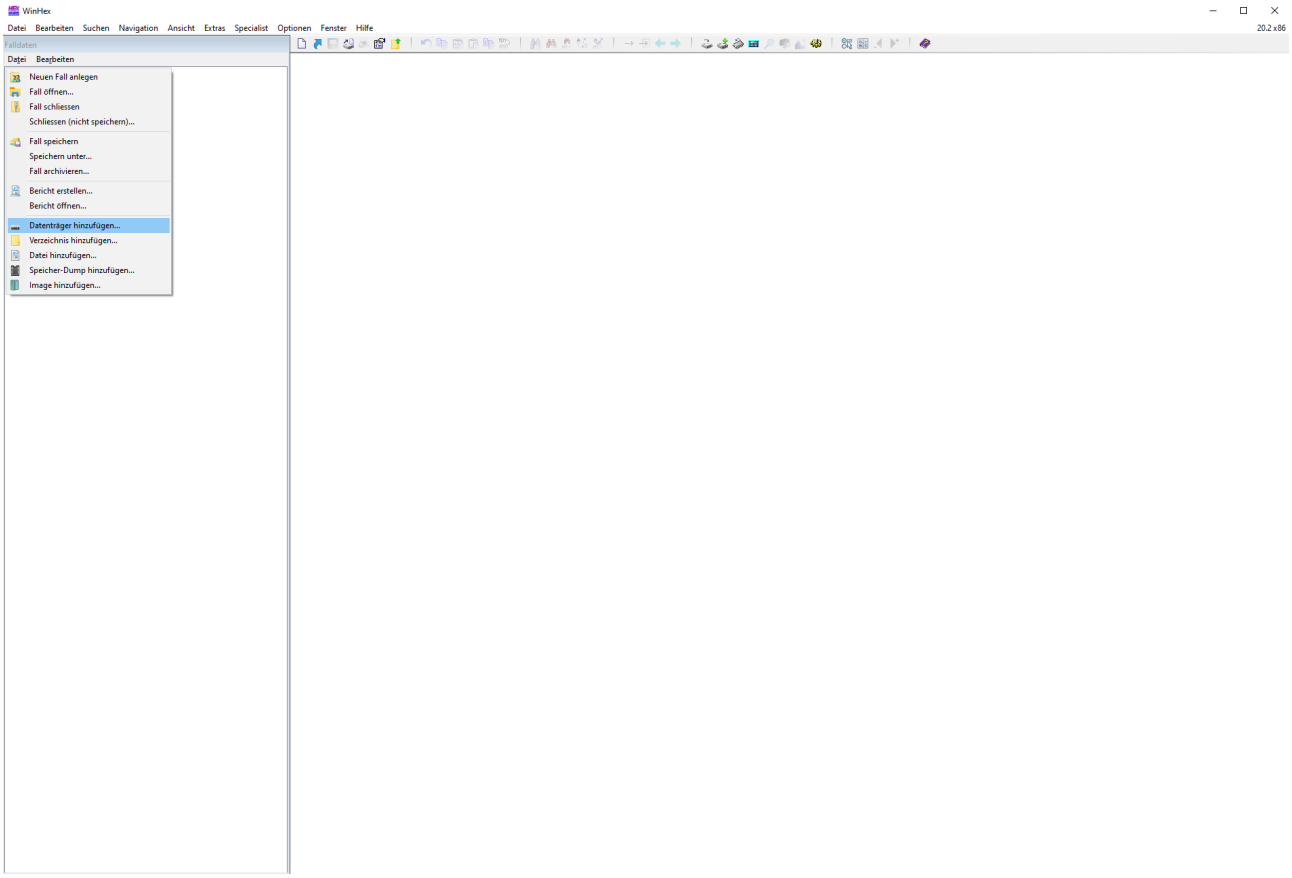


Abbildung 11: Datenträger hinzufügen

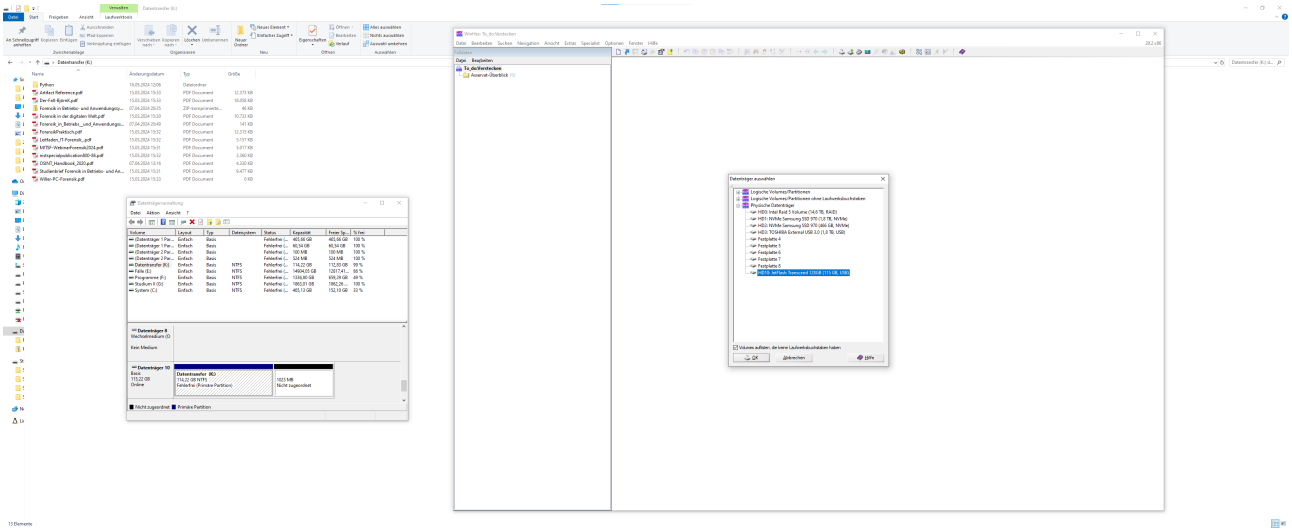


Abbildung 12: Wahl des physischen Datenträgers

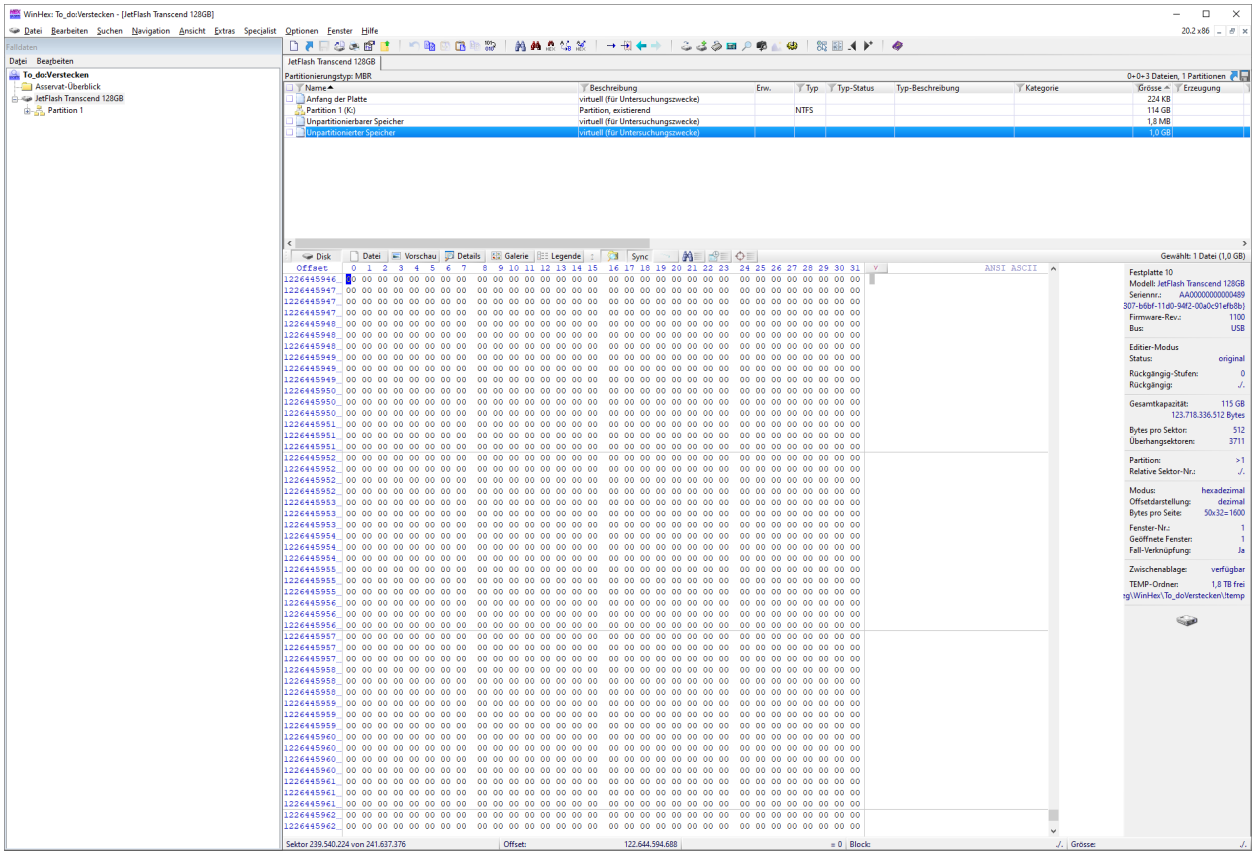


Abbildung 13: Übersicht unpartitionierter Datenspeicher unbearbeitet

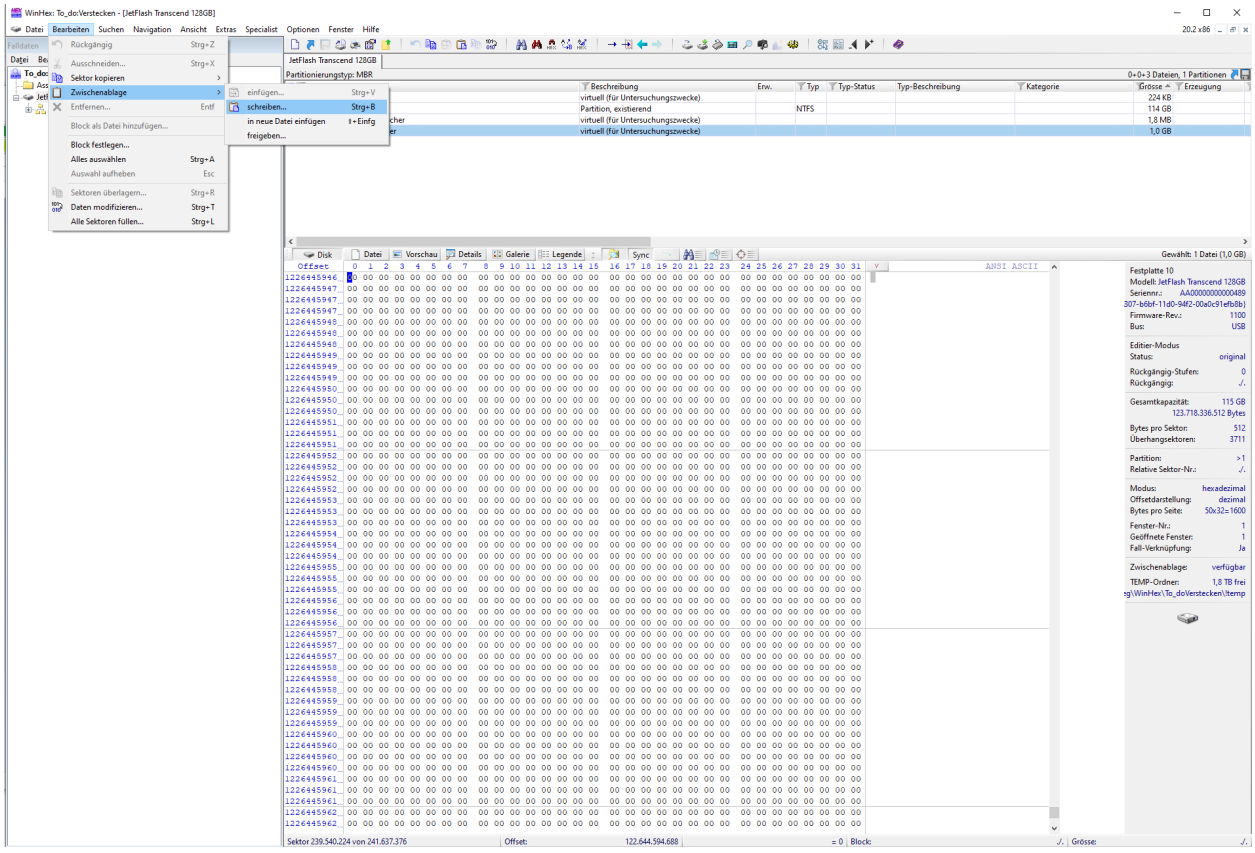


Abbildung 14: Zwischenablage schreiben

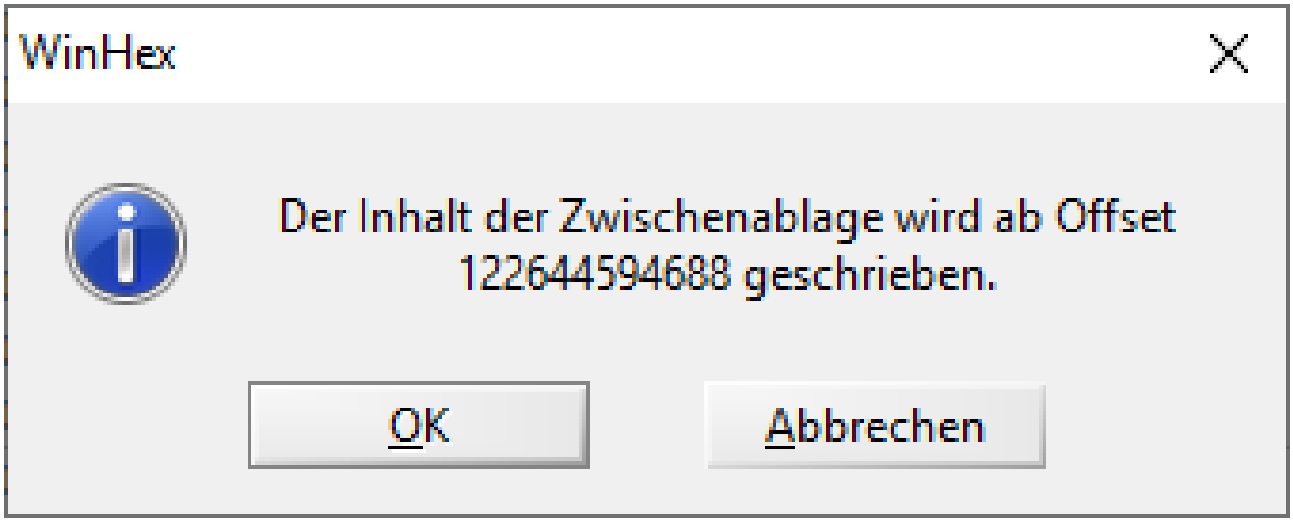


Abbildung 15: Hinweis Schreibprozess

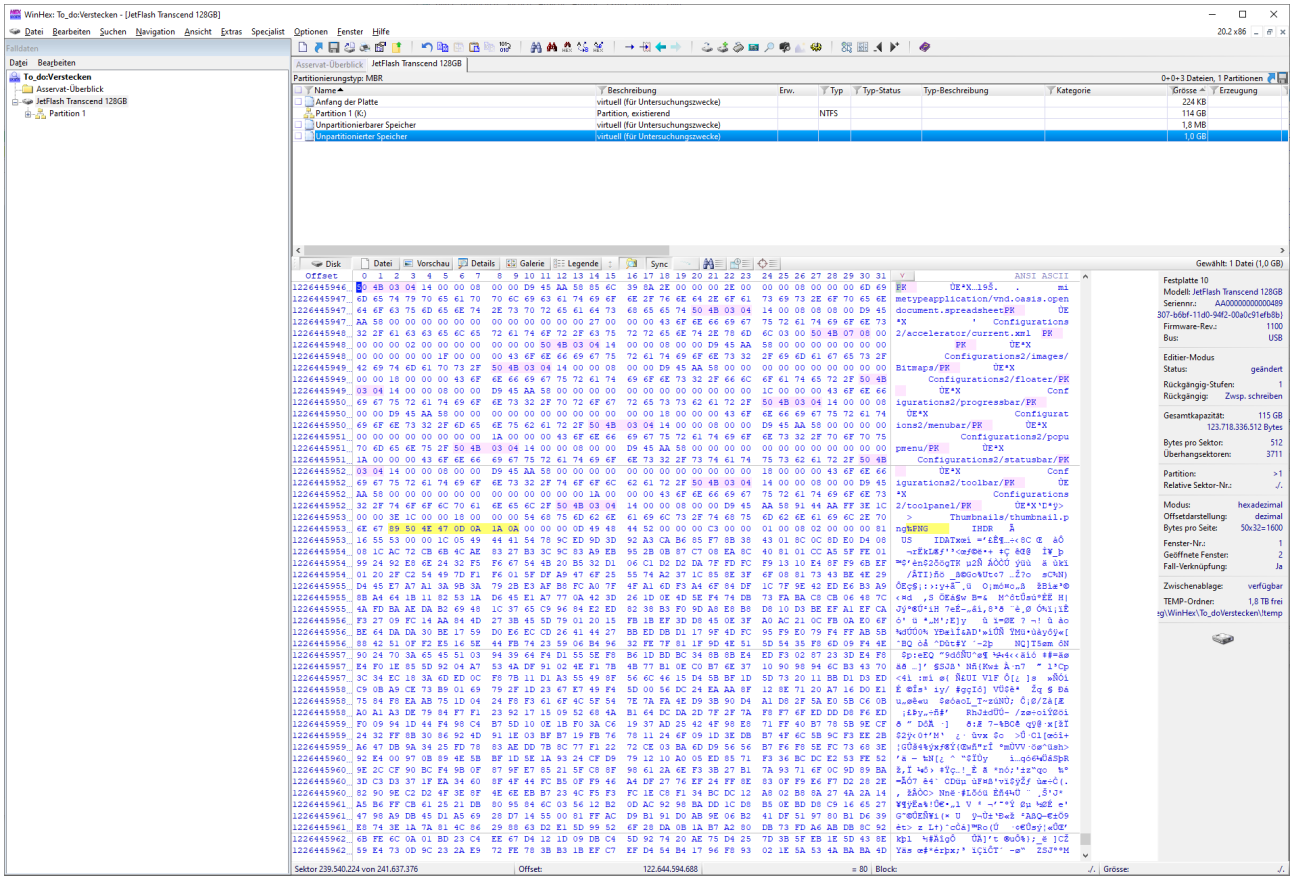


Abbildung 16: Dateiinhalt eingefügt

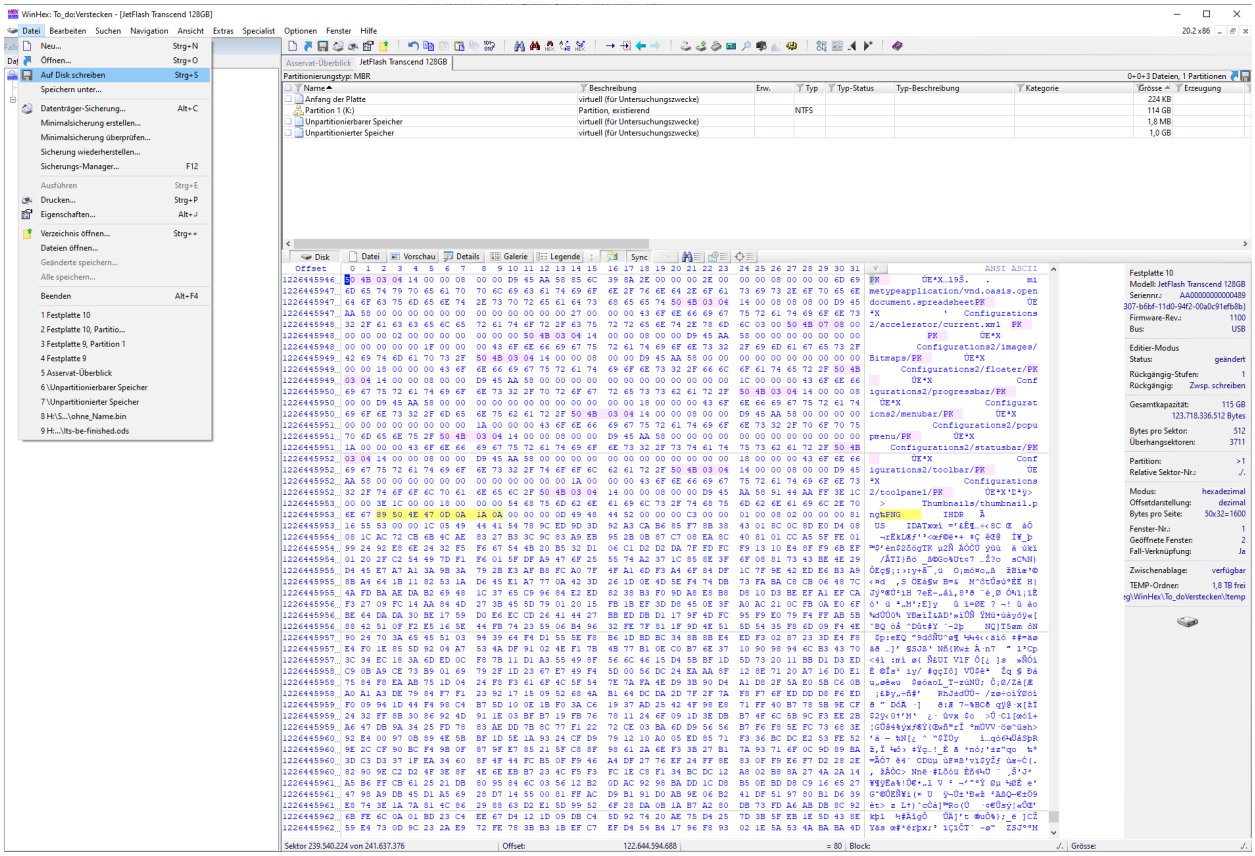


Abbildung 17: Dateiinhalt auf Datenträger schreiben

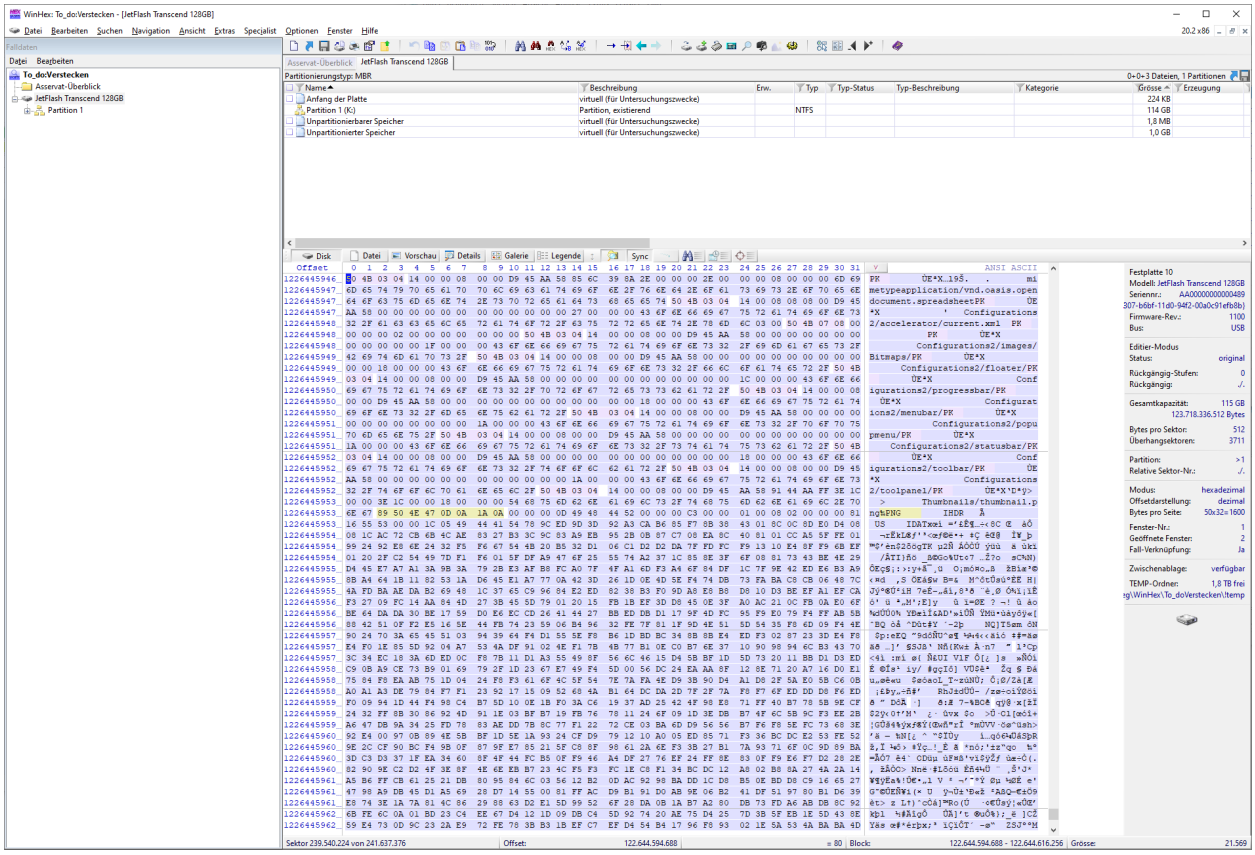


Abbildung 18: Dateiinhalt auf Datenträger geschrieben

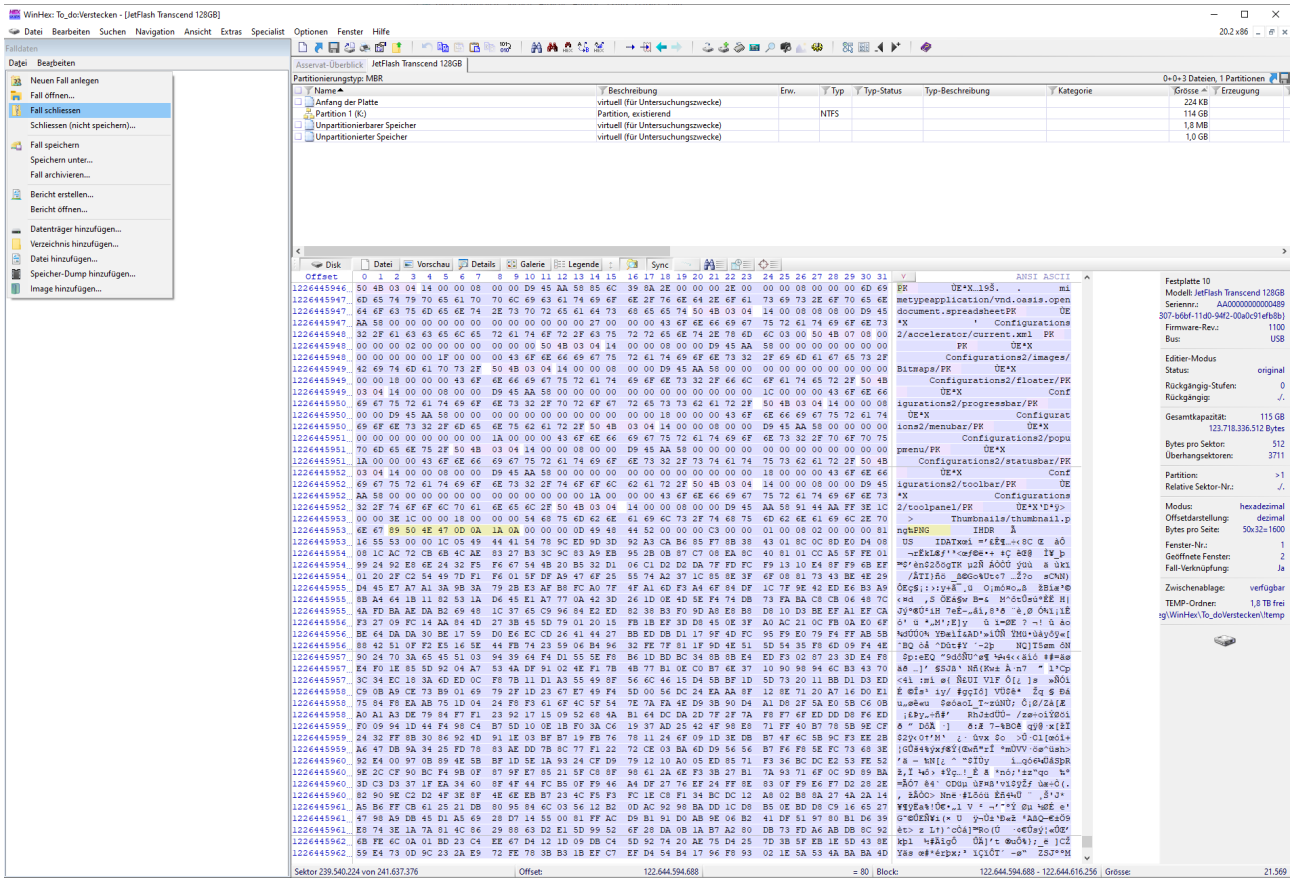


Abbildung 19: WinHex Fall geschlossen

Die optische Ansicht bei Öffnen des Explorers gibt zunächst wie in Abbildung 4 keine Anhaltspunkte auf das Vorhandensein einer Datei, welche ungewöhnliche Datenbasis enthalten könnte.

Der USB-Datenspeicher wird im weiterführenden Sachverhalt als Spur K1/2 bezeichnet.

2.3 Spurenlegung SD-Card-Kartenmodul

Um potentielle Kundschaft von der Qualität der hergestellten Substanzen zu überzeugen, nimmt der Produzent einige Bilder der Drogen und des verwendeten Labors (Abbildungen 20, 21, 22) mit einer Digitalkamera auf. Diese Bilder werden auf einer SD-Card-Karte gespeichert, welche durch die Beamten beschlagnahmt und im weiteren Verlauf einer forensischen Analyse unterzogen wird.

Abbildung 20: Laborbild 1

Abbildung 21: Laborbild 2

Abbildung 22: Laborbild 3

Abbildung 23: Hergestellte Substanzen

Die Bilder verschlüsselt der Produzent mit dem symmetrischen Verschlüsselungsalgorithmus AES[11]256, dabei nutzt er das Tool 'GnuPG' und sein eigenes Geburtsdatum '05022001' als Schlüssel. Dieser Umstand wird es den Ermittlern später verhältnismäßig leicht machen, den Schlüssel zu erraten und an die Originalbilder zu gelangen.

[11] Advanced Encryption Standard

```
    Verzeichnis: F:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         28.05.2024     19:23         182132 stoff.jpg
-a----         28.05.2024     19:26         225237 labor1.jpg
-a----         28.05.2024     19:27         213040 labor2.JPG
-a----         28.05.2024     19:27         159478 labor3.JPG


PS F:\> gpg -c -a --cipher-algo AES256 stoff.jpg
PS F:\> gpg -c -a --cipher-algo AES256 .\labor1.jpg
PS F:\> gpg -c -a --cipher-algo AES256 .\labor2.JPG
PS F:\> gpg -c -a --cipher-algo AES256 .\labor3.JPG
```

Abbildung 24: Kommandozeilen-Befehle zur Verschlüsselung mit GnuPG

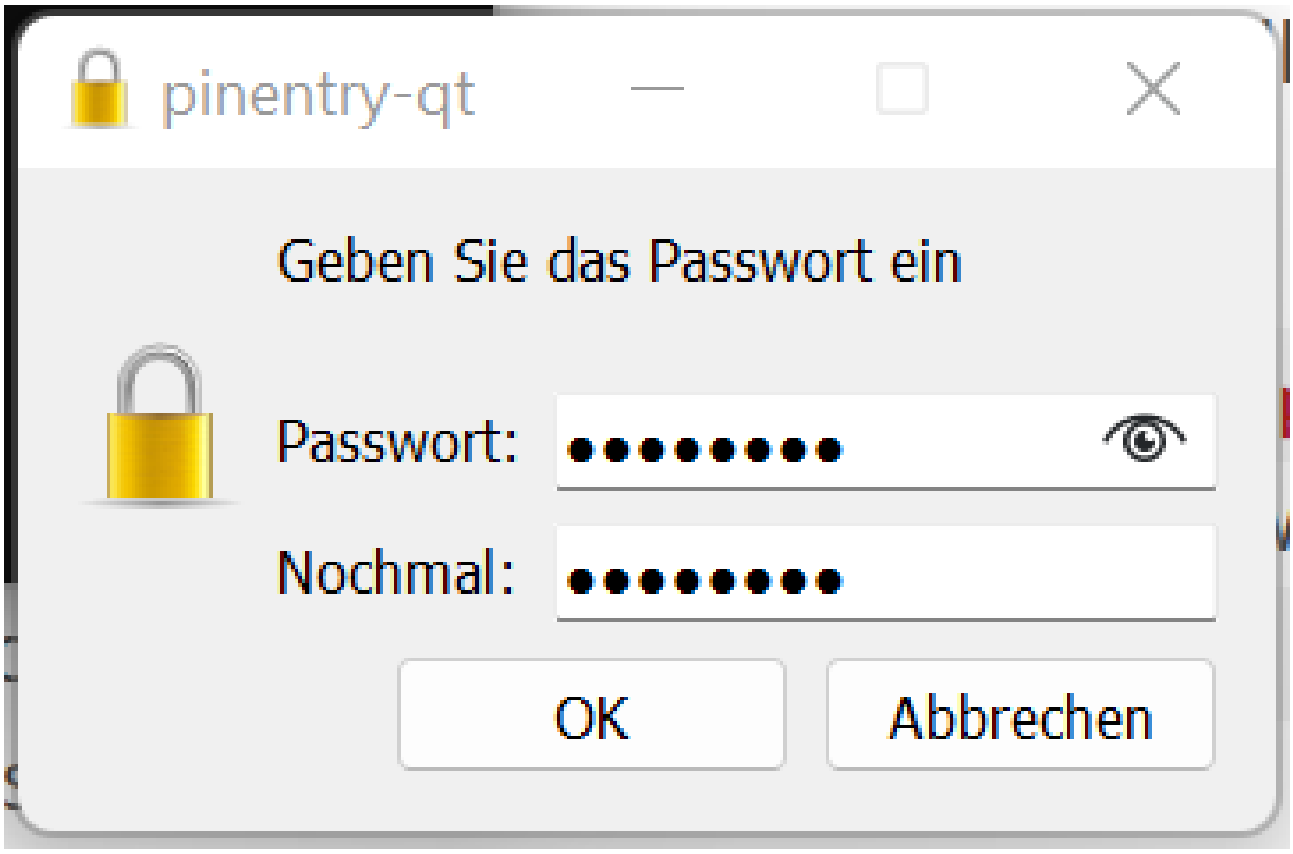


Abbildung 25: Eingabe des Schlüssels bei GnuPG

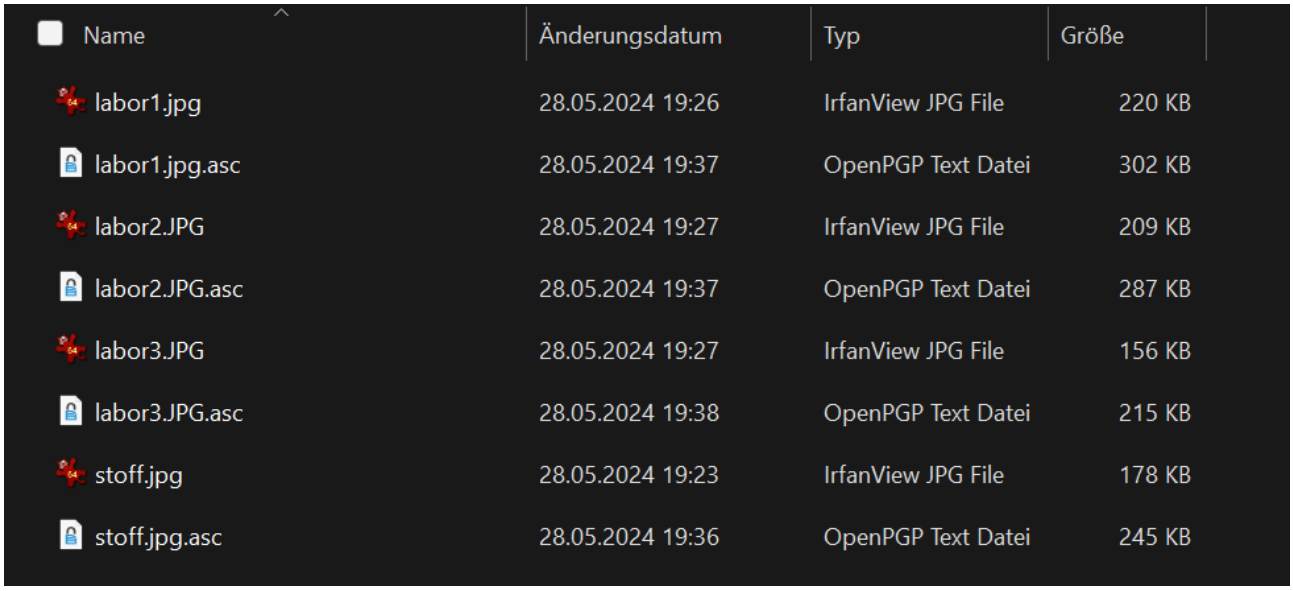


Abbildung 26: Dateiübersicht nach erfolgter Verschlüsselung

Das SD-Card-Kartenmodul wird im weiterführenden Sachverhalt als Spur K1/3 bezeichnet.

3 Untersuchungsauftrag

Laut Untersuchungsauftrag sind durch forenesische Analyse der Datenträger folgende Fragestellungen zu beantworten:

- Bitte die auf der Spur K1/1, K1/2, K1/3 gespeicherten Daten forensisch sichern.
- Befinden sich auf der Spur K1/1, K1/2, K1/3 verschlüsselte Daten, diese ggf. entschlüsseln.
- Es wird um Bereitstellung von Tabellen-, Text- und Bilddateien mit Bezug zu Betäubungsmitteln gebeten.
- Welche Aussagen können im Bezug zu Betäubungsmitteln nach Analyse der Spurenlage noch getroffen werden?

4 Vorbereitung/forensische Analyse für die Auflösung des Vorfalles

Nach erfolgreich durchgeführter Durchsuchungsmaßnahme wurden die Spuren durch die Ermittler nummeriert und mittels eines kriminaltechnischen Untersuchungsauftrages an die IT-forensische Sachbearbeitung übergeben. Es erfolgt vor Beginn der Untersuchung eine Durchschau der Spurenlage. Jede Spur wird in der Vogelperspektive von allen Seiten fotografisch dokumentiert. Spuren, welche manuell geöffnet werden müssen, werden zur Nachvollziehbarkeit in ihren einzelnen Schritten fotografisch dokumentiert.

4.1 Spur K1/1

Die Spur K1/1 wurde von der Sachbearbeitung mittels eines kriminaltechnischen Untersuchungsauftrages an die Kriminaltechnik der IT-Forensik übergeben. Die Sicherung von DNA[1] Spuren ist bereits erfolgt. Eine Sicherung flüchtiger Datenbasis war nicht möglich da die Spuren sich im ausgeschalteten Zustand befunden haben. Eine RAM[2]-Sicherung im vorliegenden Sachverhalt war nicht gegeben.

4.1.1 Vorbereitung Analyse PC mit integrierter SSD

Der PC wurde im ausgeschalteten Zustand vorgefunden. Bei dem Gerät handelt es sich um einen kleinen Desktop-PC der Marke 'Lenovo Think-Station M710q'. Am PC waren lediglich die Tastatur, eine Maus, ein Monitor und das Netzteil via Kabel angeschlossen (Abbildung 27).

Abbildung 27: Beschlagnahmter PC

[1] Desoxyribonukleinsäure
[2] Random-Access Memory

Der PC wurde vom Netz, der Tastatur, der Maus und dem Monitor getrennt (Abbildung 28). Daran anschließend wurde der PC aufgeschraubt. Auf der Oberseite des Motherboards gibt es Anschlussmöglichkeiten für 3,5 Zoll-Festplatten, die ungenutzt sind.

Abbildung 28: Oberseite offener PC

Auf der Unterseite befinden sich ein 8 GB-RAM-Speicherriegel und eine 256 GB SSD (Abbildung 29).

Abbildung 29: PC Unterseite

Die SSD wurde zur weiteren Untersuchung entfernt (Abbildung 30). Hierfür wird ein externes SSD-Gehäuse mit einschaltbaren Write-Blocker genutzt (Abbildung 32). Anschließend wurde mittels der Software 'Axiom' der Firma 'Magnet Forensics' ein Encase Evidence-Image (.E01) erstellt und eine Fall-Auswertung (Analyse) durchgeführt (Abbildung 33).

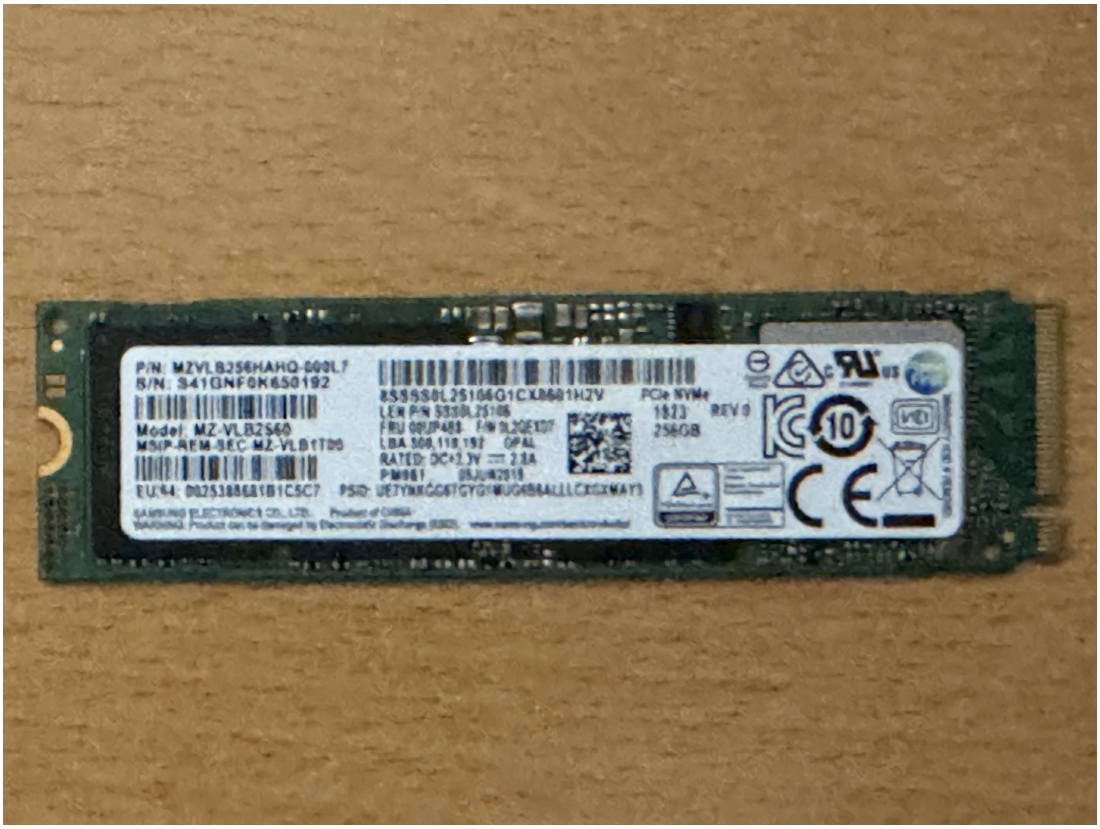


Abbildung 30: Ausgebaute SSD

Abbildung 31: Dateil-Aufnahme Typenschild SSD

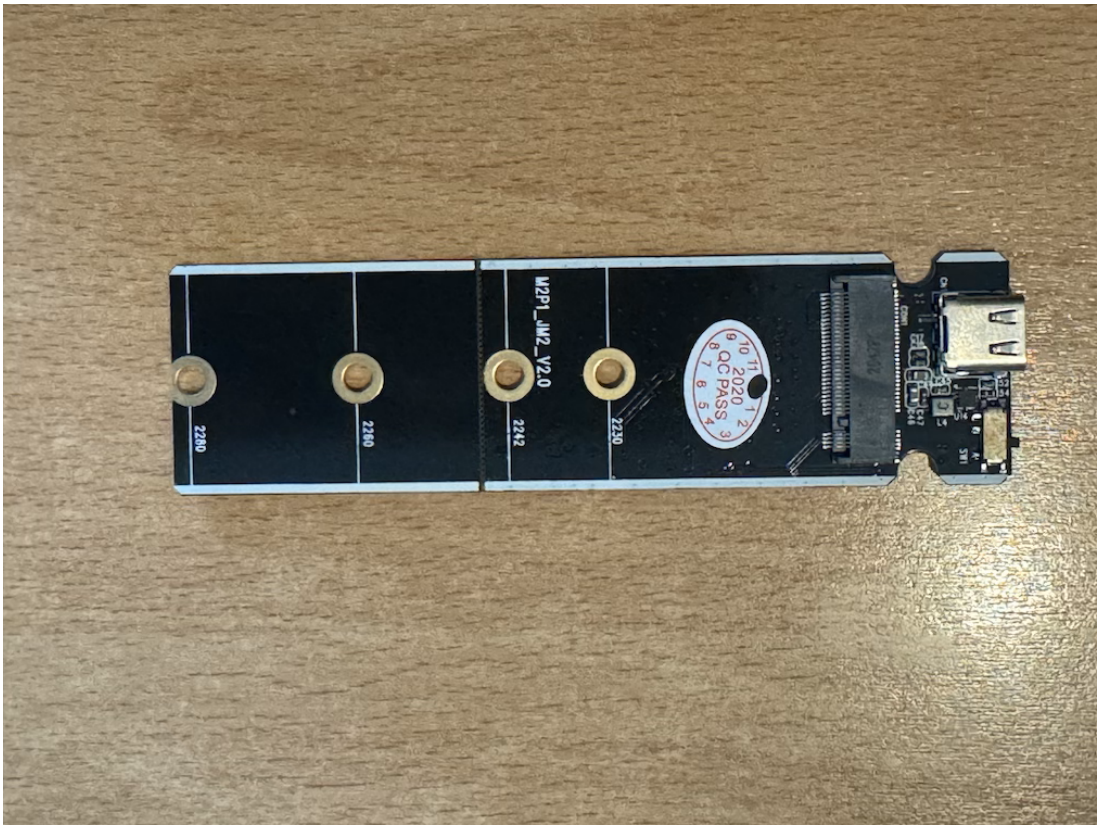


Abbildung 32: Leerer SSD-Reader

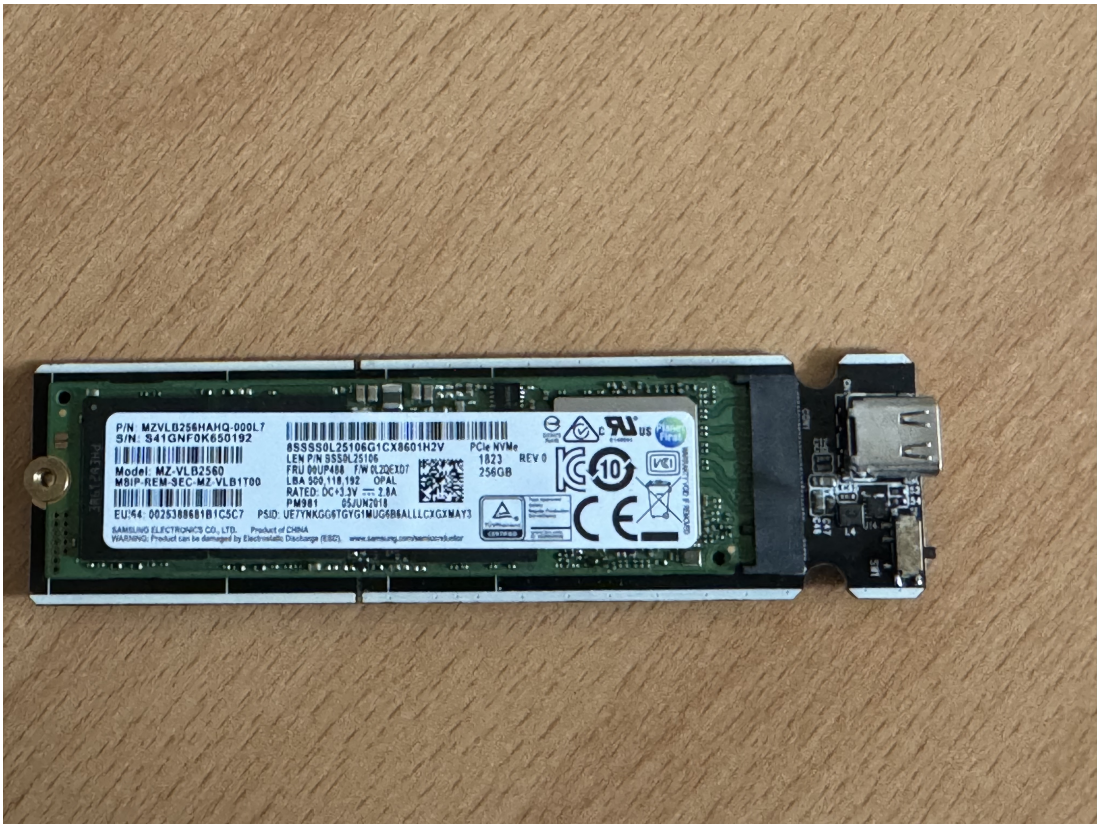


Abbildung 33: SSD im Lesegerät

Erstellung E01-Image mittels Axiom

Zu Beginn wird mittels der Softwarelösung 'Axiom' ein Fall angelegt (Abbildung 34). Es erscheint ein Auswahlfenster von welchem Gerät ein Abbild erzeugt werden soll. Mögliche Optionen sind der Computer, das Mobilgerät, die Cloud und das Fahrzeug (Abbildung 35). Für den vorliegenden Sachverhalt wird die Option 'Computer' ausgewählt. Als nächstes folgt die Auswahl des Betriebssystems (Abbildung 36). Bei dem beschlagnahmten Gerät handelt es sich um einen Windows-PC, aufgrund dessen wird Windows als Betriebssystem gewählt. Folgend wird 'Beweisquelle sichern' getätigt (Abbildung 37) und das zu sichernde Laufwerk bestimmt (Abbildung 38). Das per USB an den forensischen Auswertungscomputer angeschlossene Laufwerk wird erkannt und die Datensicherung kann beginnen. Letzter Schritt der Sicherung ist die Auswahl des Abbild-Typs. Hier stehen die Optionen 'E01', 'Raw', 'Alle Dateien und Ordner' und 'Gezielte Beweissicherung' zur Auswahl. Da der Datenträger vollständig ausgewertet werden soll, fällt die Wahl auf den Abbildtyp '.E01' (Abbildung 39). Es wird ein forensisches Image erzeugt, mit welchem später eine logische und physische Auswertung erfolgen kann.

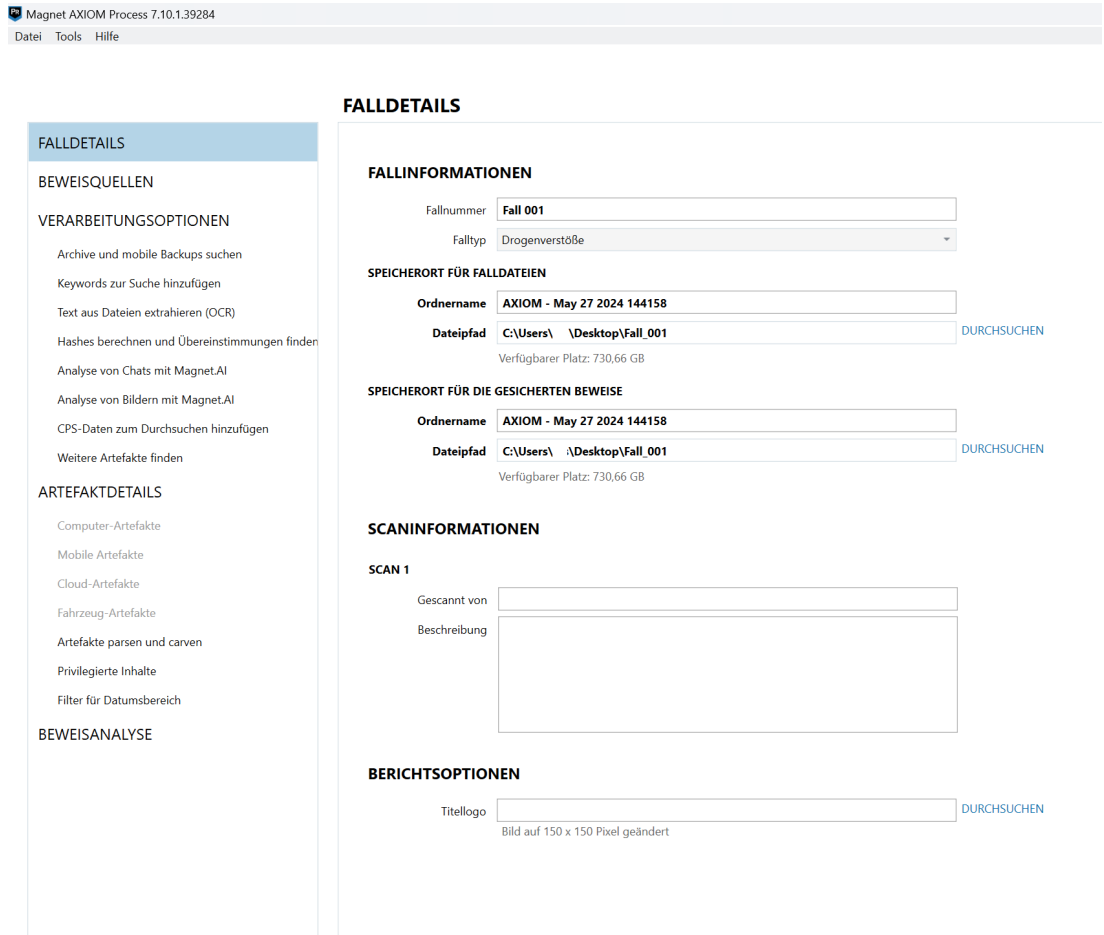


Abbildung 34: Axiom Fallübersicht

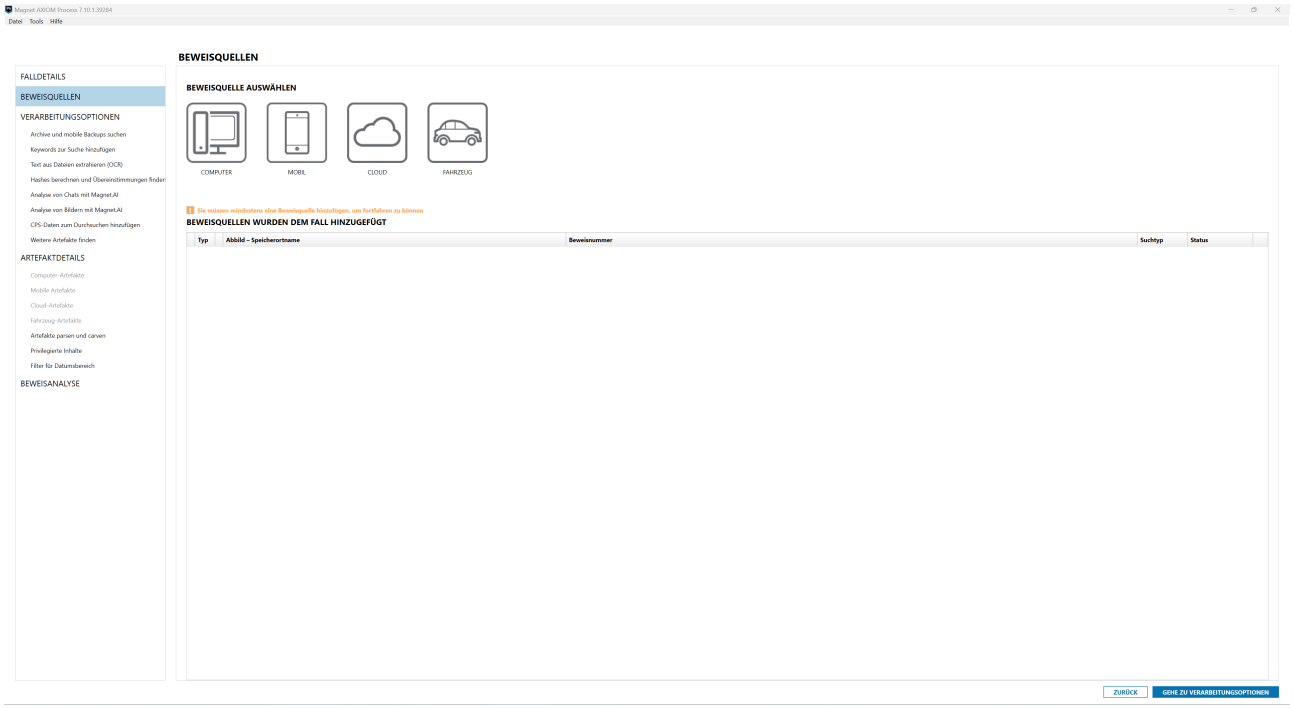


Abbildung 35: Beweisquellen

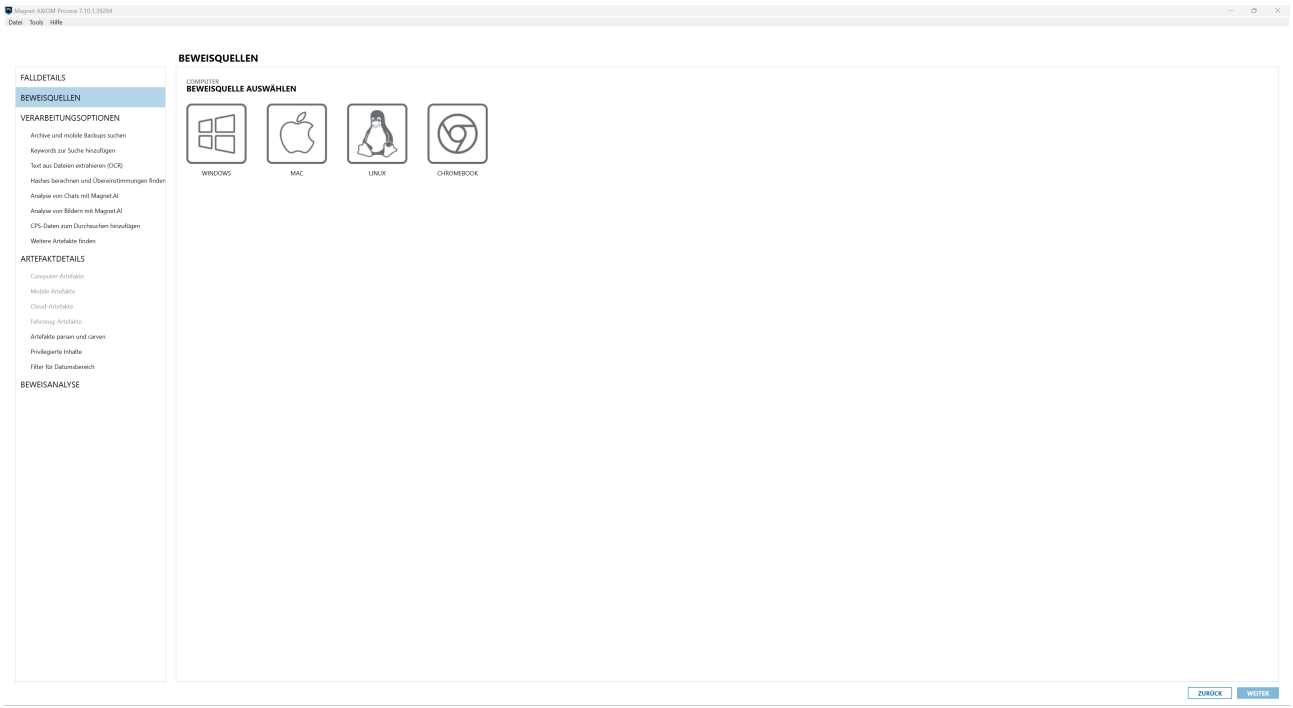


Abbildung 36: Beweisquellen-Auswahl

Abbildung 37: Beweisquellen laden oder sichern

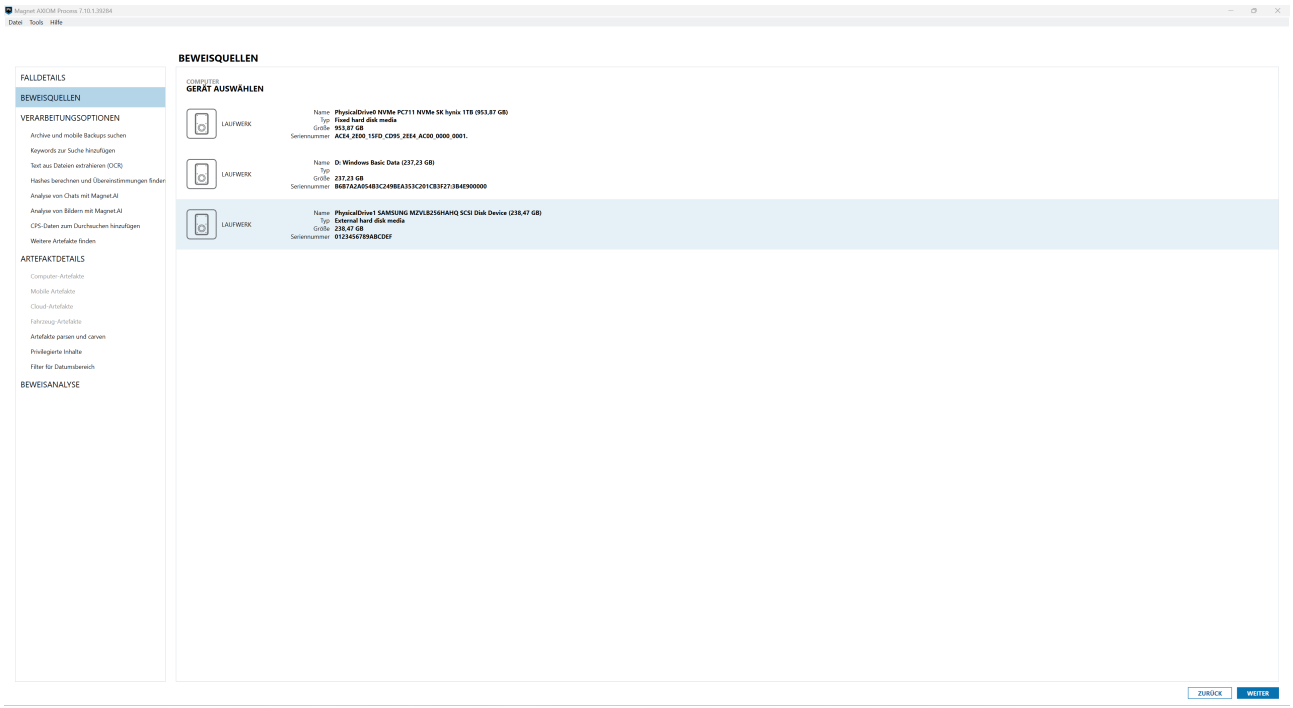


Abbildung 38: Beweisquellen SSD-Auswahl

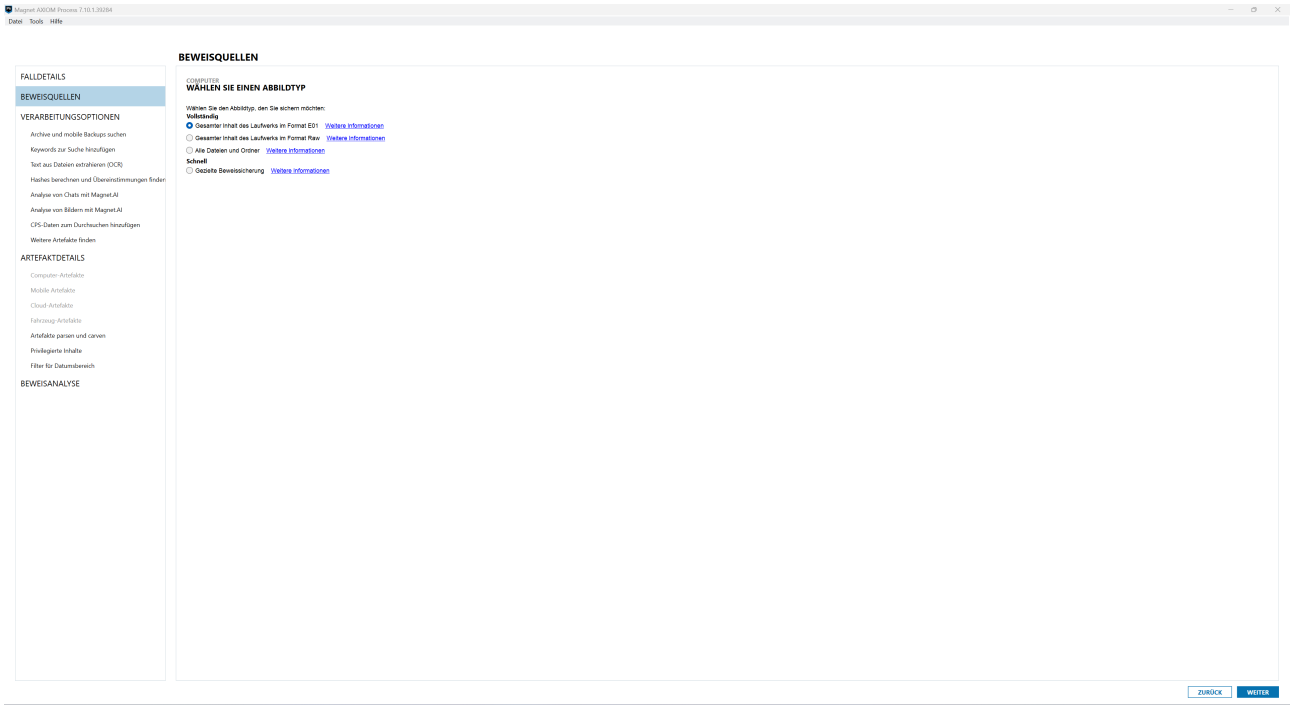


Abbildung 39: Beweisquelle sichern als '.E01'

Nach erfolgter Abbilderstellung beginnt die Untersuchung der gesicherten Datenbasis. Unter dem Punkt 'Beweisanalyse' erfolgt die entsprechende Auswahl des Images und der Untersuchungsprozess beginnt (Abbildung 43).

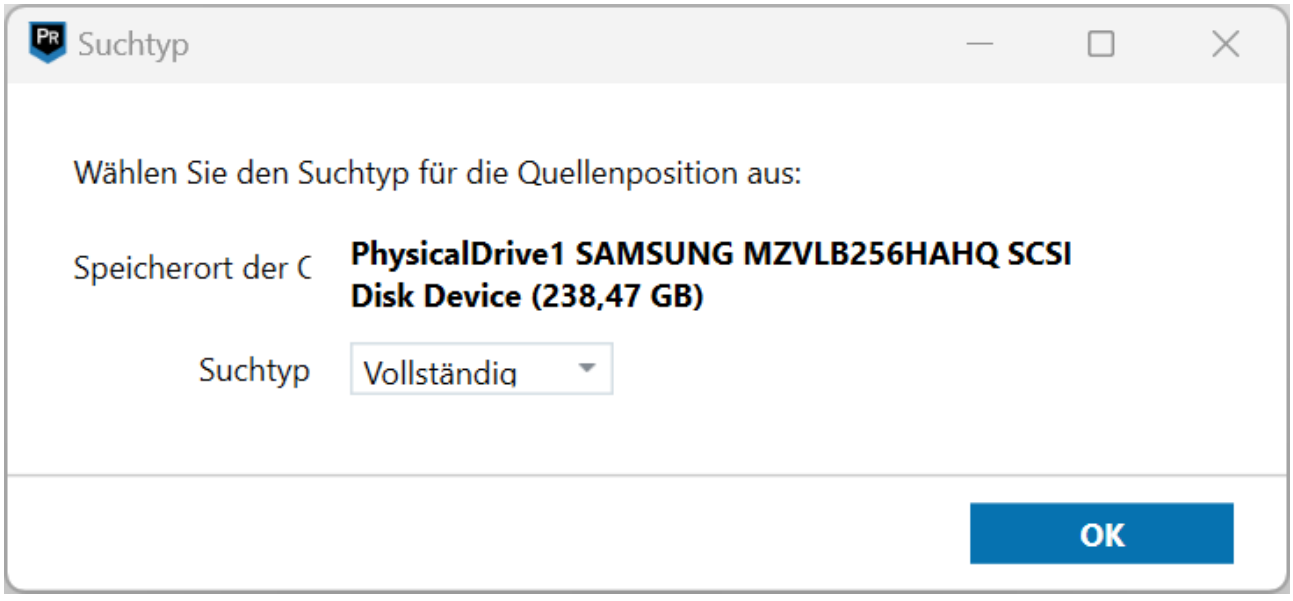


Abbildung 40: Suchtyp

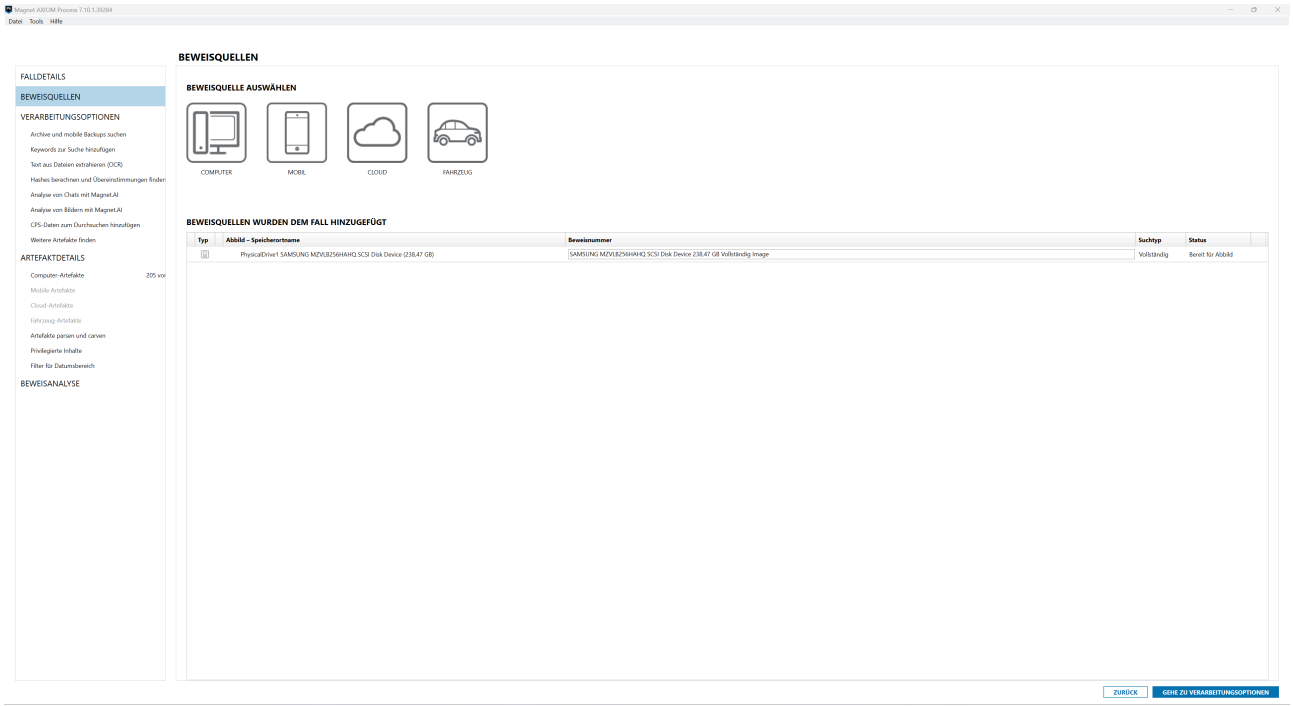


Abbildung 41: Beweisquelle zum Fall hinzugefügt

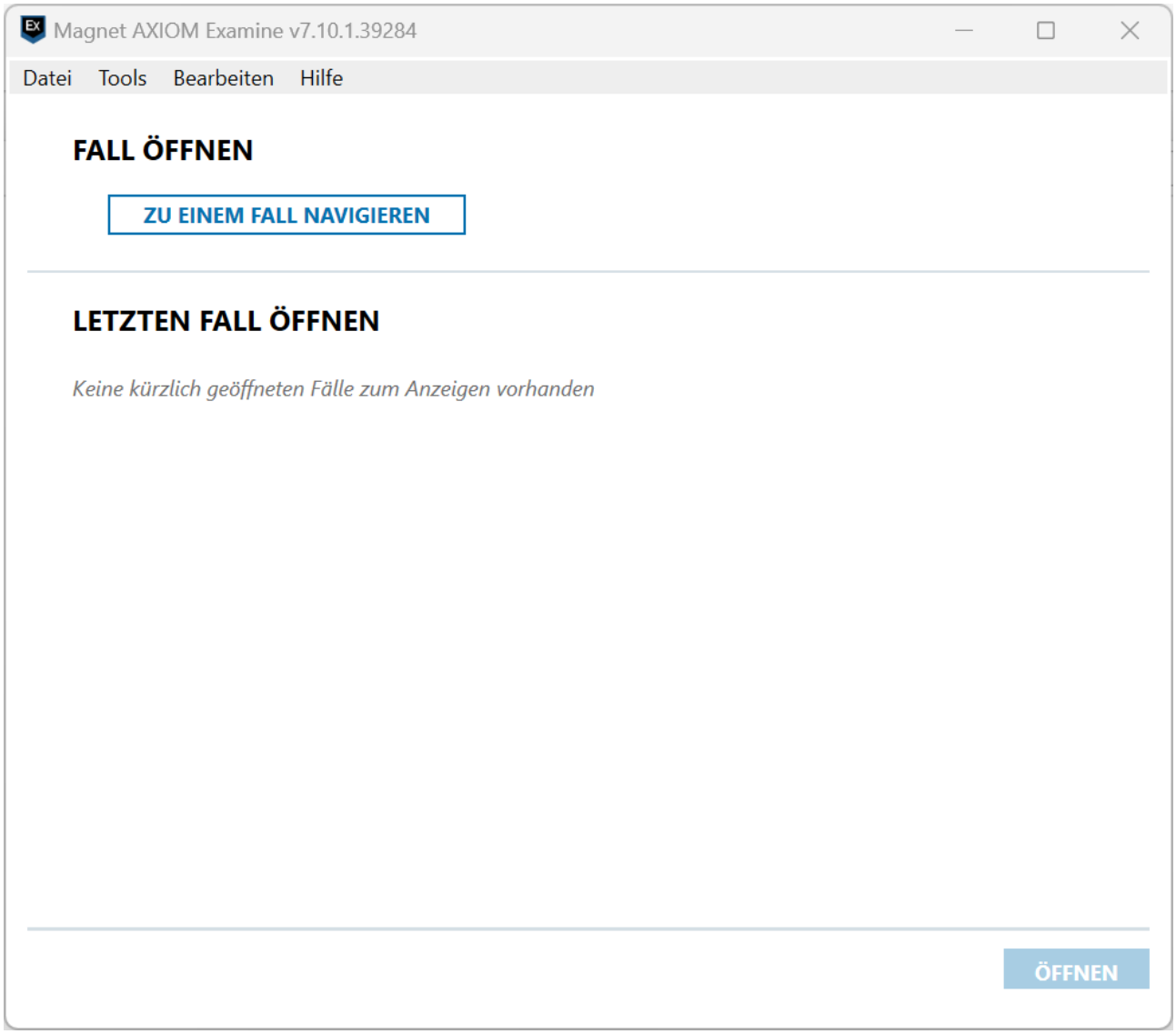


Abbildung 42: Zu einem Fall navigieren

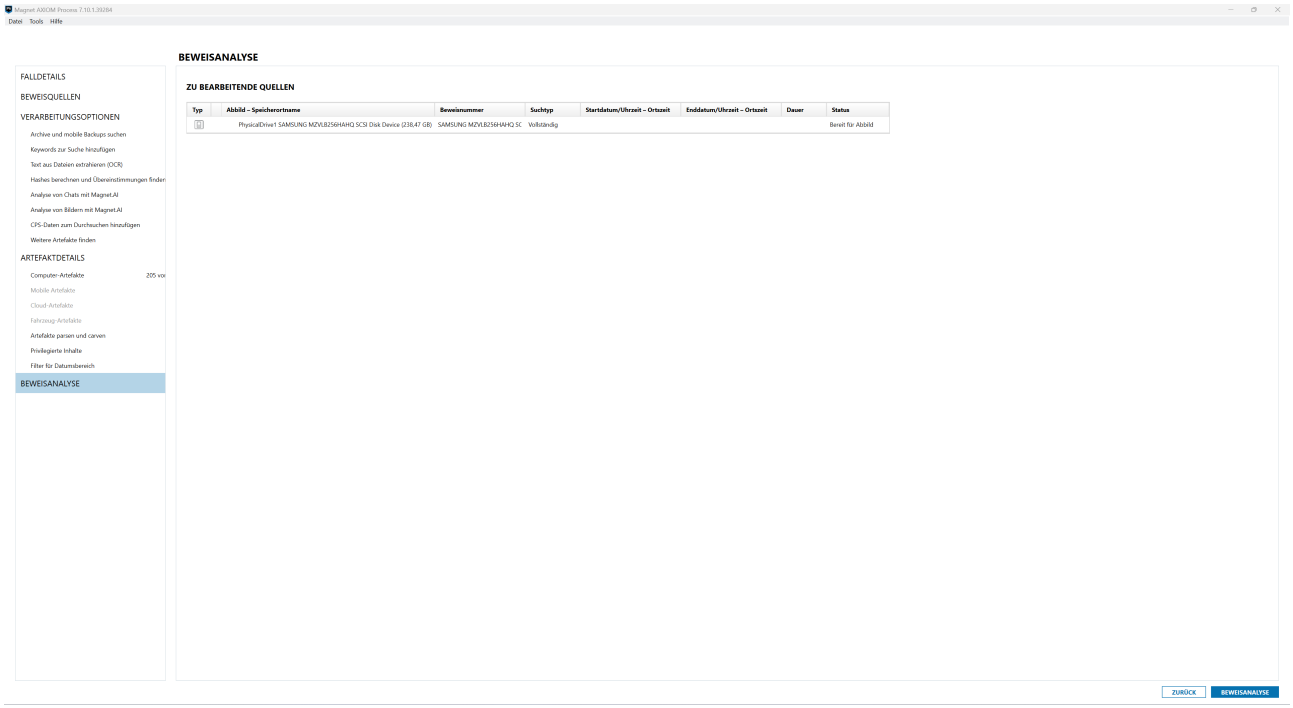


Abbildung 43: Auswahl Beweisanalyse

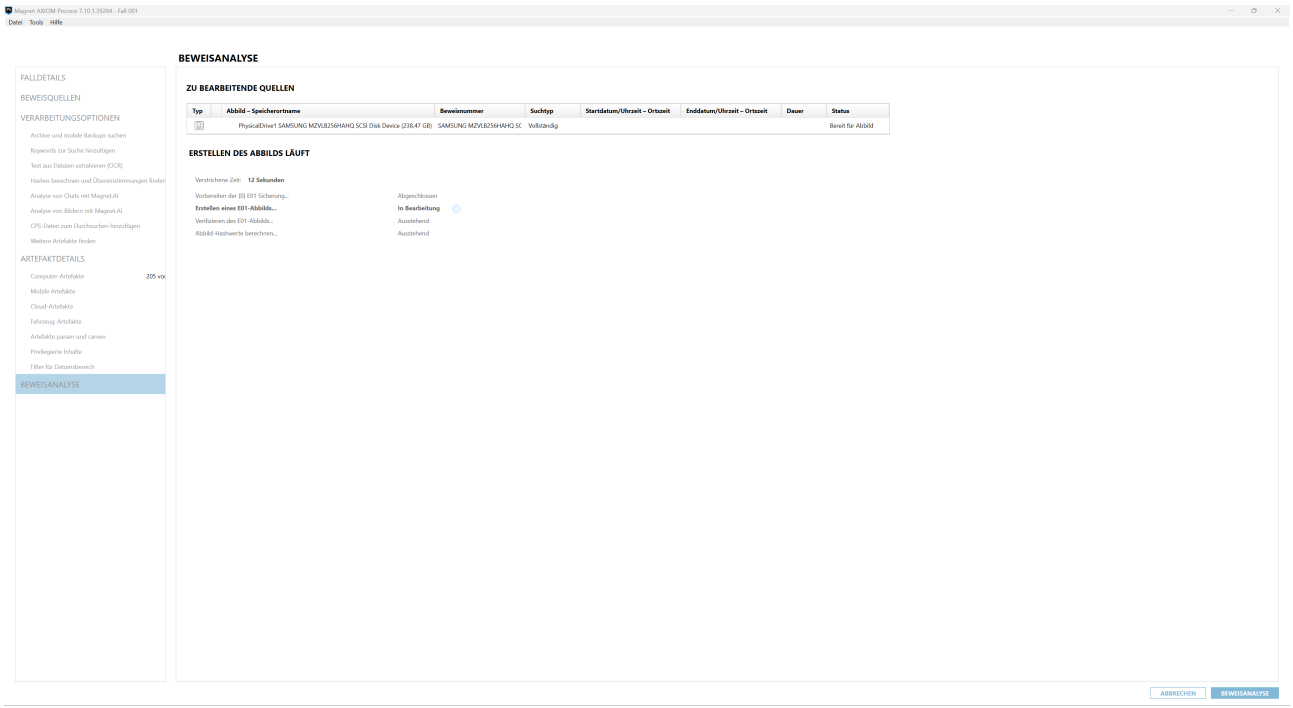


Abbildung 44: Erstellen des Abbilds

4.1.2 Forensische Analyse PC mit integrierter SSD

Nach erfolgter Abbild-Erstellung kann mit der Auswertung des forensischen Images begonnen werden. Das Programm 'Axiom Analyzer' arbeitet vollautomatisch und wertet das Image systematisch aus. Da ein sehr breites Spektrum für die Auswertung abgedeckt wird, dauert der Vorgang entsprechend. Die Analyse des vorliegenden E01-Images des PCs nahm mehrere Stunden in Anspruch und lief über Nacht.

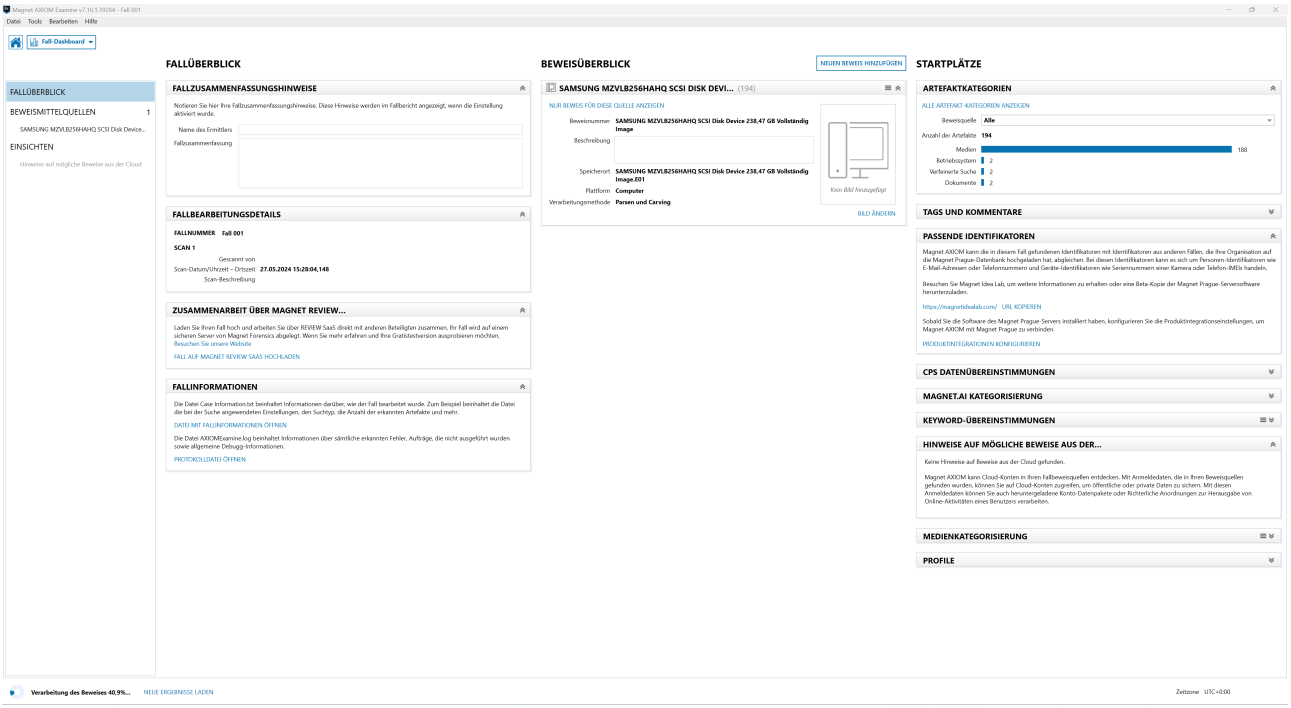


Abbildung 45: Fallüberblick

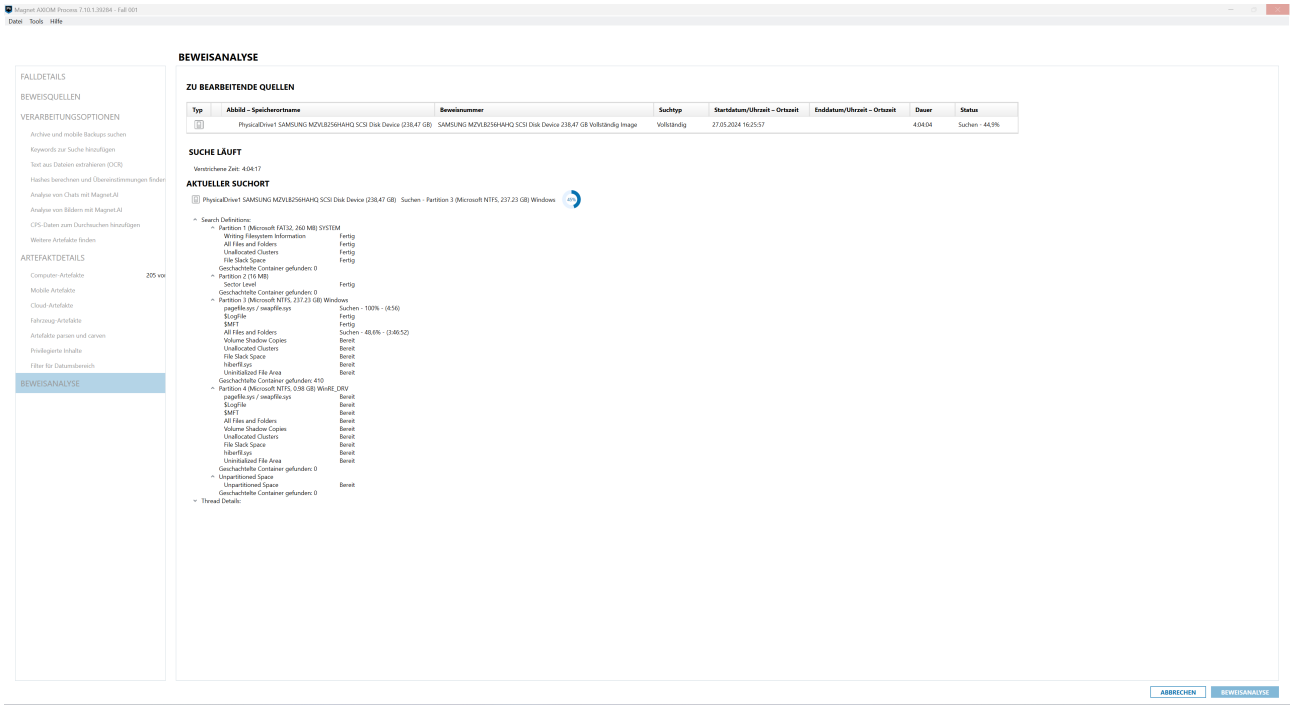


Abbildung 46: Fallüberblick mit laufender Suche

Nach abgeschlossener Analyse stellt das Programm 'Axiom' in der linken Spalte die gefundenen Beweise/Artefakte gruppiert dar. Da der Untersuchungsauftrag klar vorgegeben wurde, wird nachfolgend der Schwerpunkt auf die entsprechenden Beweise gelegt und hauptsächlich auf die gefundenen Artefakte, zumeist Dateien, eingegangen.

Die Abbildung 47 zeigt den rekonstruierten Desktop des beschlagnahmten PCs. Dem Desktop ist eine Verknüpfung zum Firefox-Browser und Signal-Desktop zu entnehmen. Zur Verifikation werden die installierten Programme näher betrachtet. Abbildung 48 zeigt einen Ausschnitt der auf dem System installierten Programme, unter denen sich auch die beiden Apps 'Firefox' und 'Signal' befinden.

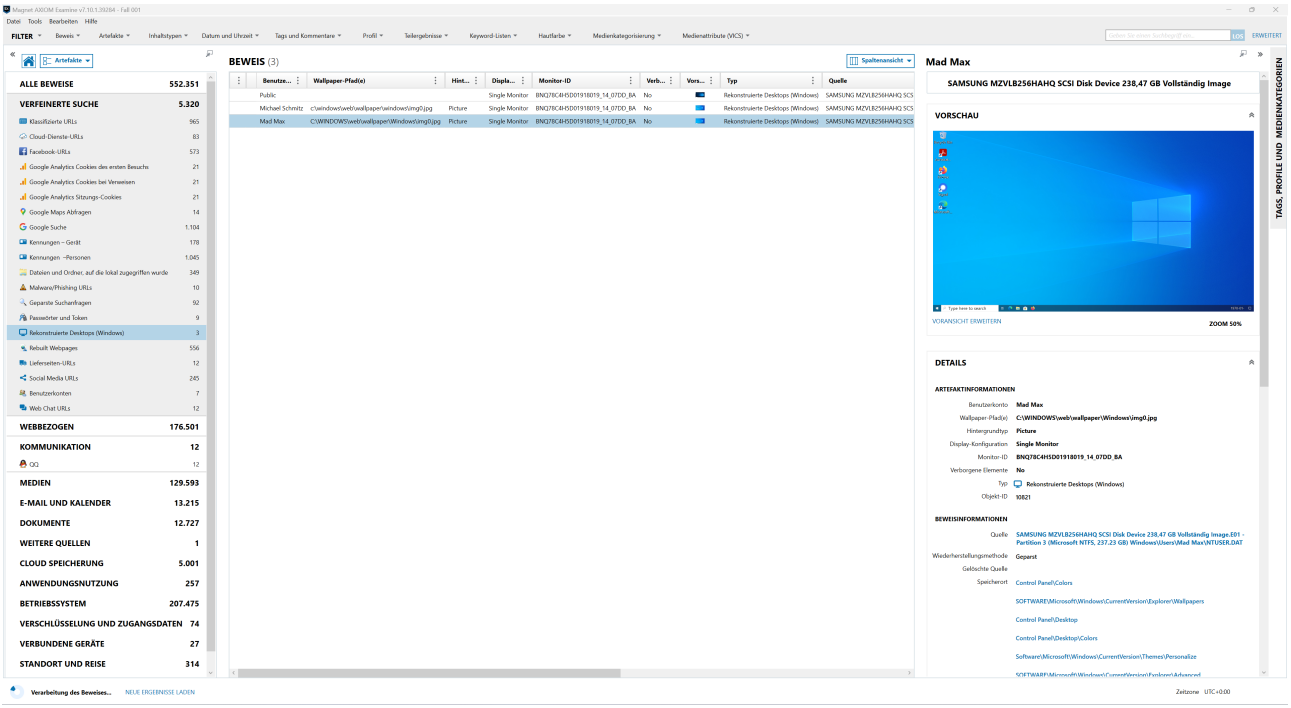


Abbildung 47: Rekonstruierter Desktop

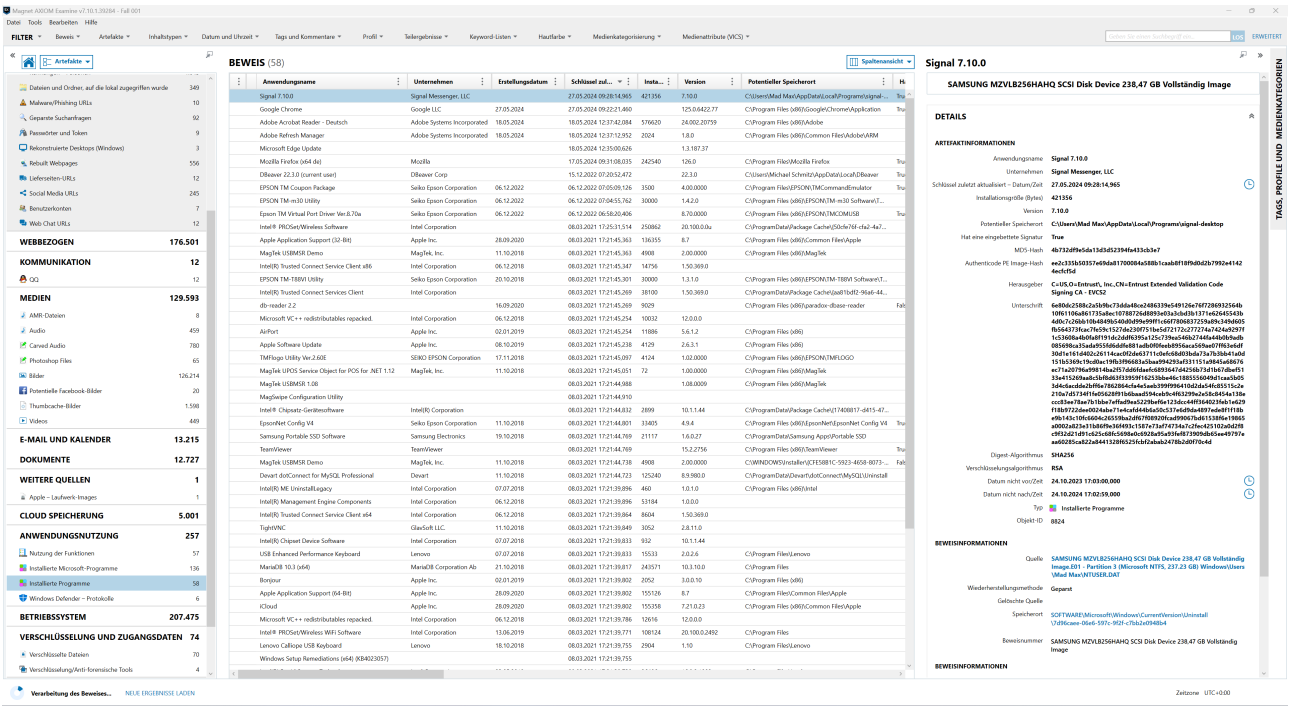


Abbildung 48: Installierte Programme

Unter dem Punkt 'Verschlüsselung und Zugangsdaten' findet sich an vierter Position ein Hinweis auf die Datei 'signal.db', auf die im weiteren Verlauf Bezug genommen wird (Abbildung 49).

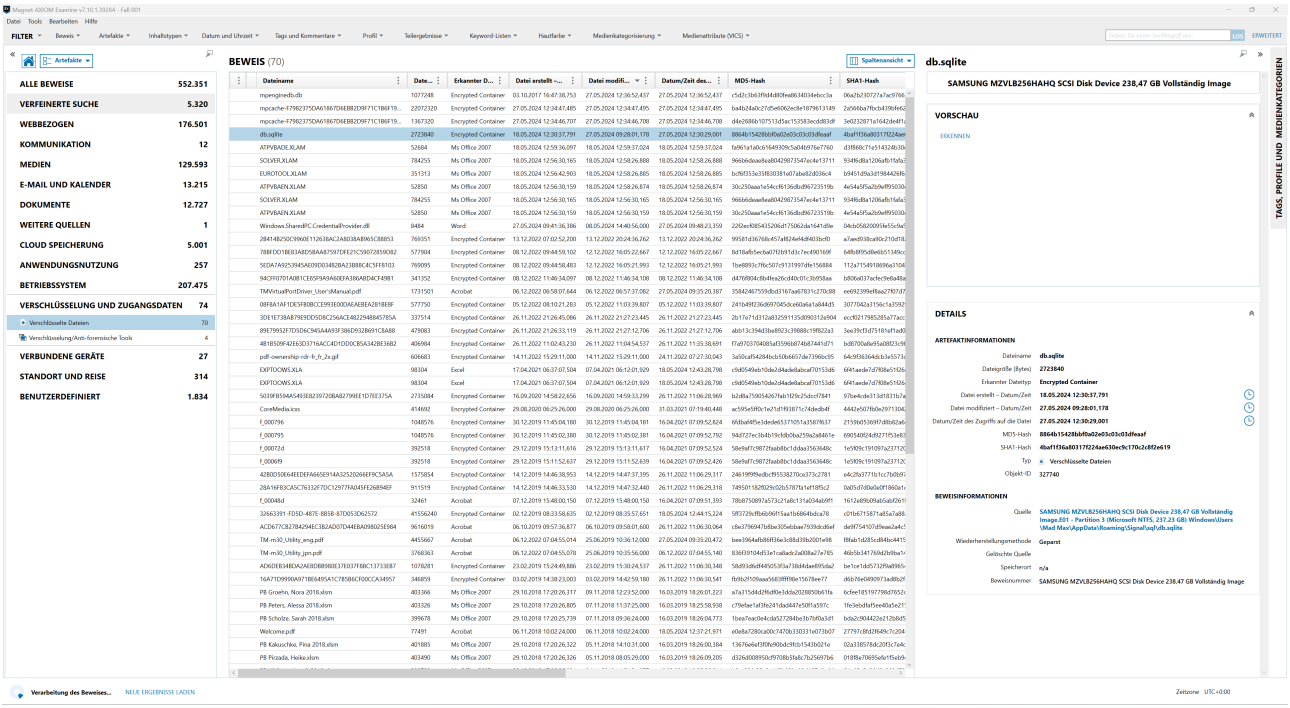


Abbildung 49: Verschlüsselung und Zugangsdaten

Es finden sich ebenso Hinweise auf 'verwendete Passwörter und Token'. Hier befindet sich das Account-Token für den Benutzer 'Mad Max' mitsamt WLAN-Namen und zugehörigem Kennwort (Abbildung 50).

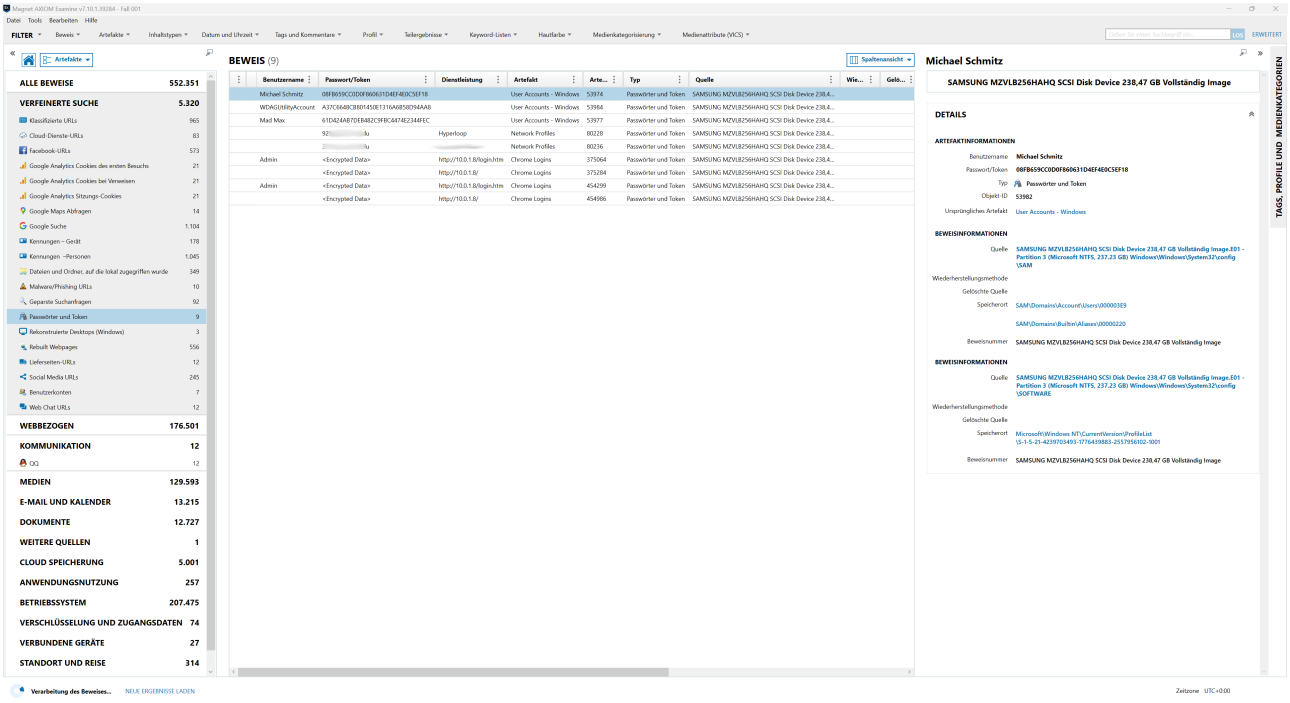


Abbildung 50: Passwörter und Token

Unter der Rubrik 'Verfeinerte Suche' besteht die Möglichkeit, sich die Google-Suche anzeigen zu lassen. Abbildung 52 zeigt die gesuchten Begriffe mit URL und Zeitstempel. Da das Tool 'Axiom' die Möglichkeit bietet, Dateien aus dem Dateisystem zu extrahieren, wurde die SQLite-Datenbank 'places.sqlite' extrahiert und mittels 'DB-Browser for SQLite' zusätzlich untersucht. Die relevanten Daten für den Browser-Verlauf befinden sich in der Tabelle 'moz_places'. Der folgende SQL-Befehl (Abbildung 51) zeigte die zur Timeline-Erzeugung benötigten Informationen:

```
select strftime('%d.%m.%Y %H:%M:%S',(last_visit_date/1000000),'unixepoch')
as zeit, url from moz_places order by last_visit_date;
```

Abbildung 51: SQL-Befehl

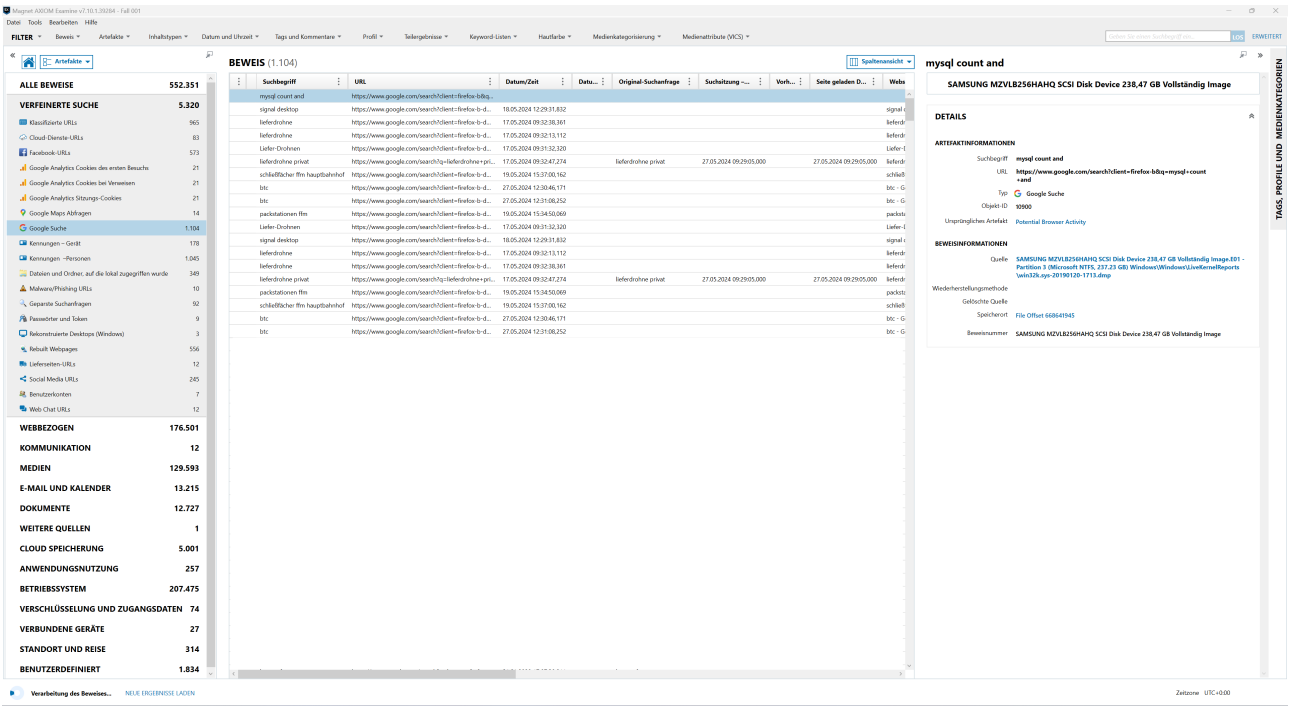


Abbildung 52: Google-Suche

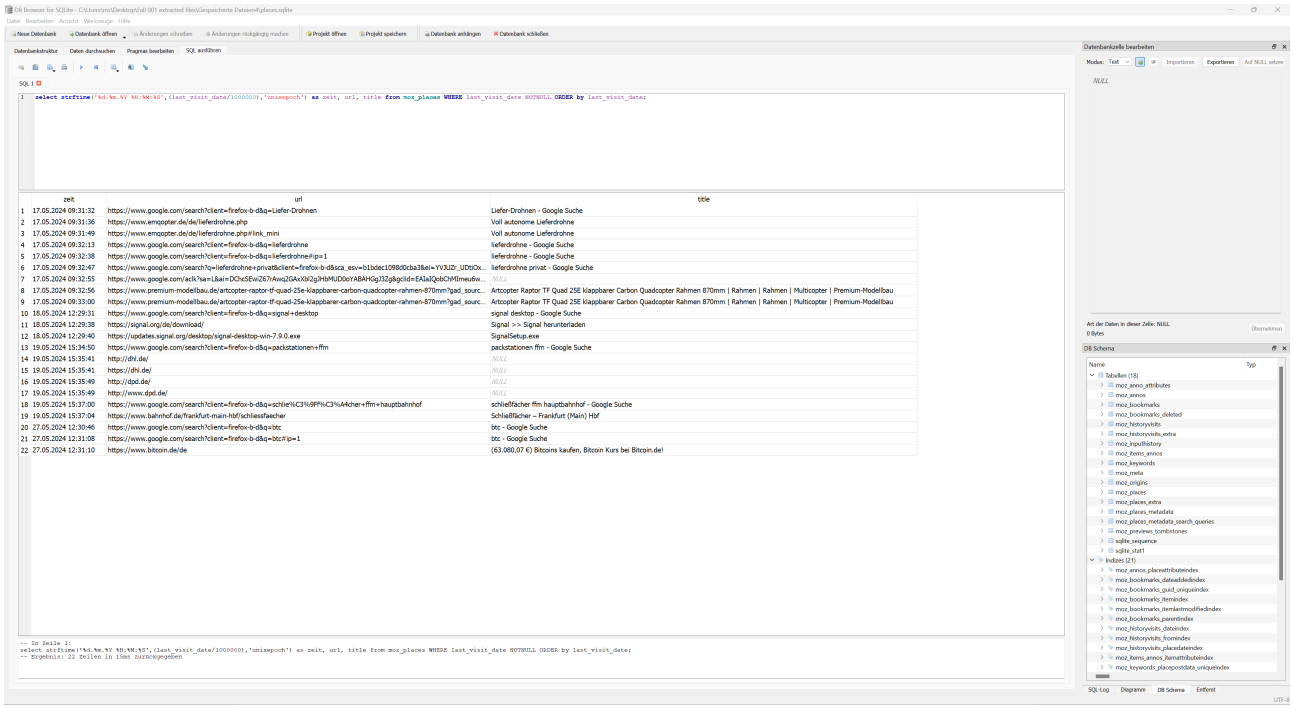
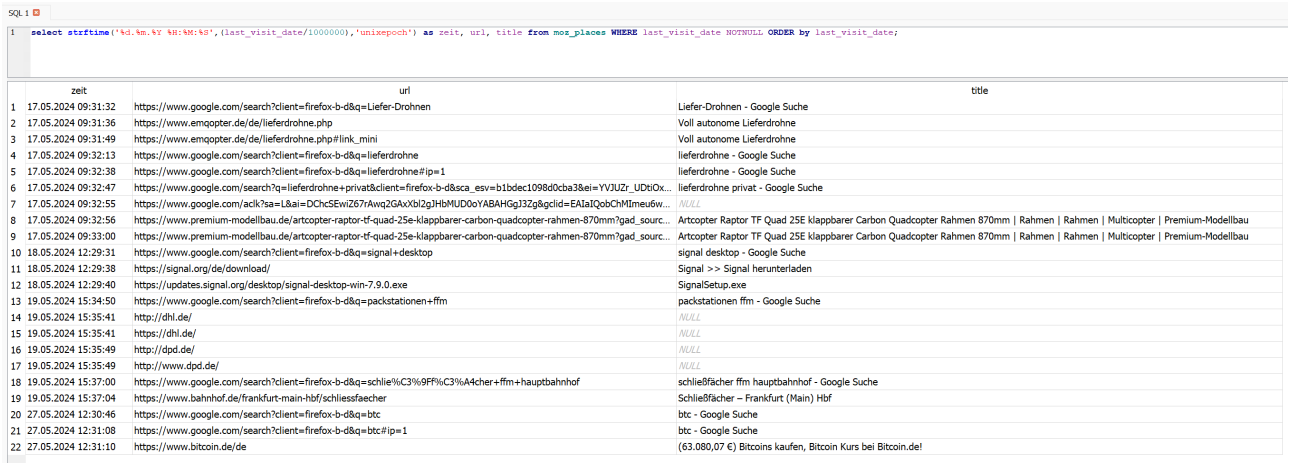


Abbildung 53: Google moz-places-db



```
select strftime('%d.%m.%Y %H:%M:%S',(last_visit_date/1000000),'unixepoch') as zeit, url, title from moz_places WHERE last_visit_date NOTNULL ORDER by last_visit_date;
```

	zeit	url	title
1	17.05.2024 09:31:32	https://www.google.com/search?client=firefox-b-d&q=Liefer-Drohnen	Liefer-Drohnen - Google Suche
2	17.05.2024 09:31:36	https://www.emqopter.de/de/lieferdrohne.php	Voll autonome Lieferdrohne
3	17.05.2024 09:31:49	https://www.emqopter.de/de/lieferdrohne.php#link_mini	Voll autonome Lieferdrohne
4	17.05.2024 09:32:13	https://www.google.com/search?client=firefox-b-d&q=lieferdrohne	lieferdrohne - Google Suche
5	17.05.2024 09:32:38	https://www.google.com/search?client=firefox-b-d&q=lieferdrohne#ip=1	lieferdrohne - Google Suche
6	17.05.2024 09:32:47	https://www.google.com/search?q=lieferdrohne+privat&client=firefox-b-d&sca_esv=b1bdec1098d0cba38ei=YVJUZr_UDtiOx...	lieferdrohne privat - Google Suche
7	17.05.2024 09:32:55	https://www.google.com/aclk?sa=L&ai=DChcSEwiZ67rAwq2GAxXbl2gJHbMUD0oYABAHGgJ3Zg&gclid=EAIaIQobChMImeu6w...	*NULL*
8	17.05.2024 09:32:56	https://www.premium-modellbau.de/artcopter-raptor-tf-quad-25e-klappbarer-carbon-quadcopter-rahmen-870mm?gad_sourc...	Artcopter Raptor TF Quad 25E klappbarer Carbon Quadcopter Rahmen 870mm | Rahmen | Rahmen | Multicopter | Premium-Modellbau
9	17.05.2024 09:33:00	https://www.premium-modellbau.de/artcopter-raptor-tf-quad-25e-klappbarer-carbon-quadcopter-rahmen-870mm?gad_sourc...	Artcopter Raptor TF Quad 25E klappbarer Carbon Quadcopter Rahmen 870mm | Rahmen | Rahmen | Multicopter | Premium-Modellbau
10	18.05.2024 12:29:31	https://www.google.com/search?client=firefox-b-d&q=signal+desktop	signal desktop - Google Suche
11	18.05.2024 12:29:38	https://signal.org/de/download/	Signal >> Signal herunterladen
12	18.05.2024 12:29:40	https://updates.signal.org/desktop/signal-desktop-win-7.9.0.exe	SignalSetup.exe
13	19.05.2024 15:34:50	https://www.google.com/search?client=firefox-b-d&q=packstationen+ffm	packstationen ffm - Google Suche
14	19.05.2024 15:35:41	http://dhl.de/	*NULL*
15	19.05.2024 15:35:41	https://dhl.de/	*NULL*
16	19.05.2024 15:35:49	http://dpd.de/	*NULL*
17	19.05.2024 15:35:49	http://www.dpd.de/	*NULL*
18	19.05.2024 15:37:00	https://www.google.com/search?client=firefox-b-d&q=schlie%C3%9Ff%C3%A4cher+ffm+hauptbahnhof	schließfächer ffm hauptbahnhof - Google Suche
19	19.05.2024 15:37:04	https://www.bahnhof.de/frankfurt-main-hbf/schliessfaecher	Schließfächer – Frankfurt (Main) Hbf
20	27.05.2024 12:30:46	https://www.google.com/search?client=firefox-b-d&q=btc	btc - Google Suche
21	27.05.2024 12:31:08	https://www.google.com/search?client=firefox-b-d&q=btc#ip=1	btc - Google Suche
22	27.05.2024 12:31:10	https://www.bitcoin.de/de	(63.080,07 €) Bitcoins kaufen, Bitcoin Kurs bei Bitcoin.de!

Abbildung 54: Vergrösserter Ausschnitt des obigen Screenshots

Im Bereich der verfeinerten Suche werden unter anderem Dateizugriffe protokolliert (Abbildung 55). Hier wurden Hinweise auf heruntergeladene Dateien aus dem Programm 'Signal-Desktop' gefunden. Ein Blick in den 'Downloads'-Ordner im System-Baum fördert diese dann zutage. Es wurden mehrere Dateien gefunden. Einerseits 'SignalSetup.exe' und andererseits die drei Dateien 'signal-2024-05-18-203244.jpeg' (Labor-Bild), 'Herstellung.txt' (ein Dokument über die Entstehung von Metamphetamin) und 'Wuscha.doc' (Abbildung 56).

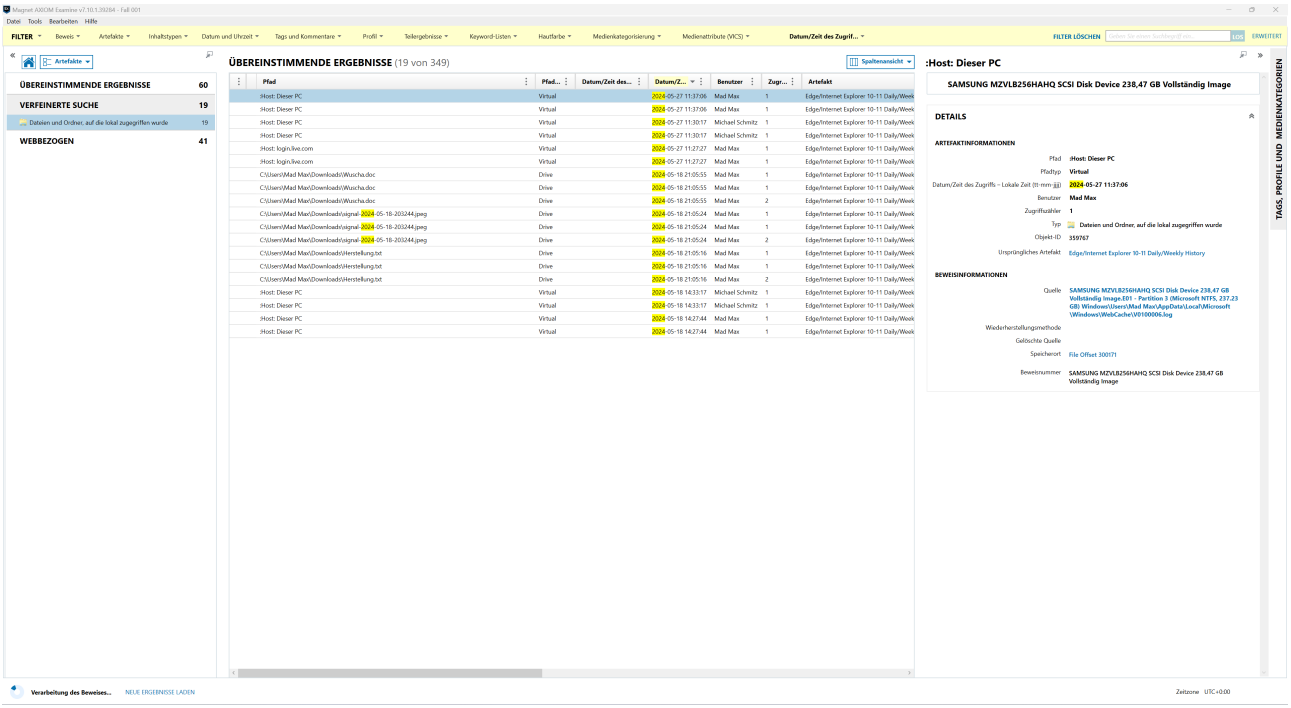


Abbildung 55: Verfeinerte Suche für den Tat-Zeitraum

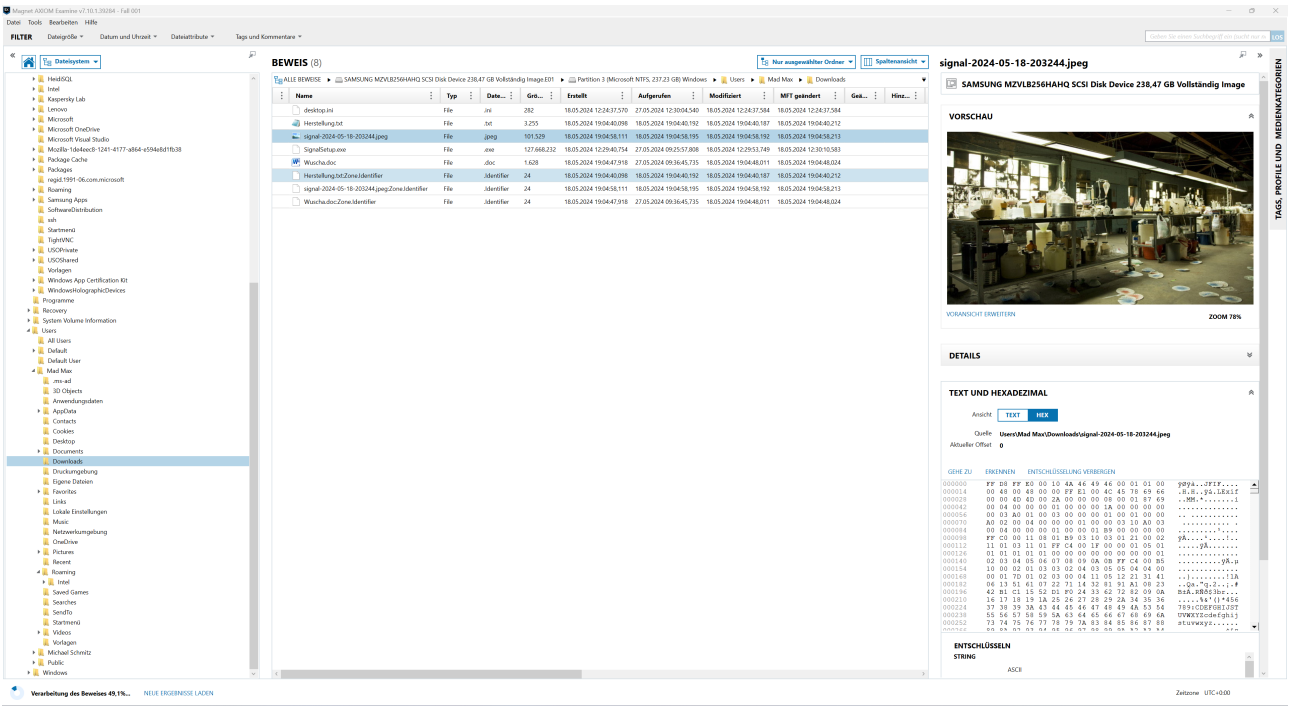


Abbildung 56: Downloads-Ordner im Dateisystem-Baum

Auswertung Signal-DB

Da von Axiom kein Chat-Verlauf aus Signal rekonstruiert werden konnte erforderten die gefundenen Hinweise zum Signal-Browser ein manuelles Auswerten. Die zur Auswertung benötigten Daten finden sich im System-Baum unter 'Users\Mad Max\AppData\Signal'. Die Datenbank mit sämtlichen Daten liegt dann im Ordner 'sql'. Dieser Ordner enthält im aktuellen Fall drei Dateien: 'db.sqlite', die eigentliche Datenbank, 'db.sqlite-shm[3]' und 'db.sqlite-wal[4]', bei denen es sich um temporäre Dateien handelt. Diese drei Dateien wurden für die weitere Untersuchung extrahiert. Bei der 'db.sqlite' handelt es sich um eine verschlüsselte SQLite-Datenbank, die mit dem Tool 'SQLcipher' der Firma 'Zetetic LLC' (Link: https://www.zetetic.net/sqlcipher/) erstellt wurde. Dieses Tool gibt es in einer kommerziellen, wie auch open source Version. Um diese Datenbank entschlüsseln zu können, greift man auf den Schlüssel im Hauptverzeichnis zurück. Dieser steht in der Datei 'config.json' (Abbildung 57).

```
key : "a6434894a6b4d678169a253143c943787479369bce0649a18799de37b9e16413"
```

Abbildung 57: Entschlüsselungs-Key der db.sqlite

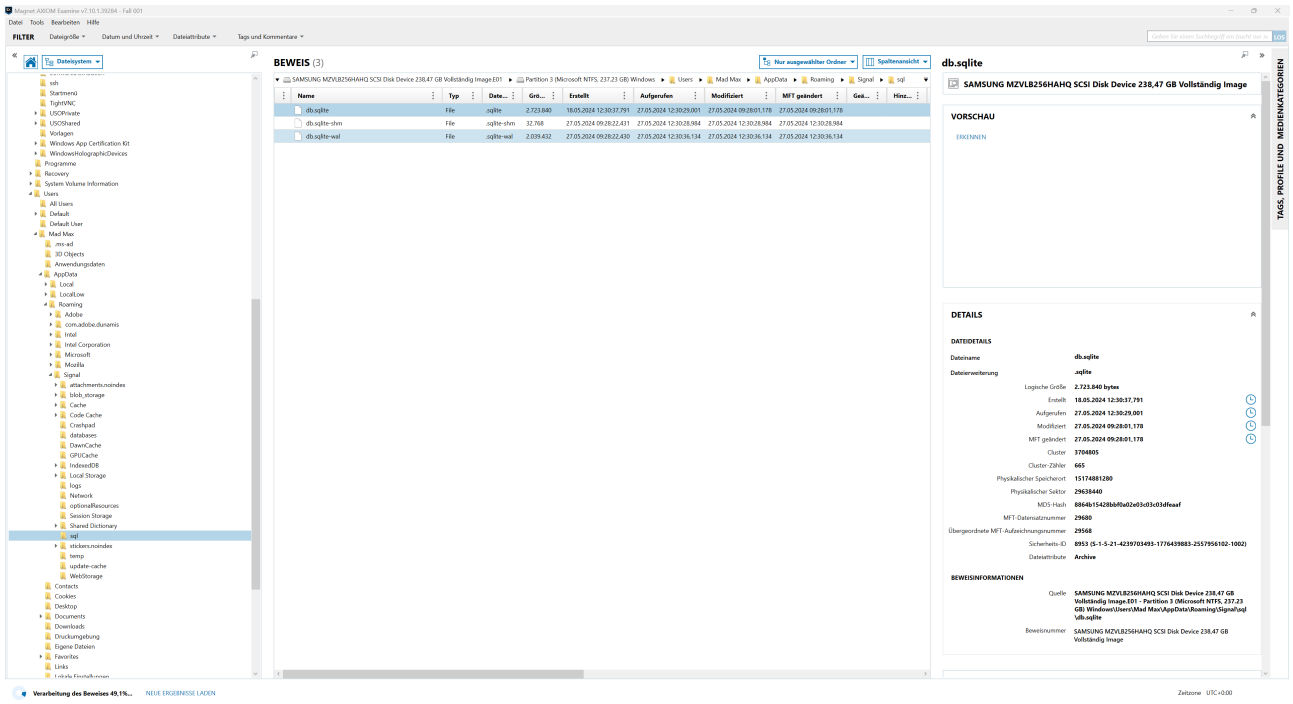


Abbildung 58: Signal-Ordner im Dateisystem

[3]shared memory
[4]write ahead log

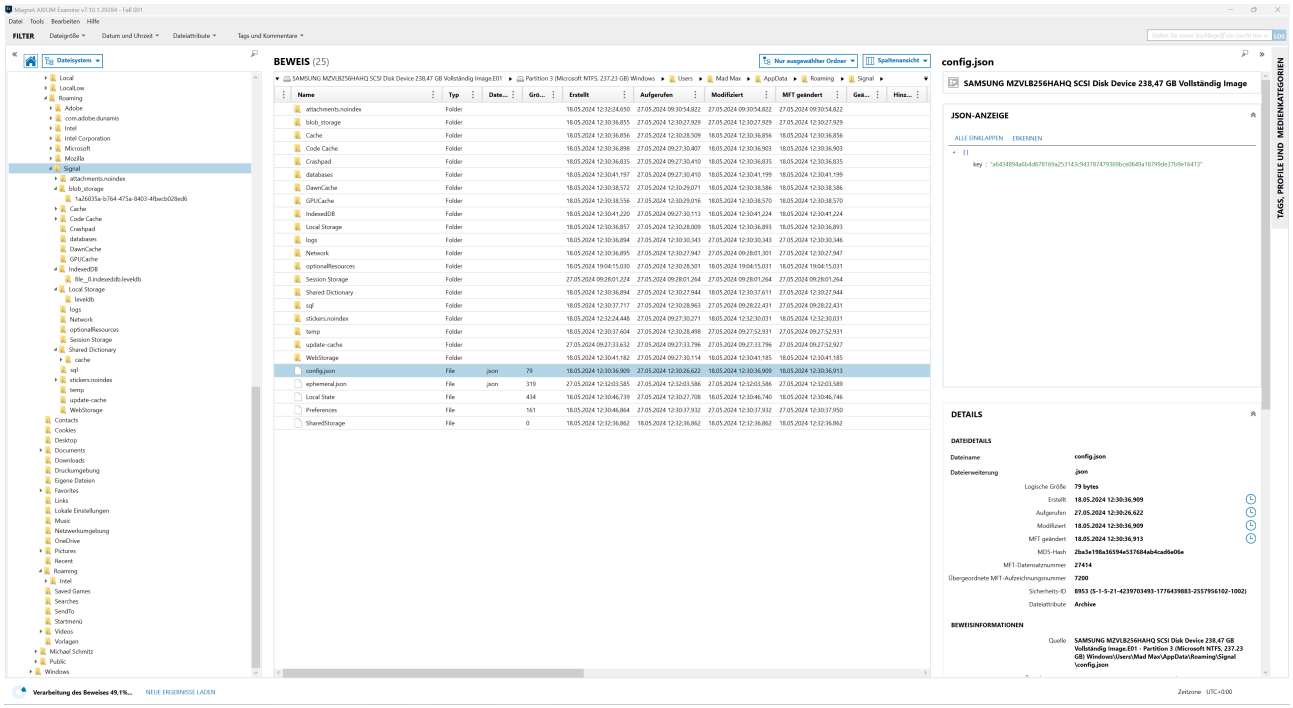


Abbildung 59: Inhalt der 'config.json' Datei

Da der Schlüssel und die Signal-Datenbank gefunden wurden, kann der Chat-Verlauf rekonstruiert werden. Hierzu könnte das Tool 'SQLCipher' verwendet werden. Es handelt sich hierbei um eine angepasste Version des SQLite-Tools, die eine Verschlüsselung der jeweiligen Datenbank ermöglicht. Da es sich allerdings für das Windows-Betriebssystem um eine kommerzielle Version handelt und eine manuelle Installation zu umständlich gewesen wäre, wurde auf den Erwerb einer Lizenz verzichtet und stattdessen im WSL die Open-Source Version installiert. (Da die Nutzung von Linux-Tools für diese Arbeit nicht gewünscht ist, sind die folgenden Schritte als Proof-Of-Concept zu werten, da lediglich gezeigt werden soll, dass eine Chat-Rekonstruktion mit der kommerziellen Version zum entsprechenden Ergebnis geführt hätte!)

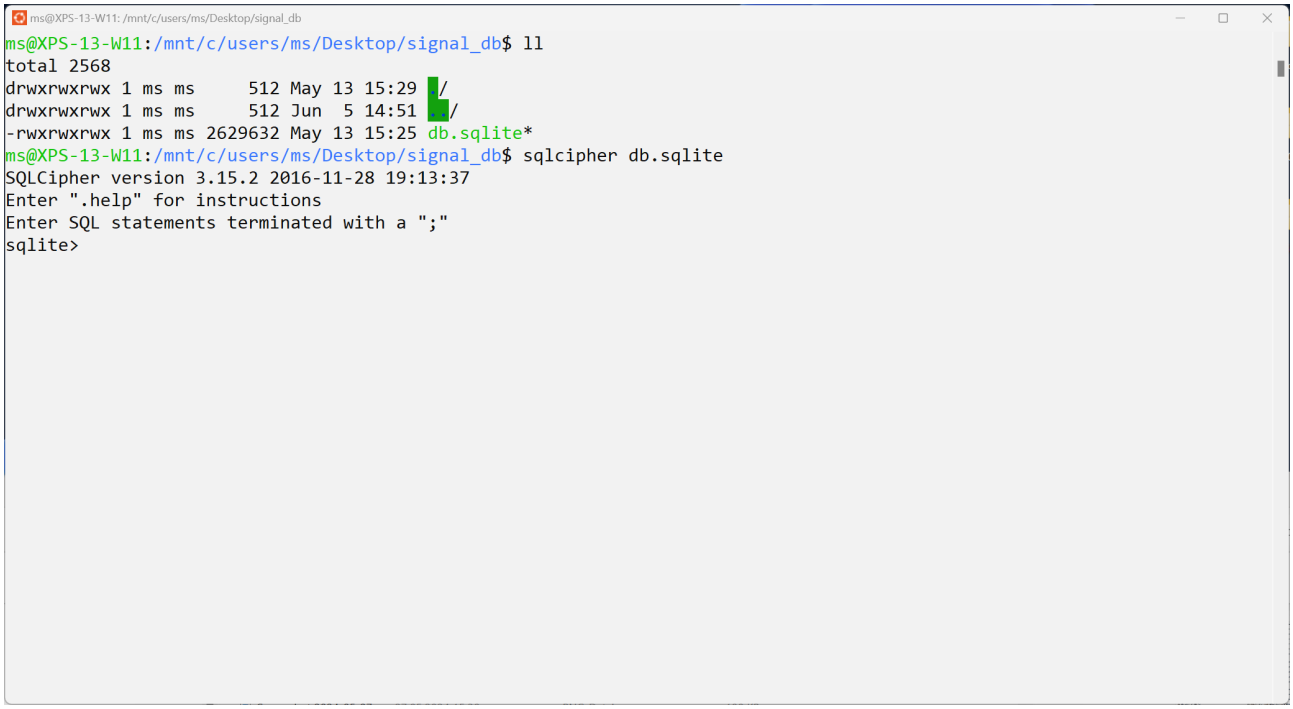


Abbildung 60: SQLCipher-Tool

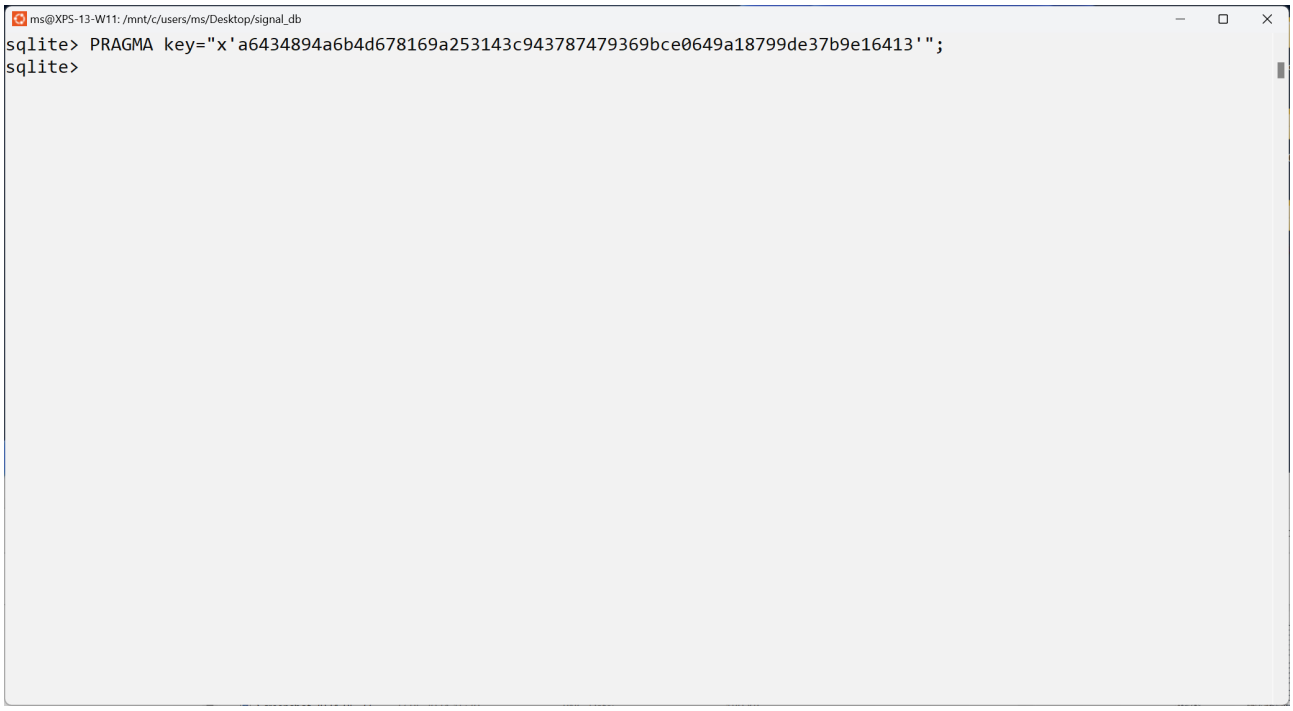
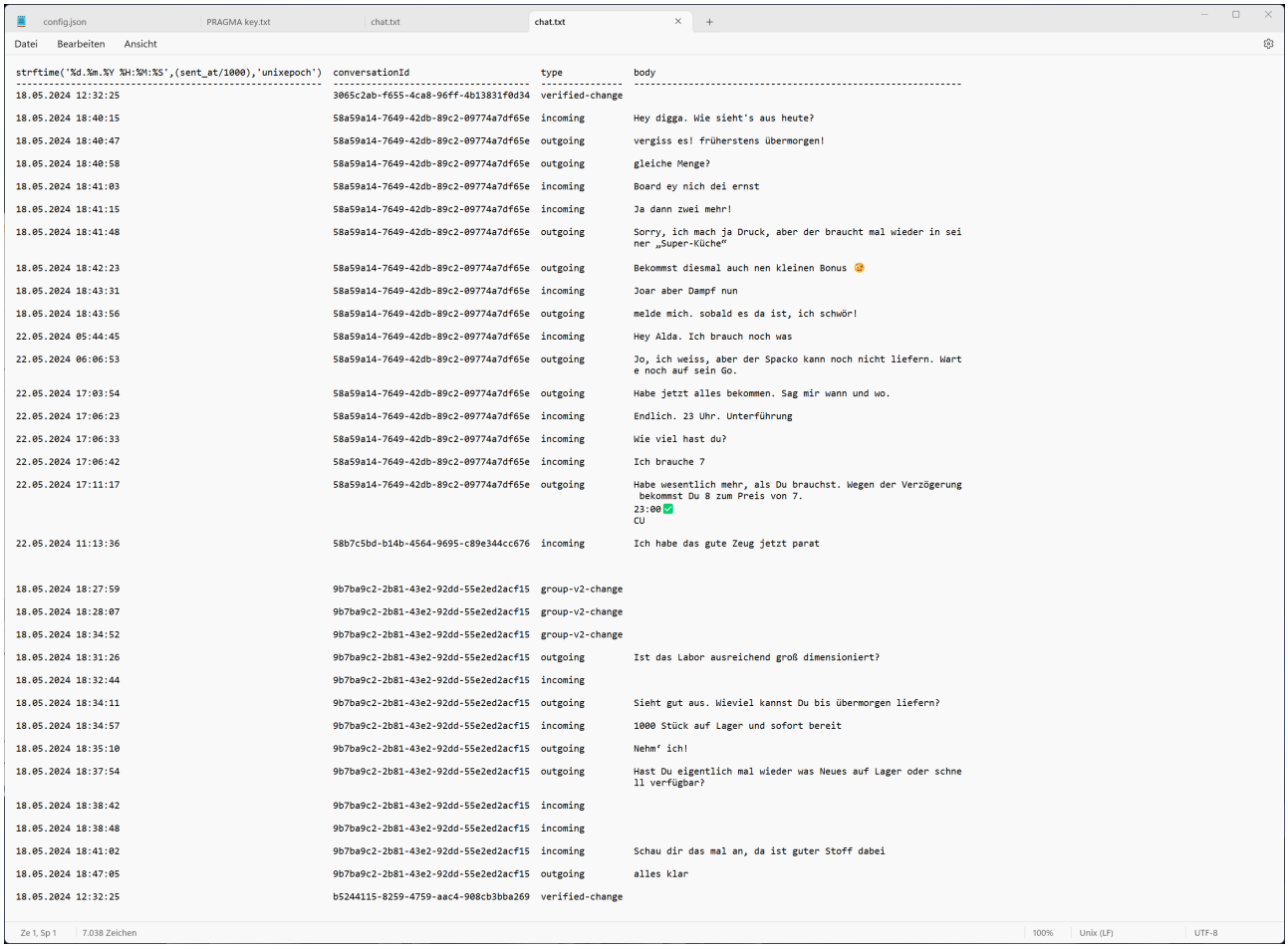


Abbildung 61: Eingabe des Schlüssels



config.json | PRAGMA key.txt | chat.txt | chat.txt

Datei Bearbeiten Ansicht

strftime('%d.%m.%Y %H:%M:%S',(sent_at/1000),'unixepoch')	conversationId	type	body
18.05.2024 12:32:25	3065c2ab-f655-4ca8-96ff-4b13831f0d34	verified-change	
18.05.2024 18:40:15	58a59a14-7649-42db-89c2-09774a7df65e	incoming	Hey digga. Wie sieht's aus heute?
18.05.2024 18:40:47	58a59a14-7649-42db-89c2-09774a7df65e	outgoing	vergiss es! früherstens übermorgen!
18.05.2024 18:40:58	58a59a14-7649-42db-89c2-09774a7df65e	outgoing	gleiche Menge?
18.05.2024 18:41:03	58a59a14-7649-42db-89c2-09774a7df65e	incoming	Board ey nich dei ernst
18.05.2024 18:41:15	58a59a14-7649-42db-89c2-09774a7df65e	incoming	Ja dann zwei mehr!
18.05.2024 18:41:48	58a59a14-7649-42db-89c2-09774a7df65e	outgoing	Sorry, ich mach ja Druck, aber der braucht mal wieder in sei ner „Super-Küche“
18.05.2024 18:42:23	58a59a14-7649-42db-89c2-09774a7df65e	outgoing	Bekommst diesmal auch nen kleinen Bonus 🍪
18.05.2024 18:43:31	58a59a14-7649-42db-89c2-09774a7df65e	incoming	Joar aber Dampf nun
18.05.2024 18:43:56	58a59a14-7649-42db-89c2-09774a7df65e	outgoing	melde mich. sobald es da ist, ich schwör!
22.05.2024 05:44:45	58a59a14-7649-42db-89c2-09774a7df65e	incoming	Hey Alda. Ich brauch noch was
22.05.2024 06:06:53	58a59a14-7649-42db-89c2-09774a7df65e	outgoing	Jo, ich weiss, aber der Spacko kann noch nicht liefern. Wart e noch auf sein Go.
22.05.2024 17:03:54	58a59a14-7649-42db-89c2-09774a7df65e	outgoing	Habe jetzt alles bekommen. Sag mir wann und wo.
22.05.2024 17:06:23	58a59a14-7649-42db-89c2-09774a7df65e	incoming	Endlich. 23 Uhr. Unterführung
22.05.2024 17:06:33	58a59a14-7649-42db-89c2-09774a7df65e	incoming	Wie viel hast du?
22.05.2024 17:06:42	58a59a14-7649-42db-89c2-09774a7df65e	incoming	Ich brauche 7
22.05.2024 17:11:17	58a59a14-7649-42db-89c2-09774a7df65e	outgoing	Habe wesentlich mehr, als Du brauchst. Wegen der Verzögerung bekommst Du 8 zum Preis von 7. 23:00 ✅ CU
22.05.2024 11:13:36	58b7c5bd-b14b-4564-9695-c89e344cc676	incoming	Ich habe das gute Zeug jetzt parat
18.05.2024 18:27:59	9b7ba9c2-2b81-43e2-92dd-55e2ed2acf15	group-v2-change	
18.05.2024 18:28:07	9b7ba9c2-2b81-43e2-92dd-55e2ed2acf15	group-v2-change	
18.05.2024 18:34:52	9b7ba9c2-2b81-43e2-92dd-55e2ed2acf15	group-v2-change	
18.05.2024 18:31:26	9b7ba9c2-2b81-43e2-92dd-55e2ed2acf15	outgoing	Ist das Labor ausreichend groß dimensioniert?
18.05.2024 18:32:44	9b7ba9c2-2b81-43e2-92dd-55e2ed2acf15	incoming	
18.05.2024 18:34:11	9b7ba9c2-2b81-43e2-92dd-55e2ed2acf15	outgoing	Sieht gut aus. Wieviel kannst Du bis übermorgen liefern?
18.05.2024 18:34:57	9b7ba9c2-2b81-43e2-92dd-55e2ed2acf15	incoming	1000 Stück auf Lager und sofort bereit
18.05.2024 18:35:10	9b7ba9c2-2b81-43e2-92dd-55e2ed2acf15	outgoing	Nehm‘ ich!
18.05.2024 18:37:54	9b7ba9c2-2b81-43e2-92dd-55e2ed2acf15	outgoing	Hast Du eigentlich mal wieder was Neues auf Lager oder schne ll verfügbar?
18.05.2024 18:38:42	9b7ba9c2-2b81-43e2-92dd-55e2ed2acf15	incoming	
18.05.2024 18:38:48	9b7ba9c2-2b81-43e2-92dd-55e2ed2acf15	incoming	
18.05.2024 18:41:02	9b7ba9c2-2b81-43e2-92dd-55e2ed2acf15	incoming	Schau dir das mal an, da ist guter Stoff dabei
18.05.2024 18:47:05	9b7ba9c2-2b81-43e2-92dd-55e2ed2acf15	outgoing	alles klar
18.05.2024 12:32:25	b5244115-8259-4759-aac4-908cb3bba269	verified-change	

Ze 1, Sp 1 | 7.038 Zeichen | 100% | Unix (LF) | UTF-8

Abbildung 62: Extrahierter Chat-Verlauf mit Zeit-Stempeln

Chat-Verlauf Mad Max

Datum	Kontakt	in/out	Text
18.05.2024 20:31:26	Prod	out	Ist das Labor ausreichend gross dimensioniert?
18.05.2024 20:32:44	Prod	in	[Labor-Bild]
18.05.2024 20:34:11	Prod	out	Sieht gut aus. Wieviel kannst Du bis übermorgen liefern?
18.05.2024 20:34:57	Prod	in	1000 Stück auf Lager und sofort bereit
18.05.2024 20:35:10	Prod	out	Nehm ich!
18.05.2024 20:37:54	Prod	out	Hast Du eigentlich mal wieder was Neues auf Lager oder schnell verfügbar?
18.05.2024 20:38:42	Prod	in	[herstellung.txt]
18.05.2024 20:38:48	Prod	in	[wuscha.doc]
18.05.2024 20:40:15	Kundin	in	Hey digga. Wie sieht's aus heute?
18.05.2024 20:40:47	Kundin	out	vergiss es! früherstens übermorgen!
18.05.2024 20:40:58	Kundin	out	gleiche Menge?
18.05.2024 20:41:02	Prod	in	Schau dir das mal an, da ist guter Stoff dabei
18.05.2024 20:41:03	Kundin	in	Board ey nich dei ernst
18.05.2024 20:41:15	Kundin	in	Ja dann zwei mehr!
18.05.2024 20:41:48	Kundin	out	Sorry, ich mach ja Druck, aber der braucht mal wieder in seiner Super-Küche
18.05.2024 20:42:23	Kundin	out	Bekommst diesmal auch nen kleinen Bonus [;-)]
18.05.2024 20:43:31	Kundin	in	Joar aber Dampf nun
18.05.2024 20:43:56	Kundin	out	melde mich. sobald es da ist, ich schwör!
18.05.2024 20:47:05	Prod	out	alles klar
22.05.2024 07:44:45	Kundin	in	Hey Alda. Ich brauch noch was
22.05.2024 08:06:53	Kundin	out	Jo, ich weiss, aber der Spacko kann noch nicht liefern. Warte noch auf sein Go.
22.05.2024 13:13:36	Prod	in	Ich habe das gute Zeug jetzt parat
22.05.2024 19:03:54	Kundin	out	Habe jetzt alles bekommen. Sag mir wann und wo.
22.05.2024 19:06:23	Kundin	in	Endlich. 23 Uhr. Unterführung
22.05.2024 19:06:33	Kundin	in	Wie viel hast du?
22.05.2024 19:06:42	Kundin	in	Ich brauche 7
22.05.2024 19:11:17	Kundin	out	Habe wesentlich mehr, als Du brauchst. Wegen der Verzögerung bekommst Du 8 zum Preis von 7. 23:00 CU

Tabelle 1: Timeline PC-Nutzer Mad Max

Timeline für PC-Nutzer Mad Max

Datum	Zeit	Vorfall
17.05.2024	09:31:32	Erste Browser-Nutzung
17.05.2024	09:33:00	Letzte Browser-Nutzung des Tages
18.05.2024	12:29:31	Browser-Nutzung
18.05.2024	12:29:40	Download signal-desktop-win-7.9.0.exe
18.05.2024	20:31:26	Chat-Begin
18.05.2024	20:32:44	Empfang: Labor-Bild
18.05.2024	20:38:42	Empfang: Herstellung.txt
18.05.2024	20:38:48	Empfang: Wuscha.doc
18.05.2024	20:47:05	letzte Chatnachricht des Tages
19.05.2024	15:35:41	Browser-Nutzung
19.05.2024	15:37:04	Letzte Browser-Nutzung des Tages
22.05.2024	07:44:45	Chat-Begin
22.05.2024	19:11:17	Letzte Chat-Nachricht
22.05.2024	23:00:00	Vereinbarter Zeitpunkt zur BTM-Übergabe
27.05.2024	09:28:14	signal-desktop auf Version 7.10.0 aktualisiert
27.05.2024	12:30:46	Browser-Nutzung
27.05.2024	12:31:10	Letzte Browser-Nutzung

Tabelle 2: Timeline PC-Nutzer Mad Max

4.2 Spur K1/2

Die Spur K1/2 wurde von der Sachbearbeitung mittels eines kriminaltechnischen Untersuchungsauftrages an die Kriminaltechnik der IT-Forensik übergeben. Die Sicherung von DNA Spuren ist bereits erfolgt. Eine Sicherung flüchtiger Datenbasis war nicht möglich da die Spuren sich im ausgeschalteten Zustand befunden haben. Eine RAM-Sicherung im vorliegenden Sachverhalt war nicht gegeben.

4.2.1 Vorbereitung Analyse USB-Datenspeicher

Zur Wahrung der Integrität der Daten wird die forensische Duplikation des Datenspeichers mithilfe eines Writeblockers durchgeführt. Ein Writeblocker sorgt dafür, dass keine Daten auf dem Speichermedium geschrieben werden und die Datenbasis so an Originalität gewahrt bleibt. Es ist lediglich ein Lesevorgang möglich. Als verwendete Hardware wurde die **Forensic USB Bridge** des Herstellers **TABLEAU** verwendet.

Abbildung 63: Datensicherung mit Schreibschutz

Unter einer forensischen Duplikation wird ein 1 zu 1 bit-genauer Kopiervorgang aller Sektoren verstanden. Dies beinhaltet neben gelöschter Datenbasis auch versteckte Datenbasis.

Die Datensicherung wurde mithilfe des Softwarewerkzeugtools 'X-Ways' (Abbildung 65) durchgeführt. Hierfür wurde der Datenträger unter Verwendung eines Schreibschutzadapters (Abbildung 64) in die Software eingebunden (Abbildung 67) und im Evidence-File Format (Abbildung 70) gesichert. Bei diesem Format handelt es sich um ein EWF[5]-Format, welches die Metadaten, Kompression, Verschlüsselung, Hashing und relevante Informationen zum Image beinhaltet. Das hierzu verwendete Format erfolgt unter der Dateinummerierung im Schema .E01. Bei größeren Dateien können diese sich in Einzeldateien (Segmente) bis zu 2048 MiB[6] aufteilen. Die

[5]Expert Witness-Format
[6]Mebibyte

Sicherung des USB-Datenspeichers beträgt final ein Segment (Abbildung 72). Weiter erfolgt die Unterteilung in Header mit Metadaten und Sektionen mit Teilen des Abbildes. Die Sektion (hash section) wird hierbei in MD5 Hash-Werte der Datenblöcke als Teilmenge der Daten gesamt erfasst. Die Aufteilung der Daten in Sektionen soll im Weiteren die Verarbeitung erleichtern und somit den Zugriff auf Teile des Images ermöglichen, ohne das gesamte Image laden zu müssen.

Abbildung 64: Schreibschutz

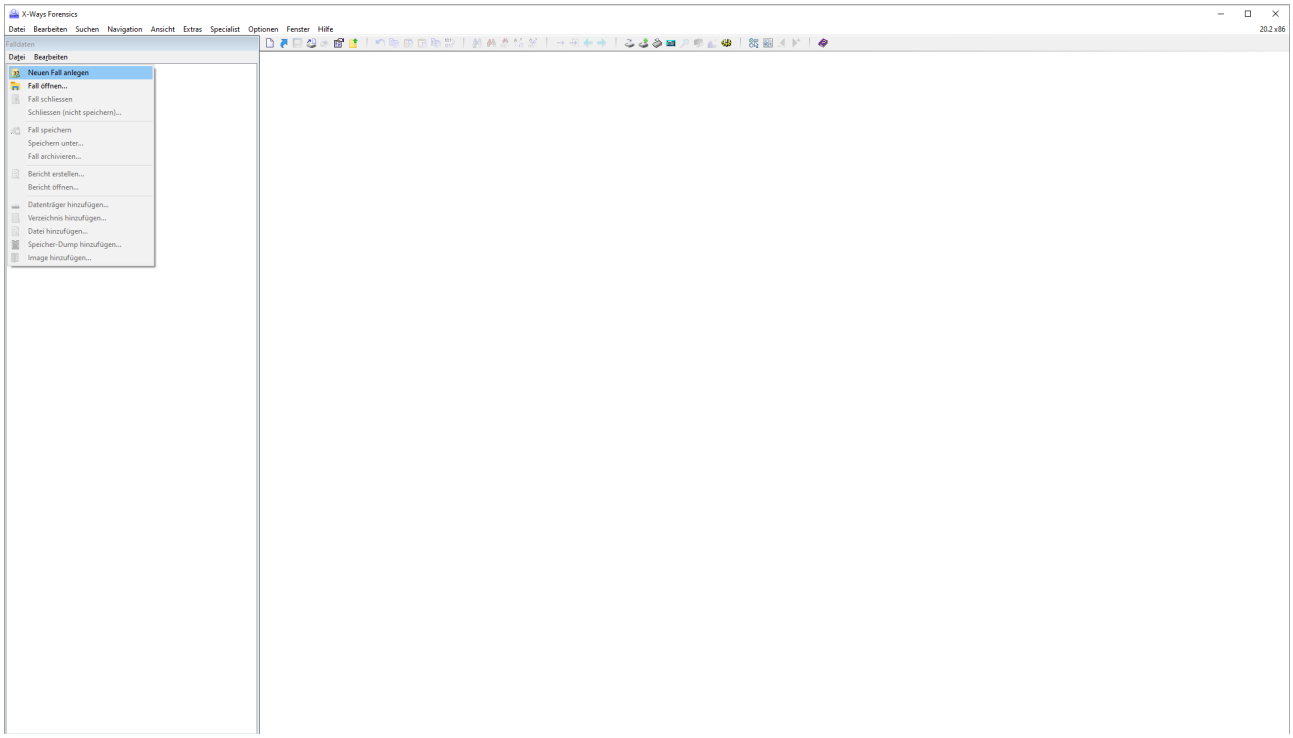


Abbildung 65: X-Ways neuen Fall anlegen

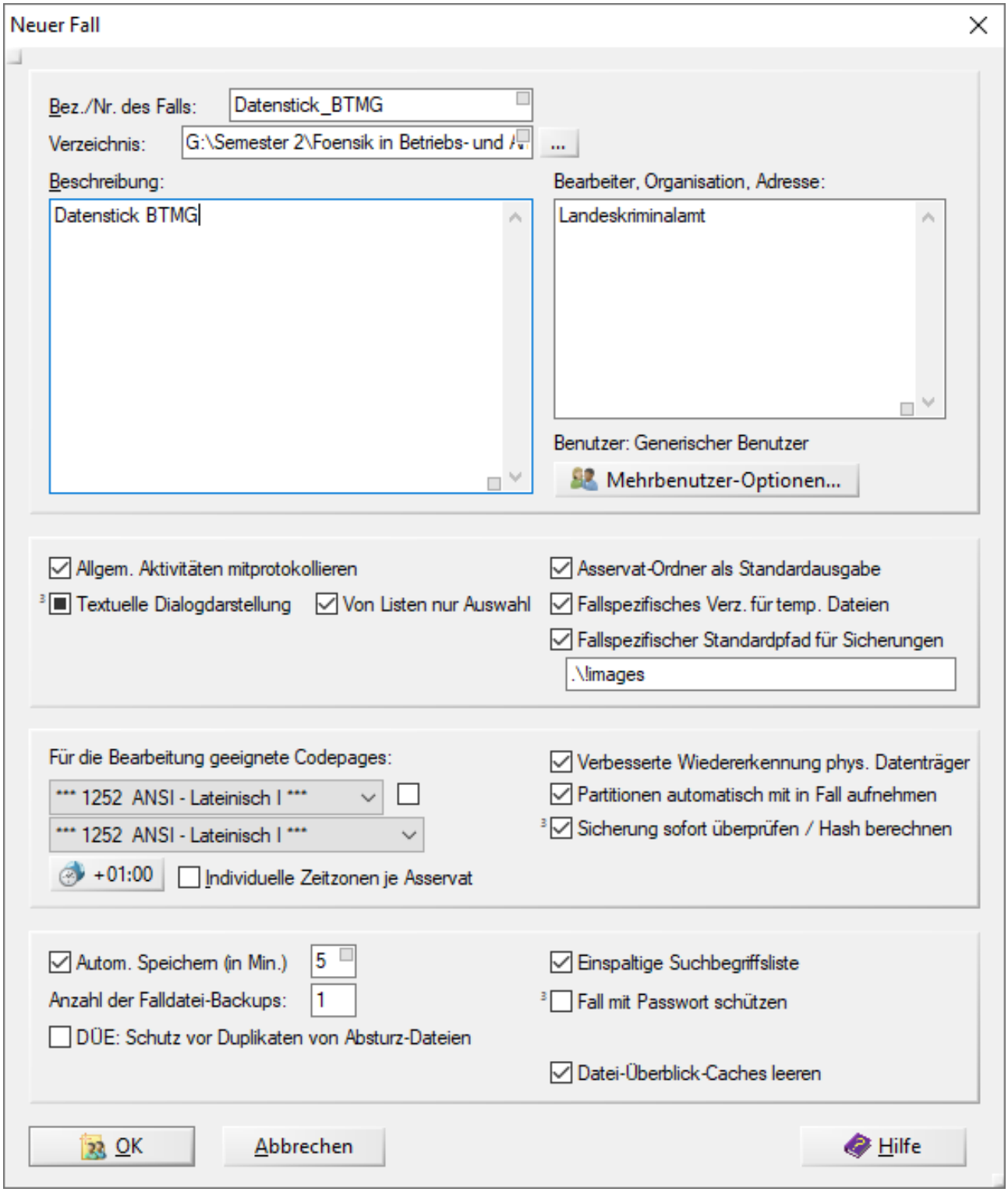


Abbildung 66: Anlegen eines neuen Falles

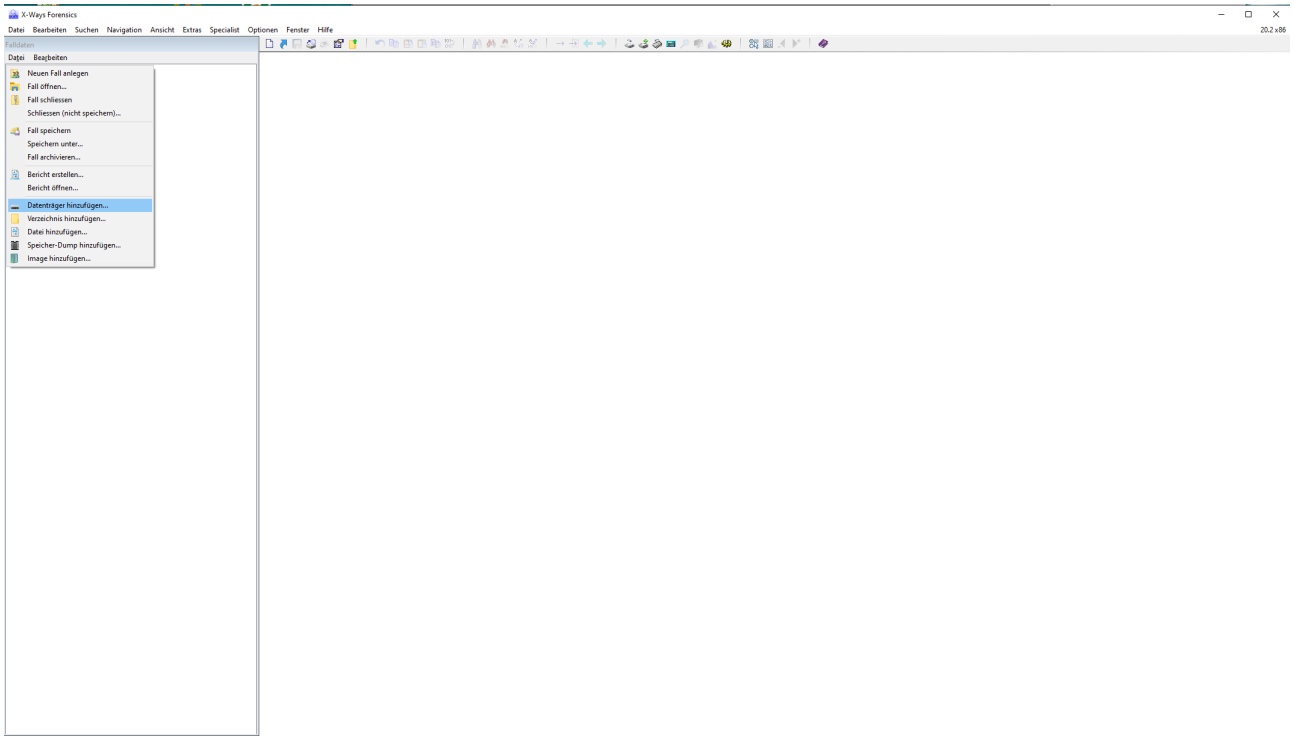


Abbildung 67: Datenträger hinzufügen

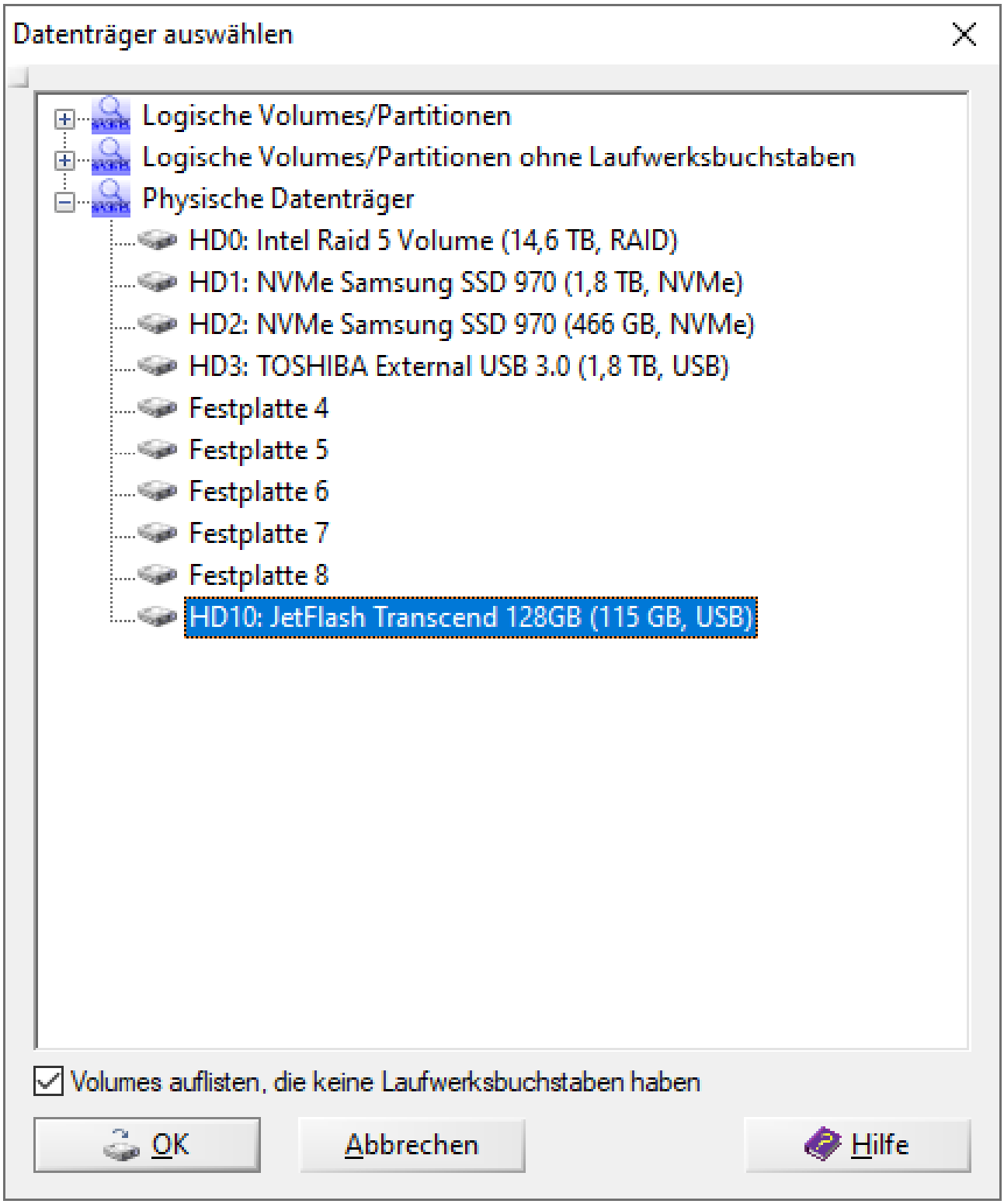


Abbildung 68: Wahl des physischen Datenträgers

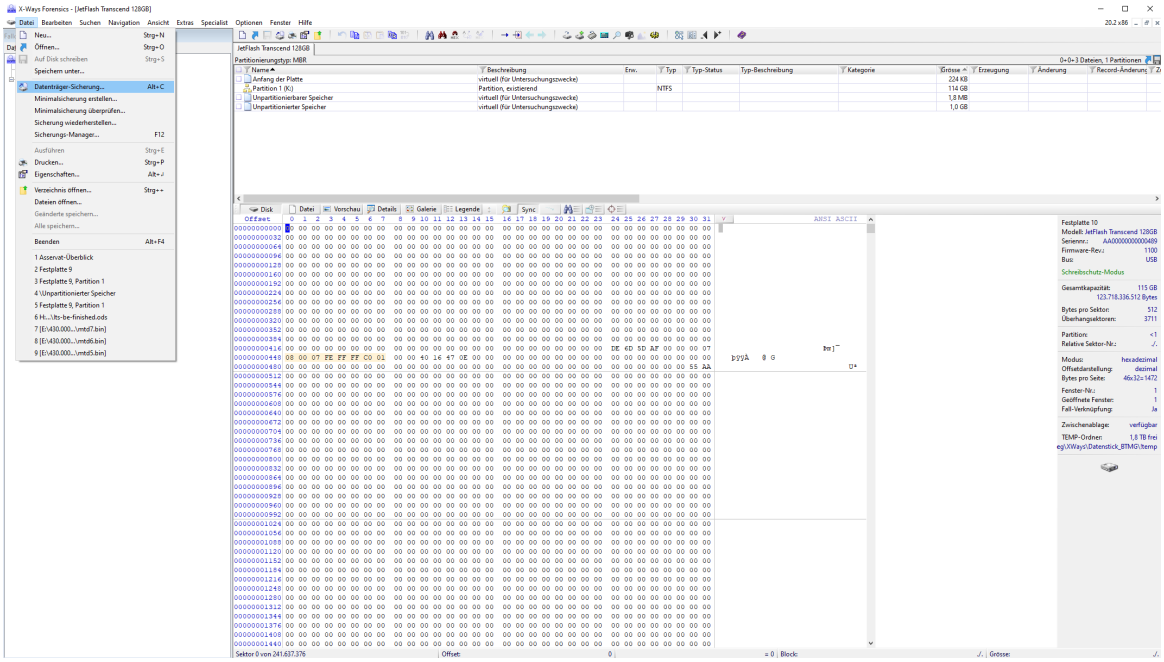


Abbildung 69: Datenträgersicherung

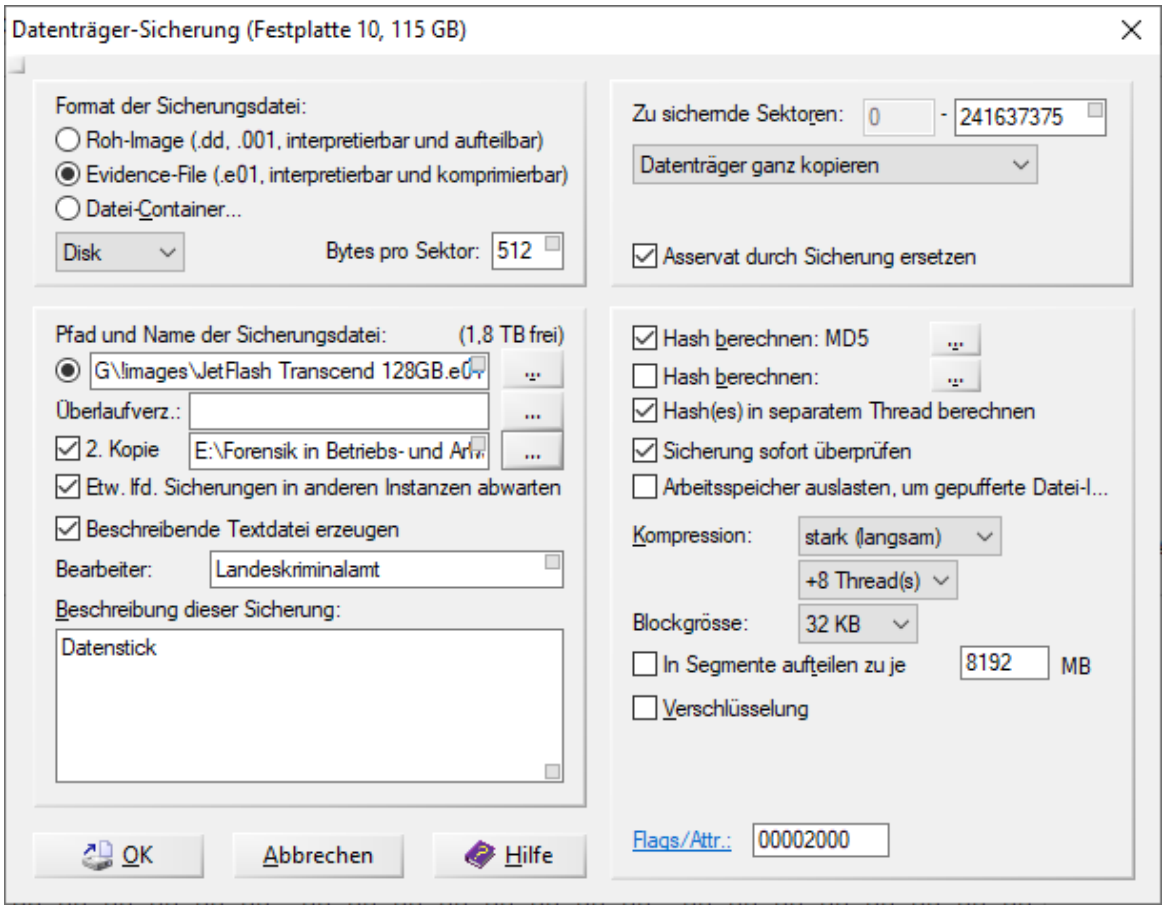


Abbildung 70: Datenträgersicherung Einstellungen

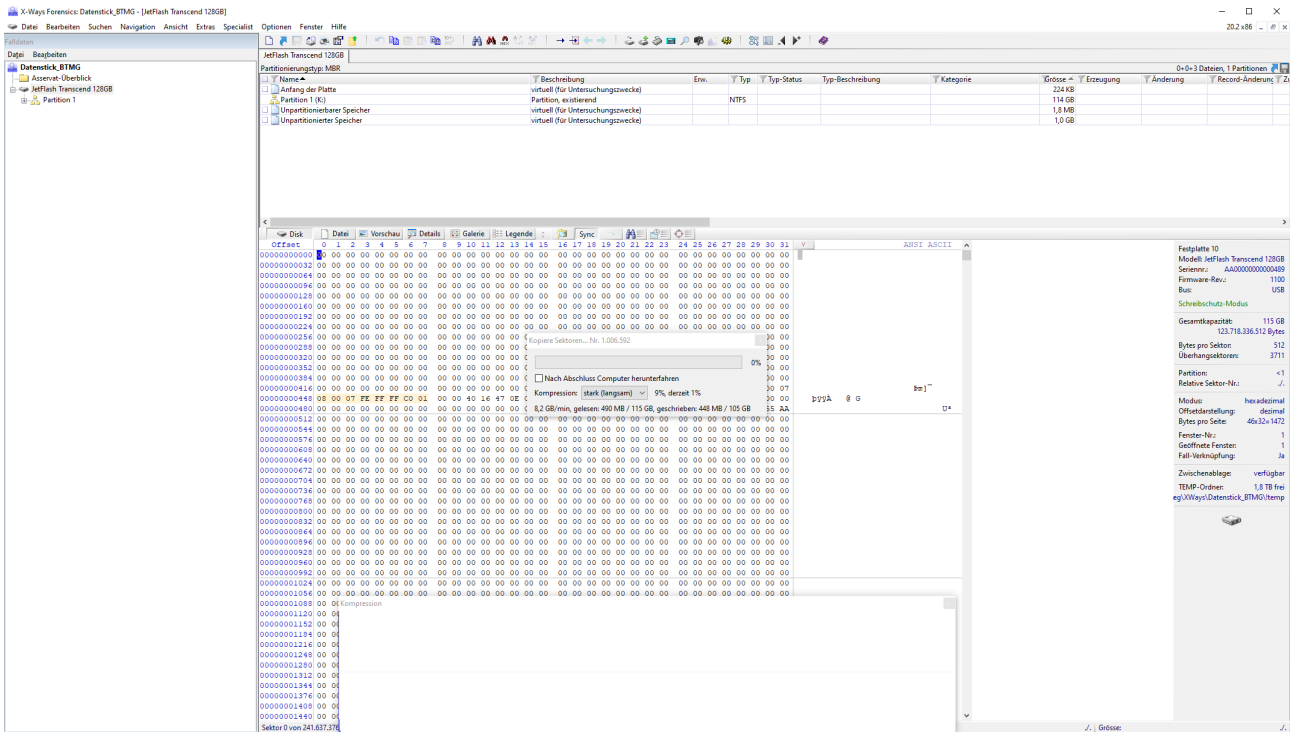


Abbildung 71: Datenträgersicherung Fortschritt

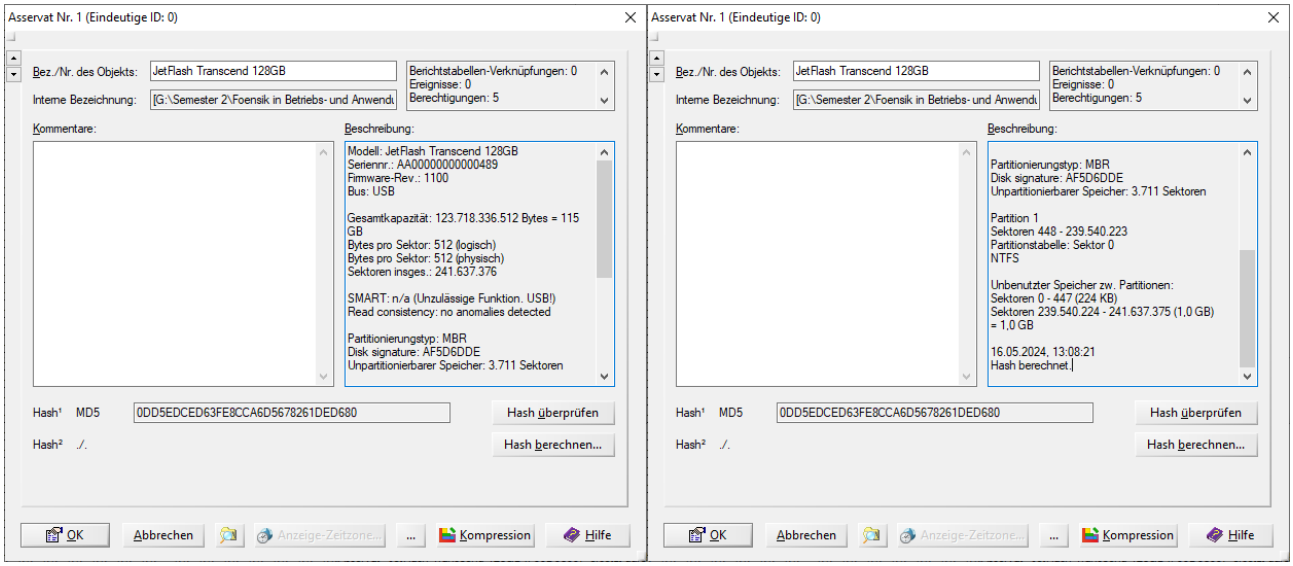


Abbildung 72: Datenträgersicherung Eigenschaften

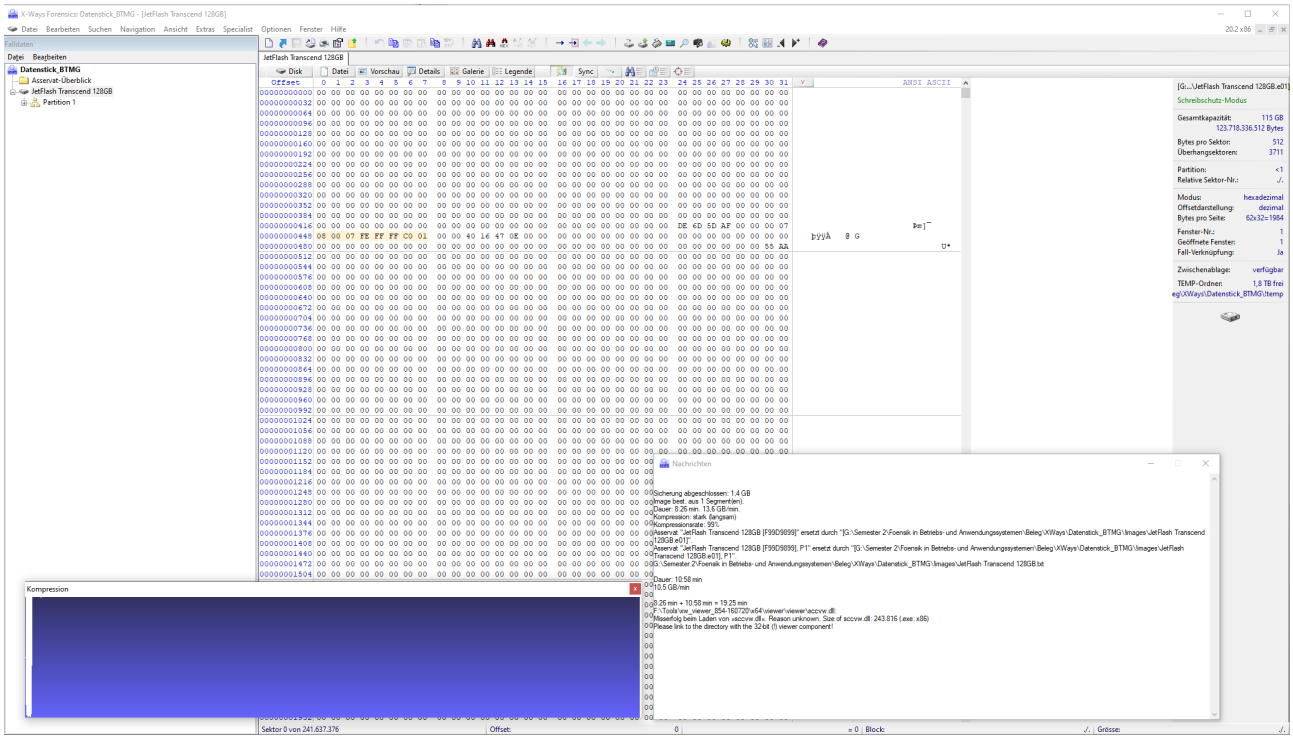


Abbildung 73: Datenträgersicherung erfolgreich

4.2.2 Forensische Analyse USB-Datenspeicher

Nach der erfolgreichen Sicherung der Datenbasis erfolgt die weitere Bearbeitung mit einer Master Kopie der forensischen Duplikation. Hierzu wird weiterhin die Softwarelösung 'X-Ways' gewählt. Nach Einbinden der Datenträgersicherung erfolgt über die gesamte Datenbasis eine rekursive Ansicht (Abbildung 74, 75).

Anschließend wird mittels 'Dateiüberblick erweitern' eine genaue Überprüfung der Datenbasis durchgeführt (Abbildung 76, 77, 78, 79, 80).

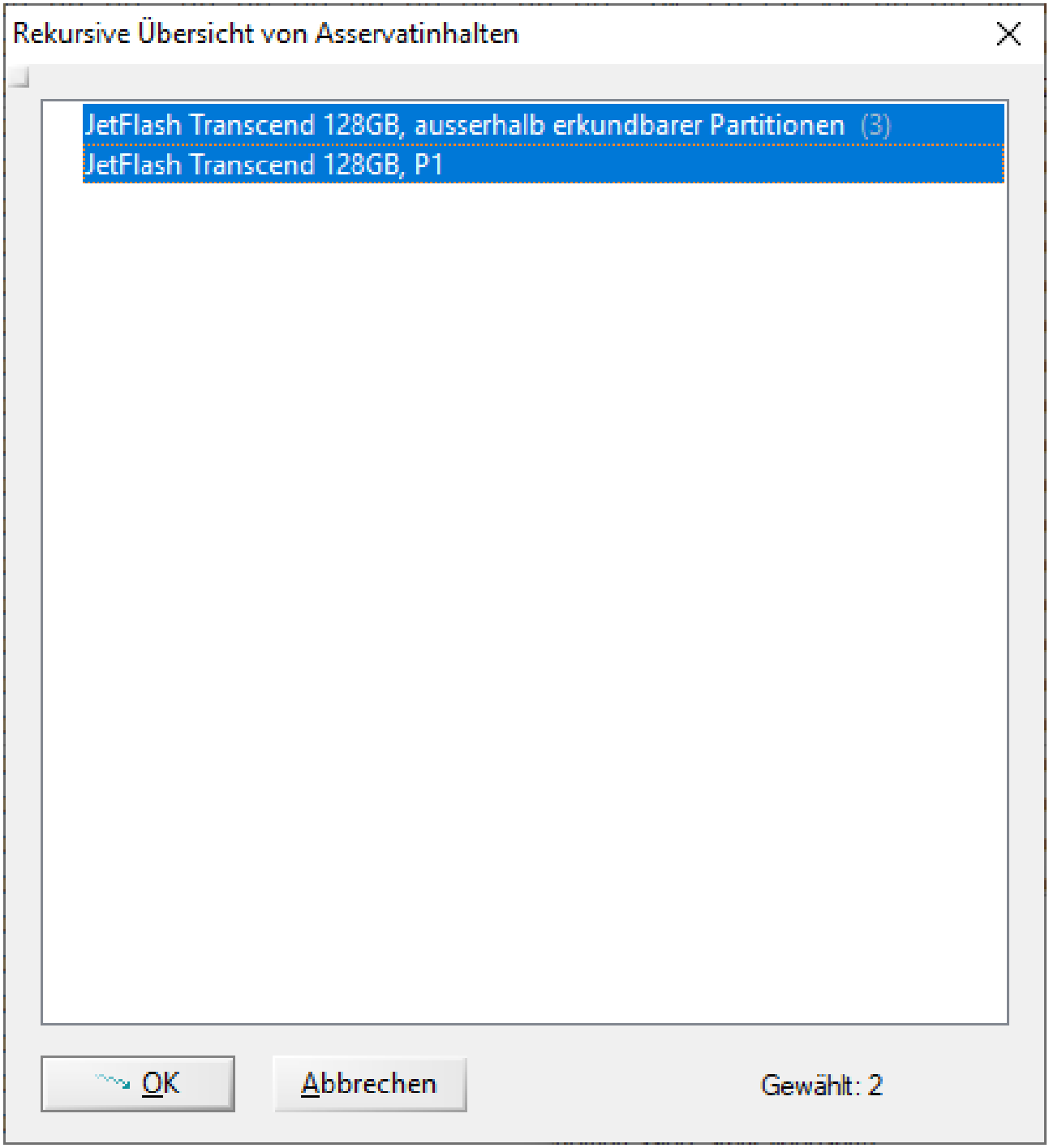


Abbildung 74: Datenträgersicherung Rekursive Ansicht - 1

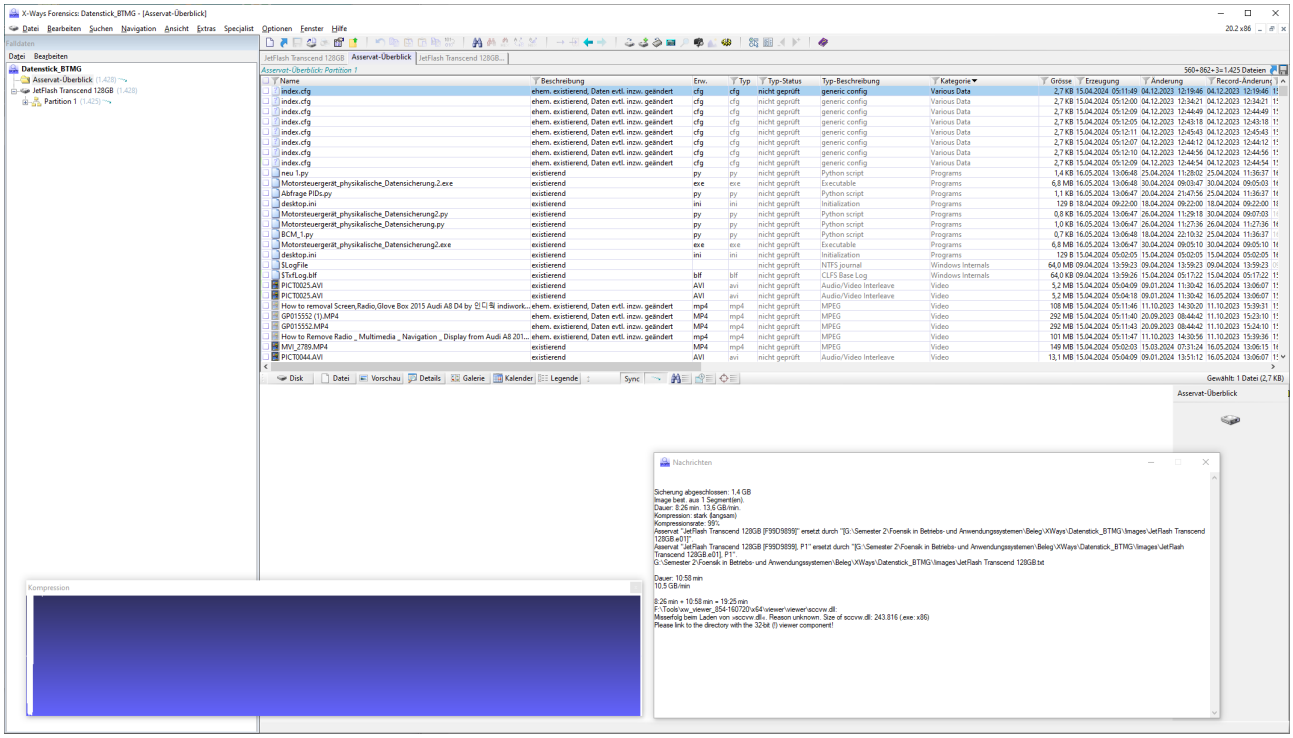


Abbildung 75: Datenträgersicherung Rekursive Ansicht - 2

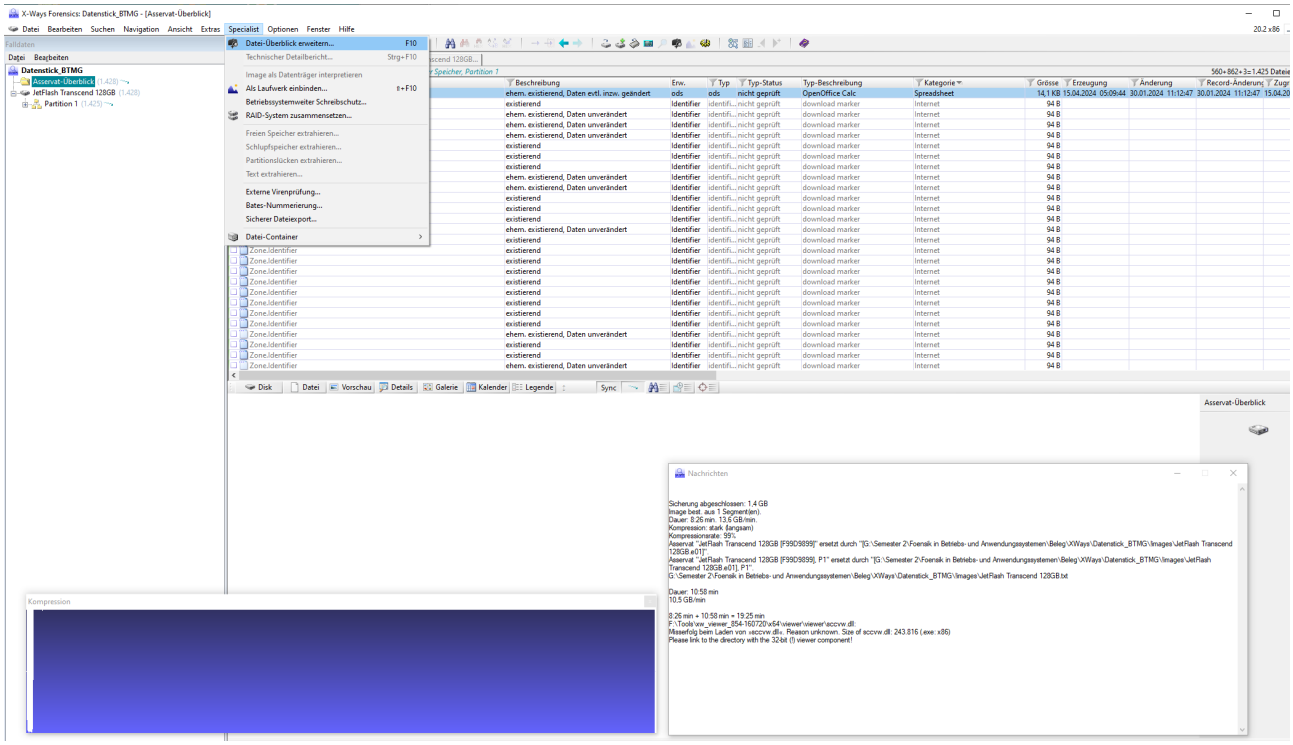


Abbildung 76: Dateiüberblick erweitern - 1

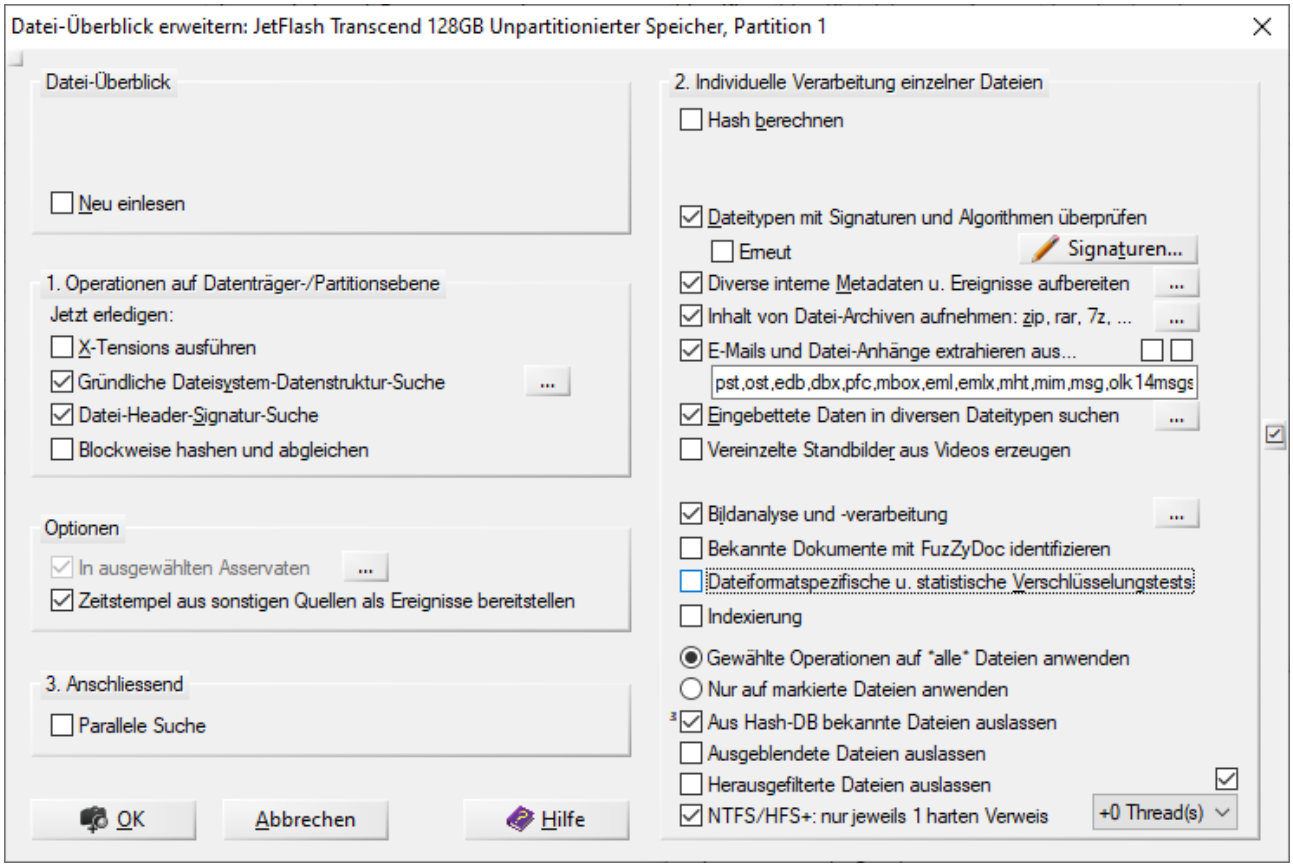


Abbildung 77: Dateiüberblick erweitern - 2

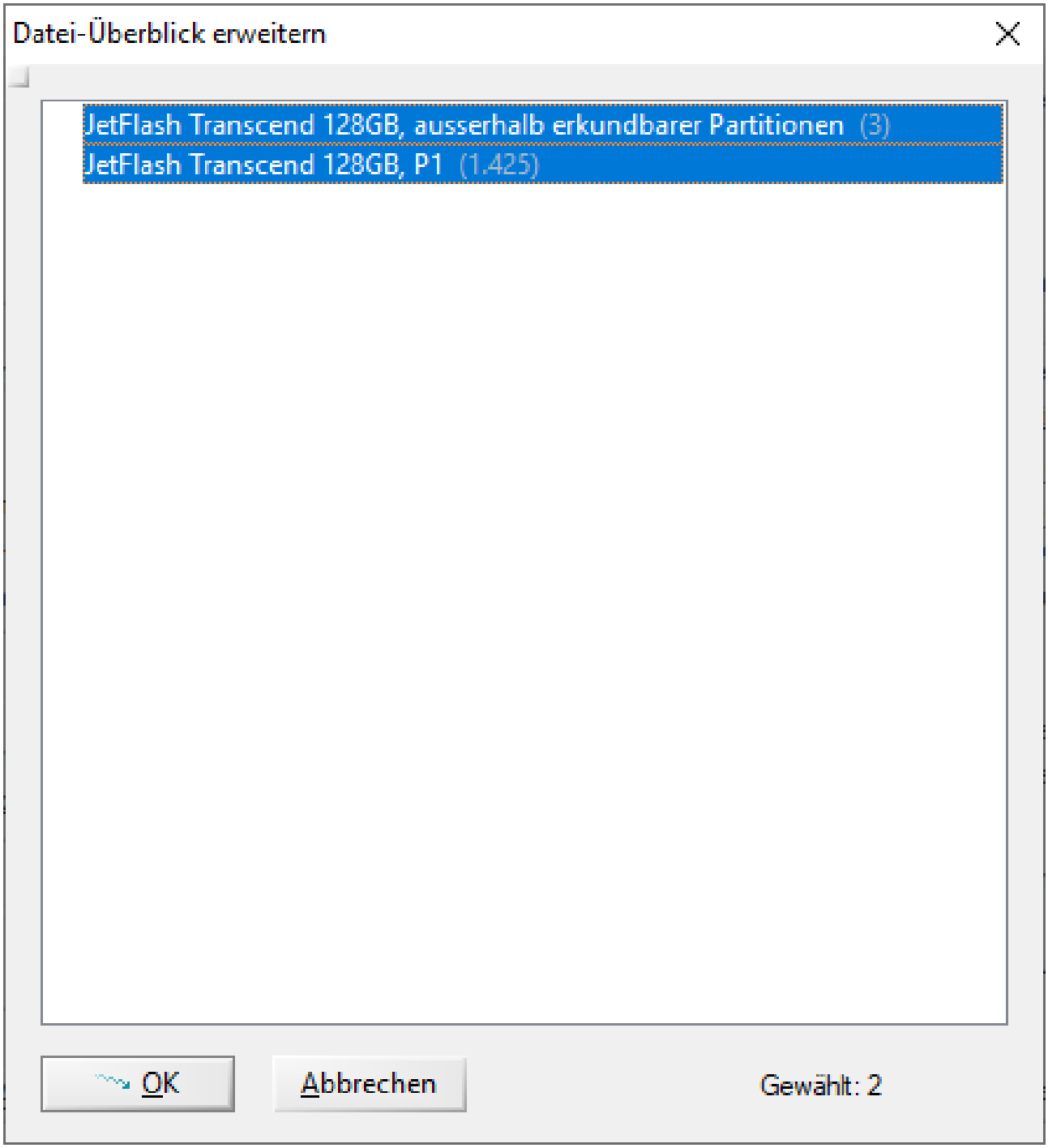


Abbildung 78: Dateiüberblick erweitern - 3

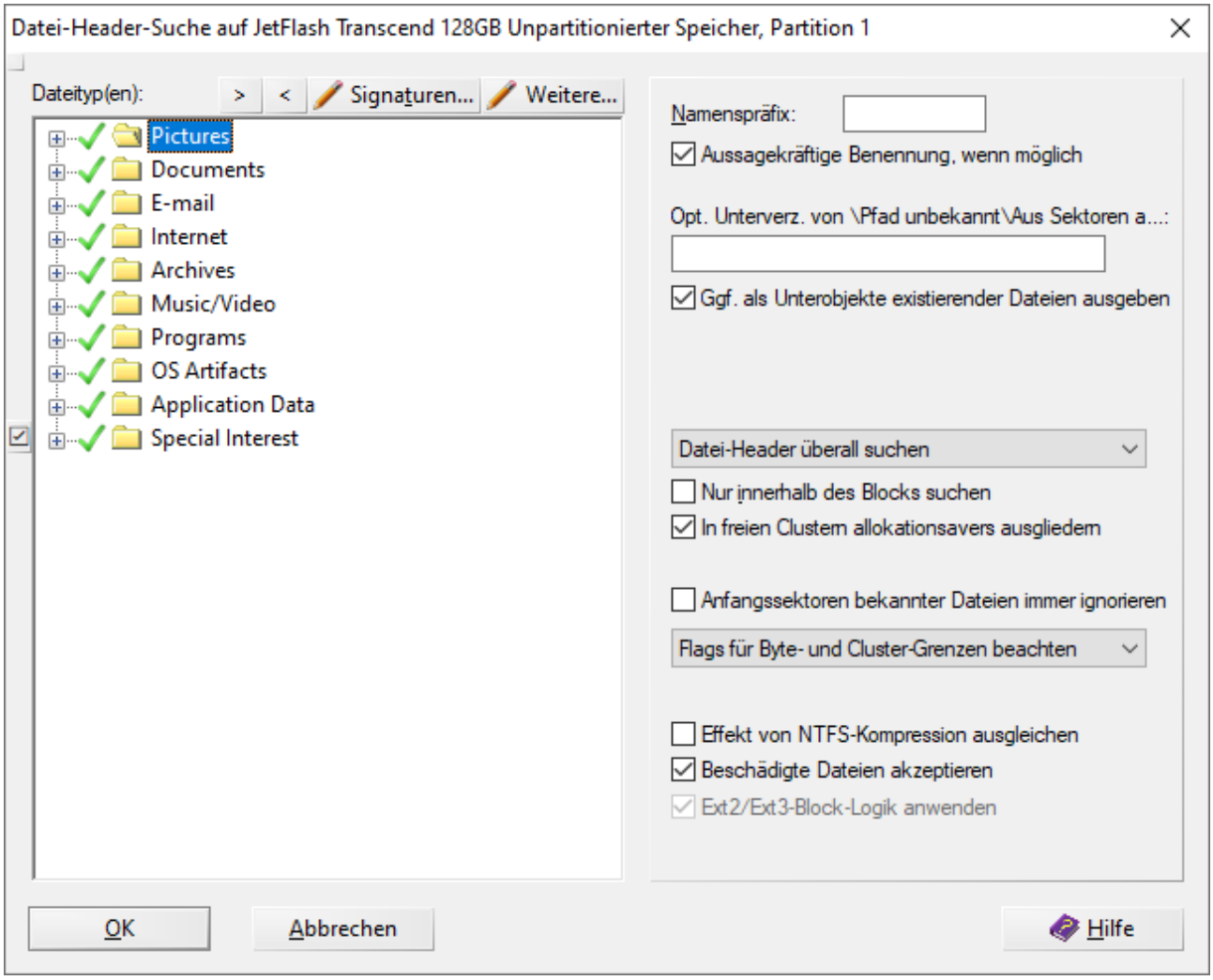


Abbildung 79: Dateiüberblick erweitern - 4

Nach erfolgter Erweiterung des Dateiüberblickes und der Datei-Header-Signatur-Suche können die einzelnen Bereiche wie der gesamte Überblick der Datenbasis (Abbildung 81), der ausgegliederten Sektoren (Abbildung 82), des Anfanges der Platte (Abbildung 83), der Partition 1 (Abbildung 84), des unpartitionierbaren Speichers (Abbildung 85) und des unpartitionierten Speichers (Abbildung 86) eingesehen werden.

Der im unpartitionierten Bereich befindliche Datenbereich (Abbildung 86) ist mit der Dateisignatur **50 4B 03 04** gekennzeichnet. Diese Signatur beschreibt ein ZIP-Dateiformat und daraufbasierende Dateiformate wie OBF[7]. Bei dem Format OBF handelt es sich um ein offenes Dateiformat, welches verschiedene Formate wie Tabellenkalkulation **.ods**, Textverarbeitung **.odt** und Präsentationen **.odp** unterstützt. Der Bytesequenz kann die Buchstabenfolge **open.document.spreadsheet** entnommen werden.

[7]Open Document Format for Office Applications

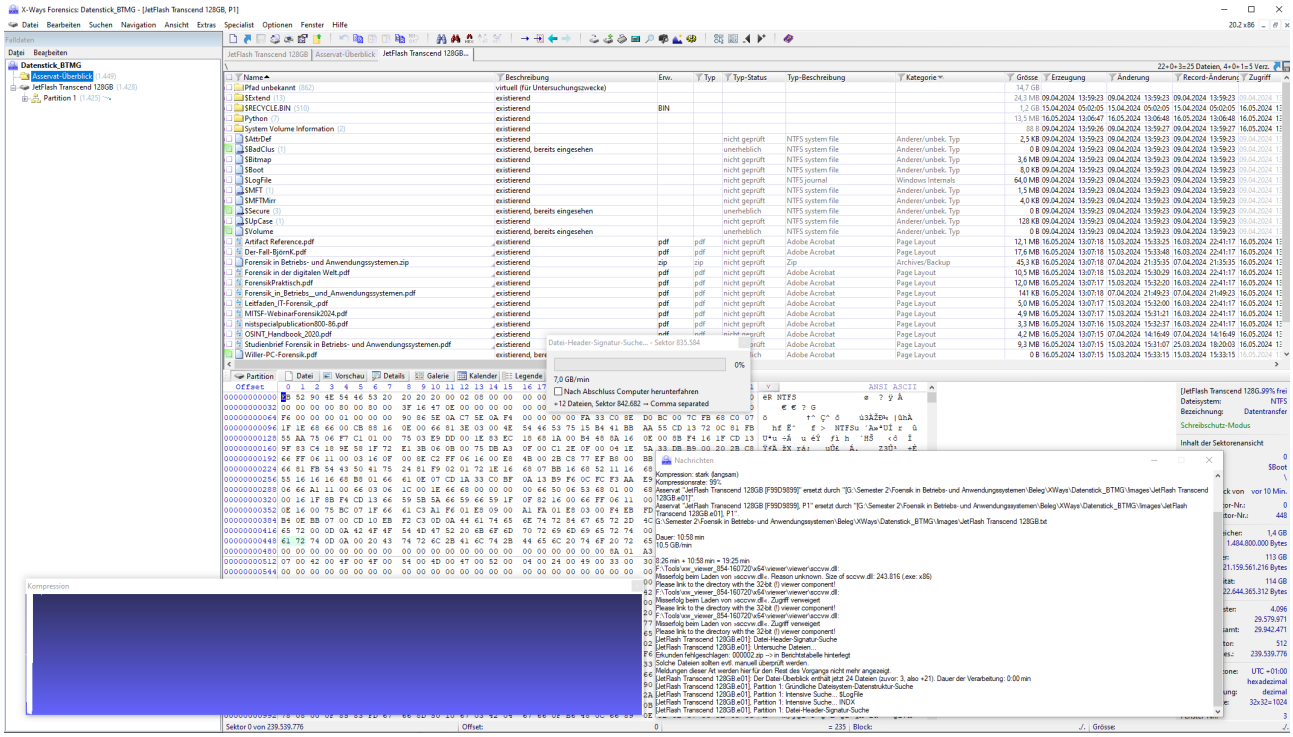


Abbildung 80: Dateiüberblick erweitern - 5

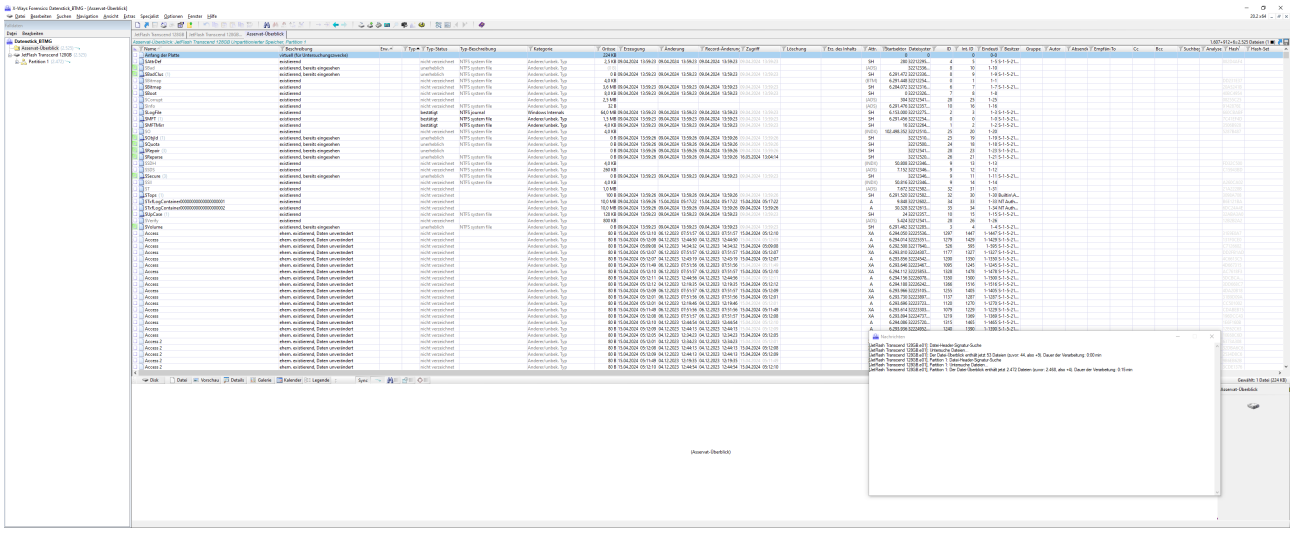


Abbildung 81: Asservat Überblick

Die aufgefundene Datenbasis im unpartitionierten Speicher kann als Verkaufsliste erkannt werden (Abbildung 87, 88).

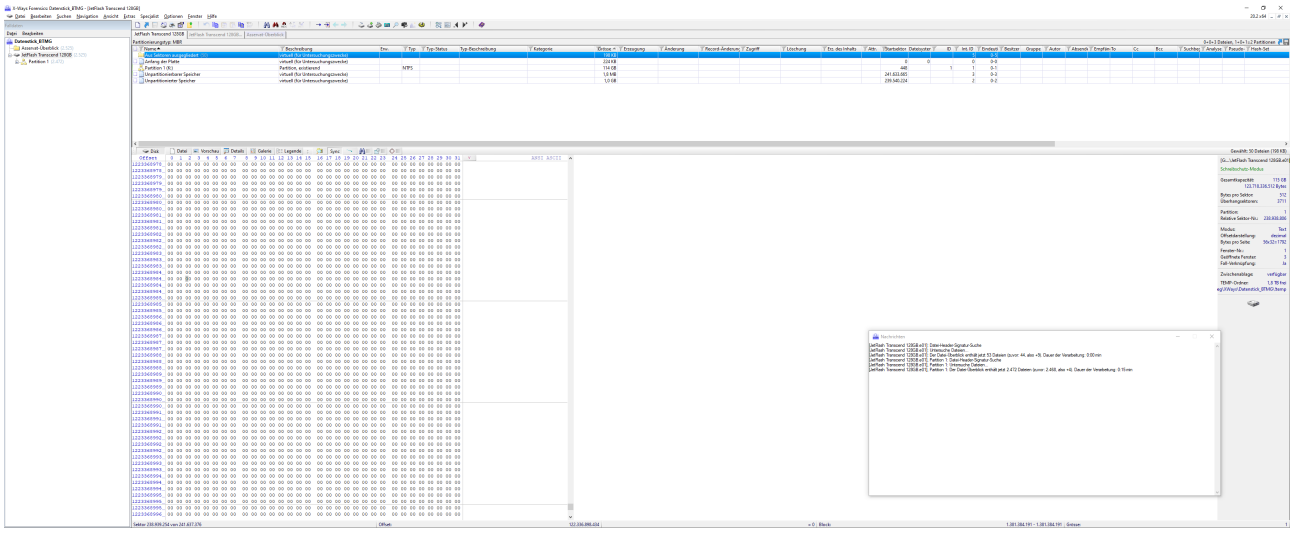


Abbildung 82: Aus Sektoren ausgegliedert

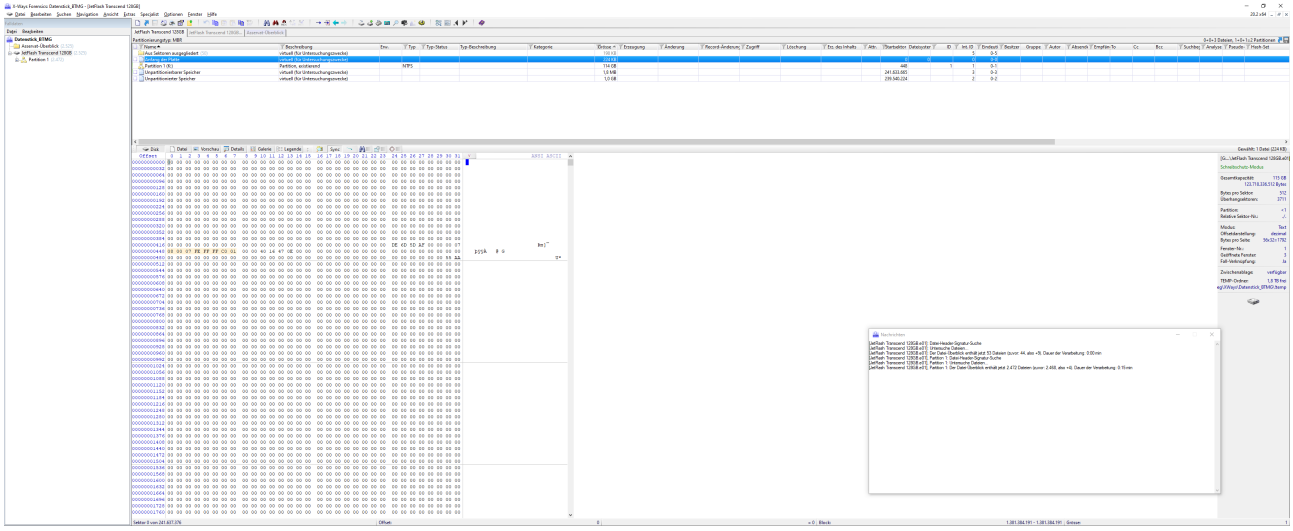


Abbildung 83: Anfang der Platte

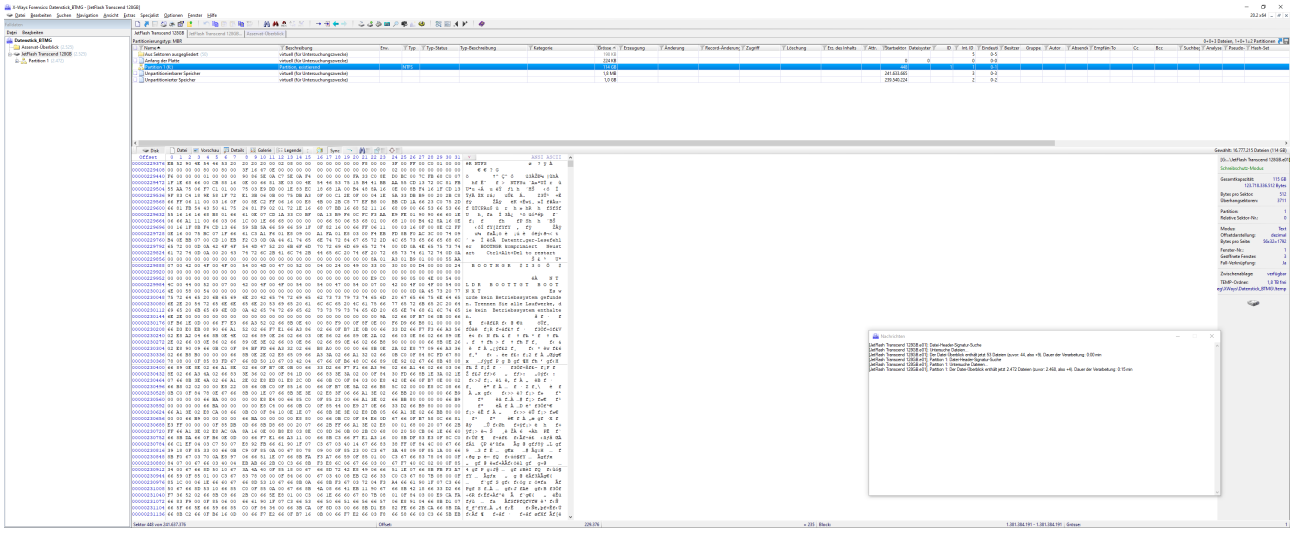


Abbildung 84: Partition 1

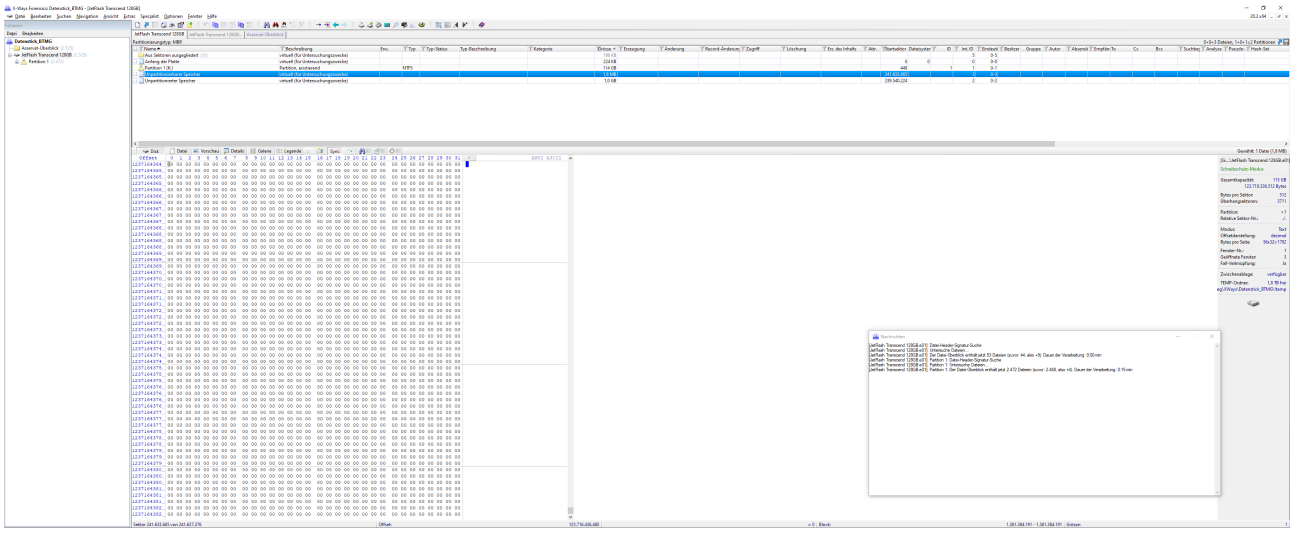


Abbildung 85: Unpartitionierbarer Speicher

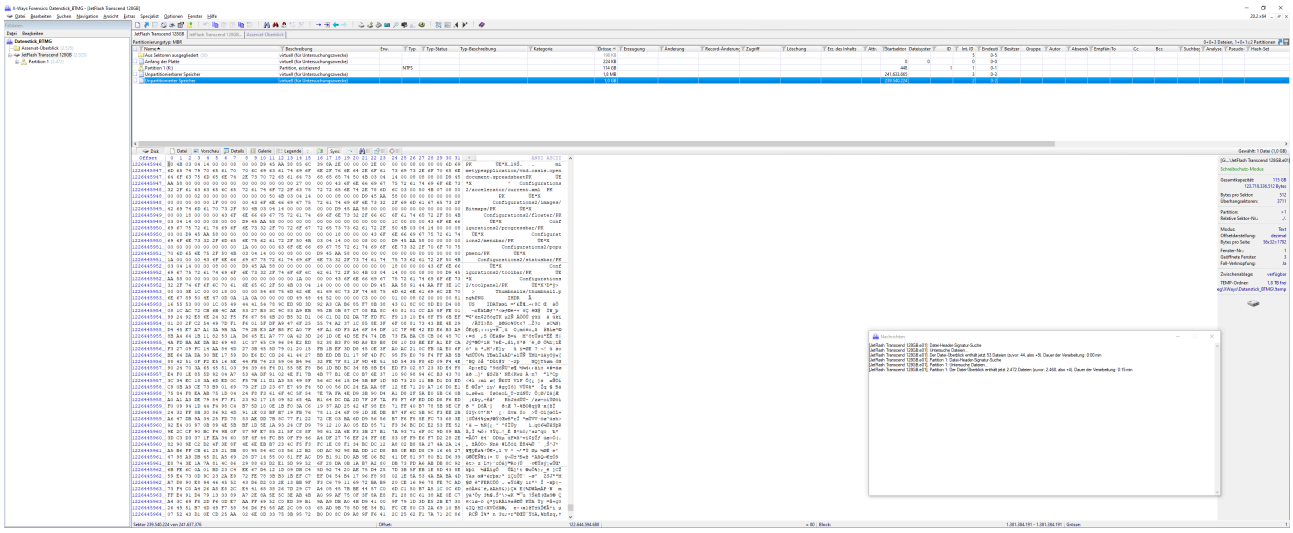


Abbildung 86: Unpartitionierter Speicher - Hexcode versteckte Datendatei

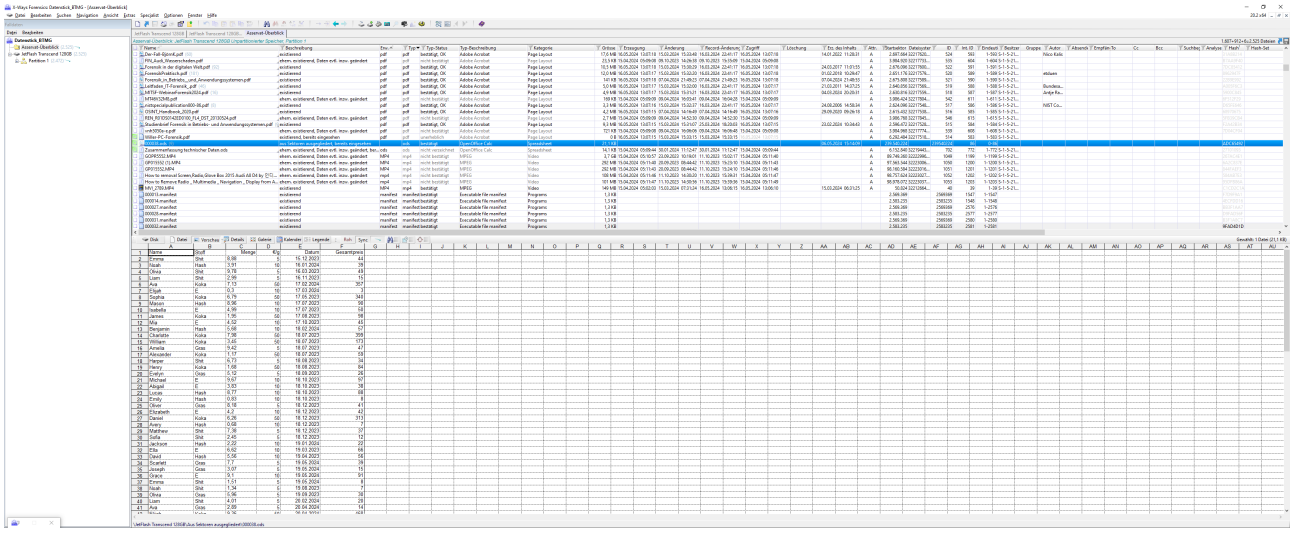


Abbildung 87: Asservat - Überblick sortiert nach Name, Erweiterung ,Typ Verkaufsliste

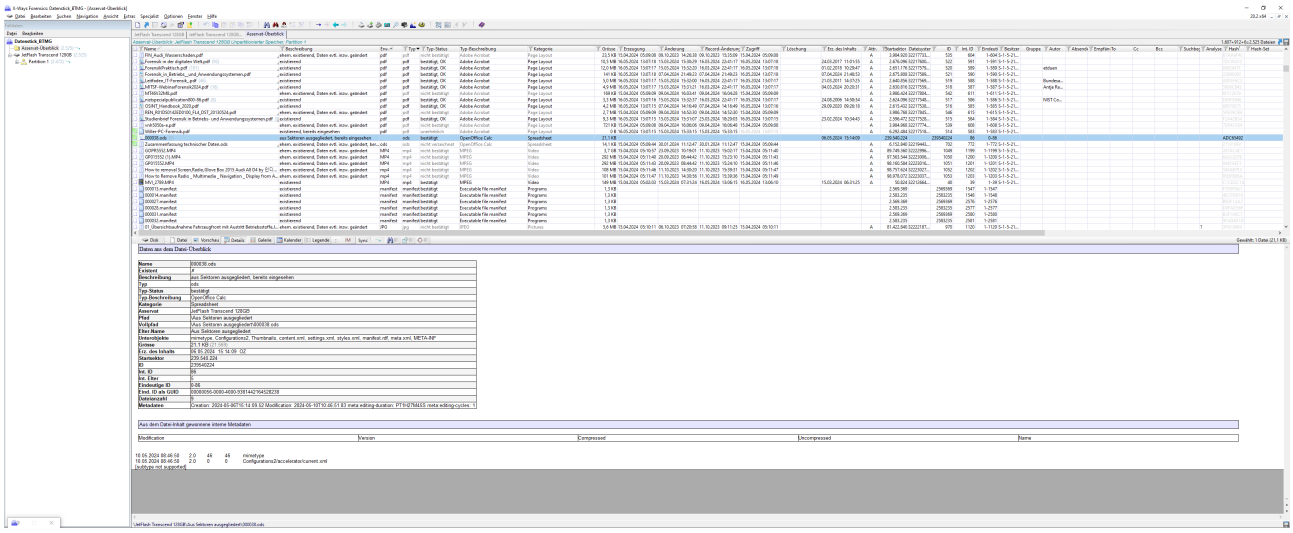


Abbildung 88: Asservat - Überblick sortiert nach Name, Erweiterung, Typ Verkaufsliste - Details

carved000037.ods - OpenOffice Calc

Datei Bearbeiten Ansicht Einfügen Format Extras Daten Fenster Hilfe

Arial 10

F19 =D19*C19

	A	B	C	D	E	F
1	Name	Stoff	Menge	€/g	Datum	Gesamtpreis
2	Emma	Shit	8,88	5	15.12.2023	44
3	Noah	Hash	3,91	10	16.01.2024	39
4	Olivia	Shit	9,78	5	16.03.2023	49
5	Liam	Shit	2,99	5	16.11.2023	15
6	Ava	Koka	7,13	50	17.02.2024	357
7	Elijah	E	0	10	17.03.2024	3
8	Sophia	Koka	6,79	50	17.05.2023	340
9	Mason	Hash	8,96	10	17.07.2023	90
10	Isabella	E	5	10	17.07.2023	50
11	James	Koka	1,95	50	17.08.2023	98
12	Mia	E	5	10	17.10.2023	45
13	Benjamin	Hash	5,68	10	18.02.2024	57
14	Charlotte	Koka	7,98	50	18.07.2023	399
15	William	Koka	3,45	50	18.07.2023	173
16	Amelia	Gras	9,42	5	18.07.2023	47
17	Alexander	Koka	1,17	50	18.07.2023	59
18	Harper	Shit	6,73	5	18.08.2023	34
19	Henry	Koka	1,68	50	18.08.2023	84
20	Evelyn	Gras	5,12	5	18.09.2023	26
21	Michael	E	10	10	18.10.2023	97
22	Abigail	E	4	10	18.10.2023	38
23	Lucas	Hash	8,77	10	18.10.2023	88
24	Emily	Hash	0,83	10	18.10.2023	8
25	Oliver	Gras	8,18	5	18.12.2023	41
26	Elizabeth	E	4	10	18.12.2023	42
27	Daniel	Koka	6,26	50	18.12.2023	313
28	Avery	Hash	0,68	10	18.12.2023	7
29	Matthew	Shit	7,38	5	18.12.2023	37
30	Sofia	Shit	2,45	5	18.12.2023	12
31	Jackson	Hash	2,22	10	19.01.2024	22
32	Ella	E	7	10	19.03.2023	66
33	David	Hash	5,56	10	19.04.2023	56
34	Scarlett	Gras	7,7	5	19.05.2024	39
35	Joseph	Gras	3,07	5	19.05.2024	15
36	Grace	E	9	10	19.05.2024	91

Tabelle1 Tabelle2 Tabelle3

Tabelle 1 / 3 Standard

Abbildung 89: Verkaufliste

4.3 Spur K1/3

Die Spur K1/3 wurde von der Sachbearbeitung mittels eines kriminaltechnischen Untersuchungsauftrages an die Kriminaltechnik der IT-Forensik übergeben. Die Sicherung von DNA-Spuren ist bereits erfolgt. Eine Sicherung flüchtiger Datenbasis war nicht möglich, da die Spuren sich im ausgeschalteten Zustand befunden haben. Eine RAM-Sicherung im vorliegenden Sachverhalt war nicht gegeben.

4.3.1 Vorbereitung Analyse SD-Card-Kartenmodul

Die SD-Karte wurde am Tatort ohne weiteres Zubehör oder die dazugehörige Kamera vorgefunden.

Abbildung 90: Vorderseite der vorgefundenen SD-Karte

Abbildung 91: Rückseite der vorgefundenen SD-Karte

Wie bereits in den vorherigen Kapiteln bezüglich der Spuren K1/1 und K1/2 beschrieben, ist an dieser Stelle ein forensisches, sektorweise angefertigtes Duplikat der SD-Karte zu erstellen. Für den weiteren Verlauf wird angenommen, dass die forensische Analyse auf ebendiesem Duplikat durchgeführt wurde, um die Integrität der originalen Spur K1/3 und somit die Chain of Custody sicherzustellen. Tatsächlich war bei dieser Arbeit mangels Writeblocker keine Erstellung eines echten forensischen Duplikats möglich.

Für die Erstellung eines E01-Images der SD-Karte wird ebenfalls Axiom genutzt. Die folgenden Abbildungen zeigen, wie die Image-Erzeugung mit Axiom vorgenommen wurde.

4.3.2 Forensische Analyse SD-Card-Kartenmodul

Nach der Erstellung des E01-Images wird von Axiom Process zu Axiom Analyzer gewechselt, um mit der Auswertung dieses Images zu beginnen.

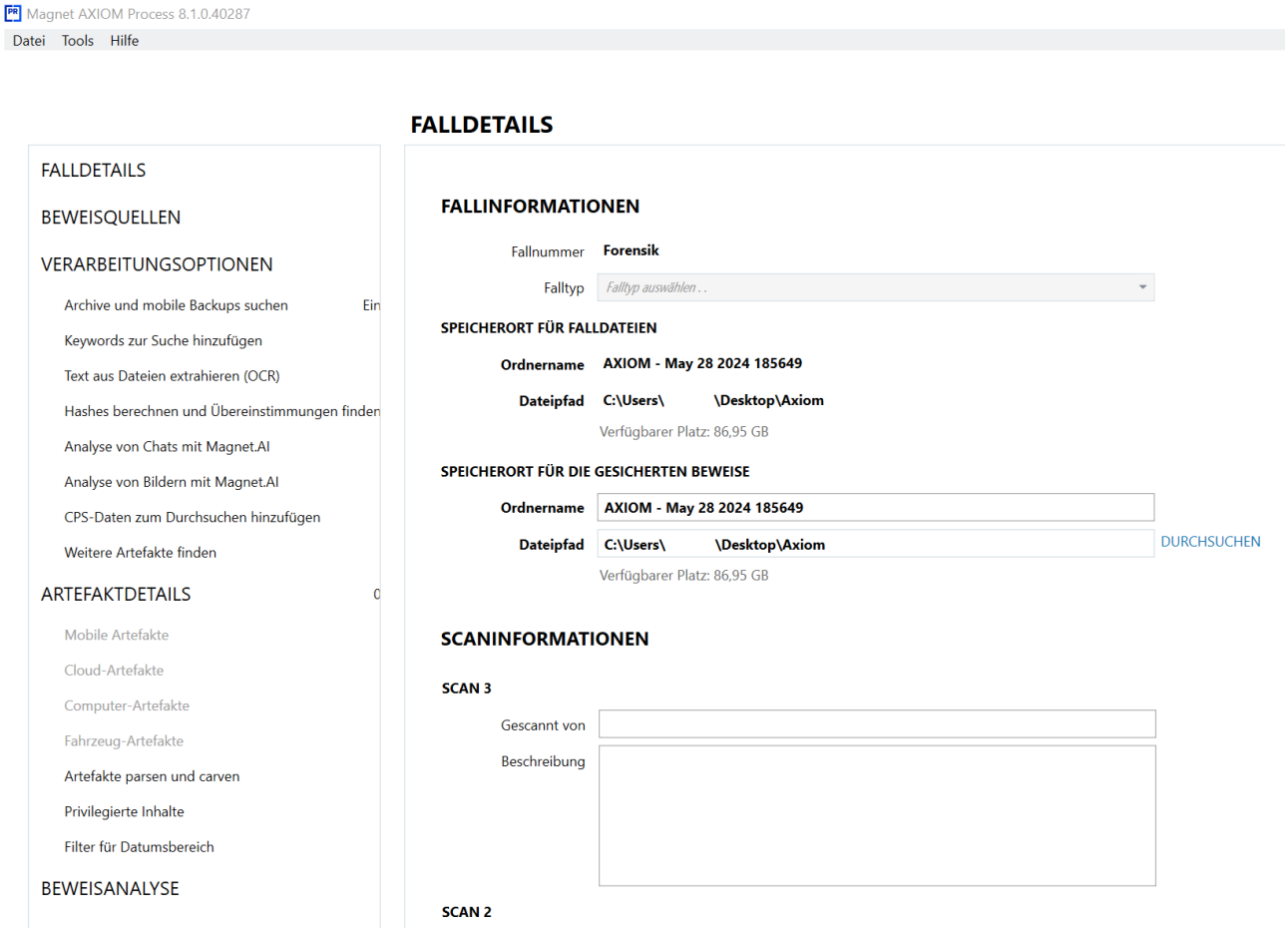


Abbildung 92: Übersicht des in Axiom angelegten Falls

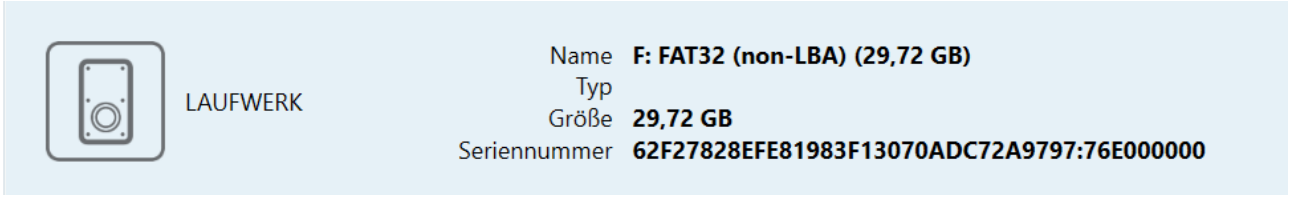


Abbildung 93: Auswählen der SD-Karte als Laufwerk/Beweisquelle

Abbildung 94: Übersicht der hinzugefügten Beweisquellen

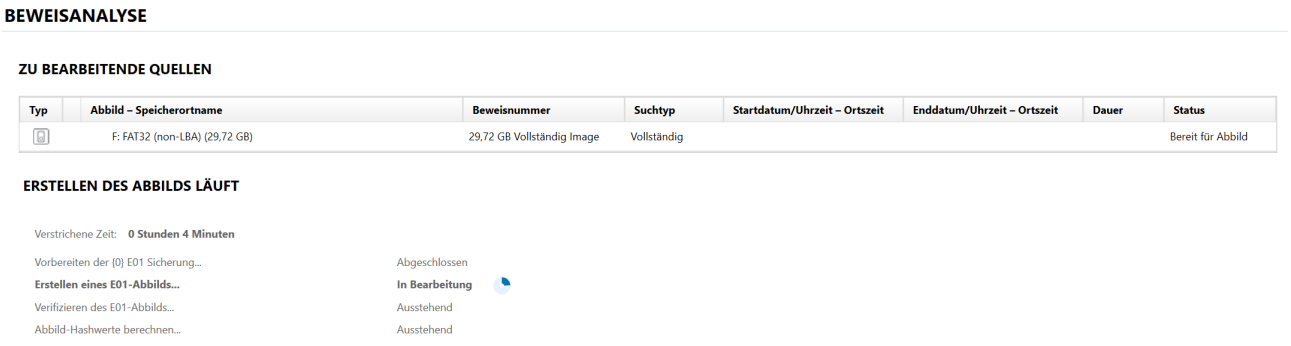


Abbildung 95: Erstellen des E01-Images

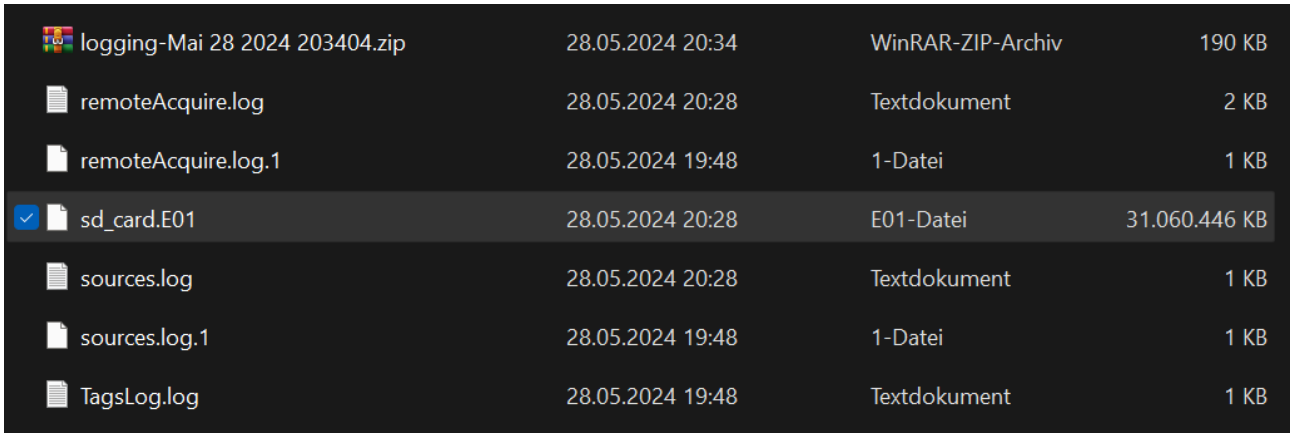


Abbildung 96: Erstelltes E01-Image der SD-Karte

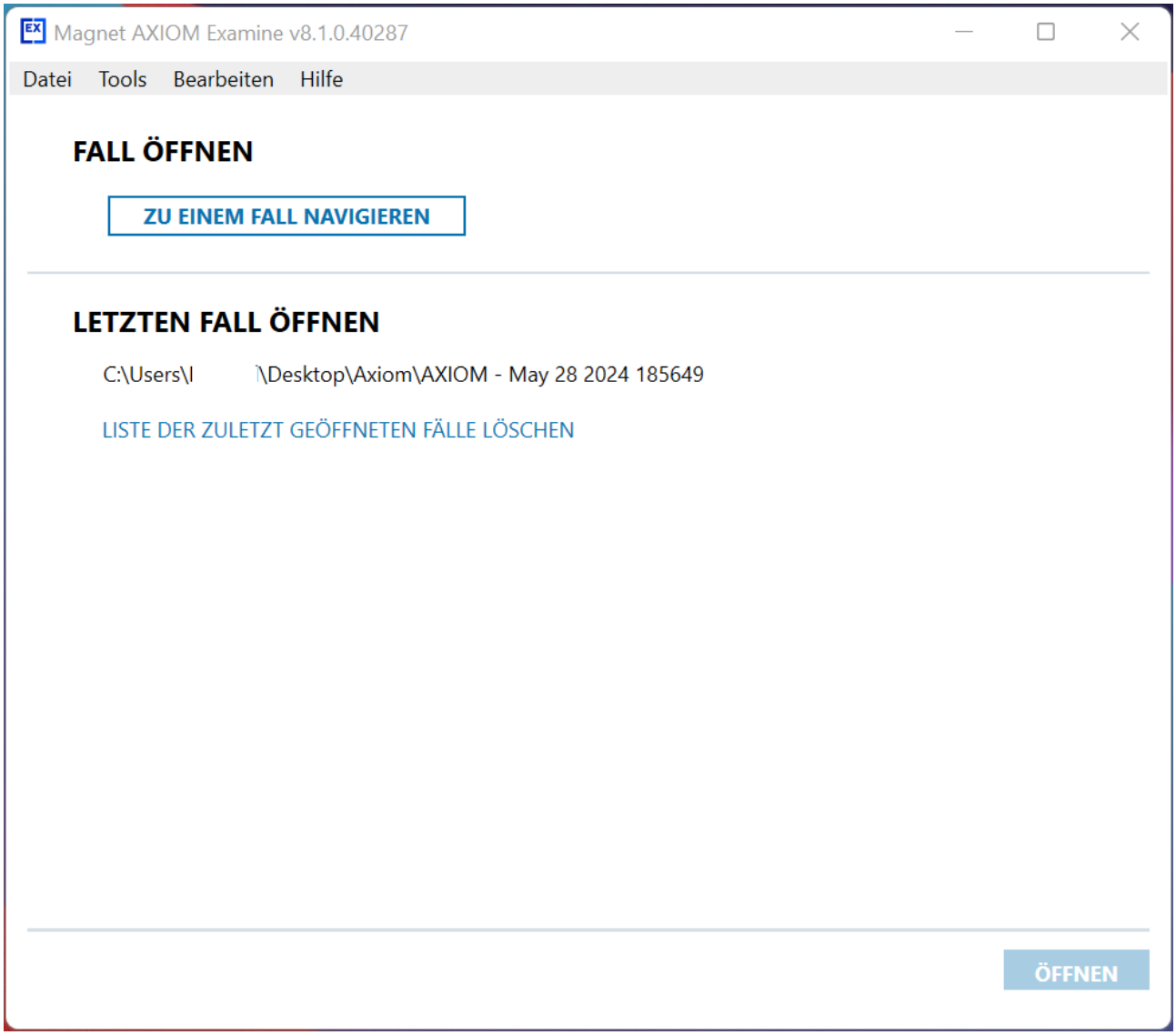


Abbildung 97: Auswahl des Falles in Axiom Analyzer

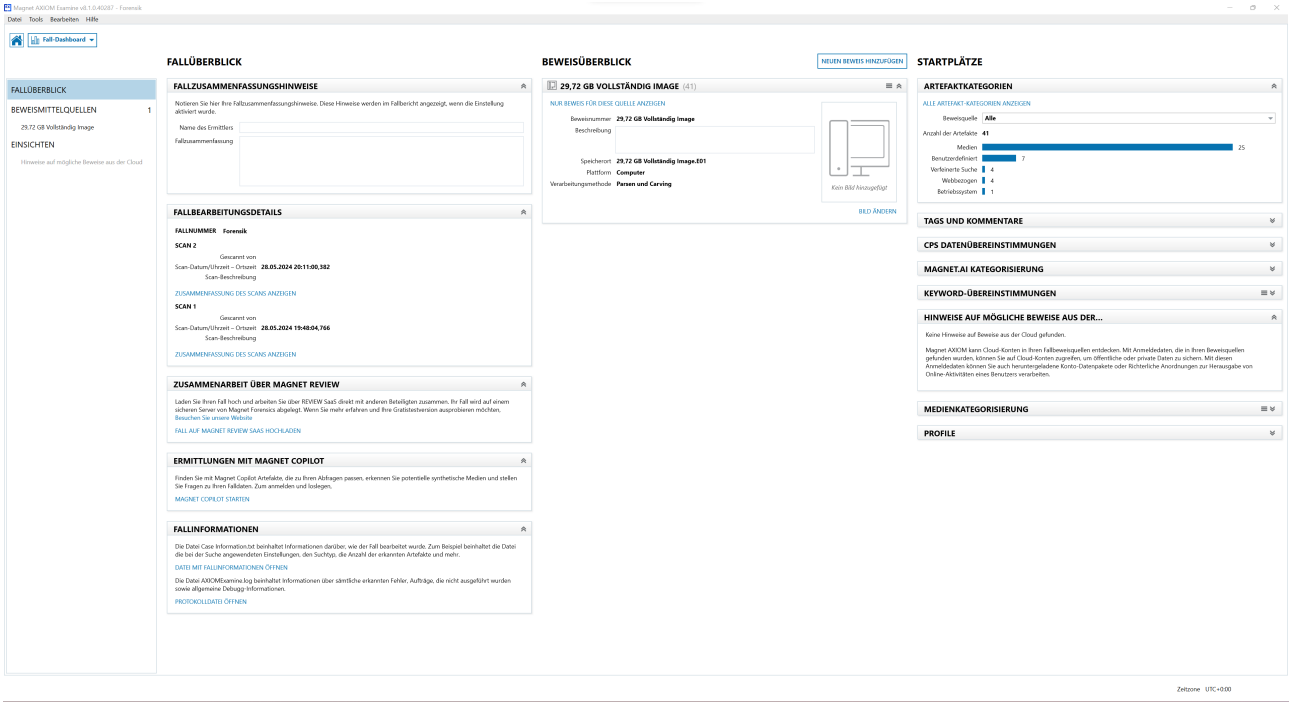


Abbildung 98: Fallübersicht mit erstelltem E01-Image

Die aus dem Image extrahierten verschlüsselten Dateien können im Rahmen der forensischen Analyse mit dem korrekten Schlüssel entschlüsselt und somit die Originalbilder eingesehen werden.

Abbildung 99: Aus dem Image extrahierte verschlüsselte Bilder

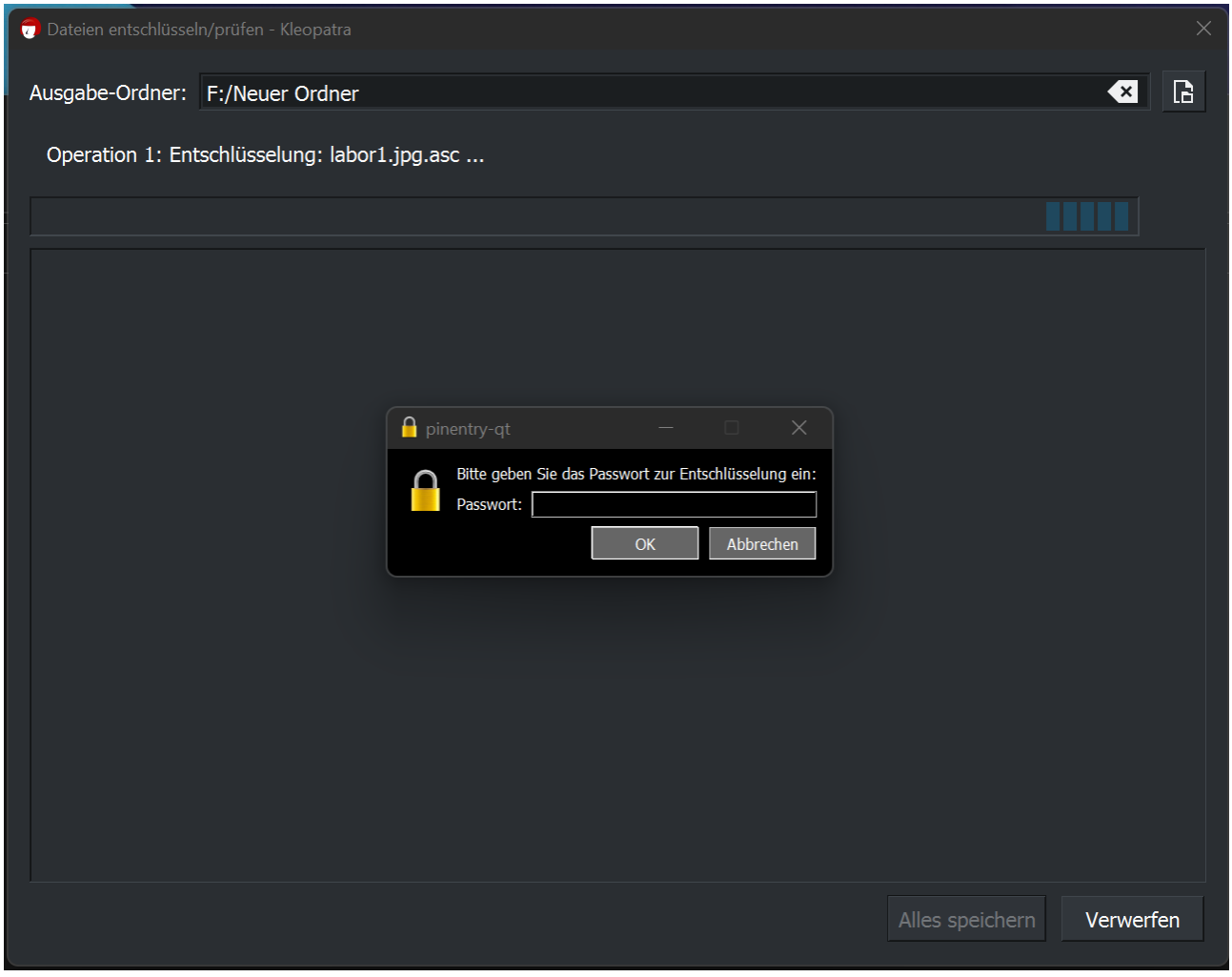


Abbildung 100: Entschlüsselungsvorgang in GnuPG mit Aufforderung zur Key-Eingabe

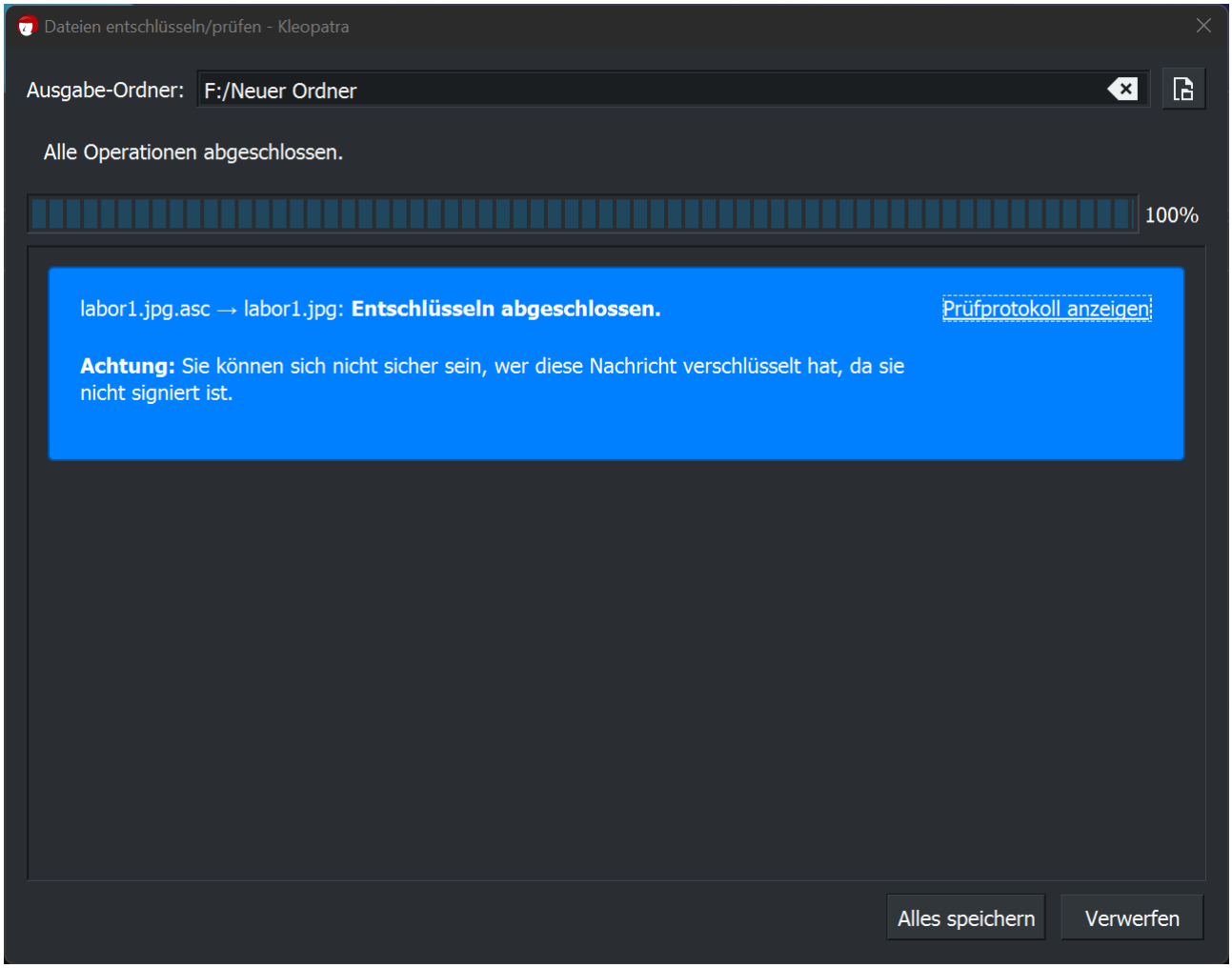


Abbildung 101: Meldung über erfolgreich entschlüsselte Datei in GnuPG

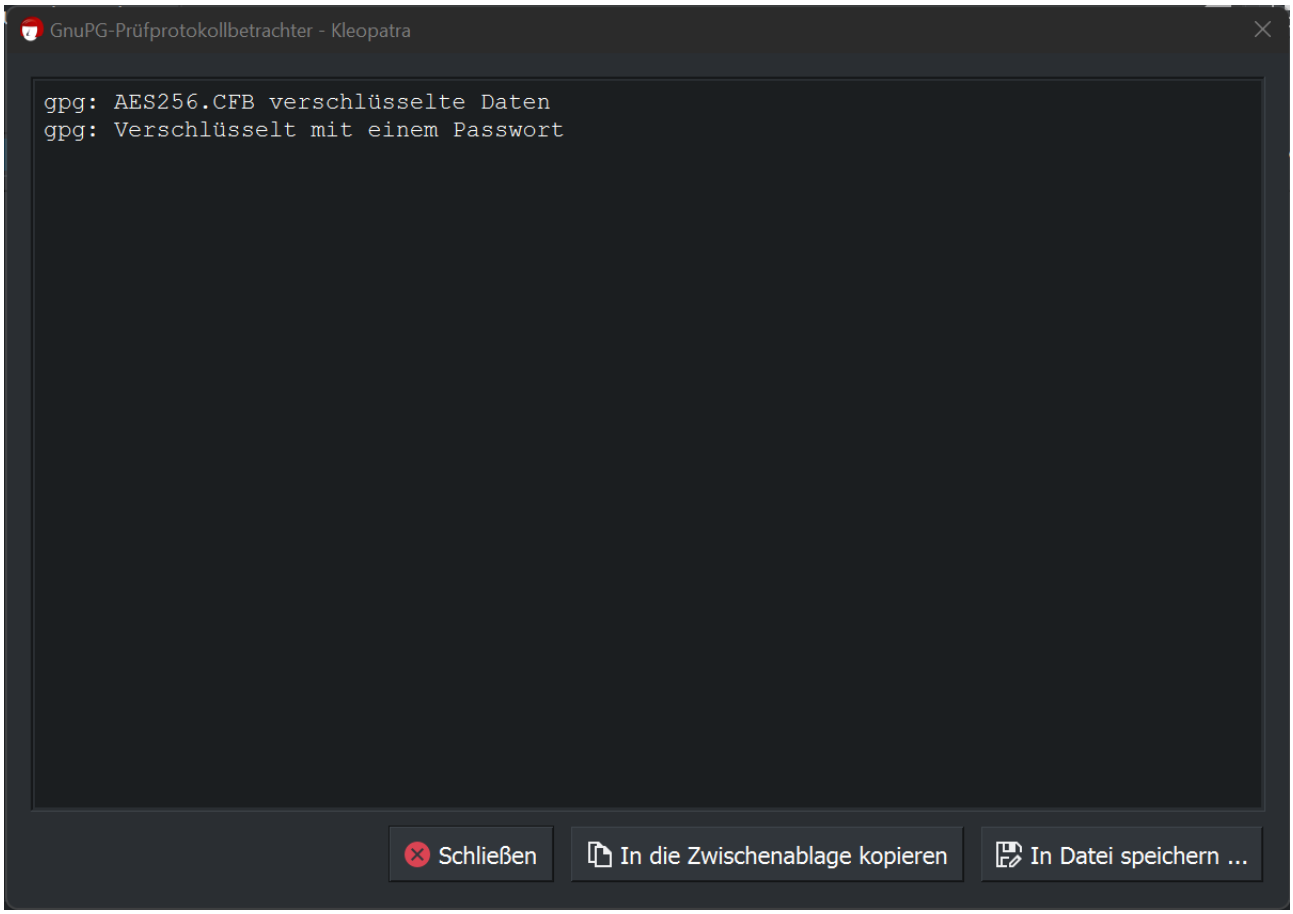


Abbildung 102: GnuPG-Prüfprotokollbetrachter

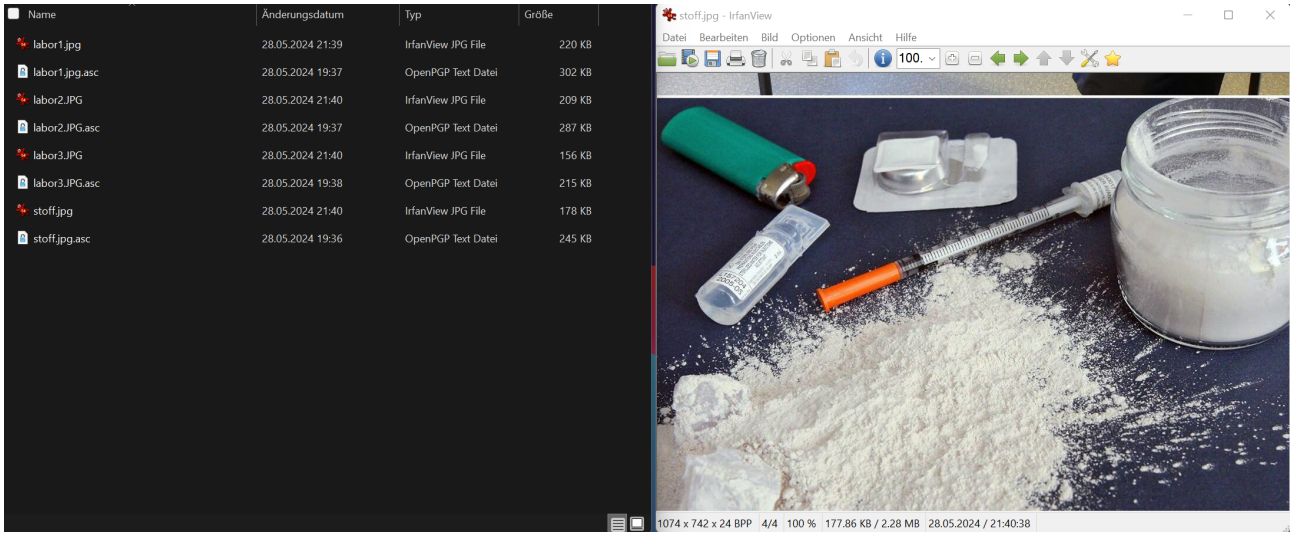


Abbildung 103: Links die entschlüsselten Dateien und rechts ein geöffnetes Bild zur Verifikation

5 Gutachten

Sachverständigengutachten

Gutachten-Nr.	GZ-1234-123
StA-AZ	123 Js 45678/24
Beschuldigter	Lutz Schuldig
Delikt	§30a Abs. 1 BtMG - Straftaten
Auftrag	Untersuchungsantrag (Protokoll über kriminaltechnische Tatortarbeit) vom 05.03.2024
erstellt durch:	..... | ..... | .....
	Philipp-Müller-Straße 14
	23966 Wismar
Telefon	03841 7530
Auftraggeber:	Frau Prof. Dr. Antje Raab-Düsterhöft
	Professorin - Elektrotechnik und Informatik
	Hochschule Wismar
Datum	30. Juli 2024

Dieses Gutachten besteht, exklusive Anlagen, aus 15 Seiten und wurde in zwei Ausfertigungen erstellt, davon ist eine Ausfertigung für das Archiv der Sachverständigen.

Inhalt

5.1 Auftrag

5.1.1 Auftraggeber

Auftraggeber:	Frau Prof. Dr. Antje Raab-Düsterhöft Professorin - Elektrotechnik und Informatik Hochschule Wismar Philipp-Müller-Straße 14 23966 Wismar
Durchführungszeitraum:	05. März 2024 - 30. Juli 2024
Auftrag:	Durchführung einer digitalforensischen Datenträgeranalyse

5.1.2 Sachverhalt

Mit Posteingang vom 05.03.2024 erhielt hiesiges Dezernat Forensische IuK[1]- die Aufforderung einer kriminaltechnischen Untersuchung und der Erstellung eines datenträgeranalytischen Gutachtens. Ausgangspunkt stellt hierzu eine Tathandlung im Deliktsbereich des Betäubungsmittelgesetzes dar. Die Datenträger sind mit Datum vom 25.02.2024 auf der Hauptbahnhofstraße in Wismar nach Durchführung einer Durchsuchungsmaßnahme durch Beschlagnahme mit Datum vom 05.03.2024 an die Unterzeichner übergeben worden. Dem Untersuchungsauftrag kann entnommen werden, dass sich zwei Gruppierungen aufeinander zubewegten, wovon eine der beiden Gruppierungen dem Betäubungsmittelhandel und die andere dessen Betäubungsmittelkonsum zuzuordnen sind. Als kausale Folge findet der erfolgreiche Übergang von Betäubungsmitteln statt.

Die zur Beweisaufnahme hinzugenommenen Datenträger sollen Erkenntnisse und Hinweise zu im folgenden Abschnitt aufgeführten Fragestellungen liefern:

5.1.3 Fragestellungen

Die zu untersuchenden Asservate wurden mit folgendem Untersuchungsauftrag übersandt:

- Bitte die auf der Spur K1/1, K1/2, K1/3 gespeicherten Daten forensisch sichern.
- Befinden sich auf der Spur K1/1, K1/2, K1/3 verschlüsselte Daten? Diese ggf. entschlüsseln.
- Es wird um Bereitstellung von Tabellen-, Text- und Bilddateien mit Bezug zu Betäubungsmitteln gebeten.
- Welche Aussagen können im Bezug zu Betäubungsmitteln nach Analyse der Spurenlage getroffen werden?

[1] Informations- und Kommunikationstechnik

5.2 Gegenstand der Untersuchung

5.2.1 Asservate

Die Asservate wurden vom Auftraggeber entgegengenommen.

Bei den zu analysierenden Asservaten handelt es sich um Datenträger im SSD, USB und SD-Card Format. Die Datenträger weisen jeweils eine unterschiedliche Datengröße auf. Eine Auflistung mit weiterführenden informationsspezifischen Angaben kann folgender Tabelle entnommen werden:

Name	Größe	Bezeichnung
SSD-Datenträger	256 GB	Spur K1/1
USB-Datenträger	256 GB	Spur K1/2
SD-Card-Datenträger	32 GB	Spur K1/3

Tabelle 3: Übersicht der Asservate

Ein Hashwert zur Überprüfung der Integrität der Datensicherung wurde bei Erstellung der forensischen Duplikation vorgenommen. Mit dem Vergleich des Hashwertes vom Original und der Kopie kann eine identische Kopie vom Original nachgewiesen werden.

Die Bildung von Hashwerten erfolgt, indem ein Eingabewert auf eine fest definierte Länge eines Ausgabewertes in hexadezimaler Schreibweise abgebildet wird.

Eine weitere Bearbeitung erfolgt mit identischen Kopien der Asservate.

5.3 Analyseumgebung und Analysewerkzeuge

5.3.1 Analysecomputer

Die forensische Untersuchung der Asservate wurde für die Spur K1/1 mit dem Analysecomputer 1, für die Spur K1/2 mit dem Analysecomputer 2 und für die Spur K1/3 mit dem Analysecomputer 3 mit folgender Hardware und Konfiguration durchgeführt:

Konfiguration	Analysecomputer 1	Analysecomputer 2	Analysecomputer 3
Hersteller:	Dell XPS 13 - 9310	Lenovo Thinkpad X220	Eigenbau
CPU:	Intel Core i7-1185G7	Intel Core i5-2450M	Intel Core i9-9900K
RAM:	16 GB	16 GB	32 GB
Ethernet:	Realtek USB GbE	Realtek PCIe RTL8812AE	Realtex I219-V
Datenträger:	1 TB SSD	128 GB SSD | 512 GB SSD	1 TB SSD | 500 GB
Betriebssystem:	Microsoft Windows 11 Home 23H2	Microsoft Windows 10 Pro 22H2	Microsoft Windows 11 Pro 21H2

Tabelle 4: Analysecomputer

5.3.2 Forensische Software

Datenträgeranlayse

Im Folgenden wird eine Auflistung und Erläuterung der Software geführt, welche für dieses Gutachten zur Datenträgeranlayse Verwendung gefunden hat:

1. X-Ways Forensics Version 20.2
   Bei dieser Software handelt es sich um eine Softwarelösung, welche für die Sicherung elektronischer Beweismittel und deren Analyse Verwendung findet.
2. Magnet Forensics - Axiom Examine Version 7.10.1.39284
   Bei Magnet AXIOM handelt es sich um ein All-in-One-Tool für forensische Untersuchungen und Sicherungen, mit dem Computer, mobile Geräte und Datenträger untersucht werden können.
3. Zetetic - SQLCipher version 3.15.2 2016-11-28 19:13:37
   SQLCipher ist eine Open-Source-Erweiterung für SQLite von der Firma Zetetic LLC, die eine transparente 256-Bit-AES-Verschlüsselung von SQLite-Datenbankdateien bietet.

Erstellung des Gutachtens

Im Folgenden wird eine Auflistung und Erläuterung der Software geführt, welche zur Erstellung des Gutachtens Verwendung gefunden hat:

1. LaTeX
   Bei dem Softwareprodukt 'LaTeX' handelt es sich um ein Softwarepaket, welches die Benutzung des Textdatensatzes TeX unter Zuhilfenahme von Makros ermöglicht. Hierbei wird der zu erstellende Text in seinem Quelldokument erstellt und erhält mit der Kompilierung in eine PDF-Datei seine endgültige Formatierung. LaTeX wurde unter Zuhilfenahme des Online-Editors 'Overleaf' genutzt, bei welchem es sich ebenfalls um einen kollaborativen, cloudbasierten Editor handelt. Das Schreiben, Bearbeiten bzw. Veröffentlichen von wissenschaftlichen Dokumenten wird mit dieser Softwarelösung vereinfacht.

5.3.3 Forensische Hardware

Im Folgenden wird eine Auflistung und Erläuterung der Hardware geführt, welche für dieses Gutachten zur Datenträgeranlayse Verwendung gefunden hat:

1. RaidSonic Icy Box IB-1817M-C31 M.2 PCIe SSD USB 3.1 Type-C HDD Gehäuse
   Dieses externe HDD-Gehäuse verfügt über einen Hardware-Write-Blocker, der eine schreibgeschützte Imageerstellung von NVMe-SSD-Geräten ermöglicht.

2. Tableau Forensic USB Bridge
   Die Tableau Forensic USB Bridge ist ein USB-Writeblocker, welcher eine schreibgeschützte Imageerstellung von USB Geräten ermöglicht.

3. Digital Intelligence USB 3.0 Forensic Card Reader
   Der Digital Intelligence USB 3.0 Forensic Card Reader ist ein USB Forensic Card Reader, welcher die Modi im Nur-Lese- und Lese-/Schreibbetrieb ermöglicht. Mit dem Nur-Lese-Modus kann das zu sichernde Gerät zur forensischen Erfassung der Datenbasis verwendet werden.

5.4 Begriffserklärungen

Im Folgenden wird eine Auflistung und Erläuterung von Begriffen geführt, welche in diesem Gutachten zur Datenträgeranlayse benannt werden:

5.4.1 Backup

Die Sicherung von Daten, wie zum Beispiel Daten einer Festplatte oder eines Verzeichnisses, auf einem externen Datenträger wird Backup genannt. Gängige Medien für Backups sind CD-Rs (beschreibbare CDs), DVD-Rs, externe Festplatten, USB-Sticks oder Magnetbänder. Dabei werden häufig die Dateien in komprimierter Form abgelegt, so dass die Daten erst nach dem Wiederherstellen (Restore) lesbar sind.

5.4.2 Image - Forensische Duplikation

Die Sicherung von Festplatten (u.a.[2] Datenträgern) erfolgt im Allgemeinen durch ein so genanntes Image. Dabei handelt es sich um ein Abbild sämtlicher auf dem Datenträger gespeicherten Informationen einschließlich der gelöschten bzw. unbenutzten Bereiche durch Lesen des Bitstroms.

5.4.3 Dateiformate

Es existiert eine Reihe von Dateiformaten und Verfahren zum Platz sparenden Komprimieren und Speichern von Video- bzw. Multimediadaten (Video, Bild- und Tondaten). Zu den bekanntesten zählen MPEG[3] und AVI[4]. Viele Videoformate sind so genannte Containerformate, dass heißt Dateiformate, die verschiedene Datenformate enthalten können. Dies bedeutet, dass sich bspw.[5] im Videoformat AVI, zwar Informationen über die Struktur der Videodatei eindeutig sind, die Struktur der Videodaten aber verschieden sein kann.

5.4.4 Hashwert

Der Hashwert ist ein aus einer Datei mit Hilfe eines mathematischen Verfahrens, einer so genannten Hashfunktion, ermittelter Wert fester Länge und stellt eine Art digitalen Fingerabdruck dieser Ausgangsdatei dar. Hashwerte müssen eindeutig sein und können so zur Identifikation einer Datei dienen.

[2] unter anderem
[3] Motion Pictures Expert Group
[4] Audio Video Interleave
[5] beispielsweise

5.4.5 Partition

Eine Partition ist eine Einheit eines definierten Speicherbereichs einer Festplatte (oder allgemein Datenträger), die als eigenständiges Laufwerk angesprochen und behandelt werden kann.

5.4.6 Speicherchip

Ein Speicherchip ist ein elektronisches Bauteil, in dem Daten in Form von binären Schaltzuständen innerhalb der integrierten Schaltungen gespeichert werden. Durch Eingabe/Ausgabe-Leitungen können die Daten in den Speicher geschrieben bzw. aus dem Speicher gelesen werden.

5.5 Methoden der Untersuchung

Spur K1/1

Der ausgebaute SSD-Datenträger des PCs wurde mittels externen USB-NVMe-Adapters mit dem Sicherungscomputer verbunden. Der Write-Blocker (Hardware-Schalter) des Adapters war dabei permanent aktiviert, so dass keine Schreibzugriffe auf dem Medium stattfanden. Die SSD wurde von der auf dem Sicherungs-PC (Windows 11) installierten Software 'Magnet Forensics Axiom Examine 7.10.1.39284' erkannt. Der Datenträger wurde mit der entsprechenden Software als forensisches Image (Encase Evidence E01-Format) gesichert. Nach erfolgreicher Sicherung wurde das Image im weiteren Verlauf mittels Axiom Examine ausgewertet.

Spur K1/2

Der USB-Datenträger wurde über die USB-Schnittstelle mittels des zuvor angebrachten Writeblockers mit dem Sicherungscomputer verbunden. Das auf dem Sicherungs-PC laufende X-Ways erkannte die neu angeschlossene Hardware als Blocklaufwerk, so dass der Speicher als Image mittels ebendieser Software forensisch gesichert werden konnte. Schreibzugriffe fanden nicht statt. Die Untersuchung der gesicherten Daten erfolgte im weiteren Verlauf unter dem Betriebssystem Windows 11 mittels der forensischen Spezialsoftware 'X-Ways 20.2'.

Spur K1/3

Die SD-Karte wurde mittels eines USB-Adapters und einem Writeblocker mit dem Sicherungscomputer verbunden. Die SD-Karte wurde in 'Magnet Forensics Axiom Examine 7.10.1.39284' als E01-Image gesichert und das erstellte Image im weiteren Verlauf forensischen Analysen unterzogen.

5.6 Ergebnisse

5.6.1 Zu Frage 1

Bitte die auf der Spur K1/1, K1/2, K1/3 gespeicherten Daten forensisch sichern.

Die **Spur K1/1** besitzt eine 256 GB groß Speichereinheit. In dem Speicherbaustein wurden Daten festgestellt, diese konnten gesichert und ausgewertet werden.

Die **Spur K1/2** besitzt eine 256 GB groß Speichereinheit. In dem Speicherbaustein wurden Daten festgestellt, diese konnten gesichert und ausgewertet werden.

Die **Spur K1/3** besitzt eine 32 GB groß Speichereinheit. In dem Speicherbaustein wurden Daten festgestellt, diese konnten gesichert und ausgewertet werden.

5.6.2 Zu Frage 2

Befinden sich auf der Spur K1/1, K1/2, K1/3 verschlüsselte Daten? Diese ggf. entschlüsseln.

Spur K1/1

Nach dem Ausbau des Datenträgers und anschließendem Einbau in den externen USB-NVMe-Adapter, erfolgte nach Anschluß an den Untersuchungscomputer eine automatische Erkennung und Systemintegration des Speichermediums. Das Speichermedium war unverschlüsselt und konnte gesichert werden. Die auf dem Speichermedium gefundene SQLite-Datenbank des Signal-Messengers war verschlüsselt. Diese konnte im weiteren Verlauf der Untersuchung entschlüsselt werden.

Spur K1/2

Nach dem Anschließen des jeweiligen USB-Gerätes und der automatischen Systemintegration in das gestartete Windowssystem kann mit der Hardware Tableau Forensic USB Bridge die Kombination aus Hersteller-ID und Produkt-ID entnommen werden. Mit Hilfe dieser Angaben konnte das Produkt identifiziert werden. Eine Verschlüsselung der Datenbasis oder einzelner Daten lag nicht vor.

Spur K1/3

Nach der Erstellung eines forensischen Duplikates der SD-Karte konnten im Rahmen der forensischen Analyse verschlüsselte Bilder entnommen werden. Durch Testen verschiedener Schlüssel konnte schlussendlich mit dem Geburtsdatum einer der Hauptverdächtigen der korrekte Schlüssel ermittelt und die Dateien entschlüsselt werden.

5.6.3 Zu Frage 3

Es wird um Bereitstellung von Tabellen-, Text- und Bilddateien mit Bezug zu Betäubungsmitteln gebeten.

Spur K1/1

Bei der untersuchten Elektronik der Spur K1/1 handelt es sich um eine NVMe-SSD eines Desktop-Computers mit Windows Betriebssystem. Im Download-Ordner des Benutzer-Kontos 'Mad Max' wurden Text- und Bilddateien gefunden. Bei den Textdateien handelt es sich um eine Datei im reinen Text-Format (.TXT) und eine MS-Word-Datei (.DOC). Die Text-Datei 'Herstellung' beinhaltet eine Anleitung zur Metamphetamin-Herstellung. Der Inhalt der Word-Datei 'Wuscha.doc' beschreibt die Stereochemie von Methamphetamin. Bei der Bilddatei Namens 'signal-2024-05-18-203244' handelt es sich um eine PNG -Datei die ein Drogen-Labor aufzeigt. Das Bild enthielt keine Exif-Daten, die einen Hinweis auf den Standort des Labors hätten liefern können. Die Dateien werden im Anhang angefügt.

Der Chat-Verlauf des Signal-Messengers wurde erfolgreich entschlüsselt und liegt in tabellarischer Form vor. Die entsprechende Tabelle befindet sich im Anhang.

Spur K1/2

Die hier untersuchte Elektronik der Spur K1/2 dient lediglich dazu Daten dauerhaft zu speichern, jederzeit abzurufen und bei Bedarf zu ändern. Es erfolgt ein Speichervorgang im Speicherchip. Als Verwendungszweck der Spur K1/2 ist die Aufzeichnung von Dateidaten in Dateiform anzusehen, welche später auf andere Medien mit USB-Anschluss übertragen und betrachtet werden können.

Im unpartitionierten Bereich kann ein Datenbereich mit der Dateisignatur **50 4B 03 04** aufgefunden werden. Diese Signatur beschreibt ein ZIP-Dateiformat mit dem daraufbasierenden Dateiformat OBF. Bei dem Format OBF handelt es sich um ein offenes Dateiformat, welches verschiedene Formate wie Tabellenkalkulation **.ods**, Textverarbeitung **.odt** und Präsentationen **.odp** unterstützt. Der Bytesequenz kann die Buchstabenfolge **open.document.spreadsheet** entnommen werden.

Die aufgefundene Datenbasis im unpartitionierten Speicher kann als Verkaufsliste erkannt werden. Extrahiert kann diese Abbildung 89 eingesehen werden.

Spur K1/3

Die untersuchte SD-Karte diente dazu, Bilder des Drogenlabors und der hergestellten Substanzen zu speichern und damit mutmaßlich Kunden anzuwerben oder von der Qualität der angebotenen Drogen zu überzeugen. Die Bilder lagen als AES256-verschlüsselte Dateien vor. Diese konnten entschlüsselt werden, da der Urheber sein Geburtstag als Schlüssel verwendet und dieses Datum den Ermittlungsbehörden bekannt war.

5.6.4 Zu Frage 4

Welche Aussagen können im Bezug zu Betäubungsmitteln nach Analyse der Spurenlage getroffen werden?

Spur K1/1

Der Speicher der Spur K1/1 enthält unter anderem die verschlüsselte Datei 'db.sqlite'. Bei dieser Datei handelt es sich um die Datenbank des Signal-Messengers. Nach erfolgreicher Entschlüsselung konnte dieser ein Kommunikations-Verlauf entnommen werden, der konkrete Hinweise auf Betäubungsmittel-Handel enthält. Der Chat-Verlauf lässt den Schluss zu, dass es sich bei dem Nutzer des Accounts 'Mad Max' um einen BTM-Dealer handelt, der sowohl mit seinem Lieferanten als auch mit einer Kundin kommuniziert. Im Gespräch dem dem Lieferanten geht es um größere Liefermengen und Lieferbarkeit und im Gespräch mit der Kundin um eine konkrete Verabredung zur Übergabe bzw. Verkauf von BTM.

Spur K1/2

Der Speicher von Spur K1/2 enthält strukturierte Daten. Insbesondere die Datei 'SchindlersListe.ods' im Speicherbereich 'Unpartitionierter Bereich' ist für den Bezug mit Betäubungsmitteln hervorzuheben. In dieser kann eine Verkaufsliste erkannt werden, welche vor den Augen Dritter verborgen wurde. Die Ablage erfolgt als ods-Tabellenkalkulationsdatei. Die Tabelleninhalte konnten manuell dekodiert werden und befinden sich aufbereitet im Anhang.

Insgesamt wurde im Hauptspeicherbereich der Spur K1/2 1 brauchbarer Datensatz festgestellt. Das Auslesen der Daten bzw. die Übertragung erfolgte hierbei kabelgebunden über die in der Abbildung 63 gekennzeichnete USB-Schnittstelle.

Plausible Datenformate sind an den nachfolgend beschriebenen Merkmalen erkennbar:

Generell steht als Startzeichen für eine Tabellenkalkulationsdatei im .ods-Dateiformat der Dateikopf auf '50 4B 03 04'. Dies kann der hexadezimalen Ansicht ebenso entnommen werden.

An dieser Stelle ist anzumerken, dass nicht alle aufgeführten Zahlenkolonnen vollständig sein müssen. Ursachen hierfür sind z. B. fehlerhaft oder anderweitig nicht korrekt abgelegte Dateien oder infolge von täterseitig angewandten Antiforensikmaßnahmen. Diese sollen gezielt eine richtige Verarbeitung der gelesenen Daten erschweren oder verhindern.

Spur K1/3

Im SD-Card-Datenspeicher der Kamera von Spur K1/3, die sich nach dem Anschließen an einen Computer als Datenträger zu erkennen gibt, wurden im Unterverzeichnis '/abc/def' 4 Bilddateien im jpg-Format festgestellt. Das Auslesen der Daten bzw. die Übertragung erfolgte ebenfalls kabelgebunden über die USB-Schnittstelle. Im gelöschten Speicherbereich sind keine Daten gespeichert. Die 4 festgestellten Dateien sowie detaillierte Informationen dazu befinden sich auf der beiliegenden Auswertungs-DVD. Detailinformationen zu den Bilddateien sind aus Anhang x ersichtlich.

Feststellungen zu Absprachen zum Anbau, der Herstellung und dem Inverkehrbringen können bei allen Spuren festgestellt werden.

5.7 Zusammenfassung der Untersuchungsergebnisse

Die Datenspeicher der Spuren wurden ausgelesen und aufbereitet. Die entsprechenden Übersichten sind, sowohl gedruckt als auch elektronisch auf beiliegender Auswertungs-DVD, als Report diesem Sachverständigengutachten als Anhang beigefügt.

5.7.1 Resumee der einzelnen Fragestellungen

Die Fragestellungen wurden durch die forensische Untersuchung des Asservates analysiert und werden hier verkürzt zusammengefasst.

1. Frage
    - Die Spuren K1/1, K1/2 und K1/3 besitzen jeweils eine Speichereinheit. In den Speicherbausteinen konnte Datenbasis festgestellt werden. Eine Sicherung der Datenbasis wurde durchgeführt.
2. Frage
    - Die Spur K1/1 besitzt eine verschlüsselte Datenbasis in Form der Datei 'db.sqlite' (Datenbank des 'Signal-Messengers'). Diese konnte erfolgreich entschlüsselt und ausgewertet werden. Der Spur K1/2 kann keine verschlüsselte Datenbasis entnommen werden. Die Spur K1/3 besitzt 4 verschlüsselte Dateien, die entschlüsselt und ausgewertet werden konnten.
3. Frage
    - Der Spur K1/1 können sowohl Bild- und Text-Dateien entnommen werden, die einen konkreten Bezug zu BTM haben, als auch ein Chat-Verlauf aus dem 'Signal-Messenger', der konkrete Hinweise auf den Handel von BTM liefert. Entsprechende Dateien und die Tabelle des Chats befinden sich im Anhang. Der Spur K1/2 kann eine Tabellenkalkulationsdatei entnommen werden, welche eine Verkaufsliste von BTM beinhaltet. Diese wird im Anhang geführt. Der Spur K1/3 können Bilder des Labors sowie ein Bild der hergestellten Substanzen entnommen werden.
4. Frage
    - Den Spuren K1/1, K1/2 und K1/3 können Hinweise zu Betäubungsmitteln entnommen werden. Zu diesen können dem Gutachten Bildmaterial zur Herstellung, Text- und Tabellenkalkulationsformate zu Absprachen, Verkaufsgesprächen und Verkaufslisten entnommen werden.

5.8 Schlussbemerkungen

Dieses Gutachten wurde nach bestem Wissen und Gewissen erstellt. Hiermit wird erklärt, dass dieses Gutachten in eigener Verantwortung, frei von jeder Bindung, ohne persönliches Interesse am Ergebnis und ohne Verfolgung von Interessen anderer Personen erstellt wurde. Eine Ausfertigung dieses Gutachtens wird im Büro der Sachverständigen archiviert. Die Archivierungsdauer beträgt zehn Jahre.

Das Gutachten ist nur mit Originalunterschrift der Sachverständigen gültig.

Wismar, 30. Juli 2024

....

5.9 Anlage

- Auslagenvormerkung (1 Blatt)
- Kopie des Auswertungsauftrages (3 Blatt)
- Ausdrucke (12 Blatt)
- 1 Auswertungs-DVD
- Spur K1/1, K1/2, K1/3

6 Forensik-Wiki-Eintrag: Hexdump

Bei 'Hexdump' handelt es sich um ein Kommandozeilenwerkzeug zur Darstellung binärer Daten, das in den 1960er Jahren für das Betriebssystem 'Unix' entwickelt wurde, um Programmierern und System-Administratoren zu helfen, binäre Daten zu interpretieren. Außerdem ist der Begriff 'Hexdump' in der IT zum Synonym für binär dargestellte Daten geworden. Binärdaten, wie z.B.[1] Dateien, Speicher-Auszüge oder Daten-Ströme, bestehen aus den ASCII-Zeichen 0 bis 255 (ursprünglich 0 bis 127), hexadezimal 0x00 bis 0xFF, wovon die ersten 32 Zeichen Steuerzeichen (0x00 bis 0x1F) sind. Diese Steuerzeichen dienen (dienten) zur Steuerung von Ausgabegeräten, wie Drucker und Monitoren. Beispiele für Steuerzeichen sind LF (Line Feed / Zeilenvorschub) 0x0A, CR (Carriage Return / Wagenrücklauf) 0x0D, BS (Backspace / Löschen) 0x08, oder ESC (Escape) 0x1B. Der Versuch, eine Binärdatei auf einem unixoiden System mittels des Befehls 'ca' oder 'less' darzustellen, wird einerseits vom Betriebssystem hinterfragt und führt andererseits zu einer schwer nachvollziehbaren Darstellung, da auch die nicht darstellbaren Steuerzeichen mit ausgegeben werden. Um diesem Umstand entgegenzuwirken, wird ein Hexdump-Tool benutzt (Abbildung 104).

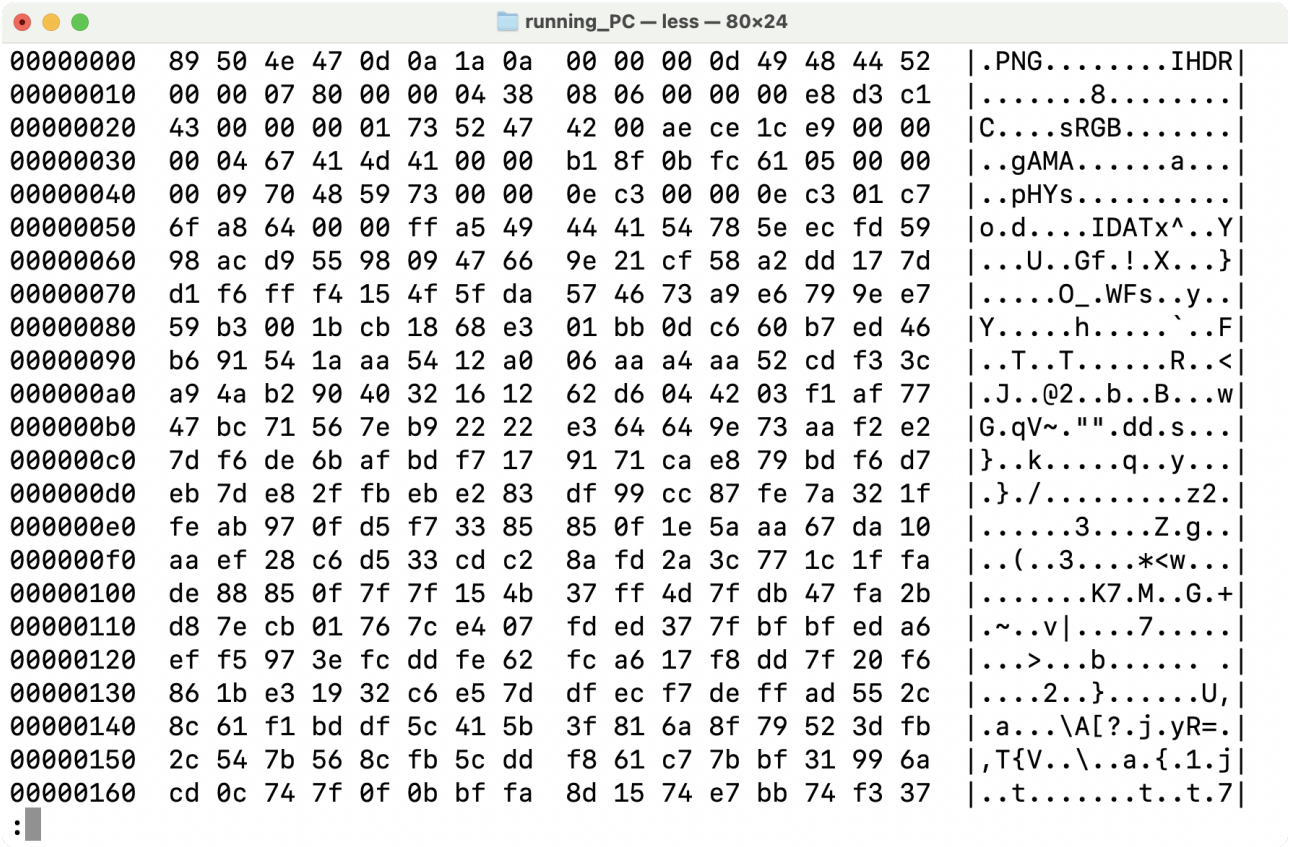


Abbildung 104: Hexdump einer PNG-Datei

[1] zum Beispiel

Seine typische Darstellung ist zwei- oder dreispaltig und zeigt pro Zeile 16 Bytes. Die Spalten unterteilen sich in hexadezimale Offsetadressen, gefolgt vom 16 Bytes-Block, in Form von einzelnen oder paarweisen Hexadezimalziffern und der optionalen dritten Spalte mit den entsprechenden darstellbaren ASCII-Zeichen. Die Steuerzeichen 0x00 bis 0x1F werden als Punkt '.' dargestellt, wodurch eine strukturierte Ausgabe von Binärdaten ermöglicht wird. Eine Darstellung im dezimalen oder oktalen Format kann per Kommandozeilen-Parameter eingestellt werden.

Hexdump ist in der IT-Forensik nach wie vor ein beliebtes und regelmäßig genutztes Werkzeug, da sich mit ihm unkompliziert und schnell ein Überblick über binäre Daten jeglicher Art verschaffen lässt. Es zählt, aufgrund seines Alters, zu den ersten IT-forensischen Werkzeugen überhaupt.

A Zeitnachweis SSD-Datenträger

Tätigkeit	Datum	Uhrzeit
Datenträgersicherung SAMSUNG MZVLB256HAHQ	27.05.2024	15:28 - 18:30
Analyse Datensicherung mittels Axiom Examine	28.05.2024	11:47 - 12:37
Fertigung Gutachten	29.05.2024	09:13 - 11:47
		14:32 - 17:51
Fertigung Zeitnachweis	29.05.2024	18:06 - 18:29
Fertigung Sachbearbeitungssystem	30.05.2024	09:00 - 11:18

Tabelle 5: Zeitnachweis SSD-Datenträger

B Zeitnachweis USB-Datenträger

Tätigkeit	Datum	Uhrzeit
Lichtbilder Datenträger	16.05.2024	12:30 - 12:50
Datenträgersicherung JetFlash Transcend 128 GB.e01 mittels TABLEAU Forensic USB Bridge	16.05.2024	12:50 - 13:00
Analyse Datensicherung mittels X-Ways	16.05.2024	13:00 - 15:00
Fertigung Gutachten	17.05.2024	08:00 - 12:00 12:30 - 16:00
Fertigung Zeitnachweis	17.05.2024	16:00 - 16:30
Fertigung Sachbearbeitungssystem	17.05.2024	16:30 - 17:00

Tabelle 6: Zeitnachweis USB-Datenträger

C Zeitnachweis SD-Card Datenträger

Tätigkeit	Datum	Uhrzeit
Datenträgersicherung	28.05.2024	20:20 - 20:30
Analyse Datensicherung mittels Axiom Examine	28.05.2024	20:30 - 21:30
Fertigung Gutachten	29.05.2024	09:30 - 11:50
		14:40 - 18:00
Fertigung Zeitnachweis	29.05.2024	18:00 - 18:30
Fertigung Sachbearbeitungssystem	30.05.2024	09:00 - 11:20

Tabelle 7: Zeitnachweis SSD-Datenträger

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe. Die Stellen der Arbeit, die anderen Quellen im Wortlaut oder dem Sinn nach entnommen wurden, sind durch Angaben der Herkunft kenntlich gemacht. Dies gilt auch für Zeichnungen, Skizzen, bildliche Darstellungen sowie für Quellen aus dem Internet.

Ich erkläre ferner, dass ich die vorliegende Arbeit in keinem anderen Prüfungsverfahren als Prüfungsarbeit eingereicht habe oder einreichen werde.

Die eingereichte schriftliche Arbeit entspricht der elektronischen Fassung. Ich stimme zu, dass eine elektronische Kopie gefertigt und gespeichert werden darf, um eine Überprüfung mittels Anti-Plagiatssoftware zu ermöglichen.

....

Wismar, 30. Juli 2024