Hochschule Wismar
Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

Hausarbeit (APL) zum Thema „IT-Sicherheitsvorfälle und deren IT-forensische Analyse mittels Windows-Tools“

Betriebsspionage bei der Speuer Sanitär Service GmbH

Eingereicht am: 17.07.2022
von: Marcel Erfurth,
Edin Mujezinovic,
Klaus Nyzak
Studiengang: IT-Sicherheit und Forensik
Modul: Forensik in Betriebs- und Anwendungssystemen
Dozentin: Frau Prof. Dr.-Ing. Antje Raab-Düsterhöft

Inhalt

1 Einleitung

Im folgenden Projektbericht der Gruppe FFM-05 (Sommersemester 2022) wird das Vorgehen einer forensischen Untersuchung anhand zweier Datenträger (Notebook + USB-Stick) exemplarisch dargestellt.
Nach der Beschreibung des Szenarios werden die technischen Abläufe und Durchführungen zur Vorbereitung und Erstellung des Szenarios beschrieben. Im Anschluss folgt das forensische Gutachten. Den Abschluss bildet der WIKI-Eintrag zum Thema „DLP – Data Leakage Prevention“.
Diese Projektarbeit stützt sich auf die Erkenntnisse und Vorarbeiten aus der Projektarbeit des Moduls "Einführung in die IT-Sicherheit und Forensik" aus dem ersten Semester. Sowohl das Unternehmen Speuer Sanitär Service GmbH und auch alle handelnden Personen, das Organigramm, und der Netzplan wurden übernommen und die aufgebaute IT Infrastruktur an diese Ideen angelehnt.
Die Personen und Handlungen dieser Projektarbeit sind frei erfunden. Etwaige Ähnlichkeiten mit tatsächlichen Gegebenheiten oder lebenden oder verstorbenen Personen sind rein zufällig und nicht beabsichtigt.

1.1 Aufgabenstellung

Das Ziel der APL besteht darin, bzgl. eines Computers und eines mobilen Gerätes ein Festplatten- oder Daten-Image zu erzeugen und diese Images unter Nutzung einer speziellen Forensik-Software zeitbasiert auszulesen und zu analysieren. Die Ergebnisse sind in einem forensischen Gutachten zu präsentieren.
Aus diesem Grund muss im Vorfeld ein Szenario für die zu entdeckenden Daten erdacht und erstellt werden, so dass passende digitale Spuren auf den Geräten erzeugt werden. In dem Szenario sollen von mindestens zwei Geräten (ein Computer und ein mobiles Gerät) ein Image erstellt und ausgewertet werden. Für die dazugehörige Dokumentation sollen die Daten der Geräte in einer Timeline dargestellt werden. Die Ergebnisse sollen in einem forensischen Gutachten präsentiert werden. Des Weiteren ist ein Begriff für das Forensik-Wiki zu erstellen und in diesem Dokument aufzunehmen

1.2 Beschreibung des Szenarios

Guido Nagel, Leiter des Innendienstes und Recruiter der Speuer Sanitär Service GmbH, hat sich mit seinem Kollegen Luigi Bonucci, Leiter des Auftragszentrums, verstritten. Vom Firmenchef Norbert Speuer findet Guido Nagel sich ferner nicht genug wertgeschätzt, denn selbst in mehrfachen Versuchen an klärenden Gesprächen mit Norbert Speuer und Luigi Bonucci wurde keine Besserung erzielt. Nach mehreren Monaten sieht Guido Nagel keine andere Möglichkeit als seine Kündigung einzureichen und mit einer Kündigungsfrist zum Ende des Monats die Speuer Sanitär Service GmbH zu verlassen.

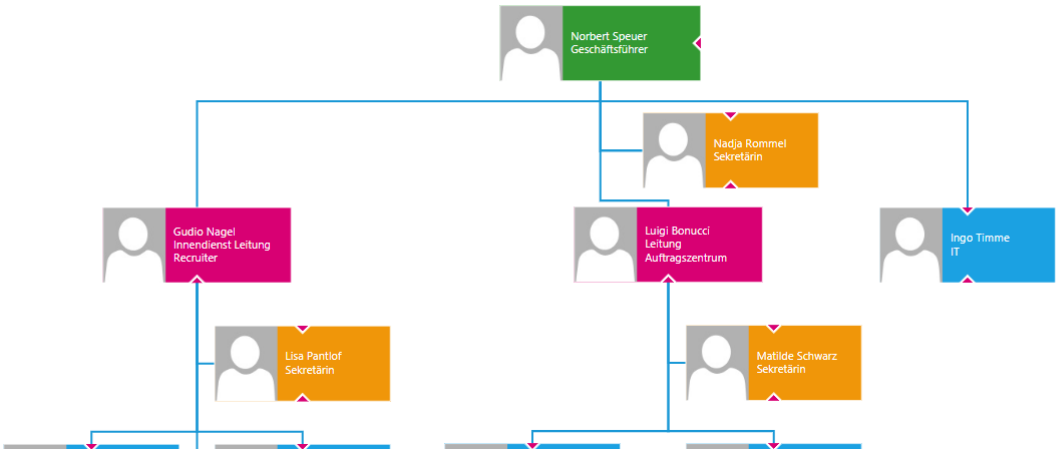


Abbildung 1 - Ausschnitt Organigramm SSS GmbH

An seinem letzten Arbeitstag sieht seine Sekretärin, Lisa Pantlof, dass Guido Nagel einen Firmen-USB-Stick an sein Notebook angeschlossen hat und Daten transferiert. Kurz bevor Guido Nagel sein Büro verlässt, verschickt er die folgende Mail:

> *„Hallo Paul,*
> *ich habe wie besprochen die Daten gesichert. Werde sie dir dann beim nächsten Treffen geben. Freu mich schon auf die nächste Zeit.*
> *Dein Guido“*

Durch eine von Guido Nagel selbst voreingestellte Email-Regel, die alle Mails seiner Sekretärin in Kopie zusendet, bekommt auch Lisa Pantlof von dieser Mail Kenntnis. Der eigentliche Empfänger der Mail, Paul Rotasch, ist Inhaber eines Mitbewerbers der Speuer Sanitär Service GmbH, die sowohl einen ähnlichen Kunden- als auch Lieferantenstamm hat. Lisa Pantlof meldet das Gesehene und die Mail dem Firmenchef Norbert Speuer, der zu diesem Zeitpunkt nicht im

Gebäude ist. Norbert Speuer informiert den Pförtner, dass dieser Guido Nagel aufhalten und den USB-Stick an sich nehmen soll.
Als Guido Nagel sich vom Pförtner verabschiedet, spricht dieser ihn auf den USB-Stick an und bittet um Herausgabe desselbigen. Erst nach Androhung von Rechtsmitteln übergibt Guido Nagel den USB-Stick dem Pförtner. Der Pförtner packt den USB-Stick in einen Briefumschlag.
Sensibilisiert durch einen IT-Vorfall im letzten Jahr informierte Norbert Speuer währenddessen das auf Forensik spezialisierte Unternehmen FFM-05 und bittet darum den Fall zu untersuchen.

1.3 Vorbereitung der Infrastruktur

Es wurde ein Teil der Infrastruktur der SSS GmbH anhand des folgenden Netzwerkplans nachgebaut.

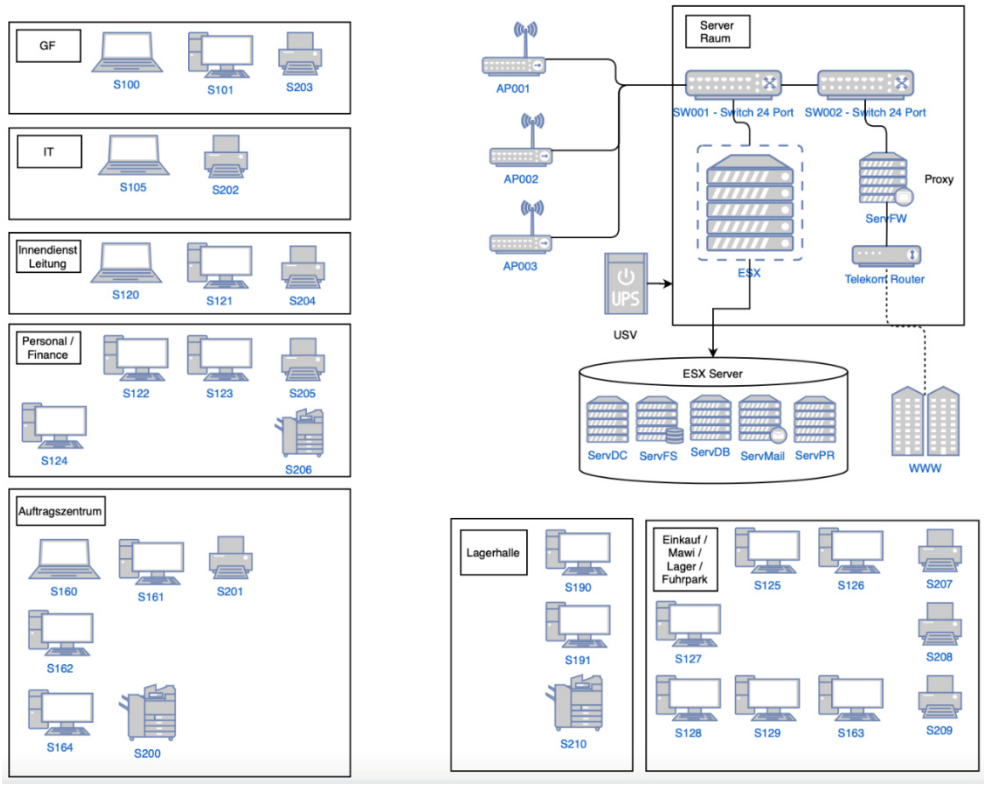


Abbildung 2 - Netzplan SSS GmbH

Mit Hilfe vom Microsoft HyperV wurde ein Domain Controler (S050), Daten-Server (S051) und ein Exchange-Server (S054) als VM erstellt. Das Notebook S120 von Guido Nagel wurde an die „speuer.dir“-Domäne angemeldet, an dem das Szenario (Mail-Kommunikation, Dateizugriffe, etc.) vorbereitet wurde.

2 Genutzte Werkzeuge

Werkzeuge, darunter fällt auch entsprechende Forensik-Software, müssen gewisse Kriterien erfüllen, damit diese im möglicherweise späteren Verlauf auch vor Gericht akzeptiert werden können, sog. Gerichtsfestigkeit:

- Akzeptanz
  Das genutzte Werkzeug muss in Fachkreisen anerkannt sein und somit auch von anderen Spezialisten genutzt werden.
- Glaubwürdigkeit / Nachvollziehbarkeit
  Forensikwerkzeuge sind Werkzeuge für Spezialisten. Genau deswegen müssen die Ergebnisse für einen möglicherweise nicht-fachkundigen Dritten nachvollziehbar und vertrauenswürdig sein.
- Wiederholbarkeit
  Bei einer erneuten Durchführung müssen dieselben Ergebnisse produziert werden. Ansonsten würde die Glaubwürdigkeit darunter leiden.
- Integrität
  Da es bei der Nutzung solcher Werkzeuge um sichergestellte Spuren geht, dürfen diese nicht unbemerkt verändert werden können.
- Dokumentation
  Bei einer forensischen Untersuchung muss eine kontinuierliche Dokumentation gewährleistet sein.

2.1 FTK Imager

„FTK Imager“ ist ein Bestandteil des Forensic Toolkit der Firma AccessData. Abbilder / Images einer Festplatte oder USB-Sticks können hiermit gespeichert und später wiederhergestellt werden. Zusätzlich werden Hash-Werte berechnet, damit die Integrität der Daten mit dem späteren forensischen Image überprüft und sichergestellt werden können. Dieses Werkzeug kommt in der Datensicherungsphase zur Nutzung.

2.2 Magnet Axiom

„Magnet Axiom“ der Firma Magnet Forensics ist ein Werkzeug, das in forensischen Ermittlungen genutzt wird. Es besteht aus den Bestandteilen „Axiom Process“ und „Axiom Examine“. Mittels Axiom Process können Falldateien erstellt werden, während Axiom Examine zur Analyse der gesicherten Daten genutzt wird. Es können sowohl Computer-, Smartphone- oder Cloud-Daten in einer einzigen Falldatei gesichert und bearbeitet werden.

2.3 Bemerkung

Obwohl mittels Axiom Process auch Images gesichert werden können, haben wir uns für die Nutzung vom FTK Imager entschieden, damit wir Erfahrung in zwei Werkzeugen sammeln können. Ferner erschien uns die Sicherung in Axiom im Vergleich zum FTK Imager weniger übersichtlich bzgl. der Dokumentation. Speziell die Hashwerte waren im FTK Imager besser ersichtlich.

3 Forensisches Gutachten

3.1 Deckblatt

Forensik für Mittelständler GmbH

Philipp-Müller-Straße 5 | 23966 Wismar
Tel. 03841 / 5050 – 05
Fallnummer:
Gutachten@FFM-05.de

Wismar, den 17.07.2022

Auftragsnummer: 37 / 2022
30030000

Gutachten

in der IT-Forensik

Im Auftrag der

Speuer Sanitär Service GmbH
Offenbacher Landstraße 341
60599 Frankfurt

Erstellt von:

Marcel Erfurth
Edin Mujezinovic
Klaus Nyzak

Fertigstellung: 17.07.2022

3.2 Auftragsspezifikation

Norbert Speuer, Inhaber der Firma Speuer Sanitär Service GmbH, hat die Firma FFM-05 mit der Analyse und Auswertung eines Firmennotebooks und eines USB-Sticks beauftragt und bittet um ein forensisches Gutachten bis zum 17.07.2022. Der Beweggrund der Beauftragung und dem bestellten forensischen Gutachten sind die Beobachtungen einer Mitarbeiterin vom 25.06.2022, die auf einen möglichen Informationssicherheitsvorfall schließen lassen.

Es besteht seitens Norbert Speuer der Verdacht, dass der ehemalige Mitarbeiter Guido Nagel Firmengeheimnisse auf einen USB-Stick gesichert hat, um diese an einen Konkurrenten zu übergeben. Ein möglicher Datenverlust und der Verlust der Datenvertraulichkeit könnten somit die Folge sein.
Aus diesem Grund übergab Norbert Speuer den Mitarbeitern der Firma FFM-05 einen USB-Stick, welcher in einem unverschlossenen Briefumschlag lag, und das ausgeschaltete Firmennotebook des Mitarbeiters Guido Nagel.

Ziel ist es, Hinweise sowie Beweismittel zu gewinnen, um den Verdacht zu erhärten oder zu widerlegen. In Abstimmung mit Norbert Speuer wurden die Schwerpunkte des Untersuchungsauftrags wie folgt vorgegeben:

- Sicherung aller auf den Endgeräten vorhandenen Daten, die in Zusammenhang mit dem Verdacht stehen - einschließlich gelöschter oder versteckter Daten.
- Suche, Nachweis und Auswertung von stattgefundenen Kommunikationsaktivitäten zwischen Guido Nagel und Paul Rotasch auf den sichergestellten Endgeräten.
- Auf eine Untersuchung der Server wird auf Wunsch von Norbert Speuer verzichtet, um zum einen keine Ausfallzeiten zu generieren und zum anderen ein größeres Aufsehen innerhalb der Firma zu vermeiden.

Norbert Speuer möchte sich die Option offenlassen, die Staatsanwaltschaft wegen möglicher Betriebsspionage einzuschalten.

3.2.1 Untersuchungszeitraum

Die beiden zu untersuchenden Asservate wurden am 25.06.2022 den Mitarbeitern der Firma FFM-05 übergeben. Die Asservate befanden sich während der Auswertung im Büro der FFM-05 und wurden per Foto dokumentiert.

Datum der Auftragserteilung	25.06.2022
Untersuchungszeitraum	25.06.2022 – 15.07.2022
Zeitsynchronisation	Zeitzone UTC + 2:00 in Magnet AXIOM Examine eingestellt

Tabelle 1 - Untersuchungszeitraum

3.2.2 Untersuchungsmethodik

Im folgenden Gutachten wird nach dem bewährtem SAP-Modell gearbeitet, welches zur Beschreibung von forensischen Untersuchungen dient. Das SAP-Modell gliedert sich in drei Phasen:

- Secure
  In der Secure-Phase werden alle Daten sorgfältig erfasst und gesichert. Dabei ist zu beachten, dass die Integrität der Daten gewährleistet bleibt und das 4-Augen-Prinzip eingehalten wird. Die erzeugte Sicherung muss eine genaue Kopie der Originaldaten sein.
- Analyse
  In der Analyse-Phase werden die Spuren sorgfältig untersucht und bewertet. Die Auswertung erfolgt nach objektiven Bewertungsmaßstäben.
- Present
  In der Present-Phase werden alle Erkenntnisse schlüssig und adressatengerecht aufbereitet. Eine entsprechende Dokumentation, die in den anderen Phasen selbstverständlich nebenherläuft, wird finalisiert.

3.2.3 Untersuchungsfragen und Sachverhaltsangaben

In der folgenden Untersuchung sollen folgende Fragen beantwortet werden:

- Asservat-100 – USB-Stick
  - Frage1:
    Sind auf dem USB-Stick Firmengeheimnisse vorhanden? Wenn ja, welche?
- Asservat-200 – Notebook von Guido Nagel
  - Frage 2:
    Wurden Firmendaten vom Notebook gelöscht? Wenn ja, welche?
  - Frage 3:
    Sind auf dem Notebook weitere Spuren zur Kommunikation zwischen Guido Nagel und Paul Rotasch vorhanden?

Es ist festzuhalten, dass Guido Nagel der vollständigen Untersuchung seines dienstlich genutzten Notebooks und des USB-Sticks ausdrücklich zugestimmt hat. Somit entfallen die datenschutzrechtlichen Aspekte.

3.3 Untersuchungsobjekte

Asservatennr	**Typ**	**Datei-system**	**Seriennummer**	**Hashwert**	**Eigent. / Nutzer**
Asservat-100 (30030000-100)	USB-Stick 16GB (Articona)	NTFS	9A934D3B	MD5: 3788728777939b8d2dbd48688f6c4dbc SHA1: 51911808675ca680345a652e6536af68d179f9fd	SSS GmbH / Guido Nagel
Asservat-200 (30030000-200)	Notebook (Dell Latitude 5500)	NTFS	33XDOZ2 MFG2019YR	MD5: f180b74a8598306ec71378f9702a0fa0 SHA1: 190ab188f88734424d34d0abf2b815f2ba97689f	SSS GmbH / Guido Nagel

Tabelle 2 – Untersuchungsobjekte

Abbildung 3 - Asservat-100 (USB-Stick)

Abbildung 4 - Asservat-200 Vorderseite (Notebook)

Abbildung 5 - Asservat-200 Rückseite (Notebook)

3.4 Untersuchungswerkzeuge

Name	Hersteller	Version	Funktion
FTK Imager	AccessData	4.7.1.2	Erstellung von digitalen Sicherungen (Images)
Magnet Axiom	Magnet Forensics	6.1.0.31400	Forensische Datenanalyse der Images / Asservate

Tabelle 3 - Untersuchungswerkzeuge

3.4.1 Untersuchungswerkzeuge des USB-Sticks (Asservat-100)

Die Sicherung der Festplatte des übergebenen USB-Sticks wurde mit der forensische Software FTK-Imager erfolgreich durchgeführt. Die Sicherung des USB-Sticks entspricht einem bitgenauen Abbild und wird im weiteren Verlauf als Image bezeichnet.
Die anschließende Auswertung wurde auf einem weiteren Image durchgeführt, damit es zu keinem Zeitpunkt zu einer Datenveränderung kommen kann und eine Masterkopie unangetastet bleibt.
Mit der Software Magnet Axiom Examine wurden die Daten anschließend analysiert und aufbereitet.

3.4.2 Untersuchungswerkzeuge des Notebooks (Asservat-200)

Die Sicherung der Festplatte des übergebenen Notebooks wurde mit der forensische Software FTK-Imager erfolgreich durchgeführt. Die Sicherung der Festplatte entspricht einem bitgenauen Abbild und wird im weiteren Verlauf als Image bezeichnet.
Die anschließende Auswertung wurde auf einem weiteren Image durchgeführt, damit es zu keinem Zeitpunkt zu einer Datenveränderung kommen kann und eine Masterkopie unangetastet bleibt.
Mit der Software Magnet Axiom Examine wurden die Daten anschließend analysiert und aufbereitet.

3.5 Untersuchung

Nach der Begutachtung des Tatortes, der mittels Fotos dokumentiert wurde, wurden die Beweise übergeben und sichergestellt. Einzelheiten zu den übergebenen Beweismitteln können dem Kapitel 3.3 Untersuchungsobjekte entnommen werden. Die beiden Asservate wurden von nur einer Person der FFM-05 berührt und verpackt. Dies und alle anderen folgenden Untersuchungen wurden im 4-Augen-Prinzip durchgeführt, so dass die potenziellen Beweismittel nie von einer einzigen Person allein bearbeitet worden sind. Die Vergabe der Fallnummer, der Beweisnummern und die Evidence-Collection wurden vor Ort durchgeführt. Evidence-Details wurden im Lab-4 der FFM-05 erhoben.

Mittels der forensischen Software Axiom Process + Examine (siehe auch 3.4. Untersuchungswerkzeuge) wurde die Fallerstellung vorgenommen die Beweise eingefügt und anschließend geladen.

Die Festplatte des Notebooks war verschlüsselt. Axiom selbst hat die Entschlüsselung durchgeführt, so dass die Untersuchung durchgeführt werden konnte.

Bei beiden Asservaten wurde eine Hardware-Writeblocker verwendet, um einen schreibenden Zugriff auf die Asservate zu verhindern[1].

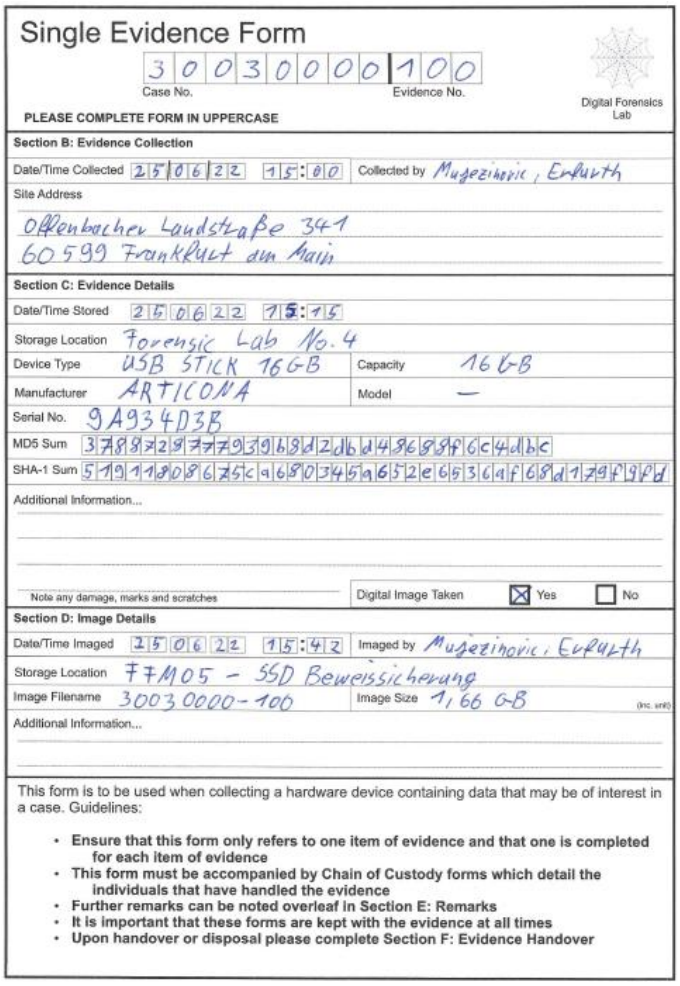
Der beiden Asservate werden derweil im Tresor der FFM-05 verwahrt.

1 Im Rahmen dieser Projektarbeit stand leider kein Write-Blocker zur Verfügung. Für ein tatsächliches forensisches Gutachten ist ein Writeblocker jedoch unabdingbar. Da jedoch ein Gutachten ohne Writeblocker nur wenig Substanz hätte, wird zumindest laut Gutachten ein Hardwareblocker genutzt, aber nicht weiter spezifiziert.

3.5.1 Untersuchung des USB-Sticks (Asservat-100)

Im Rahmen der Secure-Phase wurde zunächst der USB-Stick, welcher vom Pförtner in einem Briefumschlag am vorherigen Arbeitsplatz von Guido Nagel deponiert wurde, an diesem Arbeitsplatz sichergestellt. Der USB-Stick wurde dokumentiert, mit der Asservatennummer 100 versehen und in einem Beutel verschlossen.

Der USB-Stick wurde im Forensischen Labor (Forensic Lab No. 4) angeschlossen, um 2 Images zu erstellen. Auf dessen Basis zu Beweisintegritätszwecken die Hashwerte berechnet und dokumentiert wurden. Die Erzeugung des Images kann dem Anhang entnommen werden.



Single Evidence Form

Case No. 3 0 0 3 0 0 0 0 | Evidence No. 1 0 0

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected 25/06/22 15:00 Collected by Mujezinovic, Erfurth

Site Address

Offenbacher Landstraße 341
60599 Frankfurt am Main

Section C: Evidence Details

Date/Time Stored 25/06/22 15:15

Storage Location Forensic Lab No. 4

Device Type USB STICK 16GB Capacity 16 GB

Manufacturer ARTICONA Model —

Serial No. 9A934D3B

MD5 Sum 3788725777939b8d2db4986889f6c4dbc

SHA-1 Sum 5191180867c5c9680345a652e6536af68d179f9fd

Additional Information...

Note any damage, marks and scratches

Digital Image Taken ☒ Yes ☐ No

Section D: Image Details

Date/Time Imaged 25/06/22 15:42 Imaged by Mujezinovic, Erfurth

Storage Location FFM05 - SSD Beweissicherung

Image Filename 30030000-100 Image Size 1,66 GB (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence
- This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence
- Further remarks can be noted overleaf in Section E: Remarks
- It is important that these forms are kept with the evidence at all times
- Upon handover or disposal please complete Section F: Evidence Handover

Abbildung 6 - Singe Evidence Form (Asservat-100)

Single Evidence Form

Digital Forensics Lab

Section E: Remarks

USB Stick wurde in einem unverschlossenem Briefumschlag vorgefunden.

Section F: Evidence Handover / Disposal

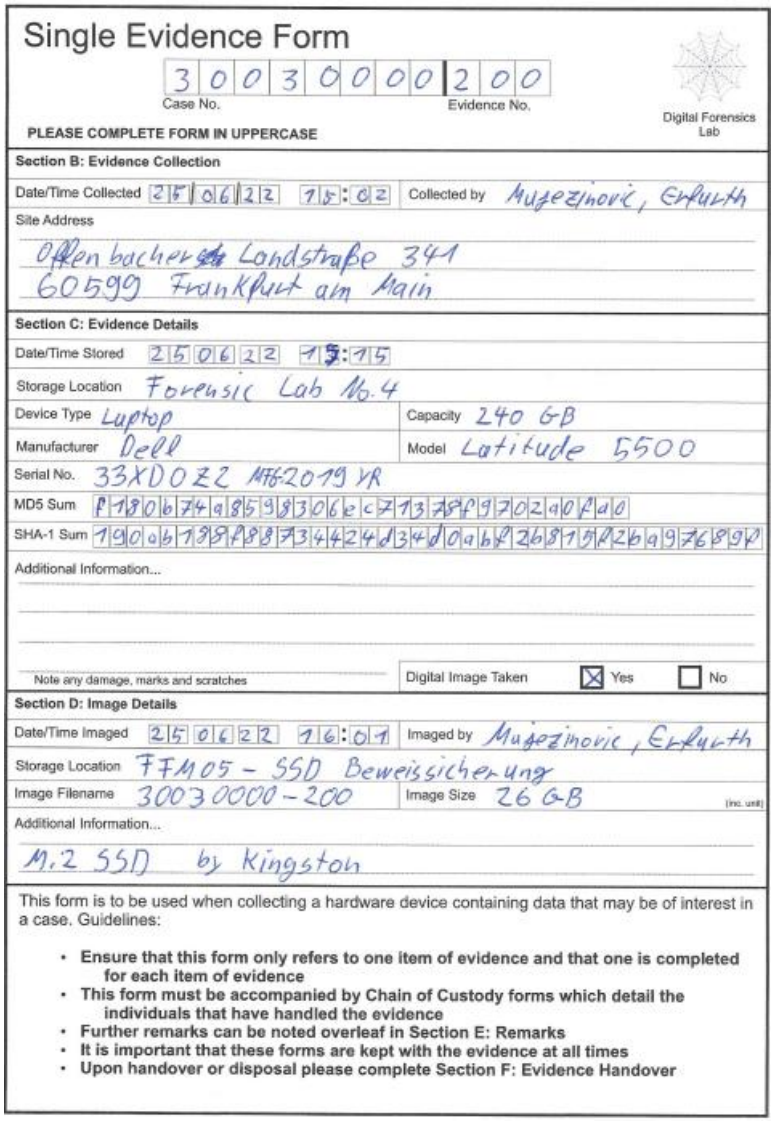
Date/Time	
Submitted by	Signature
Received by	Signature
Witnessed by	Signature

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 30030000
Evidence Number: 100
Unique description: USB Stick 16GB  Guido Nagel
Examiner: Erfurth Marcel & Mujezinovic Edin
Notes:

--------------------------------------------------------------

Information for X:\30030000-100\30030000-100:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1.912
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 30.720.001
[Physical Drive Information]
 Drive Model: ASolid USB USB Device
 Drive Serial Number: 000000000058
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 15000 MB
 Sector count:    30720001
[Computed Hashes]
 MD5 checksum:    3788728777939b8d2dbd48688f6c4dbc
 SHA1 checksum:   51911808675ca680345a652e6536af68d179f9fd

Image Information:
 Acquisition started:   Sat Jun 25 15:42:41 2022
 Acquisition finished:  Sat Jun 25 15:45:16 2022
 Segment list:
  X:\30030000-100\30030000-100.E01
  X:\30030000-100\30030000-100.E02

Image Verification Results:
 Verification started:  Sat Jun 25 15:45:16 2022
 Verification finished: Sat Jun 25 15:46:33 2022
 MD5 checksum:    3788728777939b8d2dbd48688f6c4dbc : verified
 SHA1 checksum:   51911808675ca680345a652e6536af68d179f9fd : verified
```

3.5.2 Untersuchung des Notebooks (Asservat-200)

Im Rahmen der Secure-Phase wurde anschließend das Notebook von Guido Nagel an seinem Arbeitsplatz gesichert. Das Notebook befand sich in ausgeschaltetem Zustand. Dies wurde dokumentiert, mit der Asservatennummer 200 versehen und in einem Beutel verschlossen.

Im Lab-4 der FFM-05 wurde die Festplatte entfernt und an dem Imagerechner angeschlossen. Es wurden zwei Images erstellt. Auf dessen Basis zu Beweisintegritätszwecken die Hashwerte berechnet und dokumentiert wurden. Die Erzeugung des Images kann dem Anhang entnommen werden.



Single Evidence Form

Case No. 30030000 Evidence No. 200

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected 25/06/22 15:02 Collected by Mujezinovic, Erfurth

Site Address

Offenbacher Landstraße 341
60599 Frankfurt am Main

Section C: Evidence Details

Date/Time Stored 25/06/22 15:15

Storage Location Forensic Lab No. 4

Device Type Laptop Capacity 240 GB

Manufacturer Dell Model Latitude 5500

Serial No. 33XDOZZ MF6-2019 VR

MD5 Sum f18067 4a859830 6ec713 8f97 02a0 fa0

SHA-1 Sum 190a6198 8873 4424 d34d 0a6b 2681 9a26 a976 89b

Additional Information...

Note any damage, marks and scratches

Digital Image Taken ☒ Yes ☐ No

Section D: Image Details

Date/Time Imaged 25/06/22 16:01 Imaged by Mujezinovic, Erfurth

Storage Location FFM05 - SSD Beweissicherung

Image Filename 30030000-200 Image Size 26 GB (inc. unit)

Additional Information...

M.2 SSD by Kingston

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence
- This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence
- Further remarks can be noted overleaf in Section E: Remarks
- It is important that these forms are kept with the evidence at all times
- Upon handover or disposal please complete Section F: Evidence Handover

Abbildung 7 - Single Evidence Form (Asservat-200)

Single Evidence Form

Digital Forensics Lab

Section E: Remarks

Festplatte musste aus dem Rechner ausgebaut werden und wurde über USB ausgewertet.

Section F: Evidence Handover / Disposal

Date/Time	
Submitted by	Signature
Received by	Signature
Witnessed by	Signature

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 30030000
Evidence Number: 200
Unique description: Laptop Dell Latitude 5500 240GB S120 Guido Nagel
Examiner: Erfurth Marcel & Mujezinovic Edin
Notes:

--------------------------------------------------------------

Information for X:\30030000-200\30030000-200:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 29.185
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 468.862.127
[Physical Drive Information]
 Drive Model: Generic Externa   SCSI Disk Device
 Drive Serial Number: 22222222222222220138
 Drive Interface Type: SCSI
 Removable drive: False
 Source data size: 228936 MB
 Sector count:    468862127
[Computed Hashes]
 MD5 checksum:    f180b74a8598306ec71378f9702a0fa0
 SHA1 checksum:   190ab188f88734424d34d0abf2b815f2ba97689f

Image Information:
 Acquisition started:   Sat Jun 25 16:01:35 2022
 Acquisition finished:  Sat Jun 25 16:18:21 2022
 Segment list:
  X:\30030000-200\30030000-200.E01
  X:\30030000-200\30030000-200.E02
  X:\30030000-200\30030000-200.E03
  X:\30030000-200\30030000-200.E04
  X:\30030000-200\30030000-200.E05
  X:\30030000-200\30030000-200.E06
  X:\30030000-200\30030000-200.E07
  X:\30030000-200\30030000-200.E08
  X:\30030000-200\30030000-200.E09
  X:\30030000-200\30030000-200.E10
  X:\30030000-200\30030000-200.E11
  X:\30030000-200\30030000-200.E12
  X:\30030000-200\30030000-200.E13
  X:\30030000-200\30030000-200.E14
  X:\30030000-200\30030000-200.E15
  X:\30030000-200\30030000-200.E16
  X:\30030000-200\30030000-200.E17
  X:\30030000-200\30030000-200.E18

Image Verification Results:
 Verification started:  Sat Jun 25 16:18:21 2022
 Verification finished: Sat Jun 25 16:42:14 2022
 MD5 checksum:    f180b74a8598306ec71378f9702a0fa0 : verified
 SHA1 checksum:   190ab188f88734424d34d0abf2b815f2ba97689f : verified
```

3.6 Untersuchungsergebnisse

Im Folgenden werden die Ergebnisse der forensischen Untersuchung zusammengefasst. Eine detaillierte Beschreibung der angewandten Methodik erfolgte in den vorhergehenden Kapiteln.

3.6.1 Untersuchungsergebnisse des USB-Stick (Asservat-100)

Auf dem USB-Stick wurden 1111 Artefakte gefunden.

ÜBEREINSTIMMENDE ERGEBNISSE 1.111	
VERFEINERTE SUCHE	**13**
Kennungen – Gerät	9
Kennungen –Personen	4
MEDIEN	**1.091**
Bilder	1.089
Videos	2
DOKUMENTE	**3**
PowerPoint-Dokumente	1
Word-Dokumente	2
BETRIEBSSYSTEM	**1**
Dateisystem-Info	1
BENUTZERDEFINIERT	**3**
Carved Archives (content not searched)	3

Abbildung 8 - Übersicht Artefakte USB-Stick (Asservat-100)

Bei dem Großteil davon (98%) handelt es sich um Bilder (1089 JPG-Dateien), auf denen Landschaften und Gebäude zu sehen sind. Der Aufnahmeort der Bilder konnte nicht bestimmt werden. Nach aktuellen Erkenntnissen sind die dort abgebildeten Landschaften und Gebäude jedoch nicht in unmittelbarer Nähe zum Firmenort der Speuer Sanitär Service GmbH.

Abbildung 9 - Thumbnails gefundener Bilder (Ausschnitt aus Asservat-100)

Die weiteren Bilder können dem Link im Anhang entnommen werden.

Zwei Worddateien (docx) und eine Powerpointdatei (pptx) stechen namentlich hervor:

Name	Typ	Letztes Änderungsdatum	Screenshot
Kündiung.docx	Word-Dokument	22.06.2022 18:57:22	
Qualifikationen.docx	Word-Dokument	22.06.2022 18:55:52	
Wichtig.pptx	PowerPoint-Dokument	22.06.2022 18:51:28	

Tabelle 4 - Kurzübersicht gefundener Dokumente (Asservat-100)

Bei der weiteren Untersuchung konnte kein erkennbarer Zusammenhang zwischen den gefundenen Dokumenten und der Speuer Sanitär Service GmbH hergestellt werden.

3.6.2 Untersuchungsergebnisse des Notebooks (Asservat-200)

Auf dem Notebook wurden 227.516 Artefakte gefunden.

ÜBEREINSTIMMENDE ERGEBNISSE	227.516
VERFEINERTE SUCHE	543
WEBBEZOGEN	31.688
KOMMUNIKATION	4
QQ	4
MEDIEN	38.570
E-MAIL UND KALENDER	102
E-Mail-Anhänge	32
EML(X) Dateien	2
Outlook Kontakte	4
Outlook E-Mails	8
Windows Mail	56
DOKUMENTE	12.607
WEITERE QUELLEN	1
ANWENDUNGSNUTZUNG	47
BETRIEBSSYSTEM	143.531
VERSCHLÜSSELUNG UND ZUGANGSDATEN	39
VERBUNDENE GERÄTE	28
STANDORT UND REISE	1
BENUTZERDEFINIERT	355

Abbildung 10 - Übersicht Artefakte Notebook (Asservat-200)

Laut Auftragsspezifikation soll geprüft werden, ob es (und welche) Kommunikation zwischen Guido Nagel und Paul Rotasch stattgefunden hat. Somit sind speziell die Bereiche „Email und Kalender“ (102 Artefakte) und „Webbezogen“ (31688 Artefakte) relevant.

Die versendeten und empfangenen Mails im Account von Guido Nagel zeigen vier versendete bzw. empfangene Mails an bzw. von Paul Rotasch:

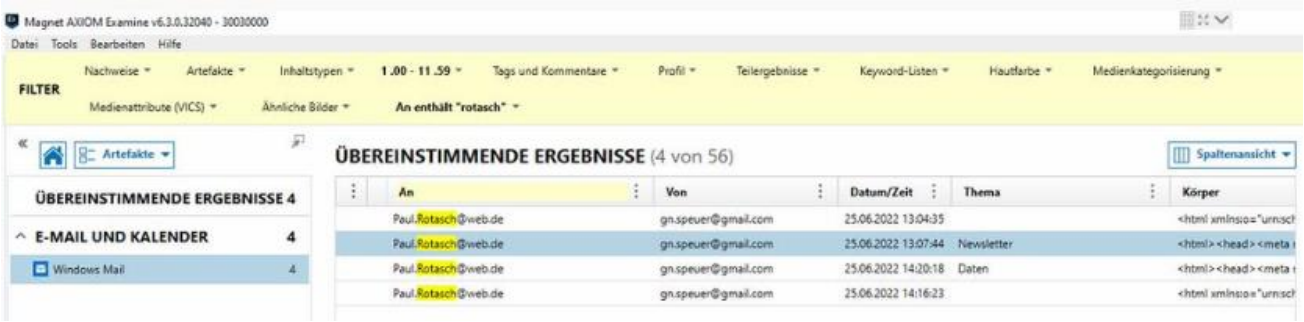


Abbildung 11 - Mails von / an Paul Rotasch

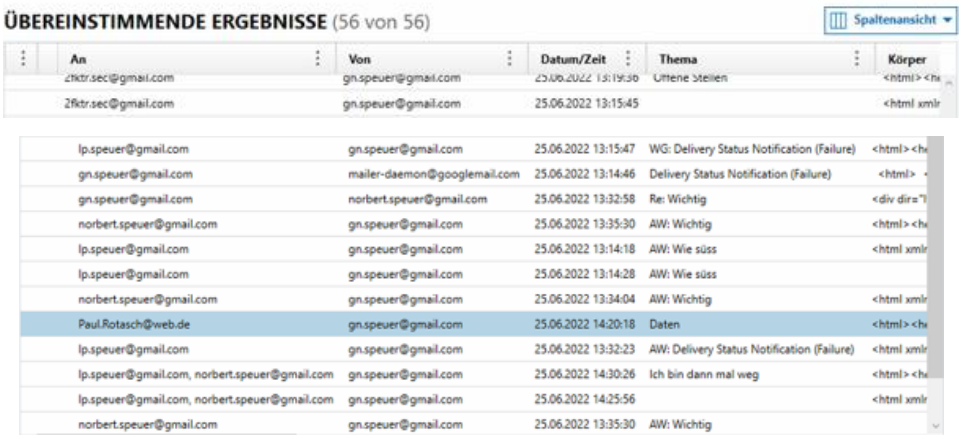
Drei dieser Mails handeln von dem Empfang eines Newsletters der Speuer Sanitär und Service GmbH, den Paul Rotasch nicht bekommen haben soll.

Die vierte Mail ist die Mail, die den Grund für die forensische Untersuchung darstellt.

Abbildung 12 - Mail an Paul Rotasch

Weitere vorhandene Mails zeigen einen erkennbaren Bezug zur täglichen Arbeit bzw. zum Kollegen-Socializing.

Alle Mails können dem Link im Anhang entnommen werden.



ÜBEREINSTIMMENDE ERGEBNISSE (56 von 56) Spaltenansicht

An	Von	Datum/Zeit	Thema	Körper
2fktr.sec@gmail.com	gn.speuer@gmail.com	25.06.2022 13:19:36	Offene Stellen	<html> <h
2fktr.sec@gmail.com	gn.speuer@gmail.com	25.06.2022 13:15:45		<html xmlr
lp.speuer@gmail.com	gn.speuer@gmail.com	25.06.2022 13:15:47	WG: Delivery Status Notification (Failure)	<html> <h
gn.speuer@gmail.com	mailer-daemon@googlemail.com	25.06.2022 13:14:46	Delivery Status Notification (Failure)	<html>
gn.speuer@gmail.com	norbert.speuer@gmail.com	25.06.2022 13:32:58	Re: Wichtig	<div dir="l
norbert.speuer@gmail.com	gn.speuer@gmail.com	25.06.2022 13:35:30	AW: Wichtig	<html> <h
lp.speuer@gmail.com	gn.speuer@gmail.com	25.06.2022 13:14:18	AW: Wie süss	<html xmlr
lp.speuer@gmail.com	gn.speuer@gmail.com	25.06.2022 13:14:28	AW: Wie süss	
norbert.speuer@gmail.com	gn.speuer@gmail.com	25.06.2022 13:34:04	AW: Wichtig	<html xmlr
Paul.Rotasch@web.de	gn.speuer@gmail.com	25.06.2022 14:20:18	Daten	<html> <h
lp.speuer@gmail.com	gn.speuer@gmail.com	25.06.2022 13:32:23	AW: Delivery Status Notification (Failure)	<html xmlr
lp.speuer@gmail.com, norbert.speuer@gmail.com	gn.speuer@gmail.com	25.06.2022 14:30:26	Ich bin dann mal weg	<html> <h
lp.speuer@gmail.com, norbert.speuer@gmail.com	gn.speuer@gmail.com	25.06.2022 14:25:56		<html xmlr
norbert.speuer@gmail.com	gn.speuer@gmail.com	25.06.2022 13:35:30	AW: Wichtig	

Abbildung 13 - Auszug Mails (Asservat-200)

Die Artefakte im Bereich „Webbezogen“ zeigen keine Anhaltspunkte, dass Daten das Netzwerk verlassen haben könnten und zeigen keinerlei Kontaktaufnahme zu Paul Rotasch.

Weitere Details zu den gefundenen Artefakten können dem Link im Anhang entnommen werden.

3.6.3 Timeline

Anhand der Timeline kann allgemein ein Vorfall zeitlich rekonstruiert werden. In diesem Fall ist zu beachten, dass die Timeline nur in Zusammenhang mit dem USB-Stick und der verdächtigen Mail erstellt worden ist.

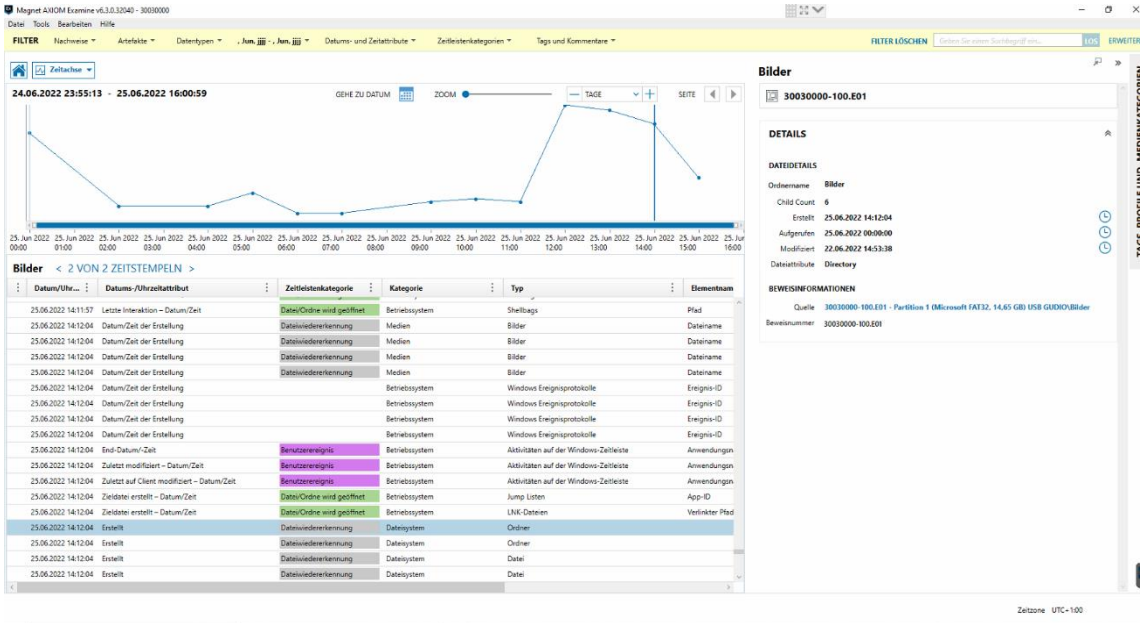
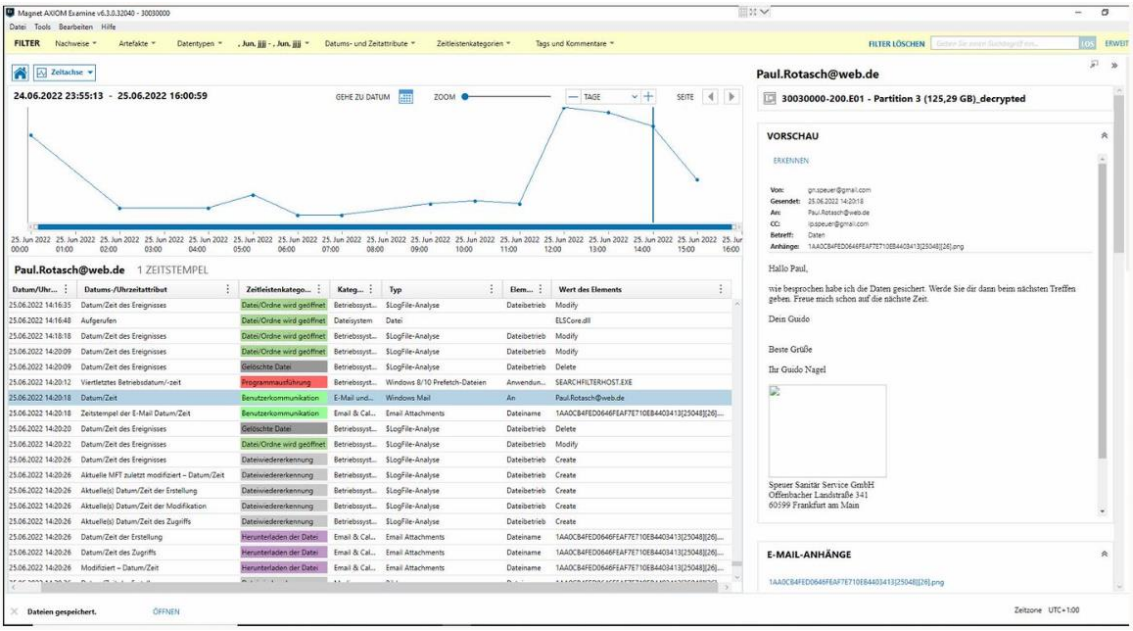


Abbildung 14 - Timeline USB-Stick / Mail



Anhand der Timeline erkennt man, dass Daten des USB-Sticks gesichert und der USB-Stick formatiert wurde. Anschließend wurden 1091 Bilder und 3 Office-Dokumente transferiert. Aufgrund der großen Datenmenge sind alte Dateifragmente vom USB-Stick nicht mehr zu rekonstruieren.

Zeitpunkt	Asservat	Aktion
25.06.2022 14:05:11	Asservat-100 an Asservat-200 (USB-Stick an Notebook)	USB angeschlossen
25.06.2022 14:06:21	Asservat-200 (Notebook)	Erstellung des lokalen Ordner „Sticks“
25.06.2022 14:06:41	Asservat-200 an Asservat-100 (Notebook an USB-Stick)	Verschieben der Daten vom USB-Stick auf den lokalen Ordner "Stick"
25.06.2022 14:11:26	Asservat-100 (USB-Stick)	Formatierung USB-Stick
25.06.2022 14:12:04	Asservat-100 (USB-Stick)	Transfer 1091 JPG-Dateien, 2 Word-Dateien und 1 Powerpoint-Datei
25.06.2022 14:20:18	Asservat-200 (Notebook)	Versand der verdächtigen Mail an Paul Rotasch
25.06.2022 14:23:00	Asservat-100 von Asservat-200 (USB-Stick von Notebook)	Abziehen des USB Sticks vom Rechner
25.06.2022 14:23:47	Asservat-200 (Notebook)	Löschen von lokalen Dateien
25.06.2022 14:30:26	Asservat-200 (Notebook)	Verabschiedungsmail an Norbert Speuer
25.06.2022 14:32:16	Asservat-200 (Notebook)	Herunterfahren des Rechners

Tabelle 5 - Timeline Handlung Guido Nagel (25.06.2022)

Die Timeline kann dem Anhang entnommen werden.

3.6.4 Schlussfolgerungen

Das von der FFM-05 erstellte Gutachten listet die Erkenntnisse auf, welche aus den Asservaten anhand der in der Auftragsspezifikation übermittelten Fragestellungen erlangt werden konnten.

Frage 1:

Sind auf dem USB-Stick Firmengeheimnisse vorhanden? Wenn ja, welche?

Antwort zu Frage 1:

Bei der forensischen Untersuchung konnte diverses Datenmaterial auf dem USB-Stick (Asservate-100) aufgefunden werden, welches jedoch nicht geeignet ist als Beweismittel zum Vorwurf der Betriebsspionage verwendet zu werden.

Auf dem USB-Stick (Asservate-100) wurden keine Firmenunterlagen gefunden. Es wurden 1091 JPG-Dateien aufgefunden, die Landschaften und Gebäude zeigen.

Frage 2:

Wurden Firmendaten vom Notebook gelöscht? Wenn ja, welche?

Antwort zu Frage 2:

Es wurden keine Firmendaten von Guido Nagels Notebook (Asservat-200) gelöscht. Gelöscht wurde der private Ordner von Guido Nage. Inhalt dieses Ordners waren die auf dem USB-Stick gesicherten Fotos.

Frage 3:

Sind auf dem Notebook weitere Spuren zur Kommunikation zwischen Guido Nagel und Paul Rotasch vorhanden?

Antwort zu Frage 3:

Zwischen dem Beschuldigten Guido Nagel und Paul Rotasch kann aufgrund des vorliegenden Datenmaterials eine Verbindung im aufgezeigten Zeitraum nachgewiesen werden. Es wurden vier Mails von Guido Nagel sichergestellt, bei der eine Mailadresse von Paul Rotasch als Empfänger oder Absender eingetragen war. Ob es sich dabei um eine Mailadresse des Mitbewerbers Paul Rotasch handelt, konnte nicht festgestellt werden.

25.06.22, 14:20 Gmail - Daten

Gmail Lisa Pantlof <lp.speuer@gmail.com>

Daten
1 Nachricht

Guido Nagel <gn.speuer@gmail.com> 25. Juni 2022 um 14:20
An: "Paul.Rotasch@web.de" <Paul.Rotasch@web.de>
Cc: "lp.speuer@gmail.com" <lp.speuer@gmail.com>

Hallo Paul,

wie besprochen habe ich die Daten gesichert. Werde Sie dir dann beim nächsten Treffen geben. Freue mich schon auf die nächste Zeit.

Dein Guido

Beste Grüße

Ihr Guido Nagel

Speuer Sanitär Service

Speuer Sanitär Service GmbH
Offenbacher Landstraße 341
60599 Frankfurt am Main

Tel.: 069 174 577 234
E-Mail: gn.speuer@gmail.com
Web: WWW.speuer-sani.de

Abbildung 15 - Kommunikation Guido Nagel ./. Paul Rotasch

Es wurden keine Hinweise zu Straftaten gefunden werden, die im engeren oder weiteren Sinne mit dem Vorwurf der Betriebsspionage in Verbindung gebracht werden konnten.

3.7 Abschließende Bemerkungen

Die Gutachten werden von unseren hochqualifizierten Sachverständigen und IT-Forensik-Experten erstellt, die über langjährige Erfahrung verfügen. Jedes IT-Forensik-Gutachten wird bei FFM-05 standardmäßig durch einen zweiten, nicht an der Auswertung beteiligten Sachverständigen, überprüft.
Unsere Gutachter sind bei der Erstellung der einzelnen Gutachten absolut, unparteiisch, objektiv und weisungsfrei.
Alle unsere IT-Forensik-Gutachten sind gerichtsfest, d.h. sie gelten vor Gericht als Beweismittel und sind ein wertvolles Hilfsmittel bei der Wahrheitsfindung in Prozessen.

4 WIKI-Artikel DLP

(https://it-forensik.fiw.hs-wismar.de/index.php/DLP)

Definition

Hinter dem Akronym DLP werden die Begriffe „Data Leakage Prevention“ oder auch „Data Loss Prevention“ verstanden. Beide Begriffe werden im Allgemeinen synonym verwendet. In Fachkreisen hingegen werden die beiden Begriffe manchmal jedoch differenziert:

In diesen Fällen bezeichnet „Data Loss Prevention“ den Schutz vor unerwünschtem Abfluss von Daten, der Schaden verursacht. Im Gegensatz zur „Data Leakage Prevention“ wird dieser Abfluss allerdings bemerkt. „Data Leakage Prevention“ hingegen bezeichnet den Schutz vor einem potenziellen Abfluss von Daten. Diesen Abfluss kann man nicht messen und manchmal sogar noch nicht einmal feststellen.

Beiden Begriffen ist jedoch gemein, dass ein ungewollter Datenabfluss verhindert werden soll.

Beim Begriff „DLP“ handelt es sich ursprünglich um einen Marketingbegriff - eine wissenschaftliche Definition des Begriffes „DLP“ existiert nicht.

Funktionen und Funktionsweise:

Das Konzept von DLP geht davon aus, dass andere Schutzmechanismen wie Virenscanner oder Firewall versagen und deshalb das DLP-System eingreifen muss. Dies bedeutet, dass das DLP-System eine Vielzahl von Aufgaben und Funktionen haben kann:

- Überwachung von Applikationen
- Erkennung gefährlicher Applikationen
- Überwachung von Datentransfers
- Durchsetzung von Richtlinien beim Datenaustausch
- Unterscheidung zwischen sensiblen und unkritischen Daten
- Blockierung der Übertragung sensibler Daten
- zentrale Erfassung der Datenbewegungen
- Alarmierung bei kritischen Regelverstößen
- usw.

Zusammengefasst bedeutet dies, dass DLP-Systeme sensible Daten identifizieren, Datenabflüsse protokollieren und möglichst den Abfluss sensibler Daten verhindern können müssen.

Um Datenabflüsse zu erkennen, werden verschiedene Scan-Methoden durchgeführt:

- Regelbasiertes Matching
  Es wird nach Daten gesucht, die einem bestimmten Muster entsprechen z.B. IBAN, BIC.

- Exact File Matching
  Dateien werden anhand ihres Hash-Wertes erkannt. Die Untersuchung erfolgt also nicht auf Dateiinhalte.

- Exact Data Matching
  Kombinationen von Daten werden in einem Index zusammengefasst z.B. Name, Vorname, Adresse. Es wird nach diesen Daten in einer beliebigen Reihenfolge in einem maximal vorgegebenen Abstand gesucht.

- Formulare
  Dateien werden auf eine vorgegebene Struktur / Muster hin untersucht z.B. Gehaltsabrechnungen.

- Dateitypen
  Spezielle Dateitypen dürfen das Netzwerk des Unternehmens nicht verlassen z.B. Konstruktionspläne

- Maschinelles Lernen
  Anhand von vielen Beispielen wird der Matcher trainiert, um selbstständig Entscheidungen zu treffen. Dieses Vorgehen kann bspw. bei der Erkennung von Quellcode genutzt werden.

- usw.

Anwendungsbereiche

In der heutigen Zeit können Daten auf viele verschiedene Arten gespeichert und ausgetauscht werden. In diesem Zusammenhang unterscheidet man

- Data in Use / Daten in Benutzung
  Es handelt sich hierbei um Daten, die zum Zeitpunkt des Abflusses aktiv genutzt werden, z.B. Daten im RAM, Cache oder CPU-Registern.

- Data in Motion / Daten in Bewegung
  Es handelt sich hierbei um Daten, die zum Zeitpunkt des Abflusses über ein Netzwerk versendet werden, z.B. Emails oder Uploads.

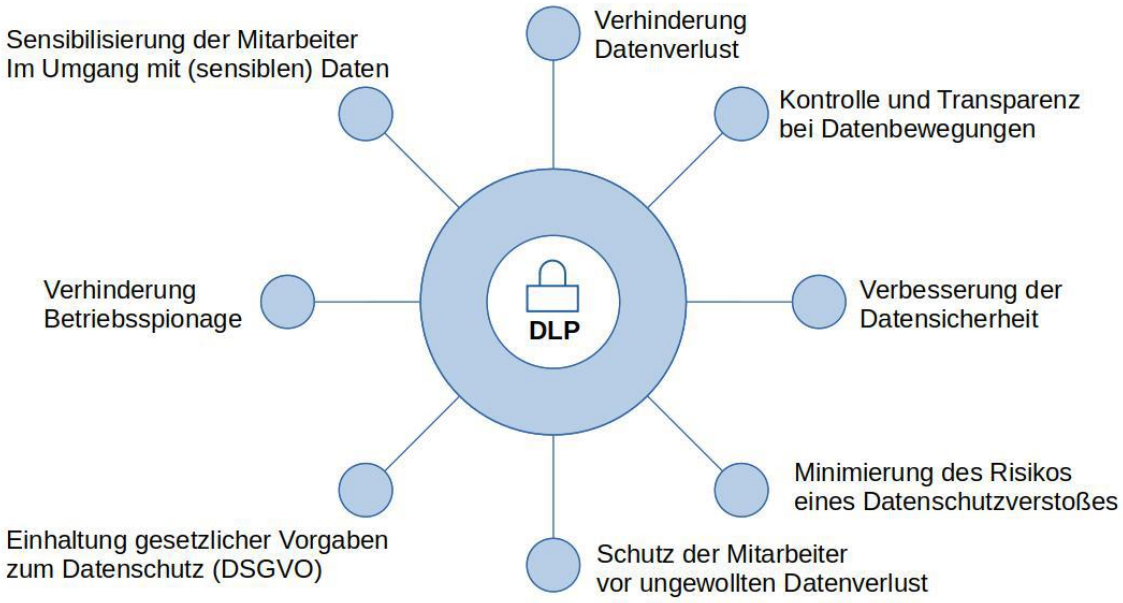
- Data at Rest / Daten im Ruhezustand
  Es handelt sich hierbei um Daten, die eigentlich zum Zeitpunkt des Abflusses ungenutzt wären, jedoch für den Abfluss verwendet werden z.B. Dateien, Datenbanken Backups.

All diese Arten sind dazu geeignet Daten abfließen zu lassen und Datentransaktionen in diesen Bereichen müssen somit überwacht werden.

- USB-Sticks
- Speicherkarten
- externe Festplatten
- E-Mails
- Netzlaufwerke
- Uploads in bspw. Cloud-Applikationen
- Smartphones
- Tablets
- Multifunktionsdrucker
- Cut & Paste / Printscreen

Durch die verstärkte Möglichkeit mobil zu arbeiten und so unbeobachtet die Daten vom Bildschirm abzufotografieren, gibt es einen Weg, der nicht oder nur mit großem Aufwand erkannt werden kann.

Vorteile beim Einsatz von DLP



Datendiebstahl-Vorfälle:

Seitdem Daten eine neue Form der Währung sind, häufen sich die Vorfälle von Datendiebstählen.

Anbei ein kleiner Auszug an bekannten Vorfällen, bei dem die Prävention nicht gegriffen hat:

- AOL-Accountdaten, 2004
- Steuerdaten der LGT Bank, 2006
- Steuerdaten der Credit Suisse, 2010
- Steuerdaten der UBS, 2012
- Sicherheitsrelevante Informationen des Flughafens London Heathrow, 2017
- usw.

Hinderungsgründe

Neben den Kosten und den üblichen technischen Problemen, die bei Einführung eines neuen Systems auftreten können, muss bei einer DLP-Einführung auf den Datenschutz im Allgemeinen, den Arbeitnehmerdatenschutz im Speziellen und die daraus resultierende Abstimmung mit dem Betriebsrat geachtet werden.

Quellen:

https://www.diva-portal.org/smash/get/diva2:1026824/FULLTEXT02

http://www.fim.uni-linz.ac.at/diplomarbeiten/Masterarbeit_BauerSimon.pdf

https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention

https://de.wikipedia.org/wiki/Data_Loss_Prevention

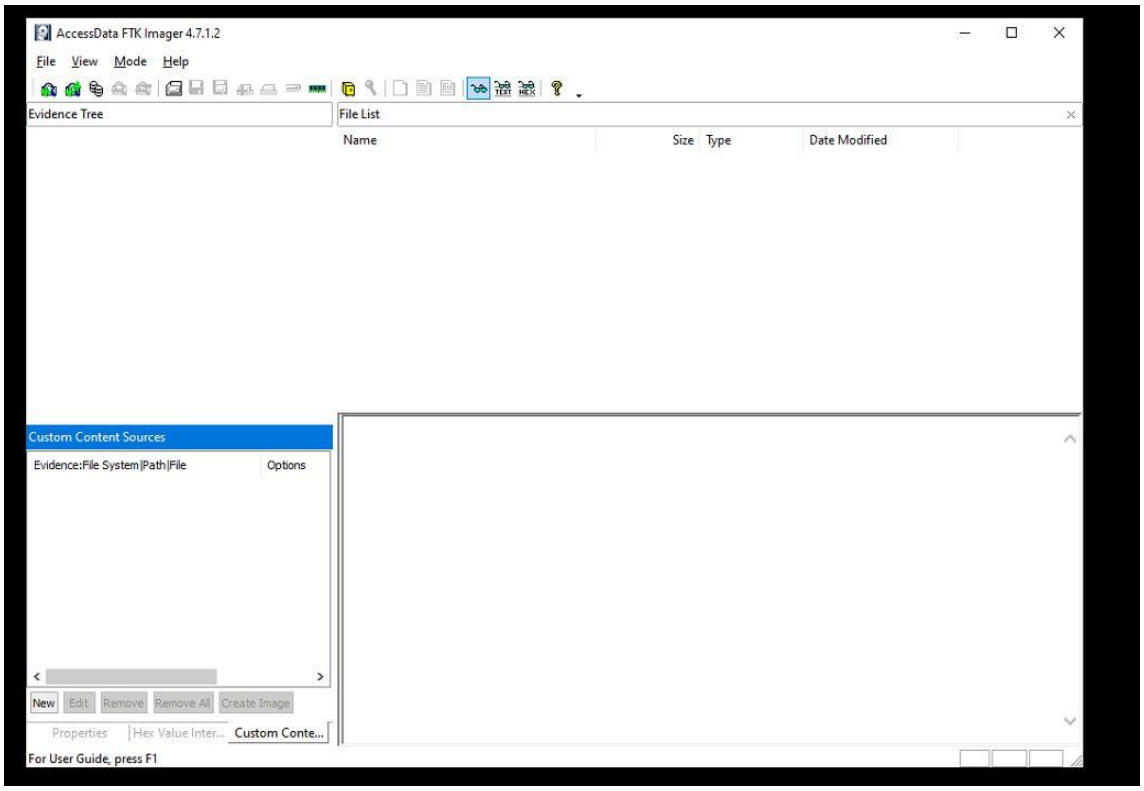
https://de.wikipedia.org/wiki/Liste_von_Datendiebst%C3%A4hlen

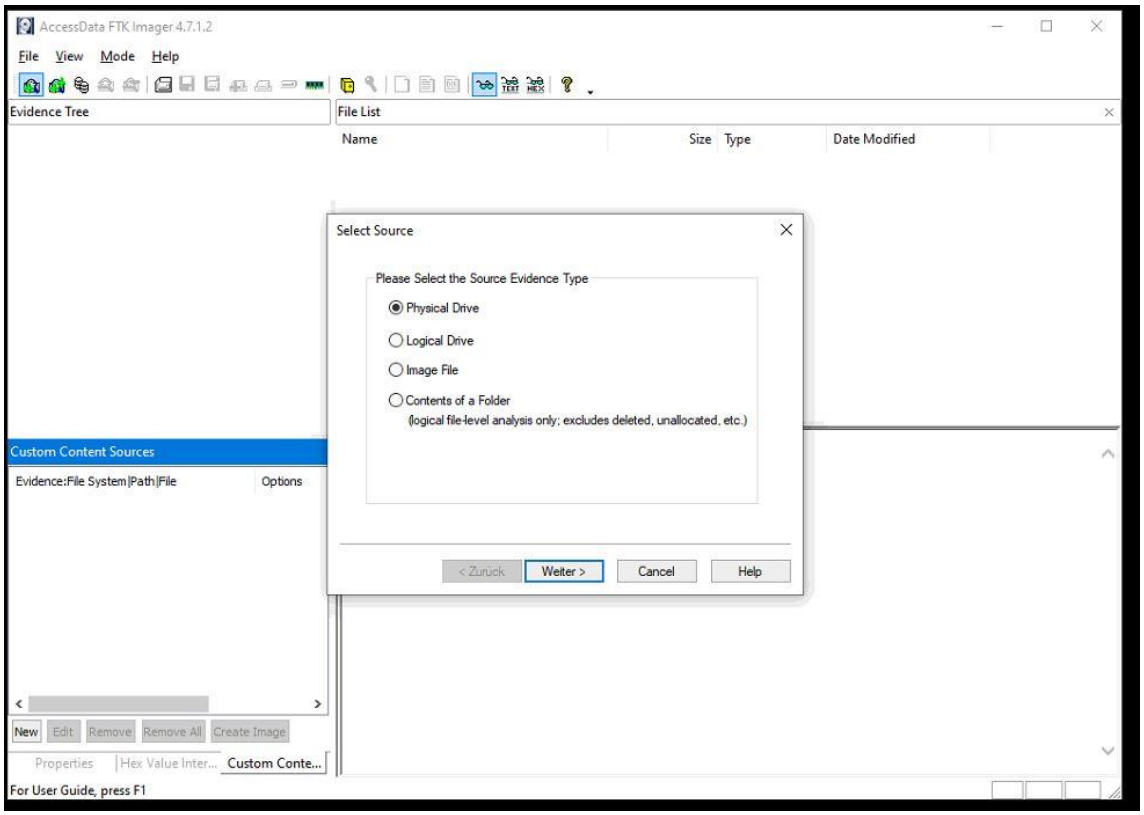
Abbildungsverzeichnis

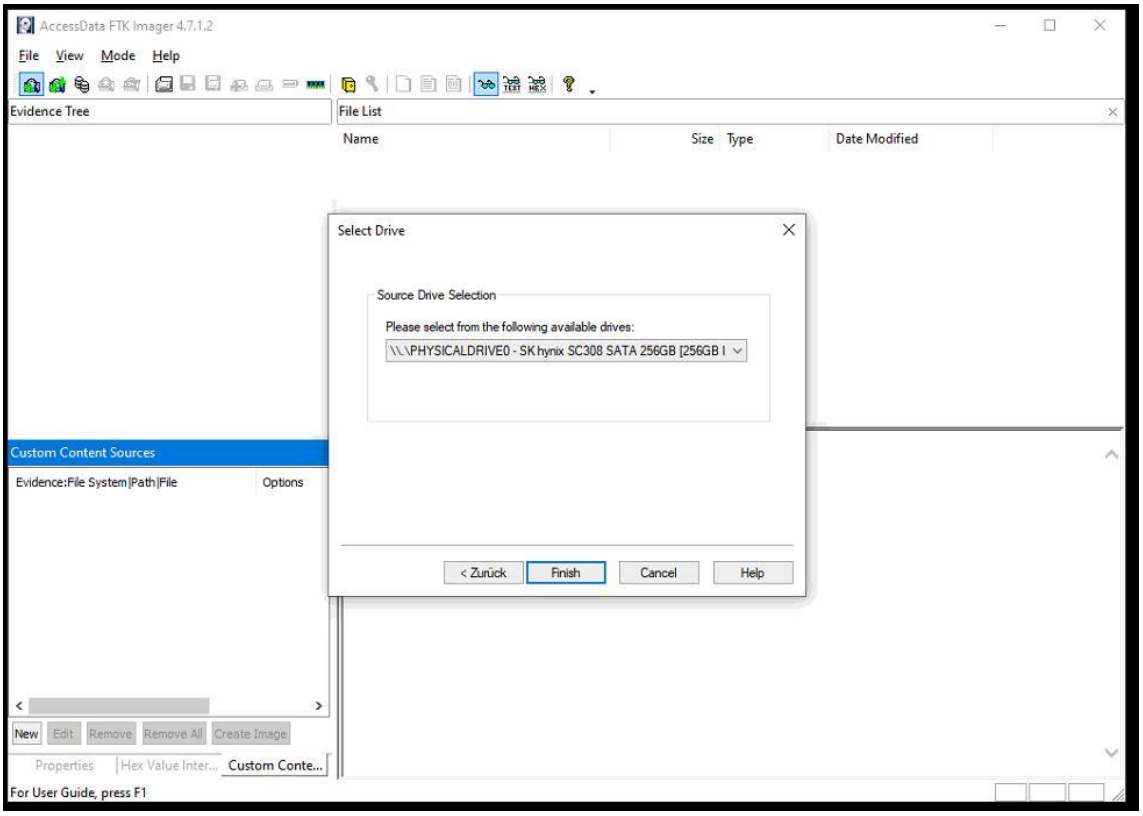
Tabellenverzeichnis

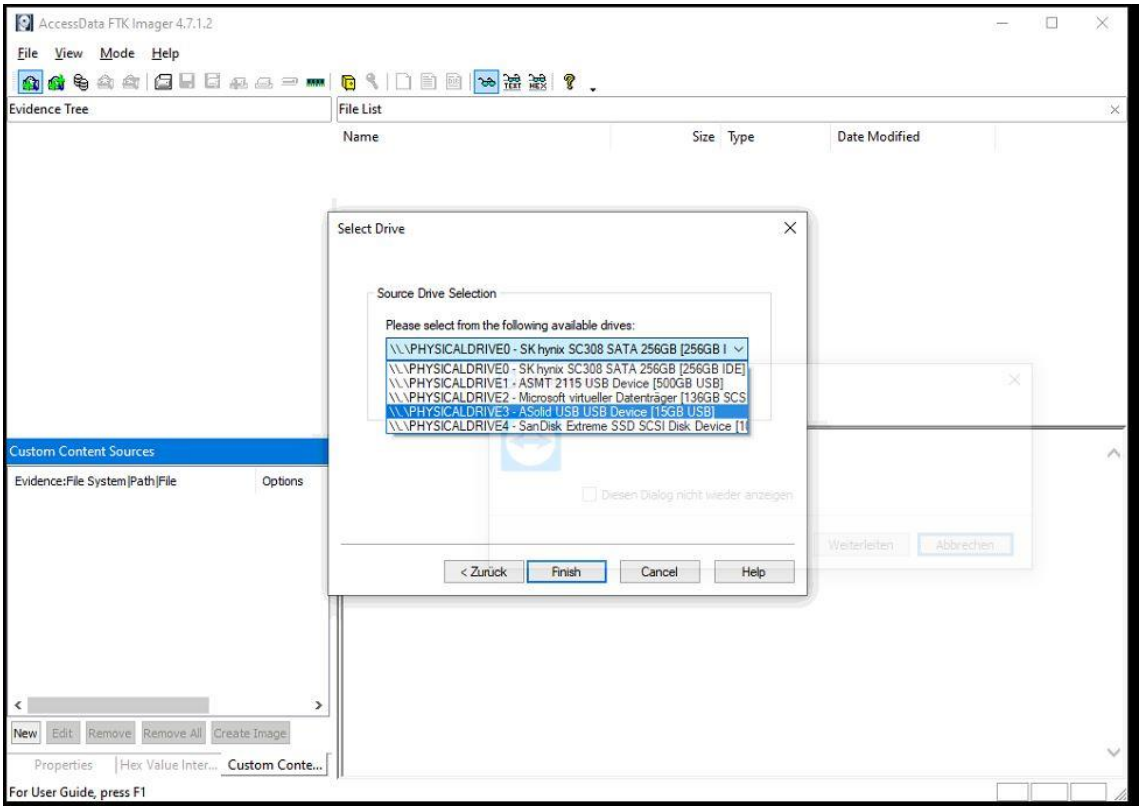
Anlagen

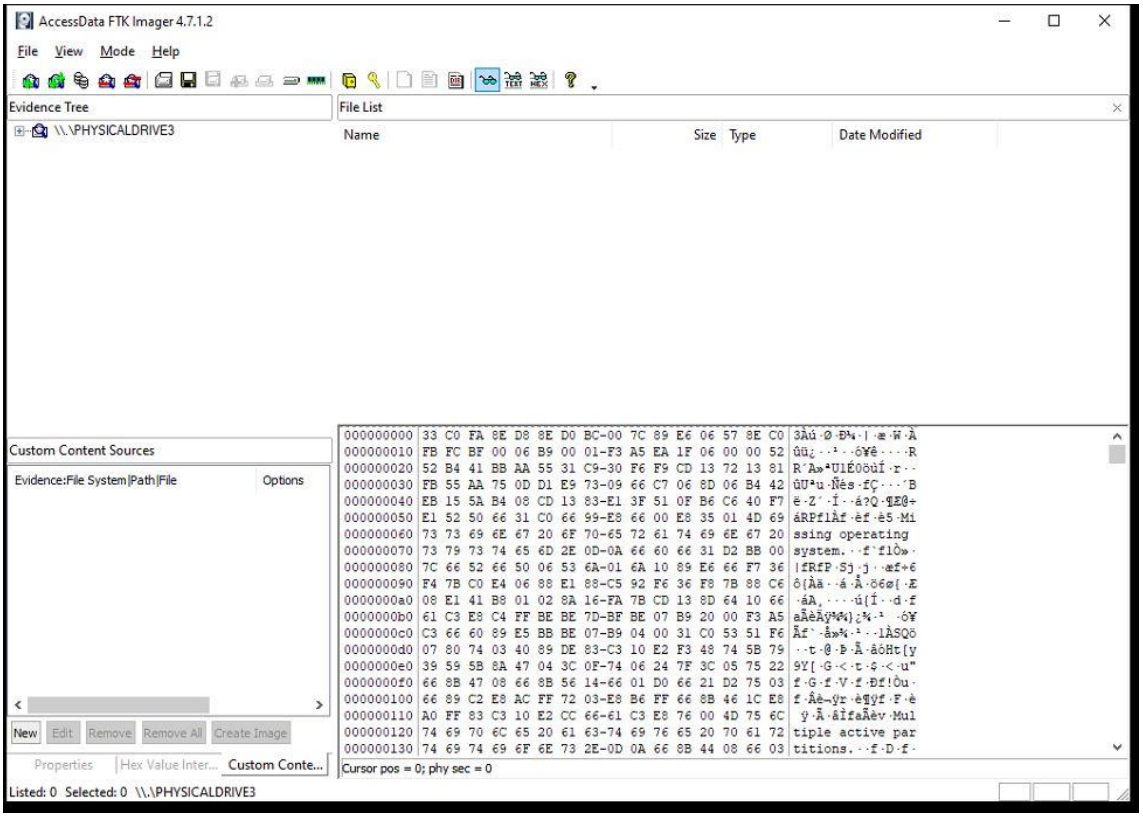
Vorgehen bei der Erstellung des Image Asservat-100 USB-Stick (FTK Imager)

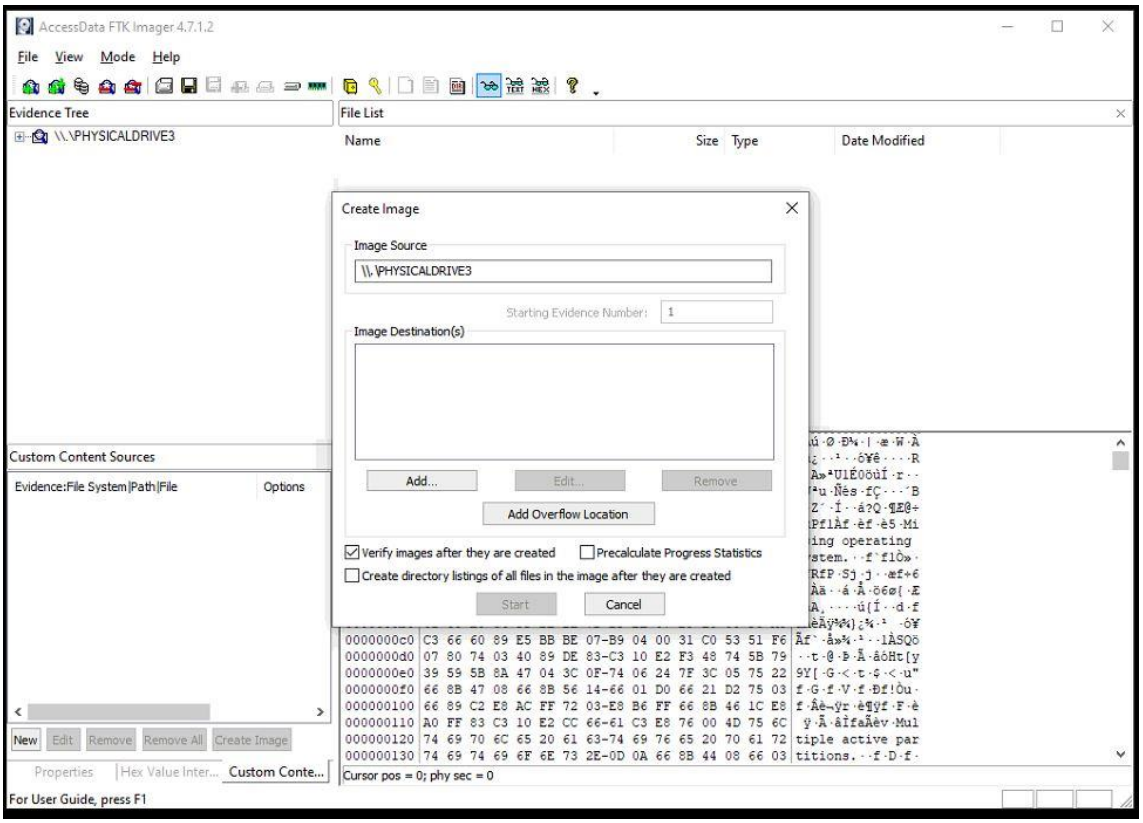


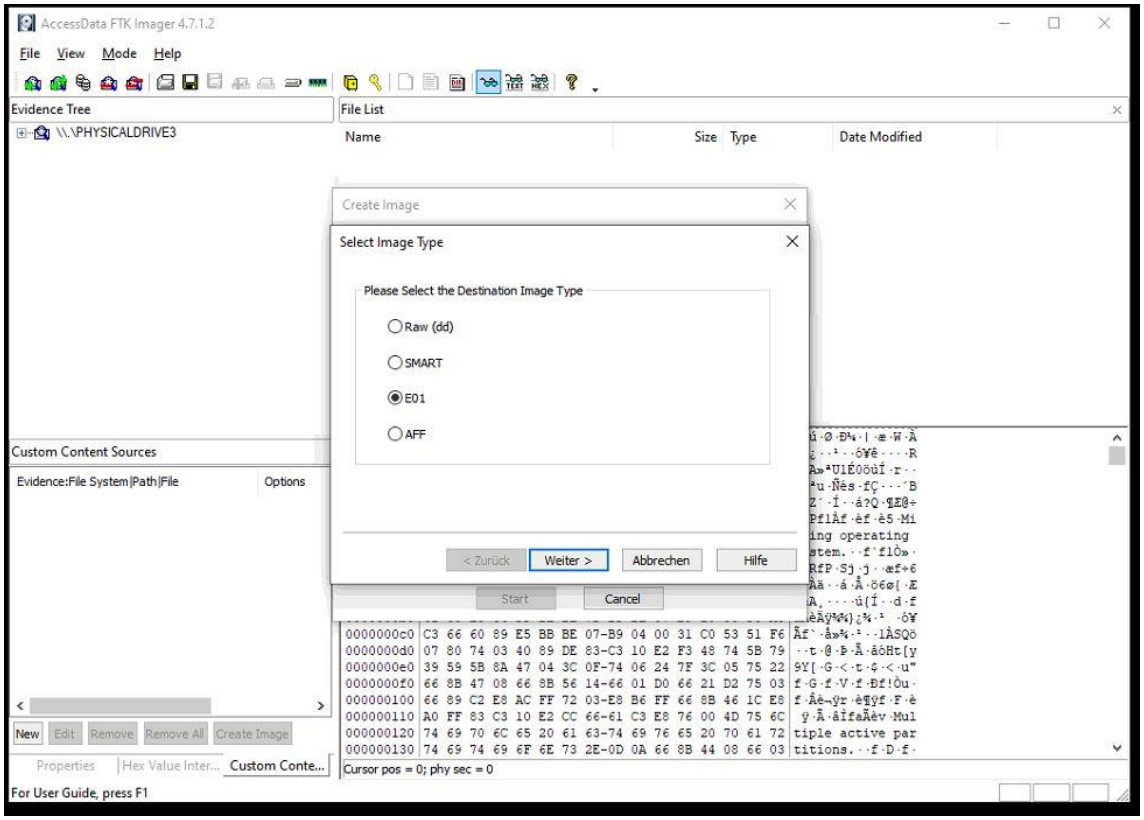


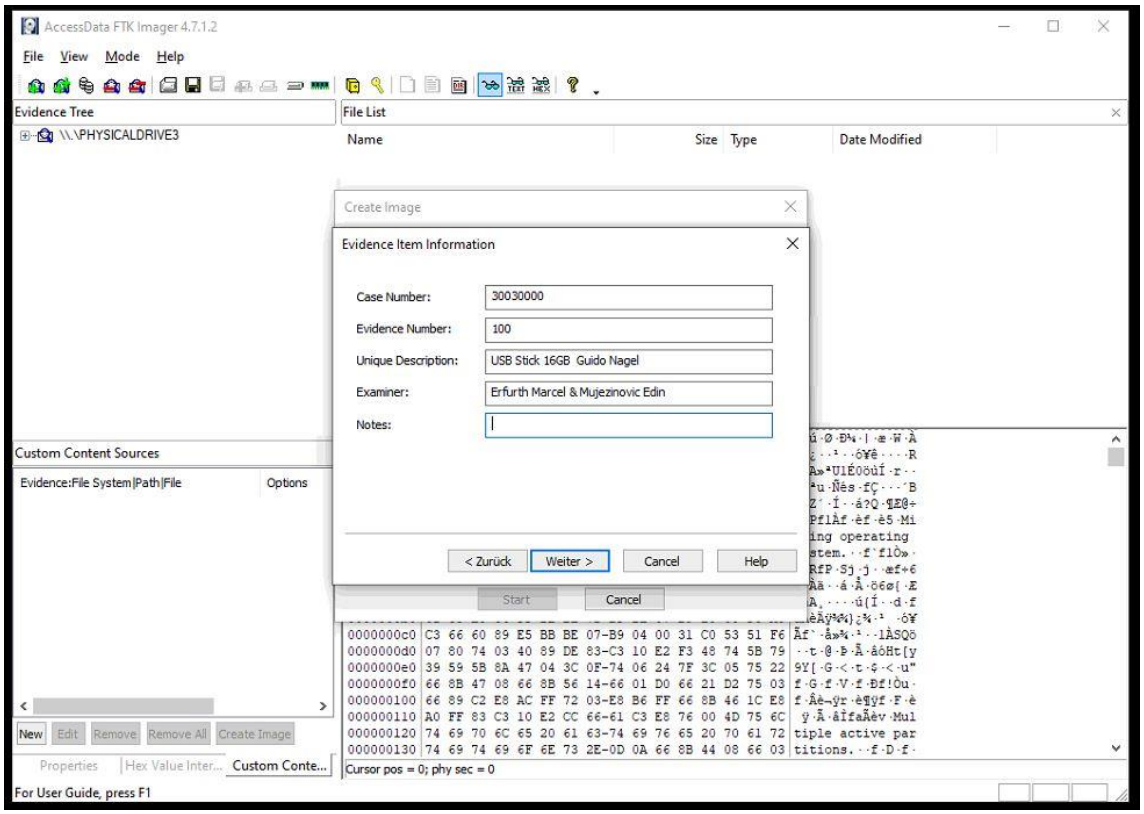

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE0 - SK hynix SC308 SATA 256GB [256GB I
< Zurück
Finish
Cancel
Help
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
For User Guide, press F1

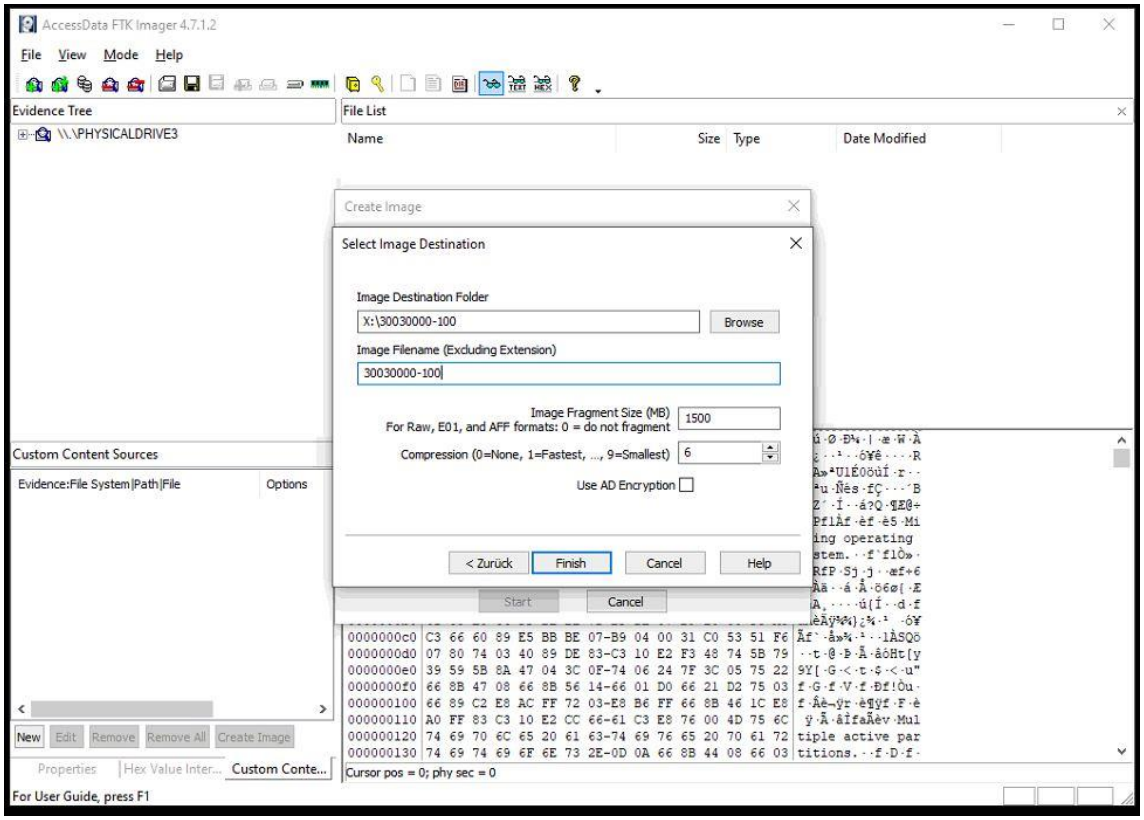

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE0 - SK hynix SC308 SATA 256GB [256GB I
\\.\PHYSICALDRIVE0 - SK hynix SC308 SATA 256GB [256GB IDE]
\\.\PHYSICALDRIVE1 - ASMT 2115 USB Device [500GB USB]
\\.\PHYSICALDRIVE2 - Microsoft virtueller Datenträger [136GB SCS
\\.\PHYSICALDRIVE3 - ASolid USB USB Device [15GB USB]
\\.\PHYSICALDRIVE4 - SanDisk Extreme SSD SCSI Disk Device [1
< Zurück
Finish
Cancel
Help
Diesen Dialog nicht wieder anzeigen
Weiterleiten
Abbrechen
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
For User Guide, press F1

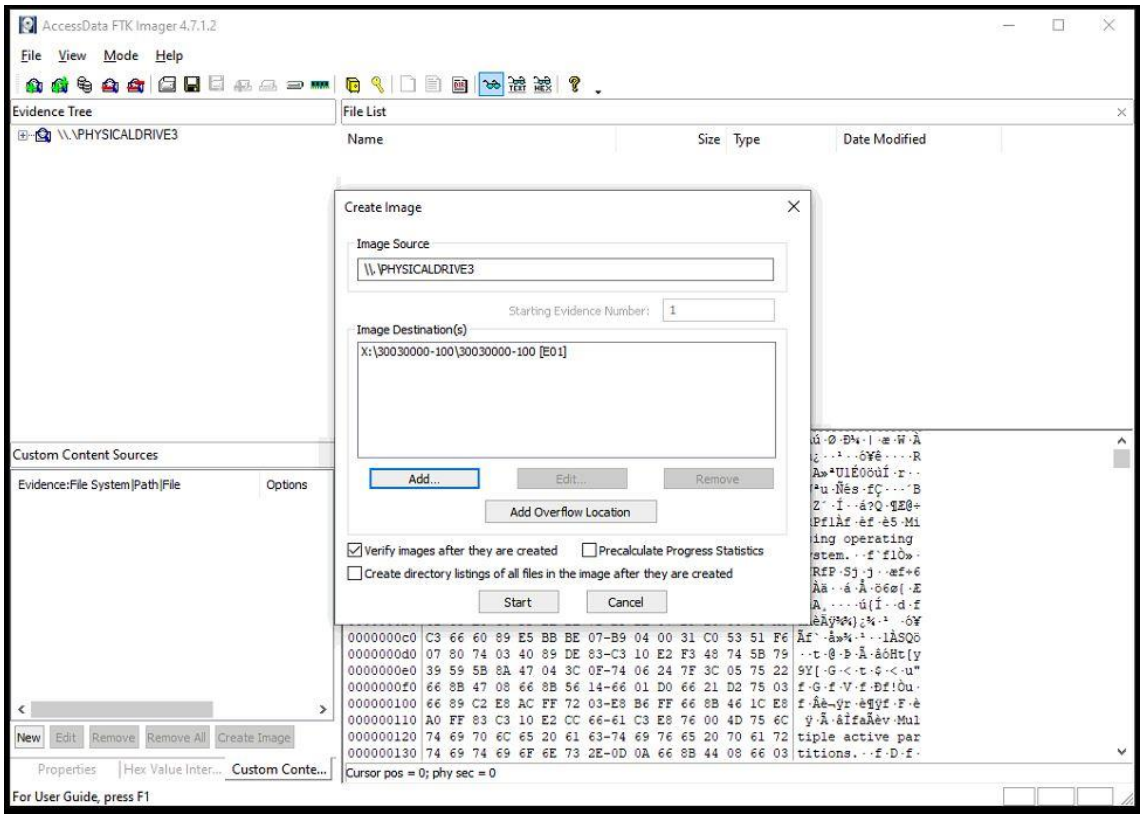

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE3
File List
Name Size Type Date Modified
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Cursor pos = 0; phy sec = 0
Listed: 0 Selected: 0 \\.\PHYSICALDRIVE3

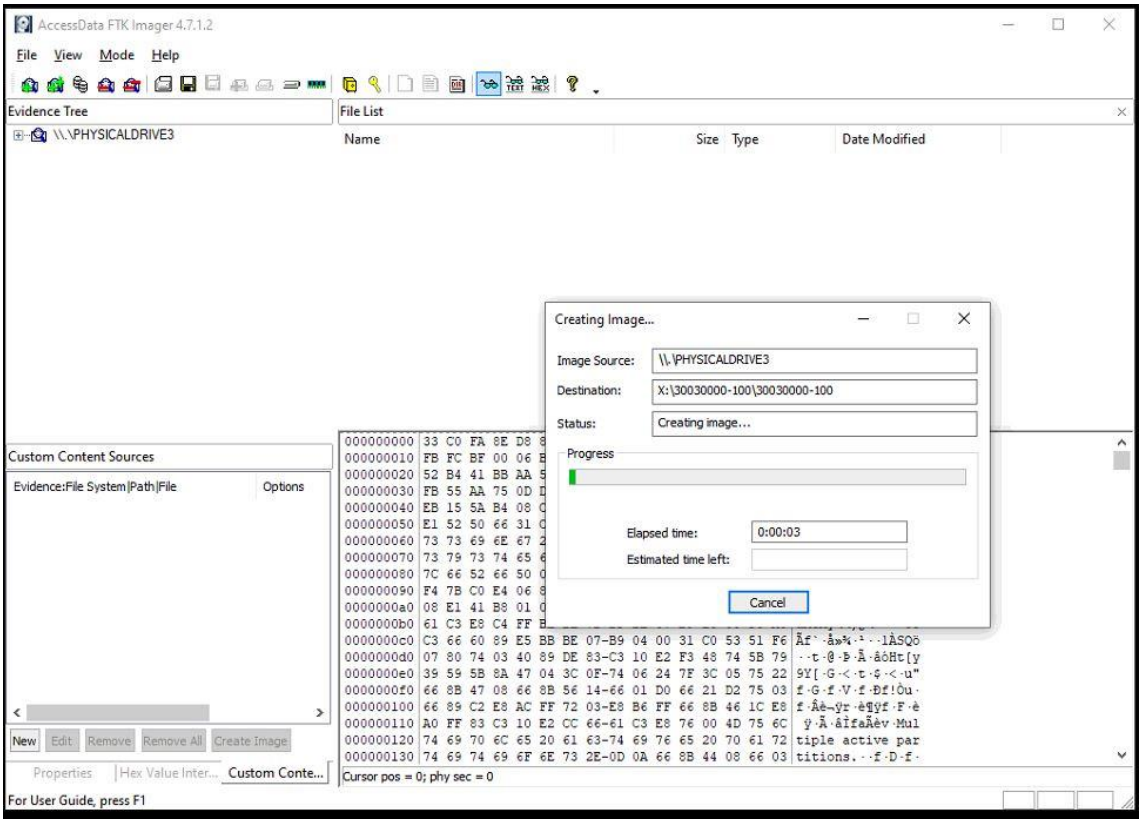

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE3
File List
Name Size Type Date Modified
Create Image
Image Source
\\.\PHYSICALDRIVE3
Starting Evidence Number: 1
Image Destination(s)
Add... Edit... Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start Cancel
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Cursor pos = 0; phy sec = 0
For User Guide, press F1

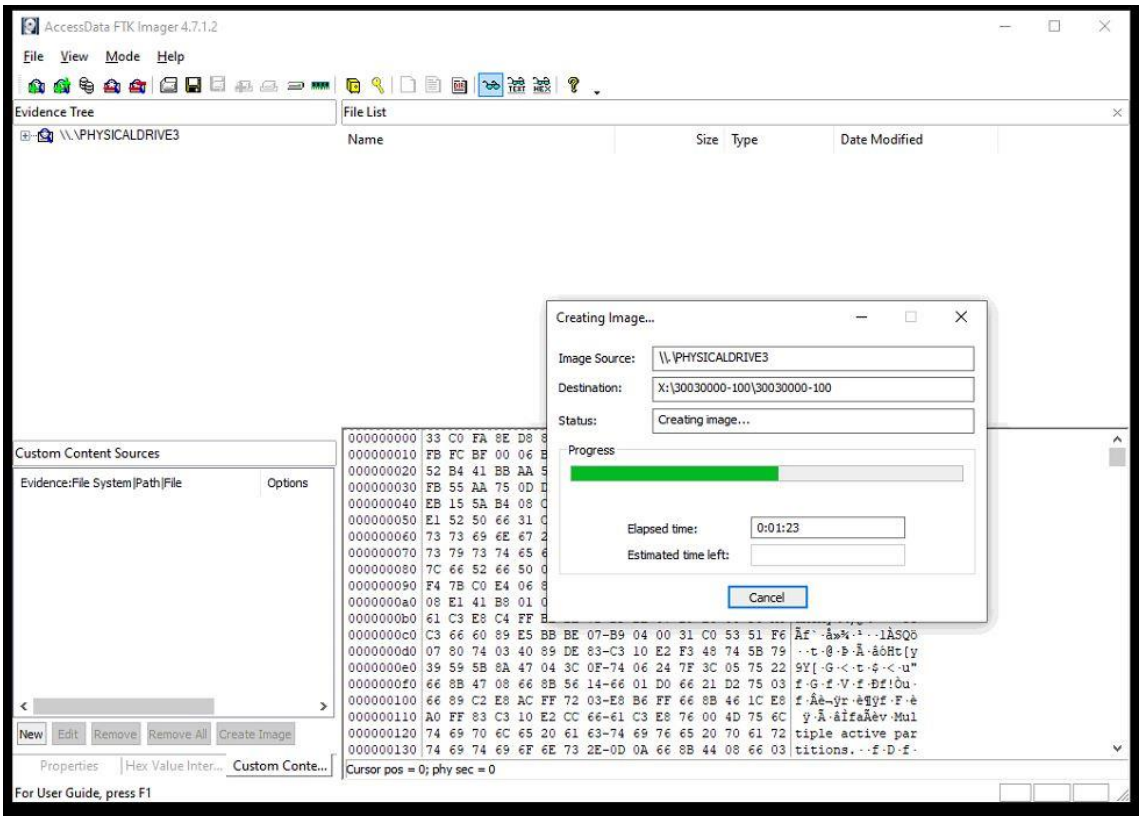

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
\\.\PHYSICALDRIVE3
Name
Size
Type
Date Modified
Create Image
Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Zurück
Weiter >
Abbrechen
Hilfe
Start
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
Cursor pos = 0; phy sec = 0
For User Guide, press F1

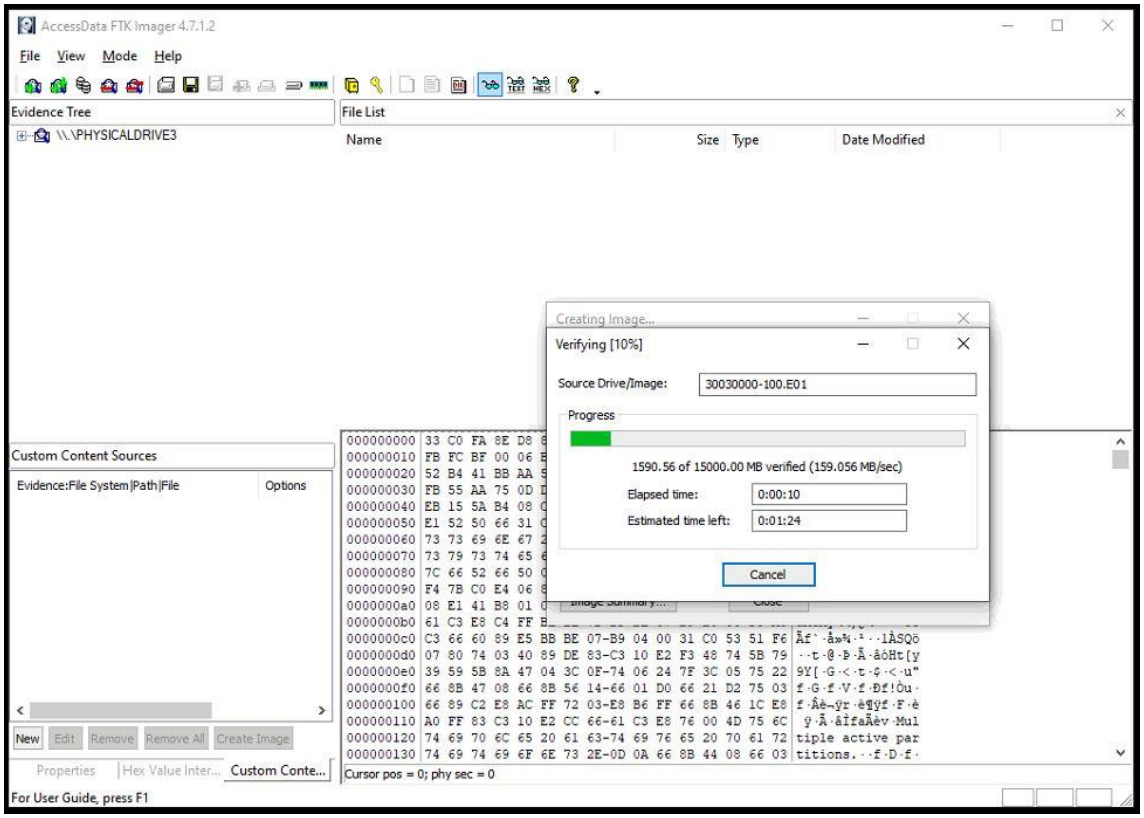

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
\\.\PHYSICALDRIVE3
Name
Size
Type
Date Modified
Create Image
Evidence Item Information
Case Number:
30030000
Evidence Number:
100
Unique Description:
USB Stick 16GB Guido Nagel
Examiner:
Erfurth Marcel & Mujezinovic Edin
Notes:
< Zurück
Weiter >
Cancel
Help
Start
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
Cursor pos = 0; phy sec = 0
For User Guide, press F1

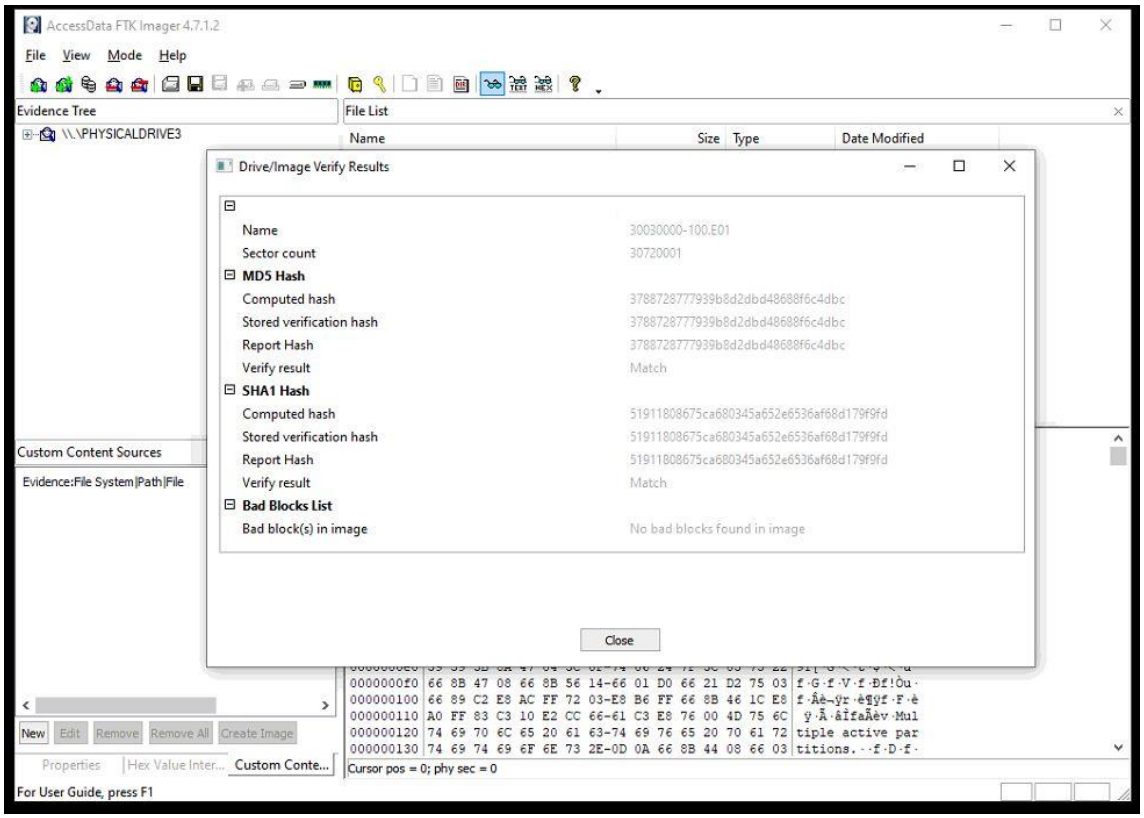

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
\\.\PHYSICALDRIVE3
Name
Size
Type
Date Modified
Create Image
Select Image Destination
Image Destination Folder
X:\30030000-100
Browse
Image Filename (Excluding Extension)
30030000-100
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
1500
Compression (0=None, 1=Fastest, ..., 9=Smallest)
6
Use AD Encryption
< Zurück
Finish
Cancel
Help
Start
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
Cursor pos = 0; phy sec = 0
For User Guide, press F1

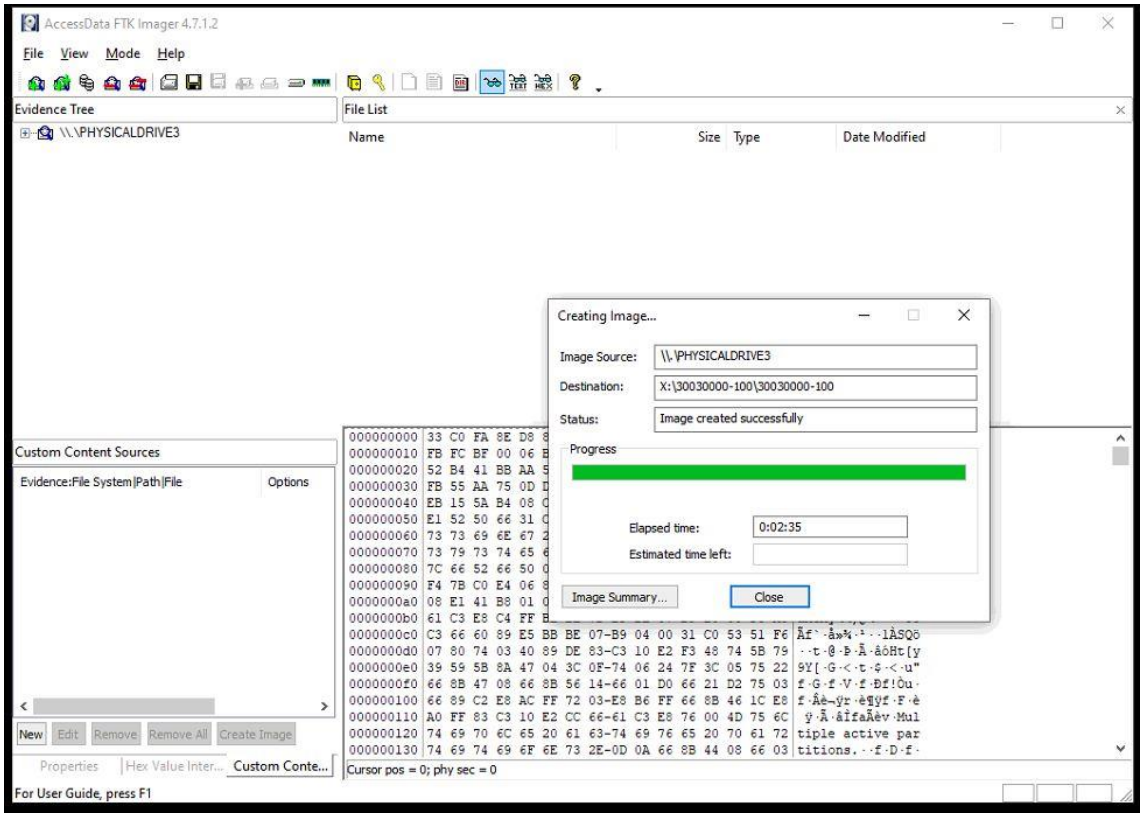

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
\\.\PHYSICALDRIVE3
Name
Size
Type
Date Modified
Create Image
Image Source
\\.\PHYSICALDRIVE3
Starting Evidence Number:
1
Image Destination(s)
X:\30030000-100\30030000-100 [E01]
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
Cursor pos = 0; phy sec = 0
For User Guide, press F1

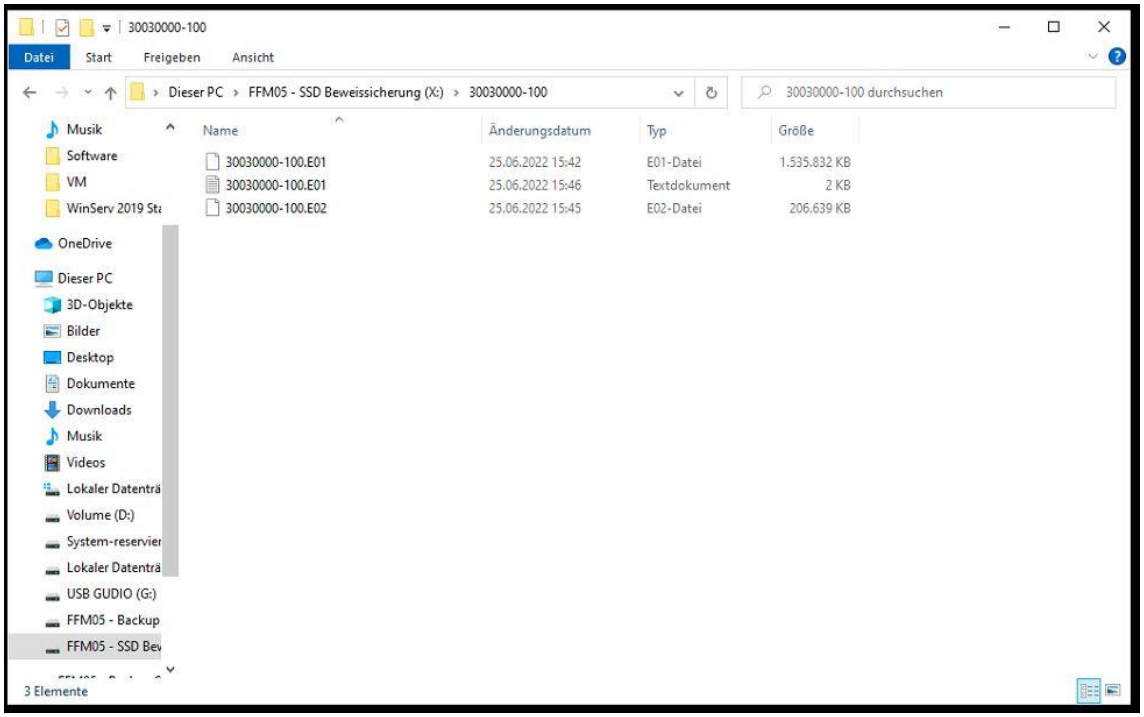

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE3
File List
Name
Size Type
Date Modified
Creating Image...
Image Source: \\.\PHYSICALDRIVE3
Destination: X:\30030000-100\30030000-100
Status: Creating image...
Progress
Elapsed time: 0:00:03
Estimated time left:
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Cursor pos = 0; phy sec = 0
For User Guide, press F1

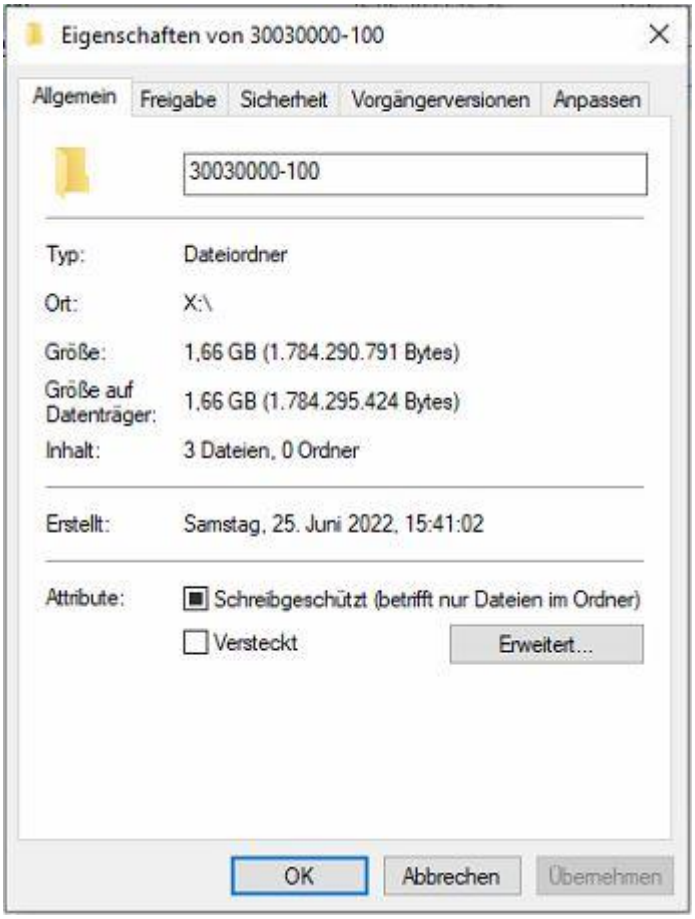

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE3
File List
Name
Size Type
Date Modified
Creating Image...
Image Source: \\.\PHYSICALDRIVE3
Destination: X:\30030000-100\30030000-100
Status: Creating image...
Progress
Elapsed time: 0:01:23
Estimated time left:
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Cursor pos = 0; phy sec = 0
For User Guide, press F1


AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE3
File List
Name
Size
Type
Date Modified
Creating Image...
Verifying [10%]
Source Drive/Image:
30030000-100.E01
Progress
1590.56 of 15000.00 MB verified (159.056 MB/sec)
Elapsed time:
0:00:10
Estimated time left:
0:01:24
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
Cursor pos = 0; phy sec = 0
For User Guide, press F1


AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE3
File List
Name
Size
Type
Date Modified
Drive/Image Verify Results
Name
30030000-100.E01
Sector count
30720001
MD5 Hash
Computed hash
3788728777939b8d2dbd48688f6c4dbc
Stored verification hash
3788728777939b8d2dbd48688f6c4dbc
Report Hash
3788728777939b8d2dbd48688f6c4dbc
Verify result
Match
SHA1 Hash
Computed hash
51911808675ca680345a652e6536af68d179f9fd
Stored verification hash
51911808675ca680345a652e6536af68d179f9fd
Report Hash
51911808675ca680345a652e6536af68d179f9fd
Verify result
Match
Bad Blocks List
Bad block(s) in image
No bad blocks found in image
Close
Custom Content Sources
Evidence:File System|Path|File
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
Cursor pos = 0; phy sec = 0
For User Guide, press F1

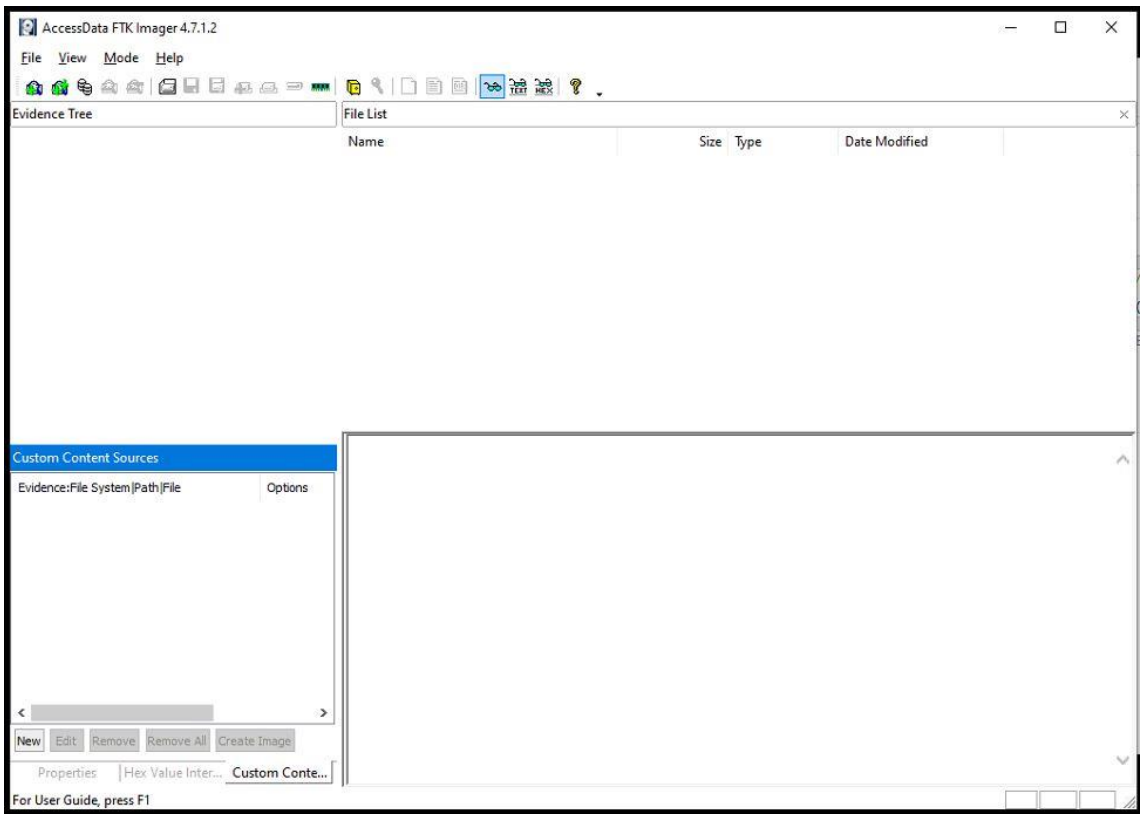

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE3
File List
Name Size Type Date Modified
Creating Image...
Image Source: \\.\PHYSICALDRIVE3
Destination: X:\30030000-100\30030000-100
Status: Image created successfully
Progress
Elapsed time: 0:02:35
Estimated time left:
Image Summary...
Close
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Cursor pos = 0; phy sec = 0
For User Guide, press F1

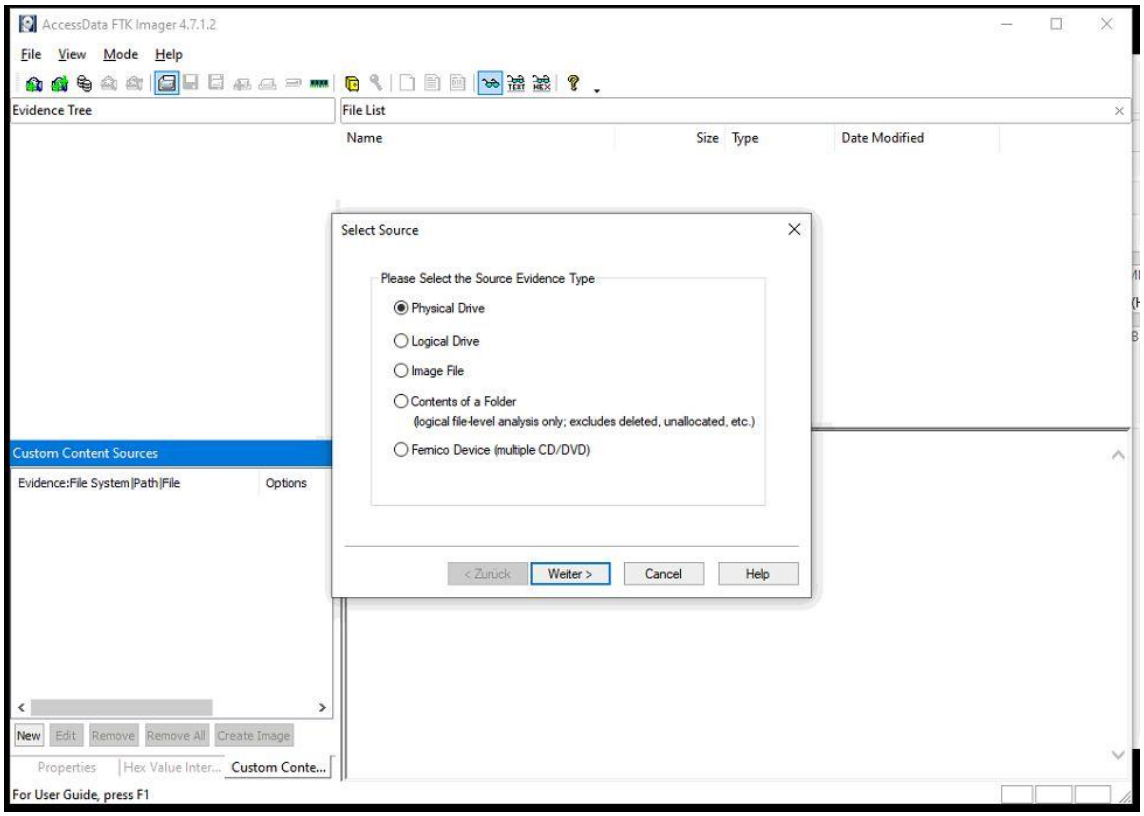

30030000-100
Datei Start Freigeben Ansicht
Dieser PC › FFM05 - SSD Beweissicherung (X:) › 30030000-100
30030000-100 durchsuchen
Musik
Software
VM
WinServ 2019 St
OneDrive
Dieser PC
3D-Objekte
Bilder
Desktop
Dokumente
Downloads
Musik
Videos
Lokaler Datenträ
Volume (D:)
System-reservier
Lokaler Datenträ
USB GUDIO (G:)
FFM05 - Backup
FFM05 - SSD Bev
Name Änderungsdatum Typ Größe
30030000-100.E01 25.06.2022 15:42 E01-Datei 1.535.832 KB
30030000-100.E01 25.06.2022 15:46 Textdokument 2 KB
30030000-100.E02 25.06.2022 15:45 E02-Datei 206.639 KB
3 Elemente

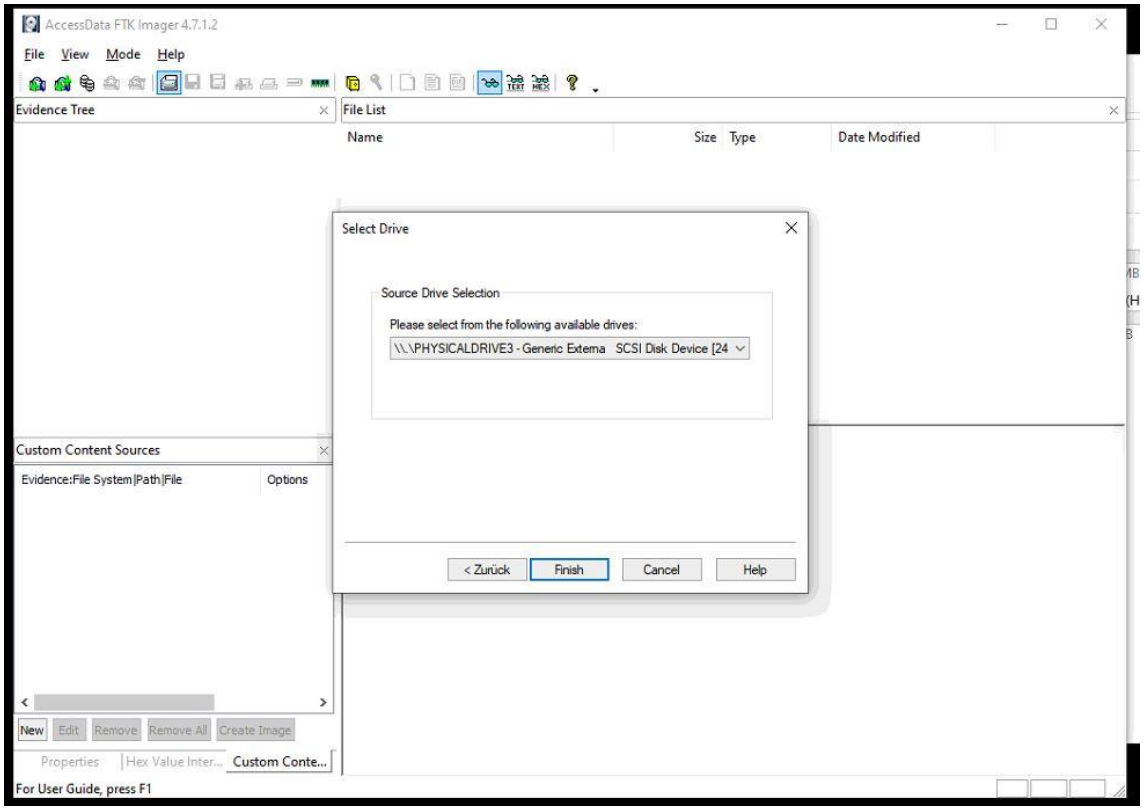

Eigenschaften von 30030000-100
Allgemein
Freigabe
Sicherheit
Vorgängerversionen
Anpassen
30030000-100
Typ:
Dateiordner
Ort:
X:\
Größe:
1,66 GB (1.784.290.791 Bytes)
Größe auf Datenträger:
1,66 GB (1.784.295.424 Bytes)
Inhalt:
3 Dateien, 0 Ordner
Erstellt:
Samstag, 25. Juni 2022, 15:41:02
Attribute:
Schreibgeschützt (betrifft nur Dateien im Ordner)
Versteckt
Erweitert...
OK
Abbrechen
Übernehmen

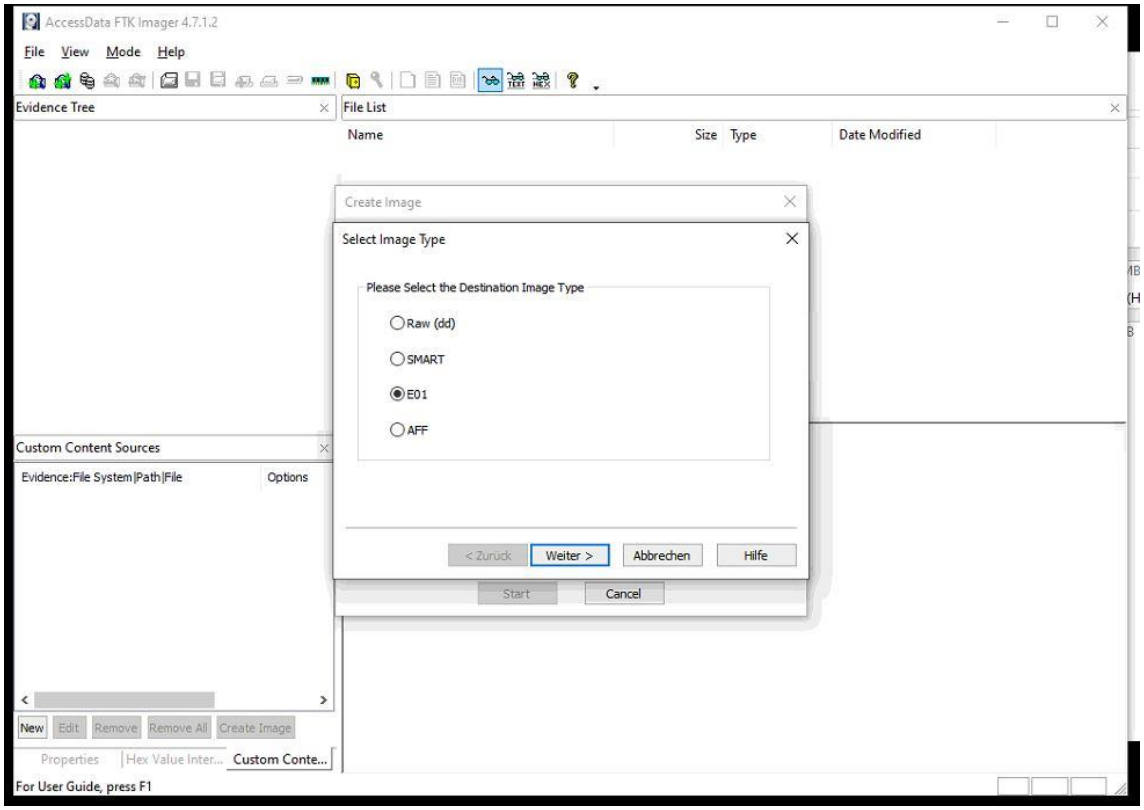
```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 30030000
Evidence Number: 100
Unique description: USB Stick 16GB  Guido Nagel
Examiner: Erfurth Marcel & Mujezinovic Edin
Notes:

--------------------------------------------------------------

Information for X:\30030000-100\30030000-100:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 1.912
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 30.720.001
[Physical Drive Information]
 Drive Model: ASolid USB USB Device
 Drive Serial Number: 0000000005□□
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 15000 MB
 Sector count:    30720001
[Computed Hashes]
 MD5 checksum:    3788728777939b8d2dbd48688f6c4dbc
 SHA1 checksum:   51911808675ca680345a652e6536af68d179f9fd

Image Information:
 Acquisition started:   Sat Jun 25 15:42:41 2022
 Acquisition finished:  Sat Jun 25 15:45:16 2022
 Segment list:
  X:\30030000-100\30030000-100.E01
  X:\30030000-100\30030000-100.E02

Image Verification Results:
 Verification started:  Sat Jun 25 15:45:16 2022
 Verification finished: Sat Jun 25 15:46:33 2022
 MD5 checksum:    3788728777939b8d2dbd48688f6c4dbc : verified
 SHA1 checksum:   51911808675ca680345a652e6536af68d179f9fd : verified
```

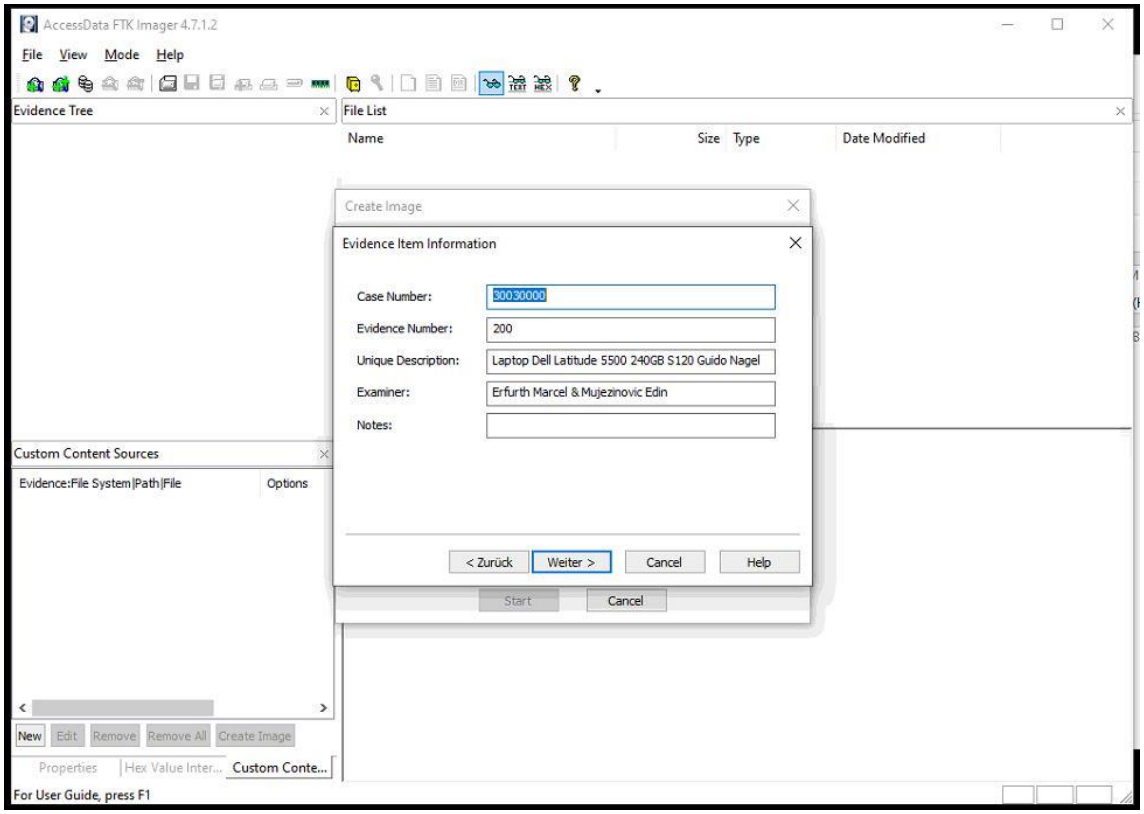
Vorgehen bei der Erstellung des Image Asservat-200 Notebook (FTK Imager)

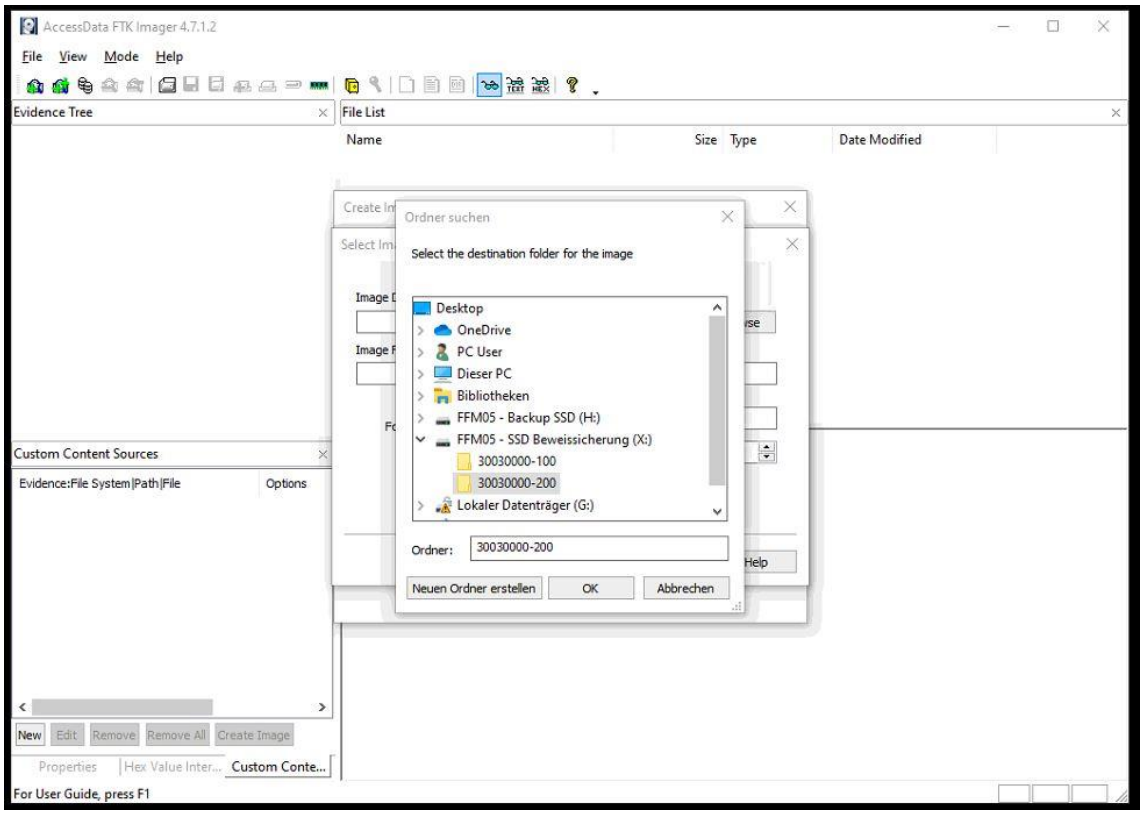


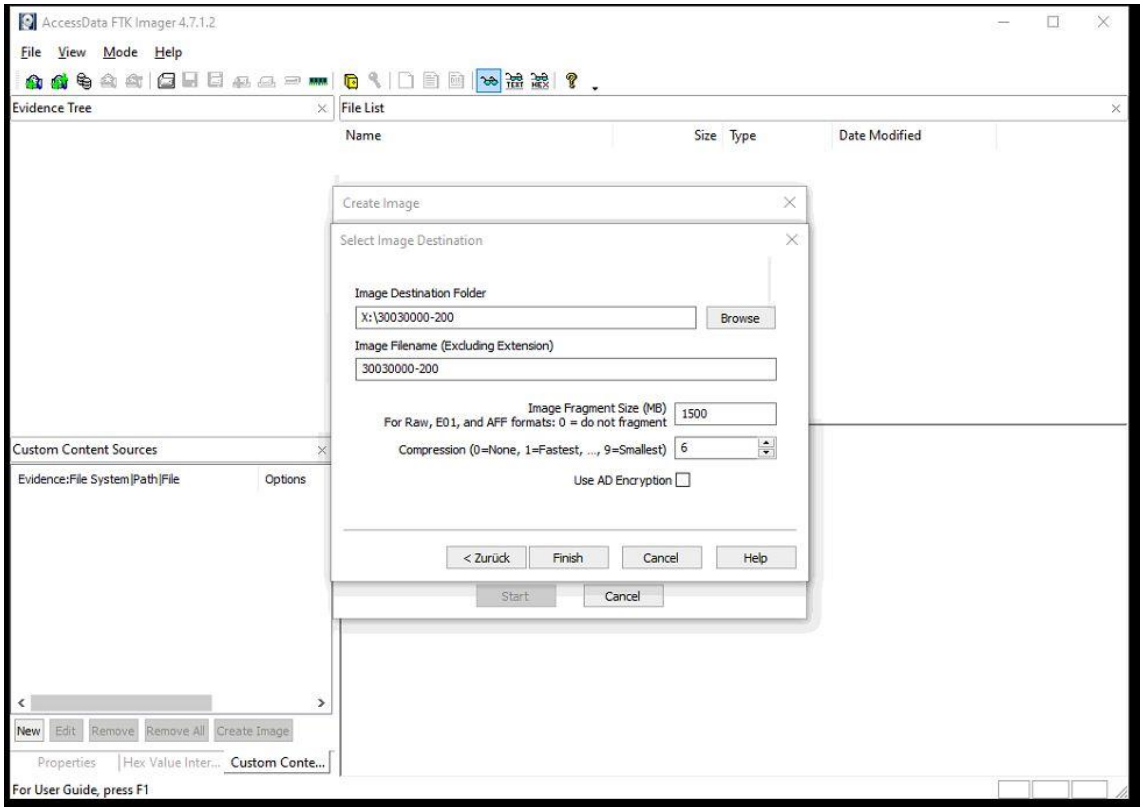


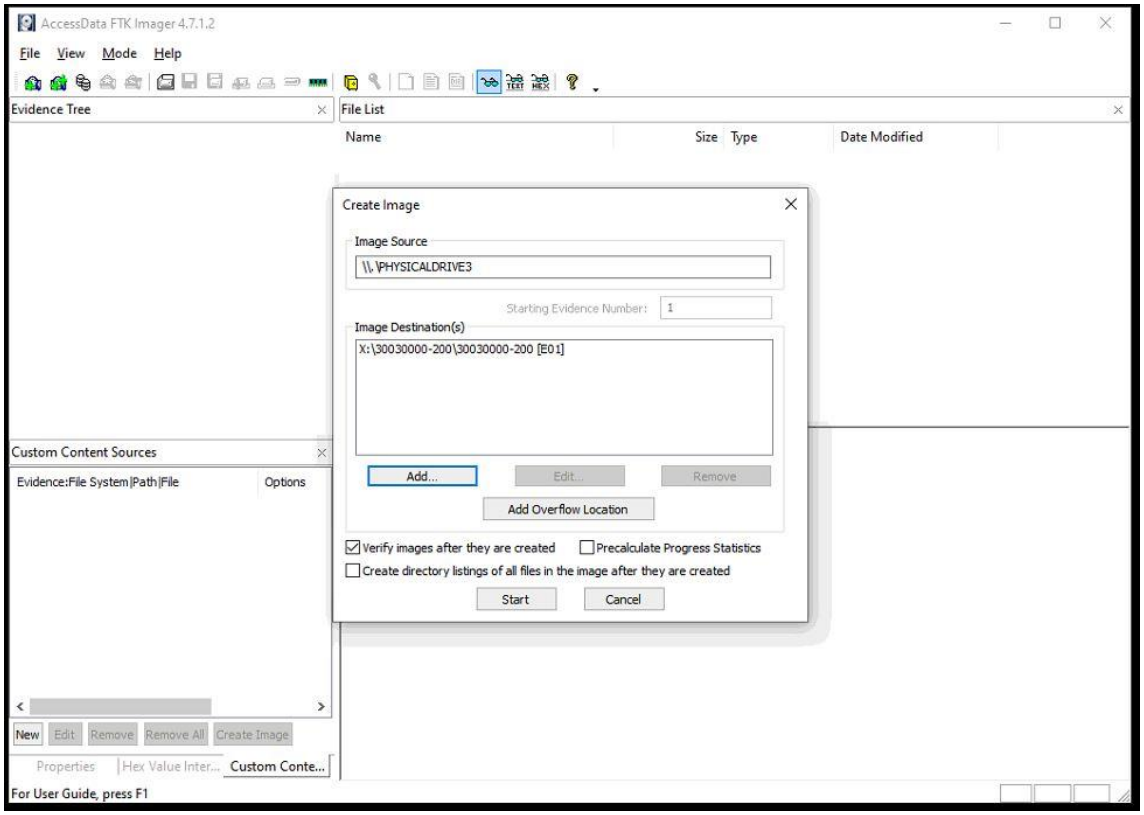

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size Type
Date Modified
Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE3 - Generic Externa SCSI Disk Device [24
< Zurück
Finish
Cancel
Help
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1

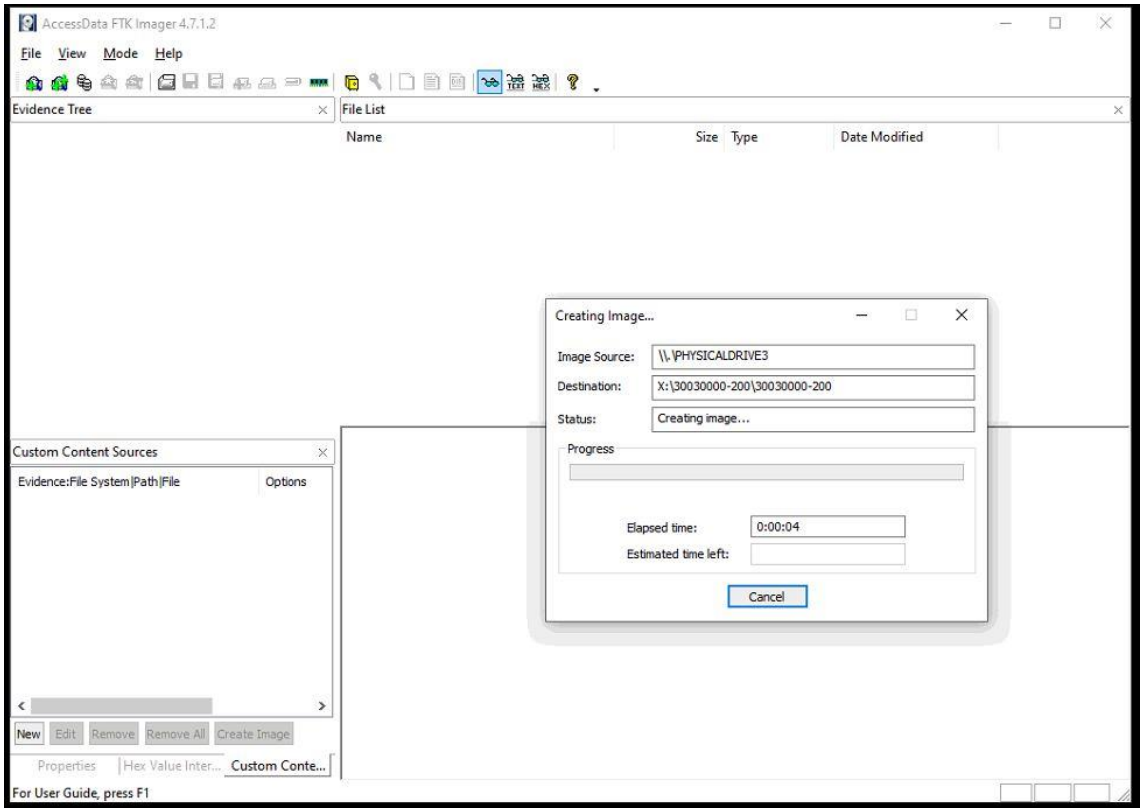

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size Type
Date Modified
Create Image
Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Zurück
Weiter >
Abbrechen
Hilfe
Start
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1

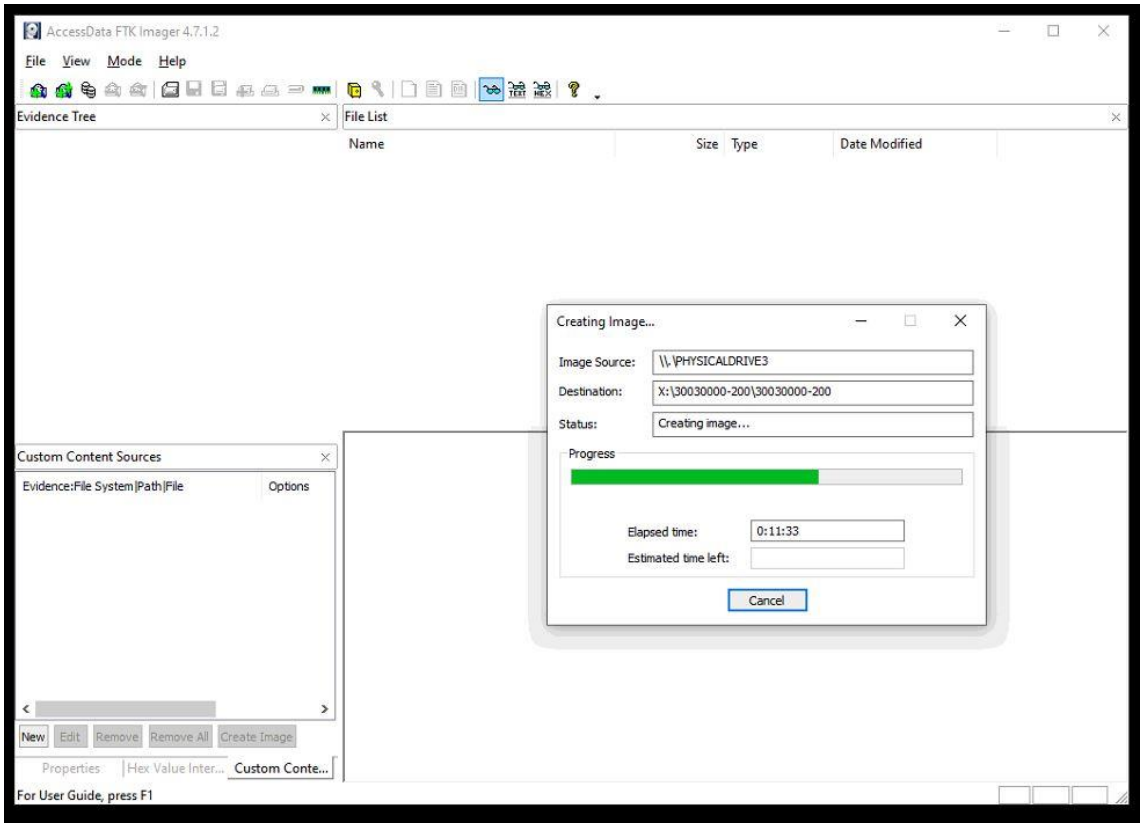

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Create Image
Evidence Item Information
Case Number:
30030000
Evidence Number:
200
Unique Description:
Laptop Dell Latitude 5500 240GB S120 Guido Nagel
Examiner:
Erfurth Marcel & Mujezinovic Edin
Notes:
< Zurück
Weiter >
Cancel
Help
Start
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
For User Guide, press F1

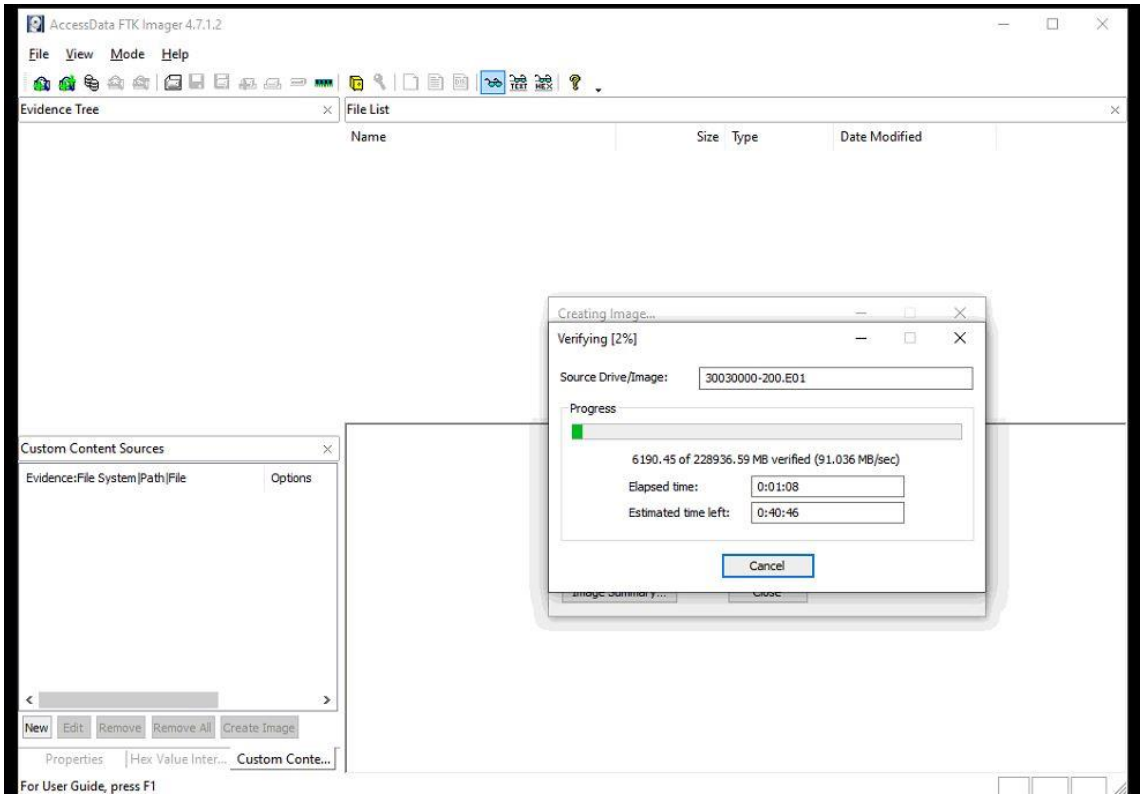

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Ordner suchen
Select the destination folder for the image
Desktop
OneDrive
PC User
Dieser PC
Bibliotheken
FFM05 - Backup SSD (H:)
FFM05 - SSD Beweissicherung (X:)
30030000-100
30030000-200
Lokaler Datenträger (G:)
Ordner:
30030000-200
Neuen Ordner erstellen
OK
Abbrechen
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
For User Guide, press F1

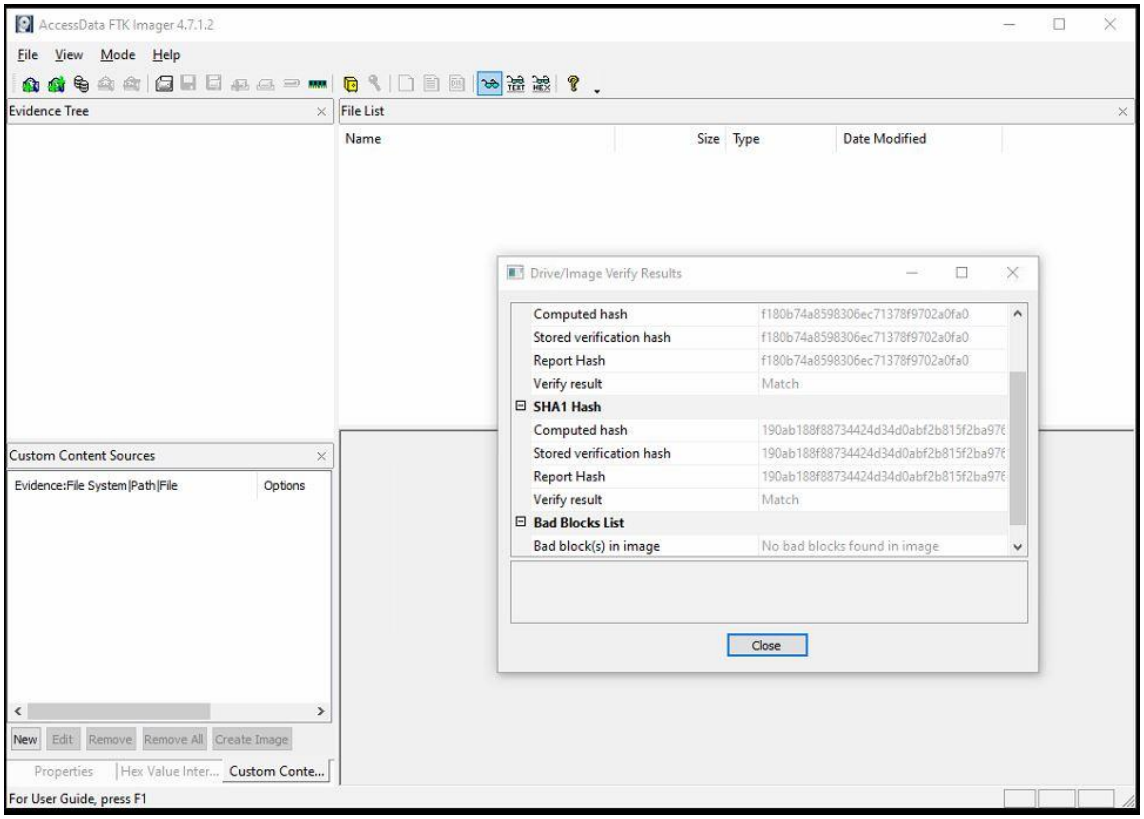

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size Type
Date Modified
Create Image
Select Image Destination
Image Destination Folder
X:\30030000-200
Browse
Image Filename (Excluding Extension)
30030000-200
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
1500
Compression (0=None, 1=Fastest, ..., 9=Smallest)
6
Use AD Encryption
< Zurück
Finish
Cancel
Help
Start
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
For User Guide, press F1

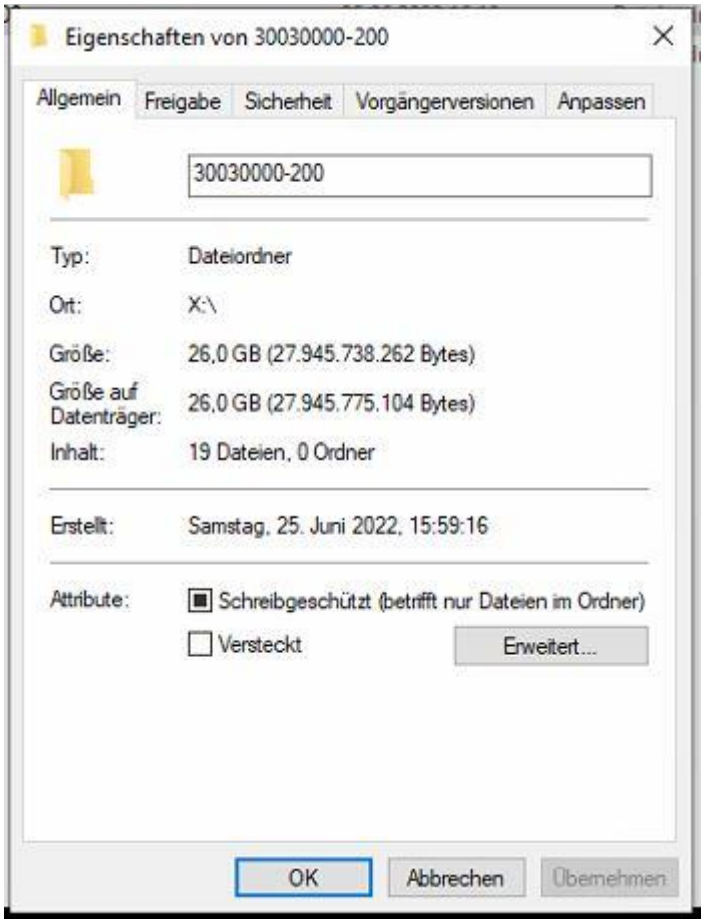

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size Type
Date Modified
Create Image
Image Source
\\.\PHYSICALDRIVE3
Starting Evidence Number:
1
Image Destination(s)
X:\30030000-200\30030000-200 [E01]
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
For User Guide, press F1


AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Creating Image...
Image Source: \\.\PHYSICALDRIVE3
Destination: X:\30030000-200\30030000-200
Status: Creating image...
Progress
Elapsed time: 0:00:04
Estimated time left:
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
For User Guide, press F1


AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modified
Creating Image...
Image Source: \\.\PHYSICALDRIVE3
Destination: X:\30030000-200\30030000-200
Status: Creating image...
Progress
Elapsed time: 0:11:33
Estimated time left:
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
For User Guide, press F1

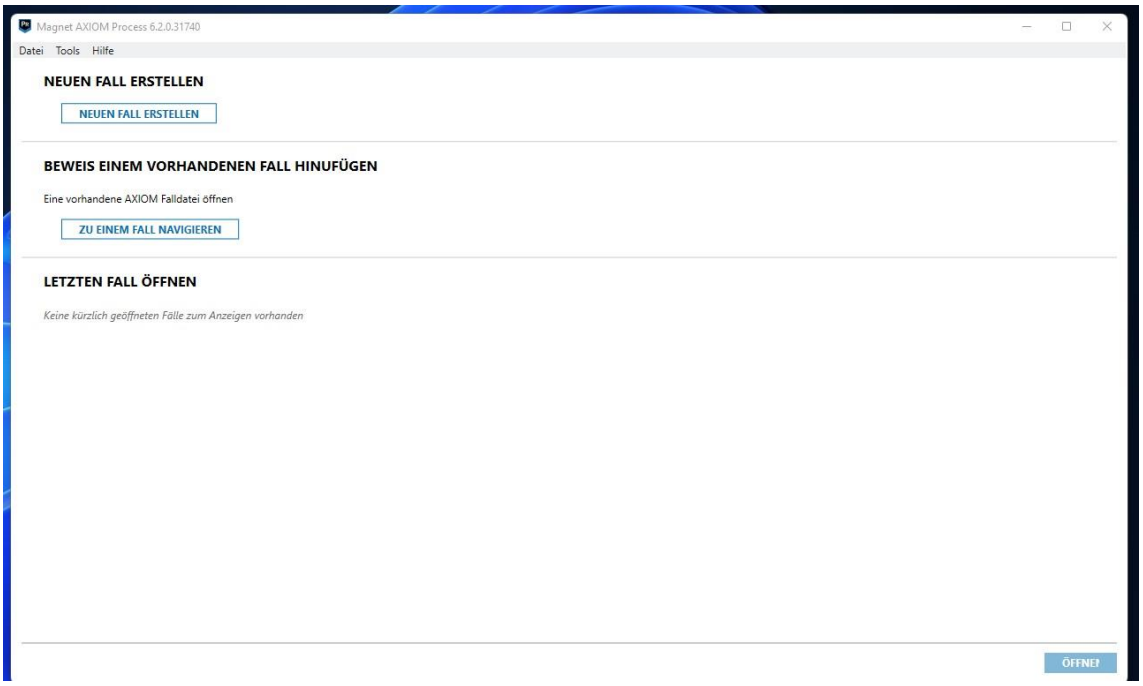

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size Type
Date Modified
Creating Image...
Verifying [2%]
Source Drive/Image:
30030000-200.E01
Progress
6190.45 of 228936.59 MB verified (91.036 MB/sec)
Elapsed time:
0:01:08
Estimated time left:
0:40:46
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1

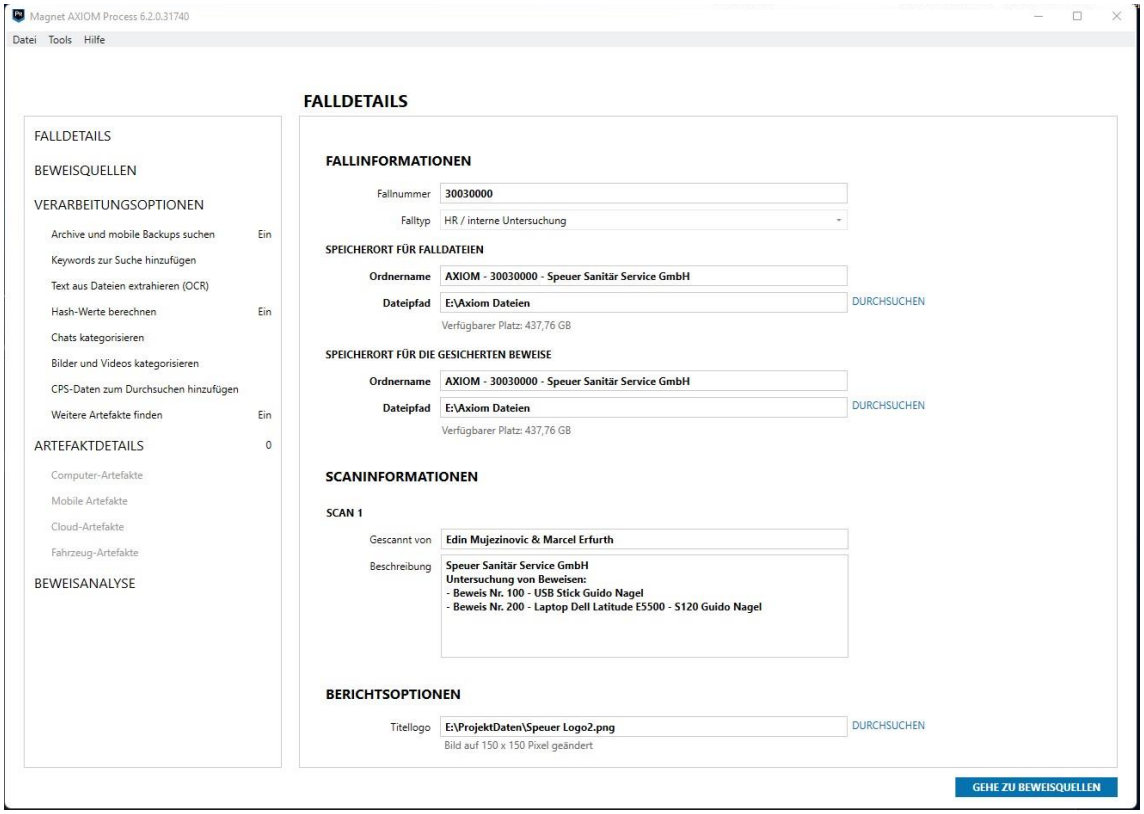

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size Type
Date Modified
Drive/Image Verify Results
Computed hash f180b74a8598306ec71378f9702a0fa0
Stored verification hash f180b74a8598306ec71378f9702a0fa0
Report Hash f180b74a8598306ec71378f9702a0fa0
Verify result Match
SHA1 Hash
Computed hash 190ab188f88734424d34d0abf2b815f2ba976
Stored verification hash 190ab188f88734424d34d0abf2b815f2ba976
Report Hash 190ab188f88734424d34d0abf2b815f2ba976
Verify result Match
Bad Blocks List
Bad block(s) in image No bad blocks found in image
Close
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1

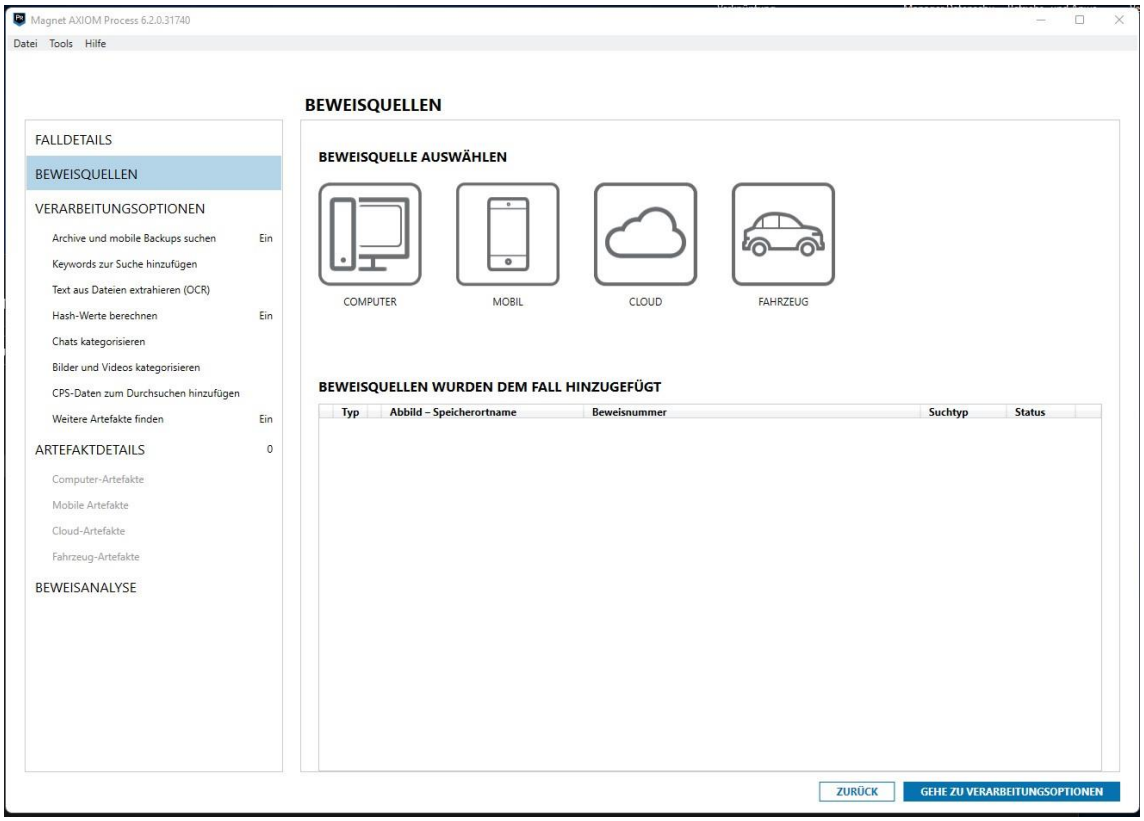

Eigenschaften von 30030000-200
Allgemein
Freigabe
Sicherheit
Vorgängerversionen
Anpassen
30030000-200
Typ:
Dateiordner
Ort:
X:\
Größe:
26,0 GB (27.945.738.262 Bytes)
Größe auf Datenträger:
26,0 GB (27.945.775.104 Bytes)
Inhalt:
19 Dateien, 0 Ordner
Erstellt:
Samstag, 25. Juni 2022, 15:59:16
Attribute:
Schreibgeschützt (betrifft nur Dateien im Ordner)
Versteckt
Erweitert...
OK
Abbrechen
Übernehmen

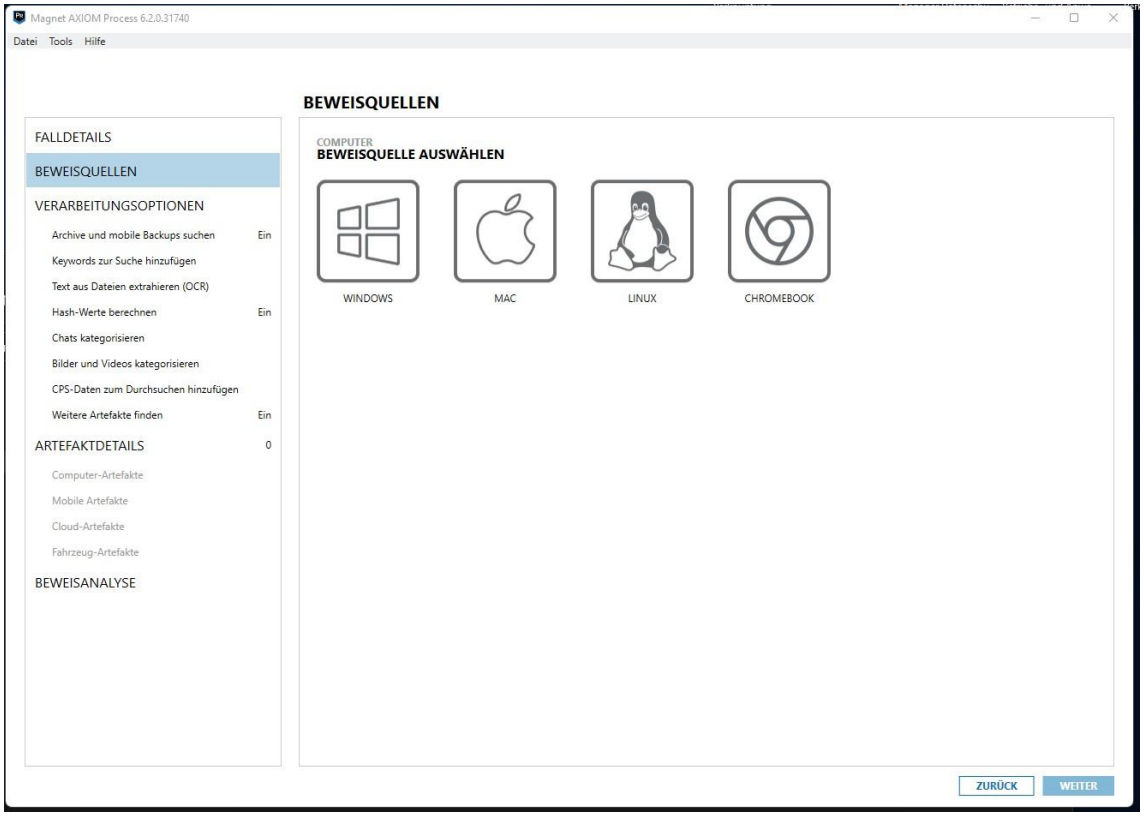
```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 30030000
Evidence Number: 200
Unique description: Laptop Dell Latitude 5500 240GB S120 Guido Nagel
Examiner: Erfurth Marcel & Mujezinovic Edin
Notes:

--------------------------------------------------------------

Information for X:\30030000-200\30030000-200:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 29.185
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 468.862.127
[Physical Drive Information]
 Drive Model: Generic Externa   SCSI Disk Device
 Drive Serial Number: 22222222222222220138
 Drive Interface Type: SCSI
 Removable drive: False
 Source data size: 228936 MB
 Sector count:    468862127
[Computed Hashes]
 MD5 checksum:    f180b74a8598306ec71378f9702a0fa0
 SHA1 checksum:   190ab188f88734424d34d0abf2b815f2ba97689f

Image Information:
 Acquisition started:   Sat Jun 25 16:01:35 2022
 Acquisition finished:  Sat Jun 25 16:18:21 2022
 Segment list:
  X:\30030000-200\30030000-200.E01
  X:\30030000-200\30030000-200.E02
  X:\30030000-200\30030000-200.E03
  X:\30030000-200\30030000-200.E04
  X:\30030000-200\30030000-200.E05
  X:\30030000-200\30030000-200.E06
  X:\30030000-200\30030000-200.E07
  X:\30030000-200\30030000-200.E08
  X:\30030000-200\30030000-200.E09
  X:\30030000-200\30030000-200.E10
  X:\30030000-200\30030000-200.E11
  X:\30030000-200\30030000-200.E12
  X:\30030000-200\30030000-200.E13
  X:\30030000-200\30030000-200.E14
  X:\30030000-200\30030000-200.E15
  X:\30030000-200\30030000-200.E16
  X:\30030000-200\30030000-200.E17
  X:\30030000-200\30030000-200.E18

Image Verification Results:
 Verification started:  Sat Jun 25 16:18:21 2022
 Verification finished: Sat Jun 25 16:42:14 2022
 MD5 checksum:    f180b74a8598306ec71378f9702a0fa0 : verified
 SHA1 checksum:   190ab188f88734424d34d0abf2b815f2ba97689f : verified
```

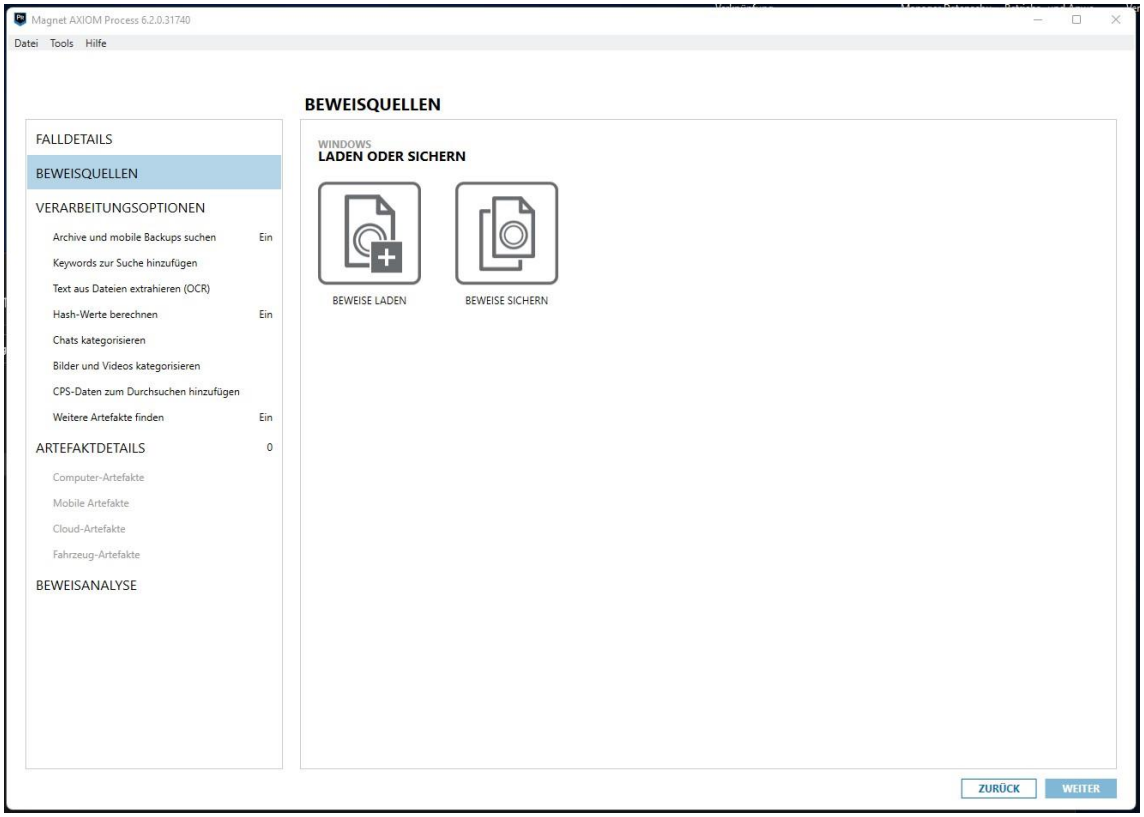
Vorgehen der Auswertung beider Asservate (Axiom)

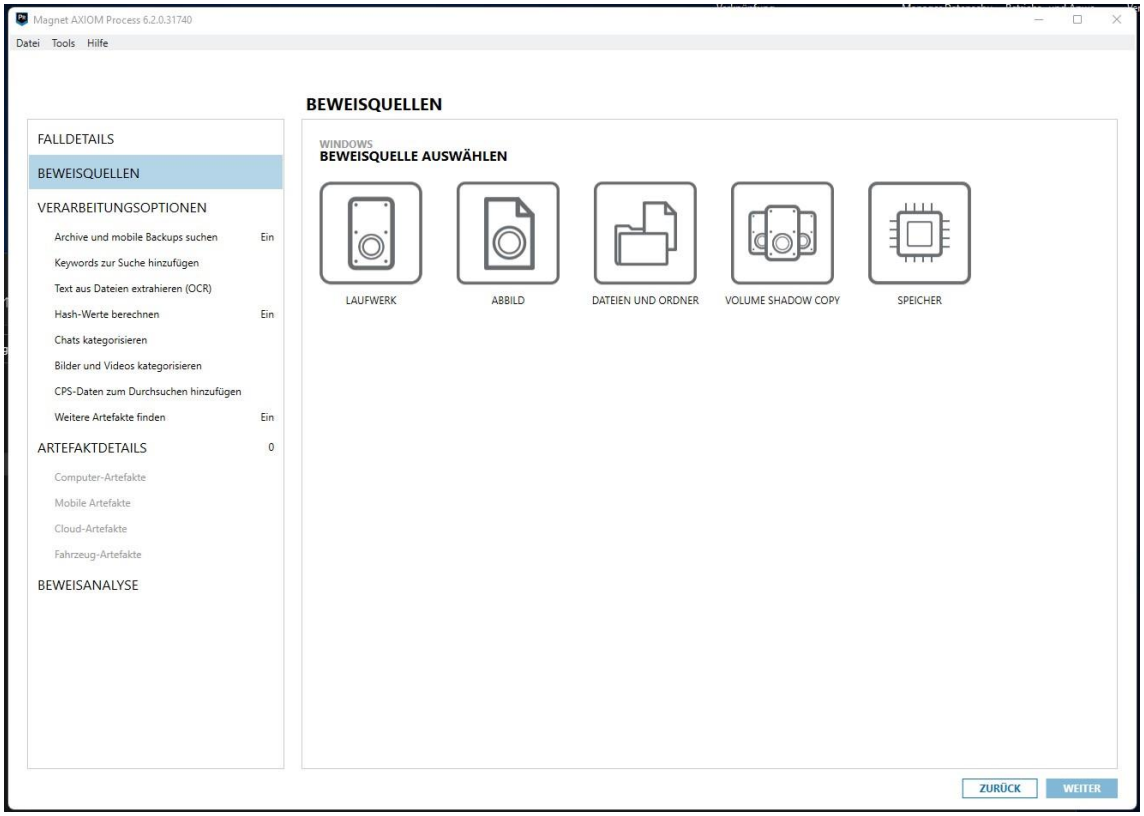


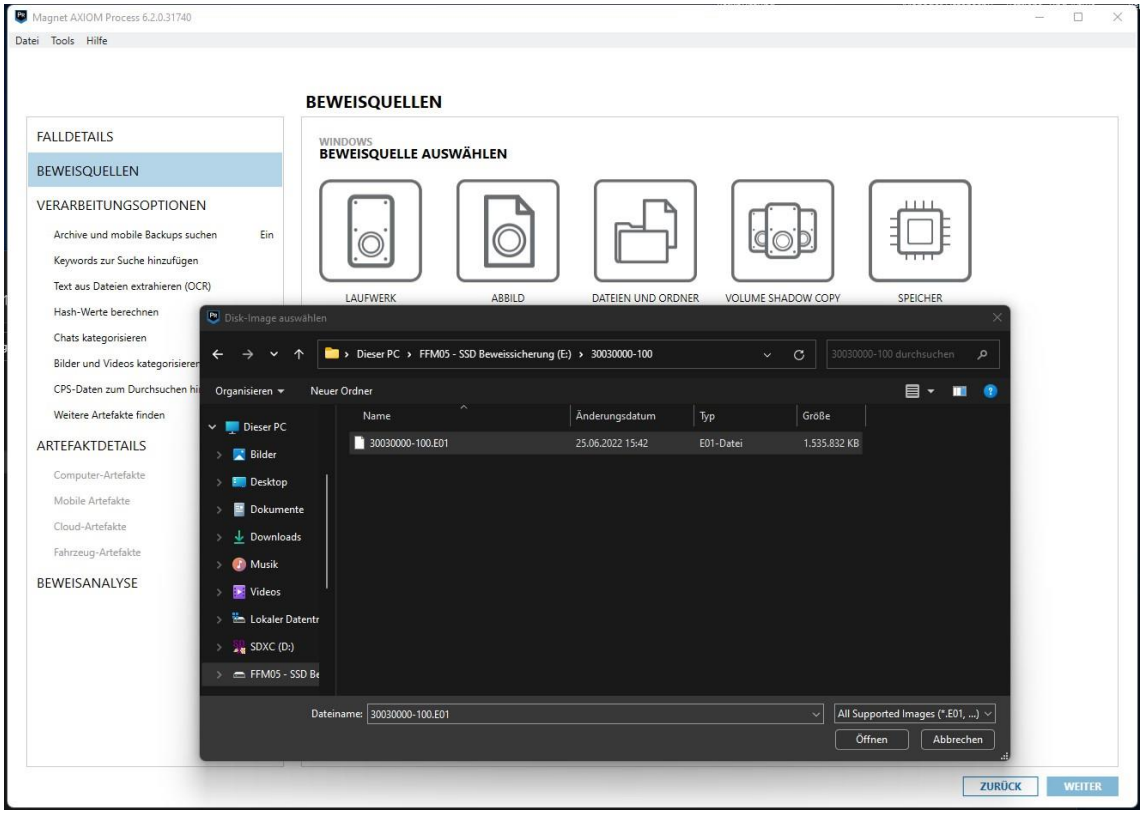

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
FALLDETAILS
FALLDETAILS
BEWEISQUELLEN
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 0
Computer-Artefakte
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
FALLINFORMATIONEN
Fallnummer 30030000
Falltyp HR / interne Untersuchung
SPEICHERORT FÜR FALLDATEIEN
Ordnername AXIOM - 30030000 - Speuer Sanitär Service GmbH
Dateipfad E:\Axiom Dateien DURCHSUCHEN
Verfügbarer Platz: 437,76 GB
SPEICHERORT FÜR DIE GESICHERTEN BEWEISE
Ordnername AXIOM - 30030000 - Speuer Sanitär Service GmbH
Dateipfad E:\Axiom Dateien DURCHSUCHEN
Verfügbarer Platz: 437,76 GB
SCANINFORMATIONEN
SCAN 1
Gescannt von Edin Mujezinovic & Marcel Erfurth
Beschreibung Speuer Sanitär Service GmbH
Untersuchung von Beweisen:
- Beweis Nr. 100 - USB Stick Guido Nagel
- Beweis Nr. 200 - Laptop Dell Latitude E5500 - S120 Guido Nagel
BERICHTSOPTIONEN
Titellogo E:\ProjektDaten\Speuer Logo2.png DURCHSUCHEN
Bild auf 150 x 150 Pixel geändert
GEHE ZU BEWEISQUELLEN

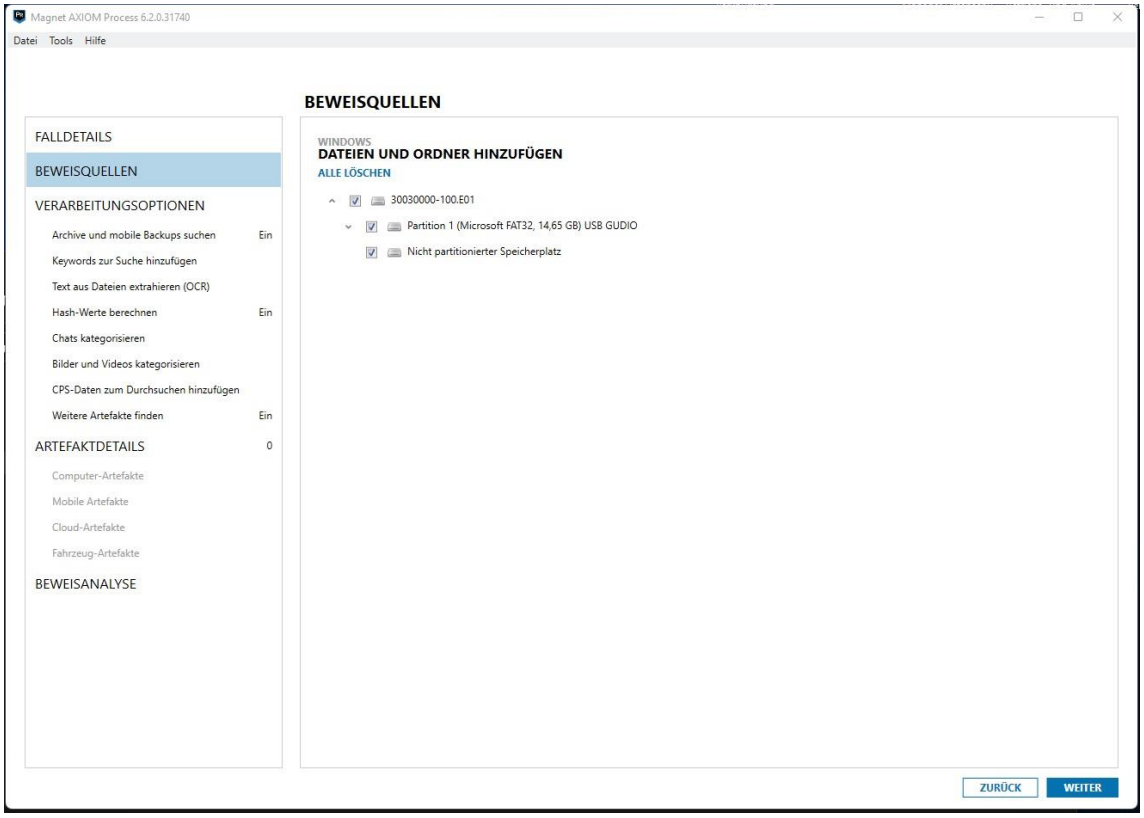

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISQUELLEN
FALLDETAILS
BEWEISQUELLEN
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 0
Computer-Artefakte
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
BEWEISQUELLE AUSWÄHLEN
COMPUTER
MOBIL
CLOUD
FAHRZEUG
BEWEISQUELLEN WURDEN DEM FALL HINZUGEFÜGT
Typ
Abbild – Speicherortname
Beweisnummer
Suchtyp
Status
ZURÜCK
GEHE ZU VERARBEITUNGSOPTIONEN

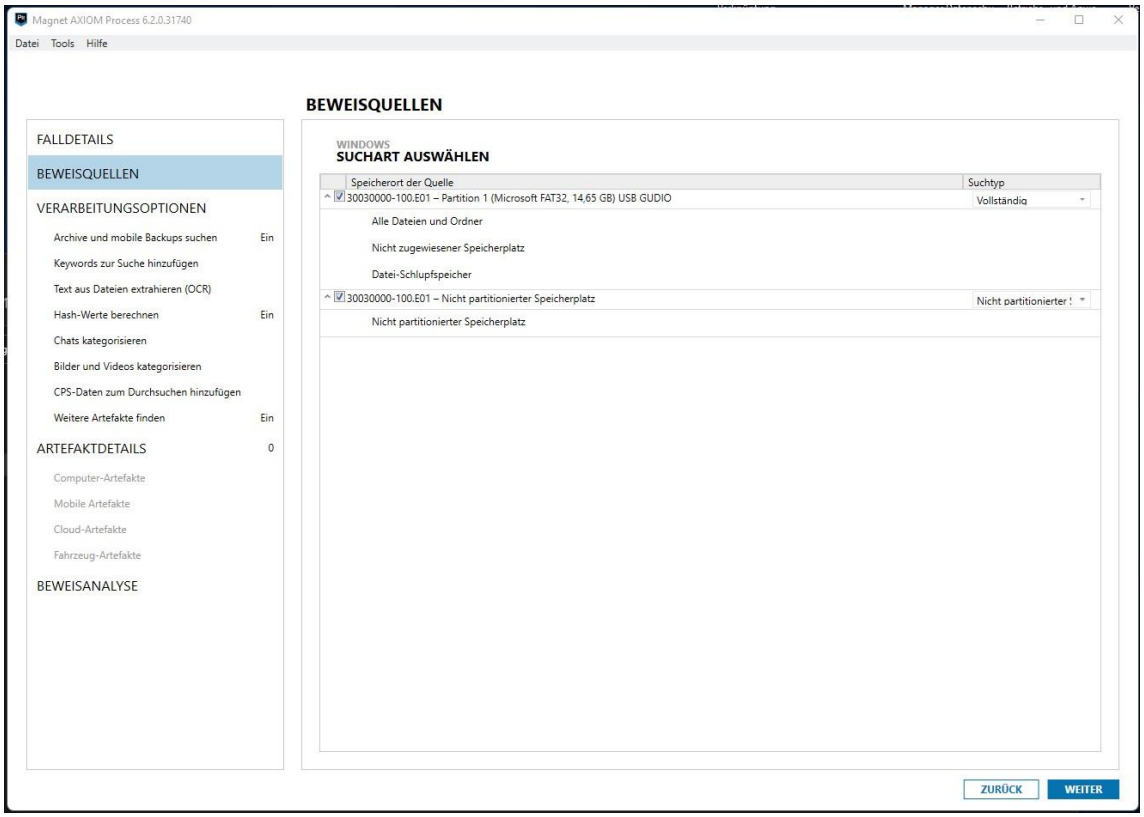

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISQUELLEN
FALLDETAILS
BEWEISQUELLEN
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 0
Computer-Artefakte
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
COMPUTER
BEWEISQUELLE AUSWÄHLEN
WINDOWS
MAC
LINUX
CHROMEBOOK
ZURÜCK
WEITER

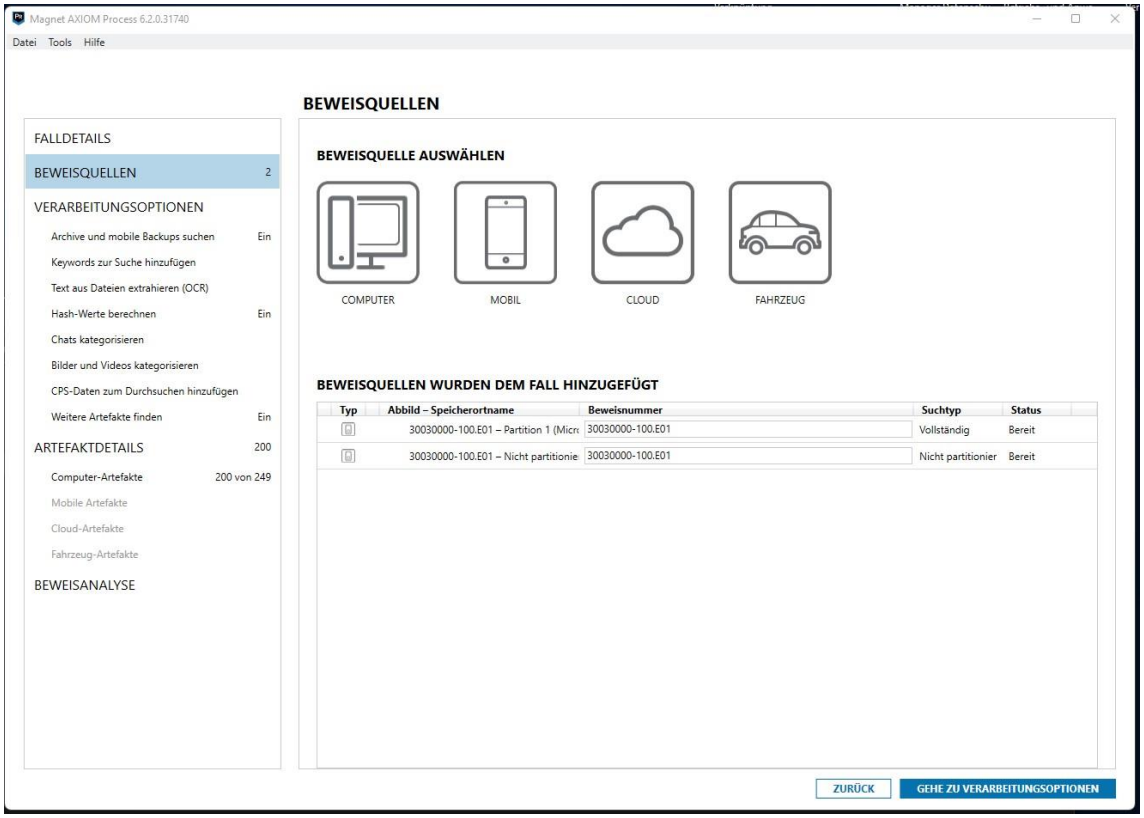

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISQUELLEN
FALLDETAILS
BEWEISQUELLEN
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 0
Computer-Artefakte
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
WINDOWS
LADEN ODER SICHERN
BEWEISE LADEN
BEWEISE SICHERN
ZURÜCK
WEITER

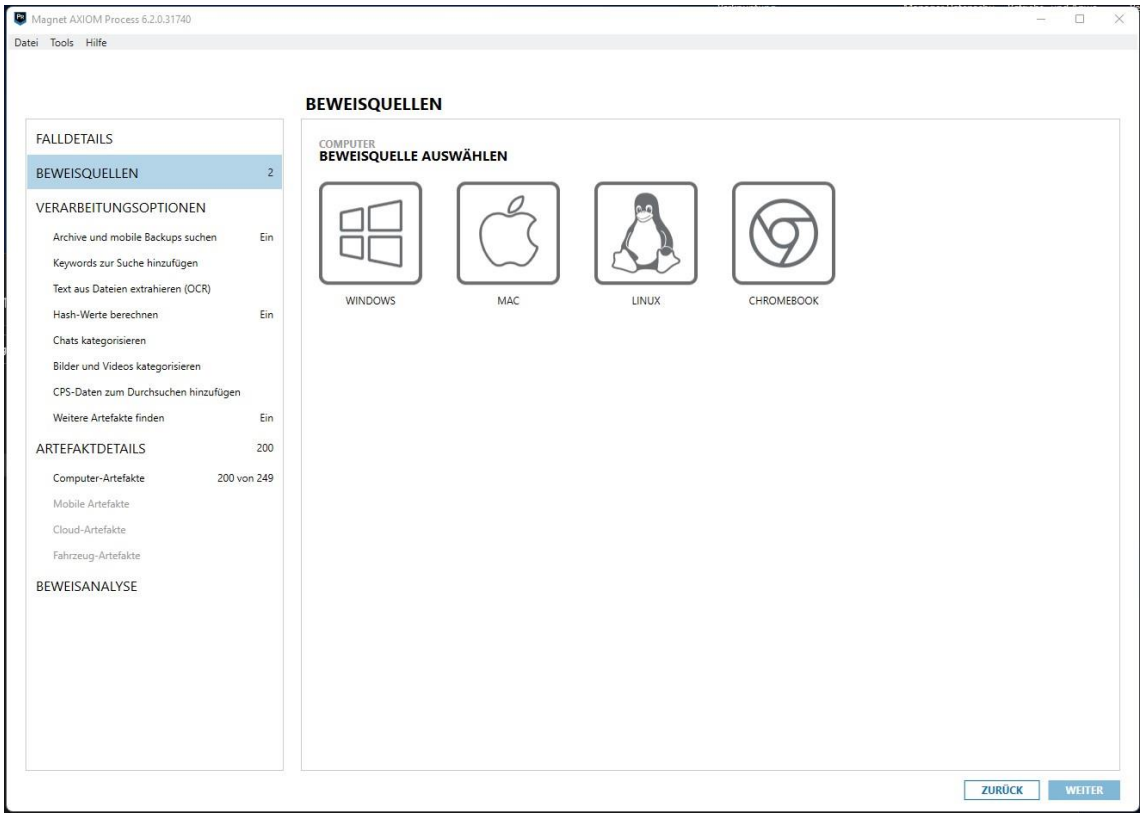

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISQUELLEN
FALLDETAILS
BEWEISQUELLEN
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 0
Computer-Artefakte
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
WINDOWS
BEWEISQUELLE AUSWÄHLEN
LAUFWERK
ABBILD
DATEIEN UND ORDNER
VOLUME SHADOW COPY
SPEICHER
ZURÜCK
WEITER

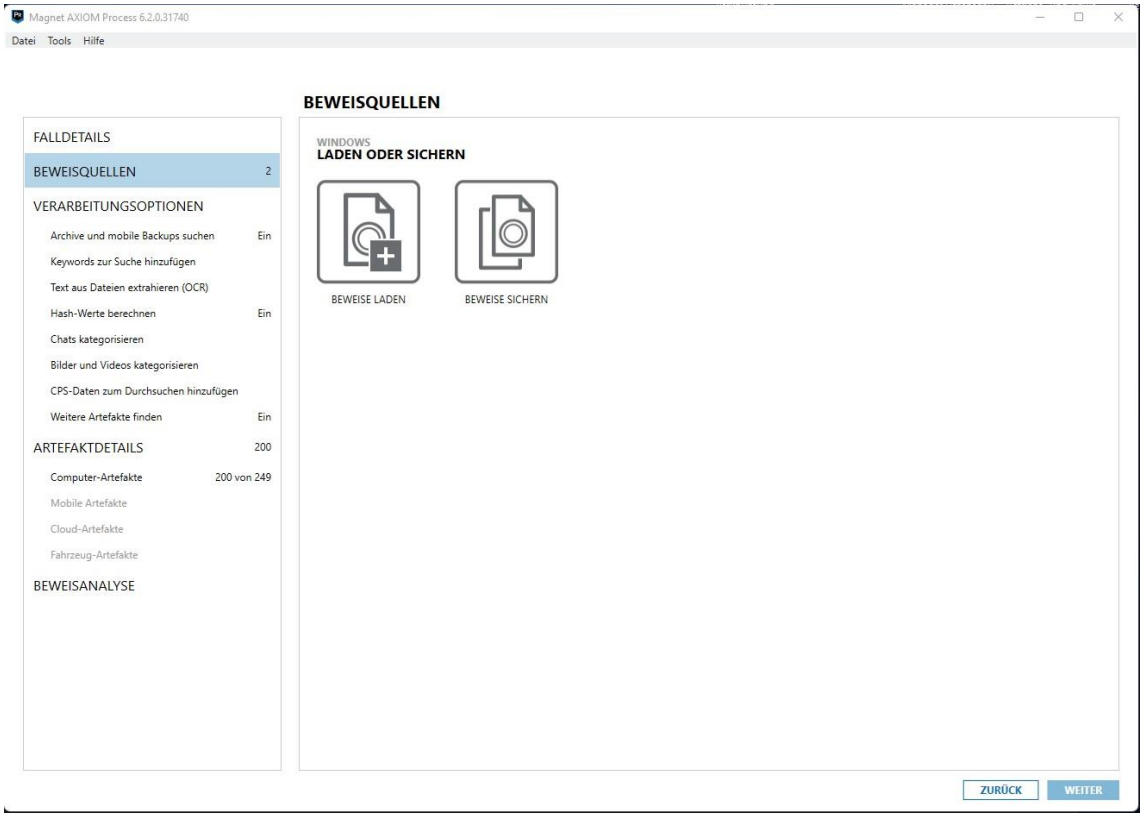

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISQUELLEN
FALLDETAILS
BEWEISQUELLEN
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hi
Weitere Artefakte finden
ARTEFAKTDETAILS
Computer-Artefakte
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
WINDOWS
BEWEISQUELLE AUSWÄHLEN
LAUFWERK
ABBILD
DATEIEN UND ORDNER
VOLUME SHADOW COPY
SPEICHER
Disk-Image auswählen
Dieser PC › FFM05 - SSD Beweissicherung (E:) › 30030000-100
30030000-100 durchsuchen
Organisieren
Neuer Ordner
Dieser PC
Bilder
Desktop
Dokumente
Downloads
Musik
Videos
Lokaler Datentr
SDXC (D:)
FFM05 - SSD Be
Name
Änderungsdatum
Typ
Größe
30030000-100.E01
25.06.2022 15:42
E01-Datei
1.535.832 KB
Dateiname: 30030000-100.E01
All Supported Images (*.E01, ...)
Öffnen
Abbrechen
ZURÜCK
WEITER

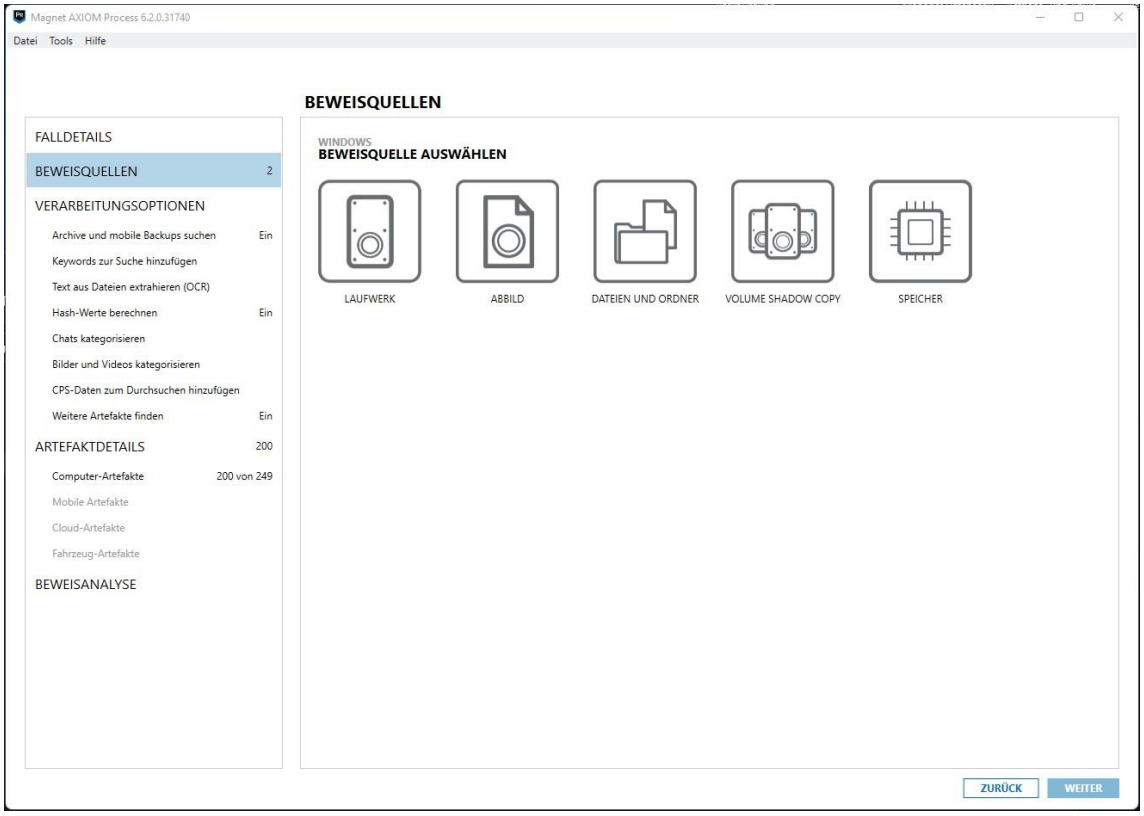

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISQUELLEN
FALLDETAILS
BEWEISQUELLEN
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 0
Computer-Artefakte
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
WINDOWS
DATEIEN UND ORDNER HINZUFÜGEN
ALLE LÖSCHEN
30030000-100.E01
Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO
Nicht partitionierter Speicherplatz
ZURÜCK
WEITER

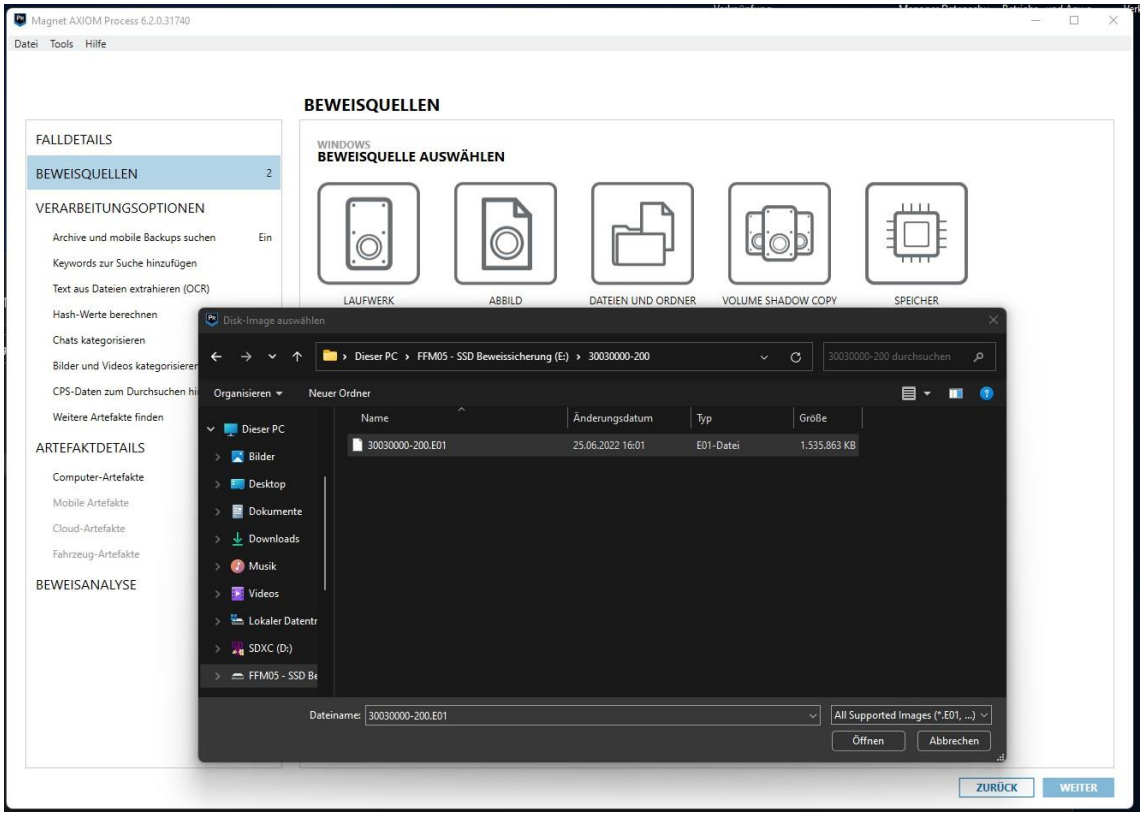

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISQUELLEN
FALLDETAILS
BEWEISQUELLEN
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 0
Computer-Artefakte
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
WINDOWS
SUCHART AUSWÄHLEN
Speicherort der Quelle
Suchtyp
30030000-100.E01 – Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO
Vollständig
Alle Dateien und Ordner
Nicht zugewiesener Speicherplatz
Datei-Schlupfspeicher
30030000-100.E01 – Nicht partitionierter Speicherplatz
Nicht partitionierter Speicherplatz
ZURÜCK
WEITER

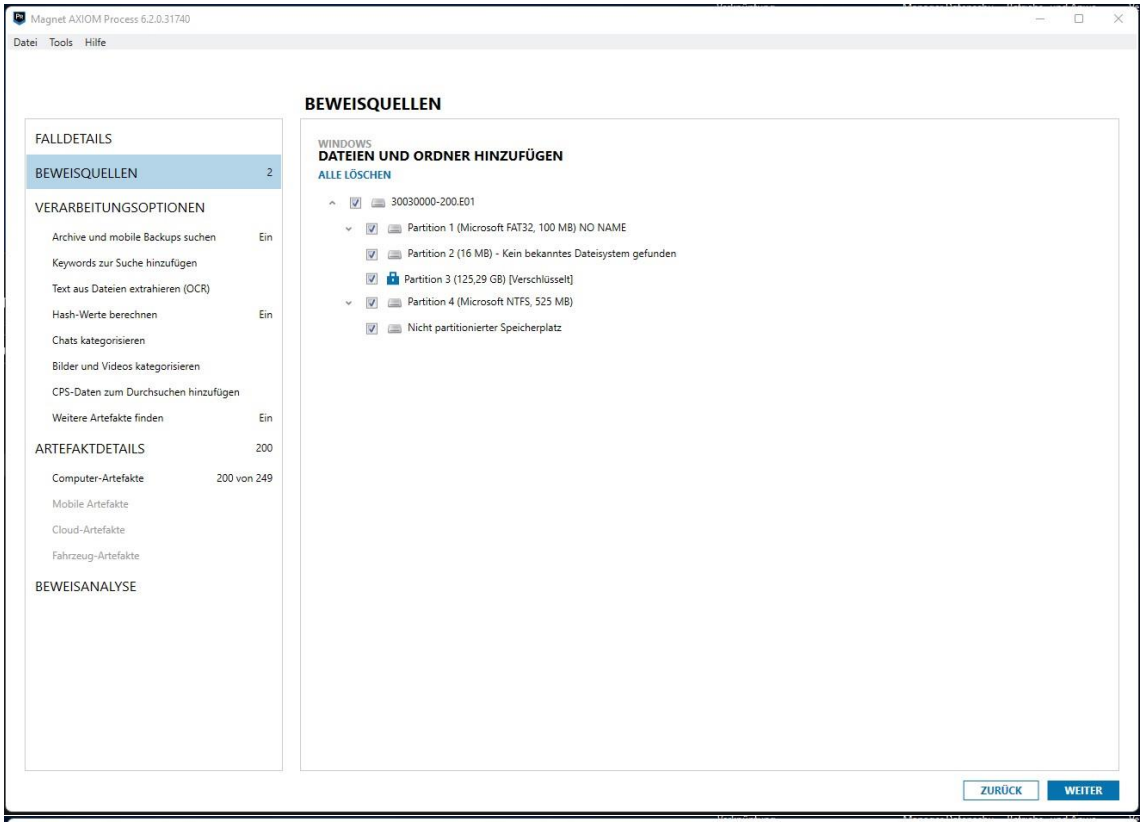

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISQUELLEN
FALLDETAILS
BEWEISQUELLEN 2
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
BEWEISQUELLE AUSWÄHLEN
COMPUTER
MOBIL
CLOUD
FAHRZEUG
BEWEISQUELLEN WURDEN DEM FALL HINZUGEFÜGT
Typ
Abbild – Speicherortname
Beweisnummer
Suchtyp
Status
30030000-100.E01 – Partition 1 (Micr
30030000-100.E01
Vollständig
Bereit
30030000-100.E01 – Nicht partitionie
30030000-100.E01
Nicht partitionier
Bereit
ZURÜCK
GEHE ZU VERARBEITUNGSOPTIONEN

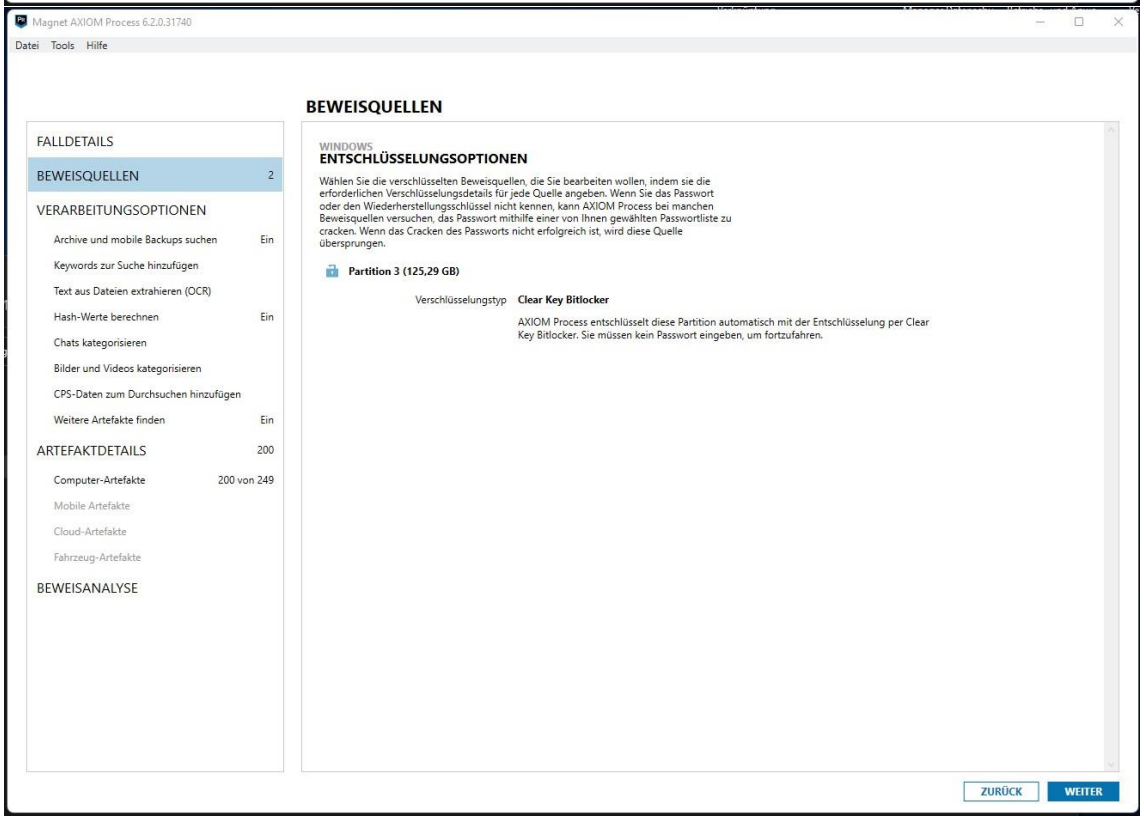

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISQUELLEN
FALLDETAILS
BEWEISQUELLEN 2
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
COMPUTER
BEWEISQUELLE AUSWÄHLEN
WINDOWS
MAC
LINUX
CHROMEBOOK
ZURÜCK
WEITER

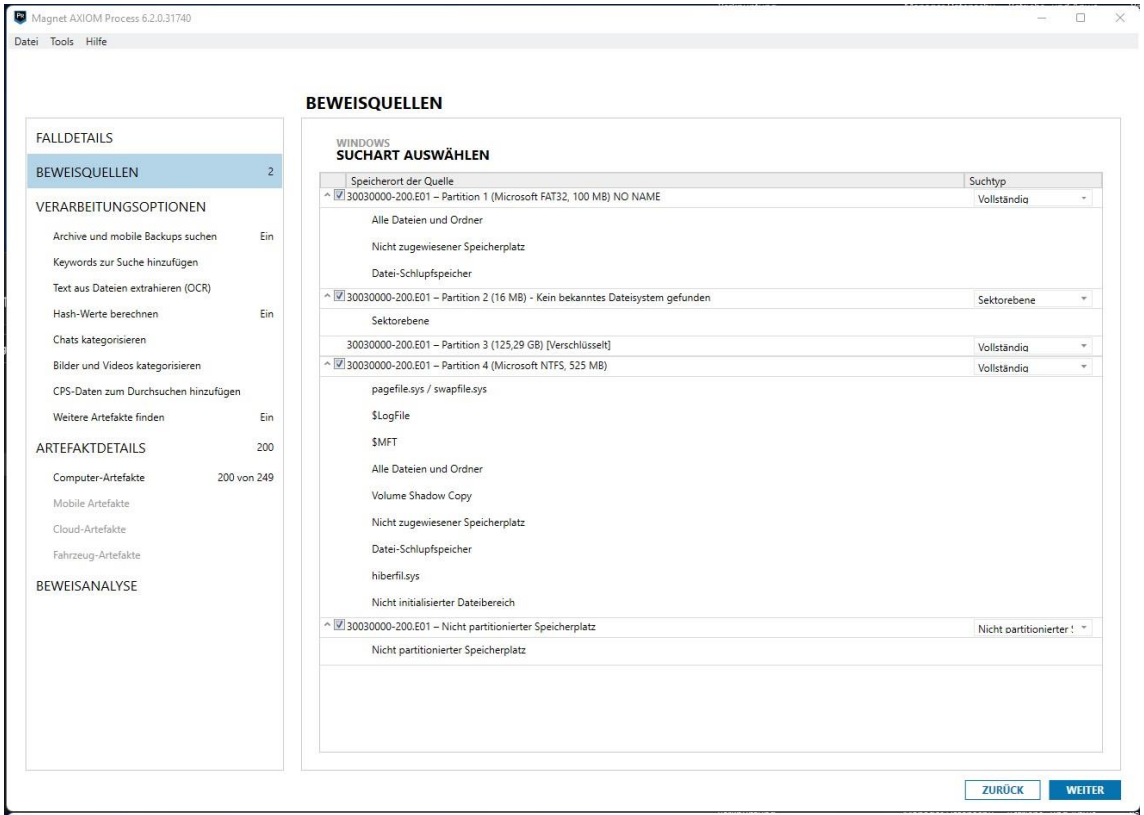

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISQUELLEN
FALLDETAILS
BEWEISQUELLEN 2
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
WINDOWS
LADEN ODER SICHERN
BEWEISE LADEN
BEWEISE SICHERN
ZURÜCK
WEITER

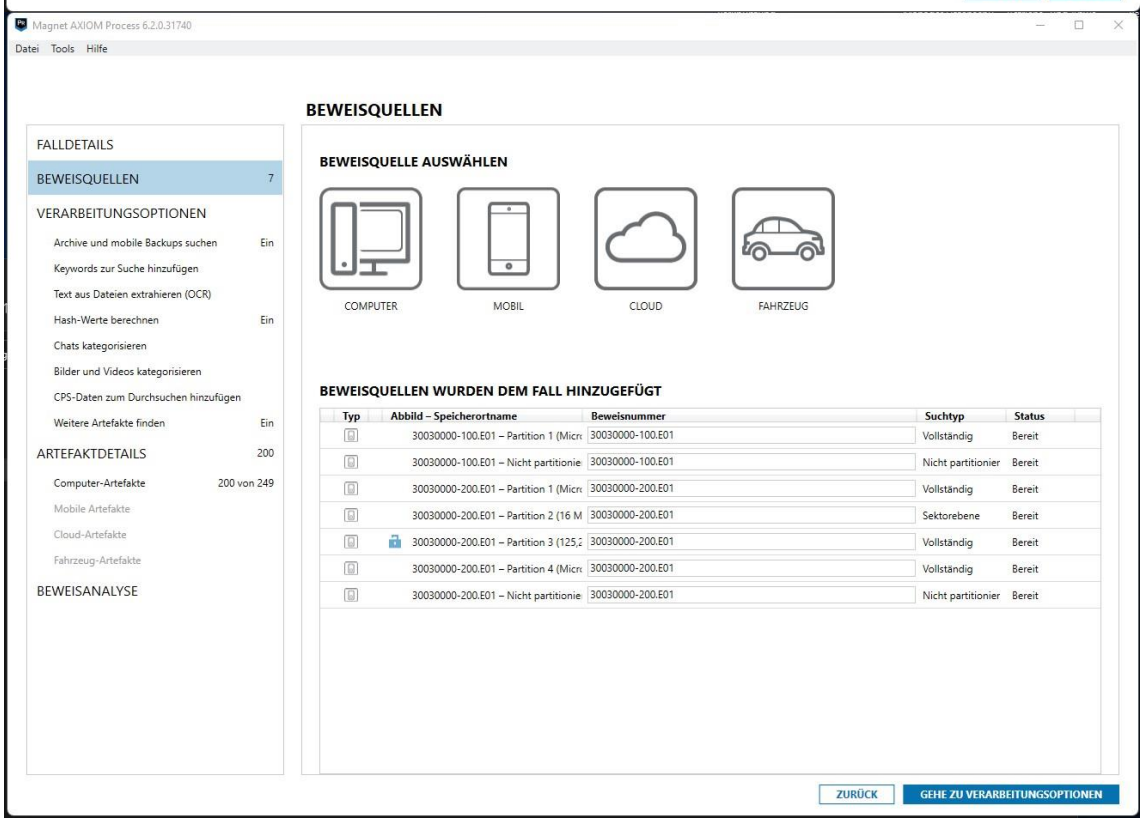

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISQUELLEN
FALLDETAILS
BEWEISQUELLEN 2
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
WINDOWS
BEWEISQUELLE AUSWÄHLEN
LAUFWERK
ABBILD
DATEIEN UND ORDNER
VOLUME SHADOW COPY
SPEICHER
ZURÜCK
WEITER

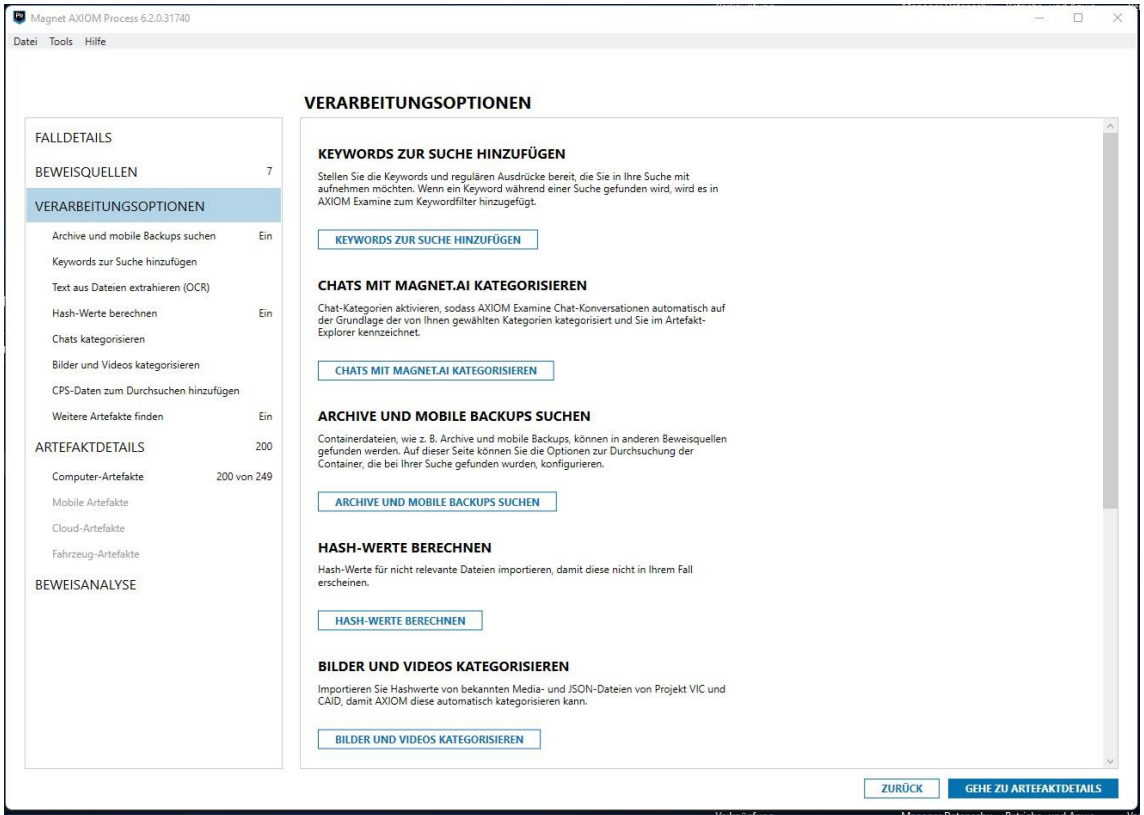

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISQUELLEN
FALLDETAILS
BEWEISQUELLEN 2
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hi
Weitere Artefakte finden
ARTEFAKTDETAILS
Computer-Artefakte
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
WINDOWS
BEWEISQUELLE AUSWÄHLEN
LAUFWERK
ABBILD
DATEIEN UND ORDNER
VOLUME SHADOW COPY
SPEICHER
Disk-Image auswählen
Dieser PC › FFM05 - SSD Beweissicherung (E:) › 30030000-200
30030000-200 durchsuchen
Organisieren
Neuer Ordner
Dieser PC
Bilder
Desktop
Dokumente
Downloads
Musik
Videos
Lokaler Datentr
SDXC (D:)
FFM05 - SSD Be
Name
Änderungsdatum
Typ
Größe
30030000-200.E01
25.06.2022 16:01
E01-Datei
1,535,863 KB
Dateiname:
30030000-200.E01
All Supported Images (*.E01, ...)
Öffnen
Abbrechen
ZURÜCK
WEITER

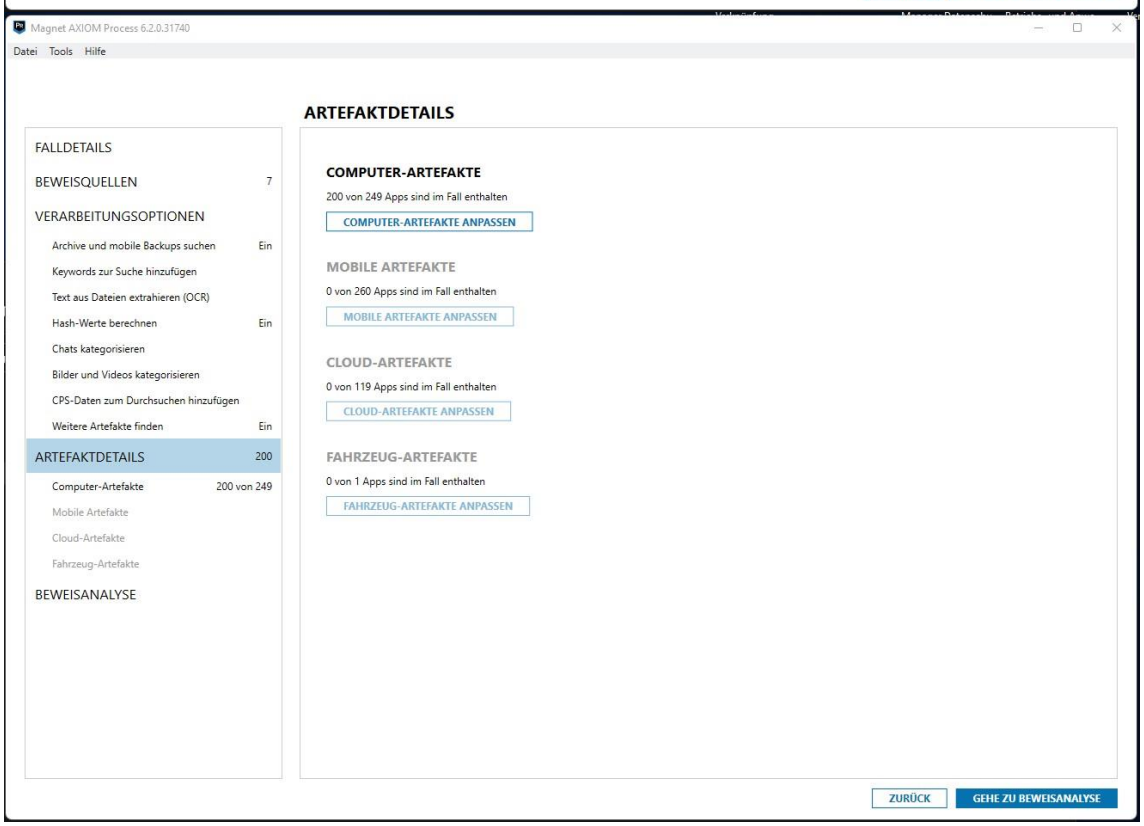

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISQUELLEN
FALLDETAILS
BEWEISQUELLEN 2
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
WINDOWS
DATEIEN UND ORDNER HINZUFÜGEN
ALLE LÖSCHEN
30030000-200.E01
Partition 1 (Microsoft FAT32, 100 MB) NO NAME
Partition 2 (16 MB) - Kein bekanntes Dateisystem gefunden
Partition 3 (125,29 GB) [Verschlüsselt]
Partition 4 (Microsoft NTFS, 525 MB)
Nicht partitionierter Speicherplatz
ZURÜCK
WEITER


Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISQUELLEN
FALLDETAILS
BEWEISQUELLEN 2
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
WINDOWS
ENTSCHLÜSSELUNGSOPTIONEN
Wählen Sie die verschlüsselten Beweisquellen, die Sie bearbeiten wollen, indem sie die erforderlichen Verschlüsselungsdetails für jede Quelle angeben. Wenn Sie das Passwort oder den Wiederherstellungsschlüssel nicht kennen, kann AXIOM Process bei manchen Beweisquellen versuchen, das Passwort mithilfe einer von Ihnen gewählten Passwortliste zu cracken. Wenn das Cracken des Passworts nicht erfolgreich ist, wird diese Quelle übersprungen.
Partition 3 (125,29 GB)
Verschlüsselungstyp Clear Key Bitlocker
AXIOM Process entschlüsselt diese Partition automatisch mit der Entschlüsselung per Clear Key Bitlocker. Sie müssen kein Passwort eingeben, um fortzufahren.
ZURÜCK
WEITER


Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISQUELLEN
FALLDETAILS
BEWEISQUELLEN 2
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
WINDOWS
SUCHART AUSWÄHLEN
Speicherort der Quelle
Suchtyp
30030000-200.E01 – Partition 1 (Microsoft FAT32, 100 MB) NO NAME
Vollständig
Alle Dateien und Ordner
Nicht zugewiesener Speicherplatz
Datei-Schlupfspeicher
30030000-200.E01 – Partition 2 (16 MB) - Kein bekanntes Dateisystem gefunden
Sektorebene
Sektorebene
30030000-200.E01 – Partition 3 (125,29 GB) [Verschlüsselt]
Vollständig
30030000-200.E01 – Partition 4 (Microsoft NTFS, 525 MB)
Vollständig
pagefile.sys / swapfile.sys
$LogFile
$MFT
Alle Dateien und Ordner
Volume Shadow Copy
Nicht zugewiesener Speicherplatz
Datei-Schlupfspeicher
hiberfil.sys
Nicht initialisierter Dateibereich
30030000-200.E01 – Nicht partitionierter Speicherplatz
Nicht partitionierter Speicherplatz
ZURÜCK
WEITER


Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISQUELLEN
FALLDETAILS
BEWEISQUELLEN 7
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
BEWEISQUELLE AUSWÄHLEN
COMPUTER
MOBIL
CLOUD
FAHRZEUG
BEWEISQUELLEN WURDEN DEM FALL HINZUGEFÜGT
Typ
Abbild – Speicherortname
Beweisnummer
Suchtyp
Status
30030000-100.E01 – Partition 1 (Micr
30030000-100.E01
Vollständig
Bereit
30030000-100.E01 – Nicht partitionie
30030000-100.E01
Nicht partitionier
Bereit
30030000-200.E01 – Partition 1 (Micr
30030000-200.E01
Vollständig
Bereit
30030000-200.E01 – Partition 2 (16 M
30030000-200.E01
Sektorebene
Bereit
30030000-200.E01 – Partition 3 (125,
30030000-200.E01
Vollständig
Bereit
30030000-200.E01 – Partition 4 (Micr
30030000-200.E01
Vollständig
Bereit
30030000-200.E01 – Nicht partitionie
30030000-200.E01
Nicht partitionier
Bereit
ZURÜCK
GEHE ZU VERARBEITUNGSOPTIONEN


Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
VERARBEITUNGSOPTIONEN
FALLDETAILS
BEWEISQUELLEN 7
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
KEYWORDS ZUR SUCHE HINZUFÜGEN
Stellen Sie die Keywords und regulären Ausdrücke bereit, die Sie in Ihre Suche mit aufnehmen möchten. Wenn ein Keyword während einer Suche gefunden wird, wird es in AXIOM Examine zum Keywordfilter hinzugefügt.
KEYWORDS ZUR SUCHE HINZUFÜGEN
CHATS MIT MAGNET.AI KATEGORISIEREN
Chat-Kategorien aktivieren, sodass AXIOM Examine Chat-Konversationen automatisch auf der Grundlage der von Ihnen gewählten Kategorien kategorisiert und Sie im Artefakt-Explorer kennzeichnet.
CHATS MIT MAGNET.AI KATEGORISIEREN
ARCHIVE UND MOBILE BACKUPS SUCHEN
Containerdateien, wie z. B. Archive und mobile Backups, können in anderen Beweisquellen gefunden werden. Auf dieser Seite können Sie die Optionen zur Durchsuchung der Container, die bei Ihrer Suche gefunden wurden, konfigurieren.
ARCHIVE UND MOBILE BACKUPS SUCHEN
HASH-WERTE BERECHNEN
Hash-Werte für nicht relevante Dateien importieren, damit diese nicht in Ihrem Fall erscheinen.
HASH-WERTE BERECHNEN
BILDER UND VIDEOS KATEGORISIEREN
Importieren Sie Hashwerte von bekannten Media- und JSON-Dateien von Projekt VIC und CAID, damit AXIOM diese automatisch kategorisieren kann.
BILDER UND VIDEOS KATEGORISIEREN
ZURÜCK
GEHE ZU ARTEFAKTDETAILS


Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
ARTEFAKTDETAILS
FALLDETAILS
BEWEISQUELLEN 7
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
COMPUTER-ARTEFAKTE
200 von 249 Apps sind im Fall enthalten
COMPUTER-ARTEFAKTE ANPASSEN
MOBILE ARTEFAKTE
0 von 260 Apps sind im Fall enthalten
MOBILE ARTEFAKTE ANPASSEN
CLOUD-ARTEFAKTE
0 von 119 Apps sind im Fall enthalten
CLOUD-ARTEFAKTE ANPASSEN
FAHRZEUG-ARTEFAKTE
0 von 1 Apps sind im Fall enthalten
FAHRZEUG-ARTEFAKTE ANPASSEN
ZURÜCK
GEHE ZU BEWEISANALYSE

Magnet AXIOM Process 6.2.0.31740

Datei Tools Hilfe

HASH-WERTE BERECHNEN

FALLDETAILS

BEWEISQUELLEN 7

VERARBEITUNGSOPTIONEN

- Archive und mobile Backups suchen Ein
- Keywords zur Suche hinzufügen
- Text aus Dateien extrahieren (OCR)
- Hash-Werte berechnen Ein
- Chats kategorisieren
- Bilder und Videos kategorisieren
- CPS-Daten zum Durchsuchen hinzufügen
- Weitere Artefakte finden Ein

ARTEFAKTDETAILS 200

- Computer-Artefakte 200 von 249
- Mobile Artefakte
- Cloud-Artefakte
- Fahrzeug-Artefakte

BEWEISANALYSE

HASHWERTE ALLER DATEIEN BERECHNEN

Ermöglichen Sie AXIOM Process, die Hash-Werte für jede Datei in einer Beweisquelle zu berechnen, sodass AXIOM Examine die Hash-Werte für jede Datei im Abschnitt Details des Dateisystem Explorers anzeigt.

Konfigurieren Sie Hash-Einstellungen, um das Format zu ändern, in dem diese Hash-Werte berechnet werden, um zu ändern, wo importierte Hash-Werte gespeichert werden, und um die Größe der gehashten Dateien zu begrenzen, um die Bearbeitungszeiten zu verringern.

☑ Hashwerte aller Dateien berechnen, damit AXIOM Examine diese Werte im Dateisystem Explorer anzeigt.

HASH-EINSTELLUNGEN KONFIGURIEREN

TAG-DATEIEN MIT ÜBEREINSTIMMENDEN HASH-WERTEN

Importieren Sie MD5 und SHA1 Hash-Werte für Dateien, für Ihren Fall möglicherweise interessant sind, sodass Examine die übereinstimmenden Dateien im Dateisystem-Explorer markiert.

Sie können zum Beispiel Hash-Werte für bekannte Dokumente oder Dateien eingeben, sodass Sie schnell ermitteln können, ob diese Dateien in Ihrem Beweis bereits vorhanden sind. Jeder MD5- und SHA1-Hashwert muss in einer eigenen Zeile erscheinen. AXIOM berechnet die Hashwerte für alle Dateien, wenn diese Funktion aktiviert ist.

DATEI HINZUFÜGEN ALLE DATEIEN AKTIVIEREN Geladene Einträge: 0

Aktivie	Dateiquelle	Ladedatum	Anzahl an Einträge	Tag

NICHT RELEVANTE DATEIEN IGNORIEREN

MD5-, SHA1- und NSRL-Hashwerte für Dateien importieren, von denen Sie wissen, dass diese nicht für Ihren Fall relevant sind, sodass AXIOM für diese Dateien keine Artefakte erstellt. Sie können beispielsweise Hashwerte für standardmäßige OS-Icons und Bildschirmschoner bereitstellen, damit diese Ihre Nachweise nicht überladen. Jeder MD5-, SHA1- und NSRL-Hashwert muss in einer eigenen Zeile stehen.

ZURÜCK GEHE ZU CHATS KATEGORISIEREN

Magnet AXIOM Process 6.2.0.31740

Datei Tools Hilfe

BILDER UND VIDEOS KATEGORISIEREN

FALLDETAILS

BEWEISQUELLEN 7

VERARBEITUNGSOPTIONEN

- Archive und mobile Backups suchen Ein
- Keywords zur Suche hinzufügen
- Text aus Dateien extrahieren (OCR)
- Hash-Werte berechnen Ein
- Chats kategorisieren
- Bilder und Videos kategorisieren
- CPS-Daten zum Durchsuchen hinzufügen
- Weitere Artefakte finden Ein

ARTEFAKTDETAILS 200

- Computer-Artefakte 200 von 249
- Mobile Artefakte
- Cloud-Artefakte
- Fahrzeug-Artefakte

BEWEISANALYSE

BILDER MIT MAGNET.AI VERARBEITEN

Wenn Sie Bilder mit Magnet.AI verarbeiten, hilft Ihnen AXIOM Examine, Bilder zu finden, die für Ihre Untersuchung relevant sind. Magnet.AI bearbeitet alle Bilddateien und Elemente, die Bilder enthalten (beispielsweise ein Bild, das in eine DOC-Datei eingebettet ist).

BILDERVERGLEICH ZUSAMMENSTELLEN

Sie können in AXIOM Examine nach Bildern suchen, die einem Referenzbild in Ihrem Fall ähneln, oder ein externes Bild importieren, um ähnliche Bilder zu finden.

☑ Bildervergleich zusammenstellen, um das Auffinden ähnlicher Bilder in AXIOM Examine zu ermöglichen

BILDER MIT MAGNET.AI KATEGORISIEREN

Wenn Sie Bilderkategorien aktivieren, werden diese automatisch von AXIOM Examine kategorisiert und im Artefakt Explorer gekennzeichnet.

● zeigt Kategorien an, die mehr Verarbeitungszeit benötigen

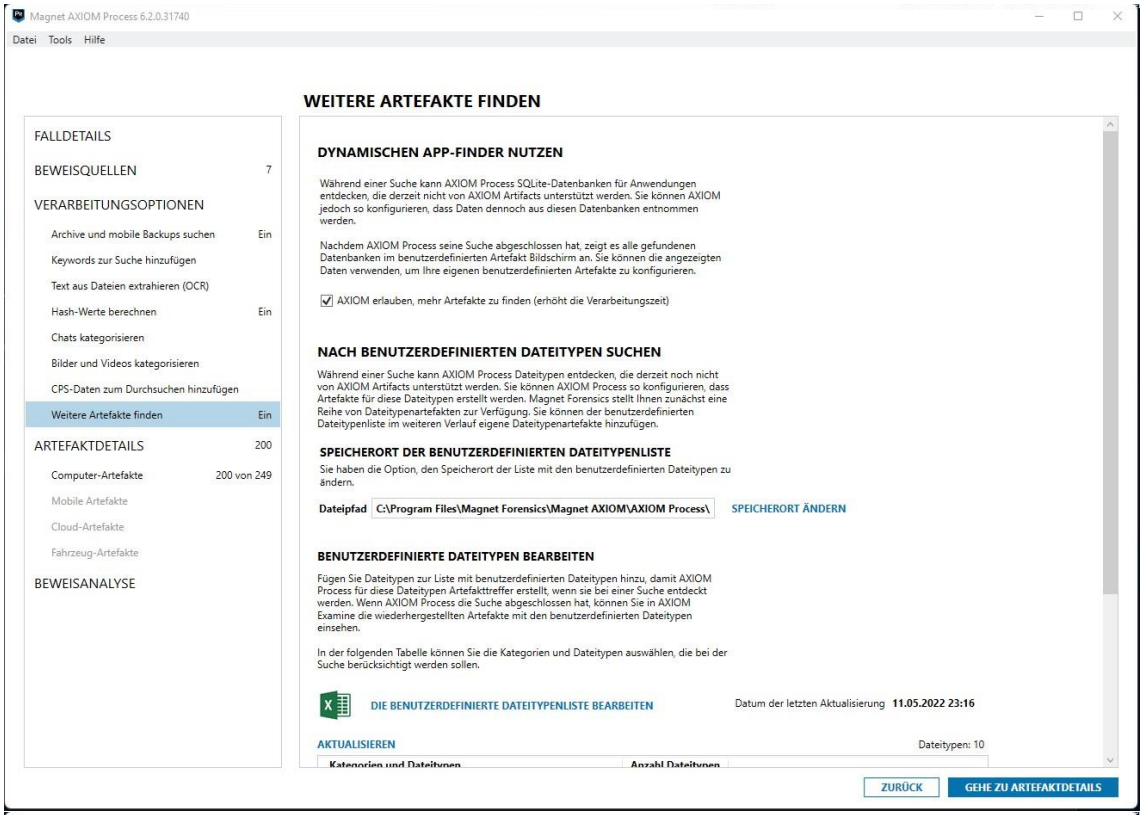
Aktiviert	Kategorie	Tag
☐	Ausweisdokumente	
☐	Bildschirmaufnahmen	
☐	Dokumente	
☐	Drogen	
☐	Dronen/UAVs	
☐	Fahrzeuge (Autos/LKWs/Vans/Buss	

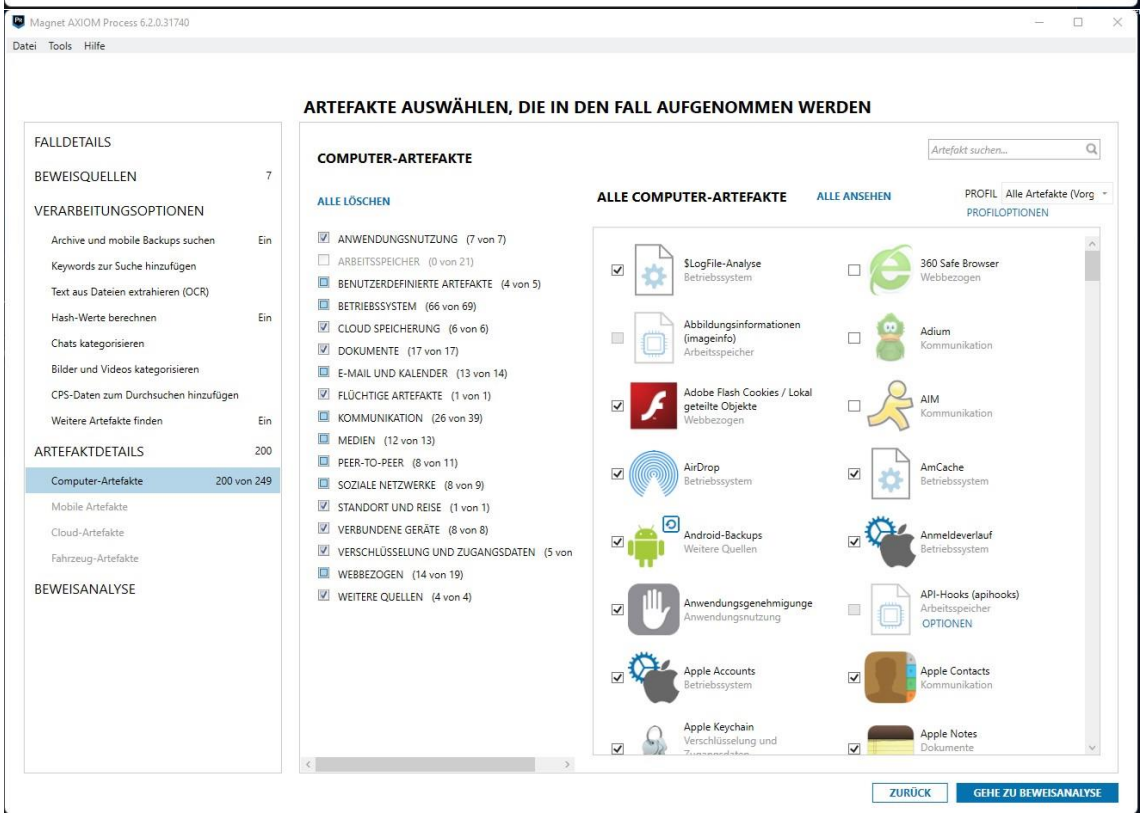
BILDER UND VIDEOS NACH HASHWERT KATEGORISIEREN

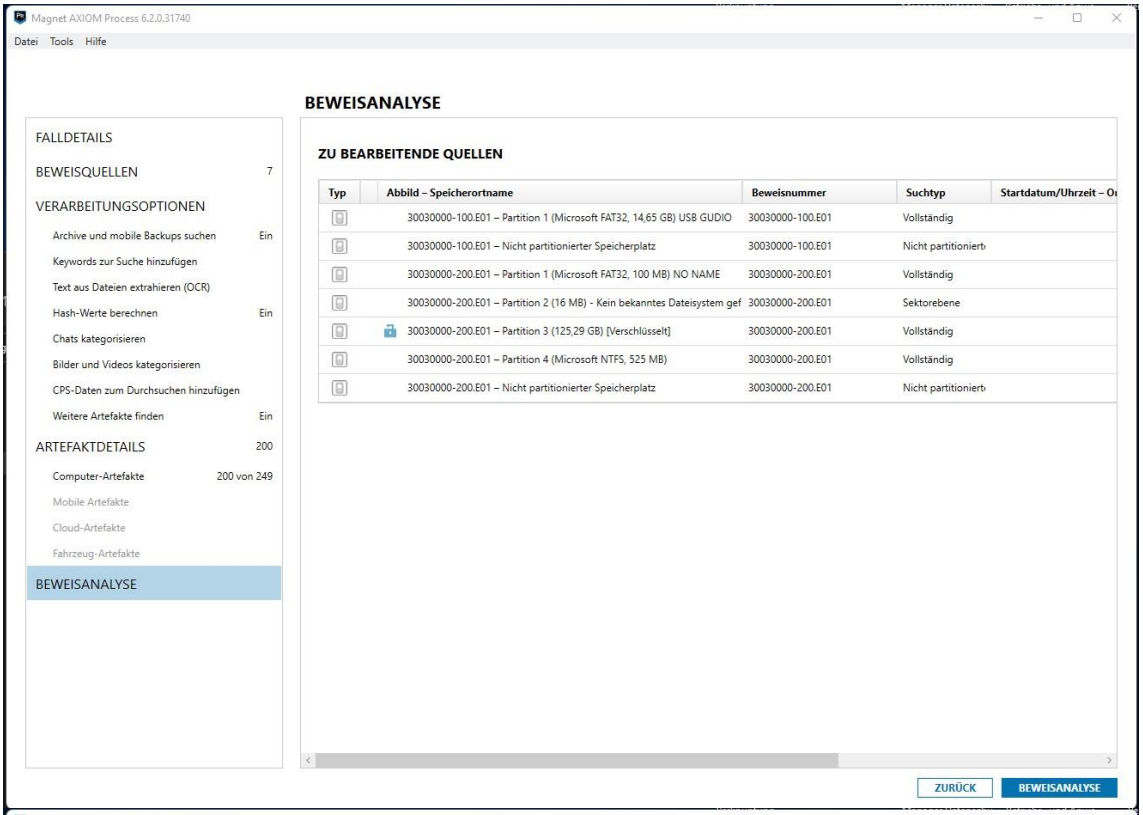
Importieren Sie Hash-Listen mit MD5- oder SHA1-Hashes für Bilder und Videos, sodass AXIOM Examine die gefundenen Bilder und Videos automatisch mit entsprechenden Hashes aus diesen Dateien kategorisiert. Sie können JSON-Dateien aus den Organisationen Project VIC und CAID oder Ihre eigenen Textdateien importieren. Nachdem Sie eine Hash-Liste importiert haben, können Sie die Liste einem Hash-Set hinzufügen und auswählen, welche Kategorien in dem Hash-Set aktualisiert werden sollen.

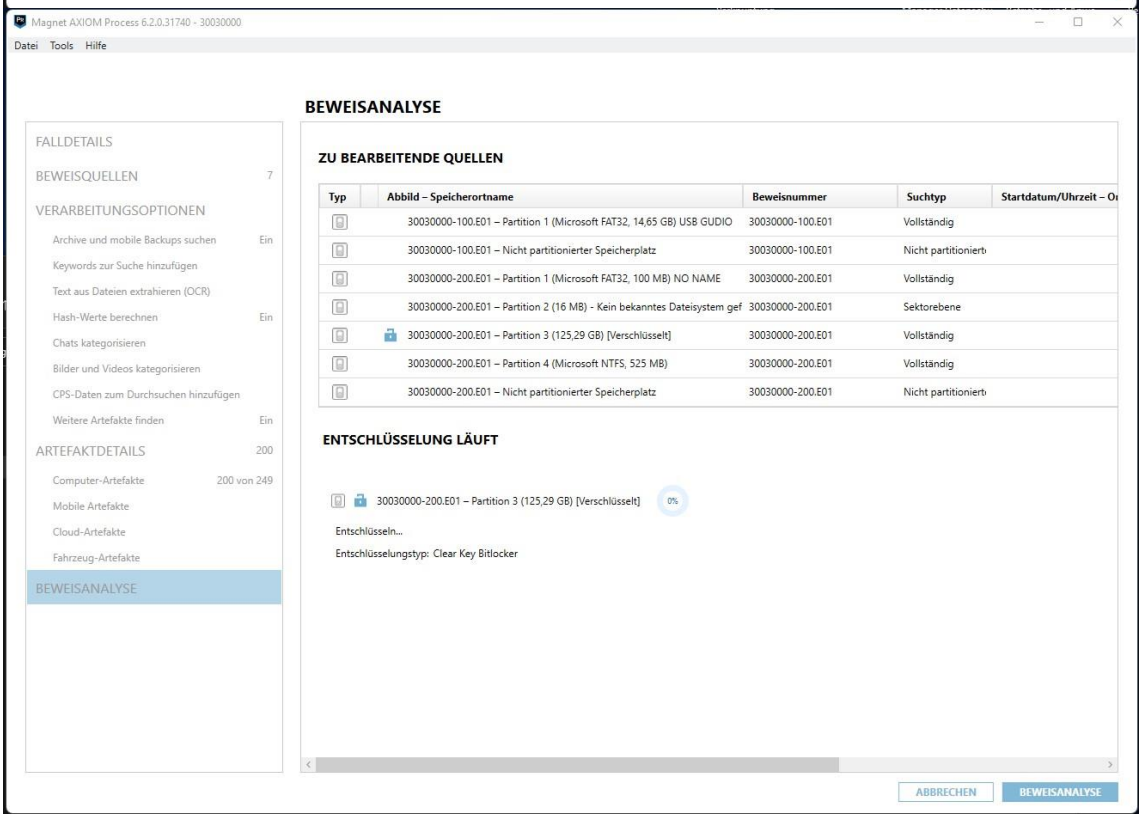
Durch die Reihenfolge der Hash-Sets in der Tabelle wird festgelegt, wie AXIOM Process die Bilder und Videos kategorisiert, wenn in mehr als einem

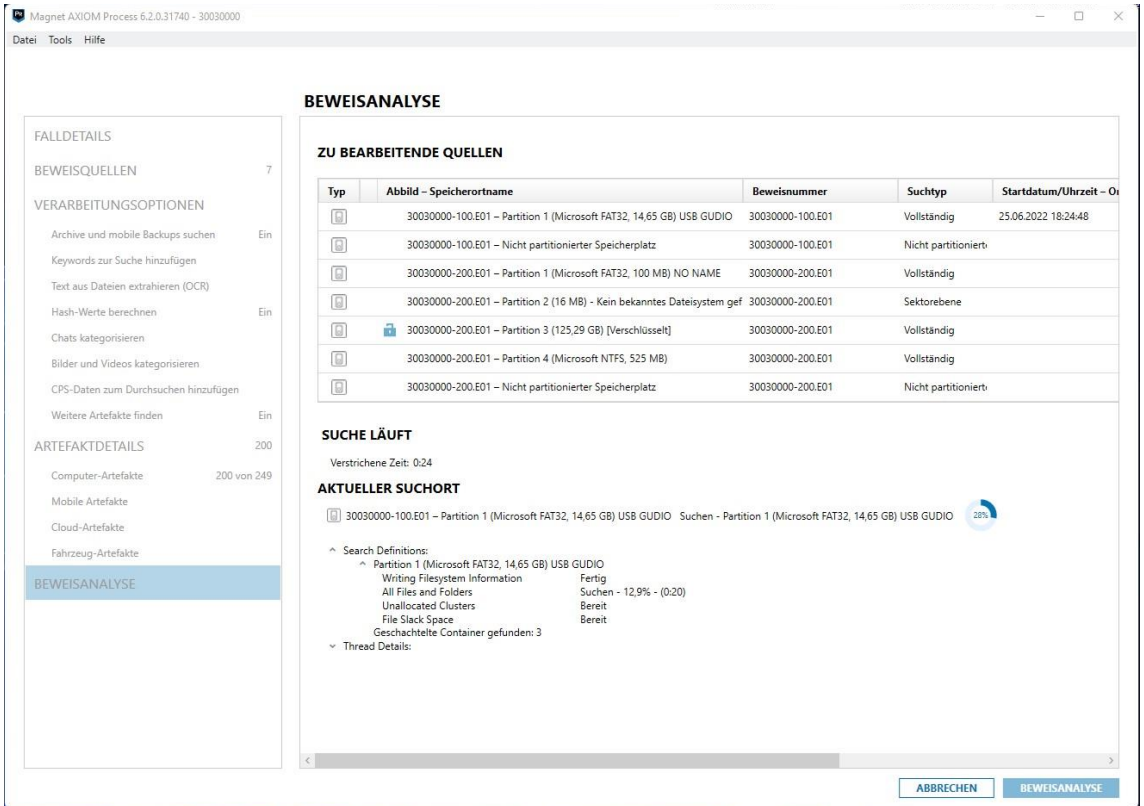
ZURÜCK GEHE ZU CPS-DATEN ZUM DURCHSUCHEN HINZUFÜGEN

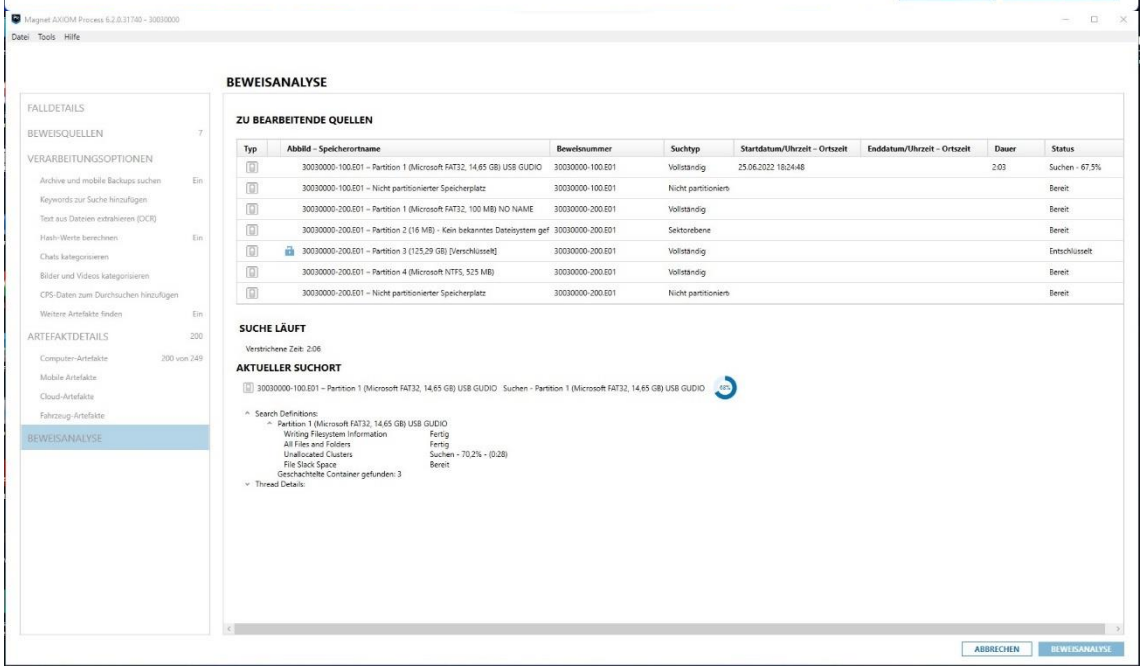

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
WEITERE ARTEFAKTE FINDEN
FALLDETAILS
BEWEISQUELLEN 7
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
DYNAMISCHEN APP-FINDER NUTZEN
Während einer Suche kann AXIOM Process SQLite-Datenbanken für Anwendungen entdecken, die derzeit nicht von AXIOM Artifacts unterstützt werden. Sie können AXIOM jedoch so konfigurieren, dass Daten dennoch aus diesen Datenbanken entnommen werden.
Nachdem AXIOM Process seine Suche abgeschlossen hat, zeigt es alle gefundenen Datenbanken im benutzerdefinierten Artefakt Bildschirm an. Sie können die angezeigten Daten verwenden, um Ihre eigenen benutzerdefinierten Artefakte zu konfigurieren.
AXIOM erlauben, mehr Artefakte zu finden (erhöht die Verarbeitungszeit)
NACH BENUTZERDEFINIERTEN DATEITYPEN SUCHEN
Während einer Suche kann AXIOM Process Dateitypen entdecken, die derzeit noch nicht von AXIOM Artifacts unterstützt werden. Sie können AXIOM Process so konfigurieren, dass Artefakte für diese Dateitypen erstellt werden. Magnet Forensics stellt Ihnen zunächst eine Reihe von Dateitypenartefakten zur Verfügung. Sie können der benutzerdefinierten Dateitypenliste im weiteren Verlauf eigene Dateitypenartefakte hinzufügen.
SPEICHERORT DER BENUTZERDEFINIERTEN DATEITYPENLISTE
Sie haben die Option, den Speicherort der Liste mit den benutzerdefinierten Dateitypen zu ändern.
Dateipfad C:\Program Files\Magnet Forensics\Magnet AXIOM\AXIOM Process\
SPEICHERORT ÄNDERN
BENUTZERDEFINIERTE DATEITYPEN BEARBEITEN
Fügen Sie Dateitypen zur Liste mit benutzerdefinierten Dateitypen hinzu, damit AXIOM Process für diese Dateitypen Artefakttreffer erstellt, wenn sie bei einer Suche entdeckt werden. Wenn AXIOM Process die Suche abgeschlossen hat, können Sie in AXIOM Examine die wiederhergestellten Artefakte mit den benutzerdefinierten Dateitypen einsehen.
In der folgenden Tabelle können Sie die Kategorien und Dateitypen auswählen, die bei der Suche berücksichtigt werden sollen.
DIE BENUTZERDEFINIERTE DATEITYPENLISTE BEARBEITEN
Datum der letzten Aktualisierung 11.05.2022 23:16
AKTUALISIEREN
Dateitypen: 10
ZURÜCK
GEHE ZU ARTEFAKTDETAILS

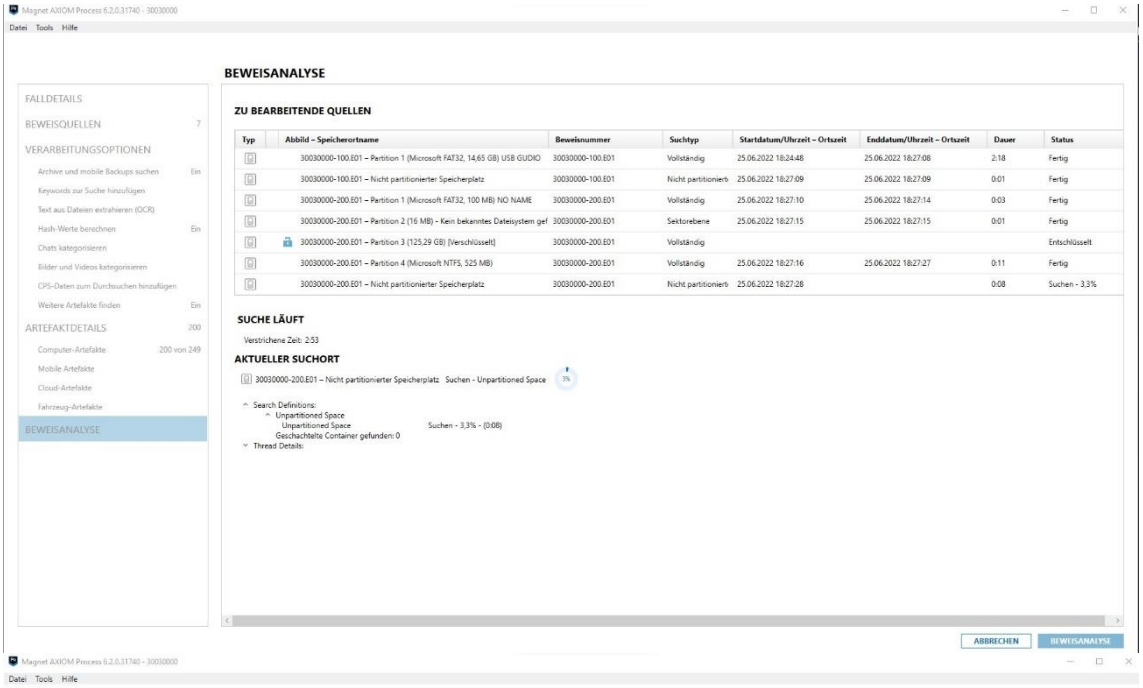

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
ARTEFAKTE AUSWÄHLEN, DIE IN DEN FALL AUFGENOMMEN WERDEN
FALLDETAILS
BEWEISQUELLEN 7
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
COMPUTER-ARTEFAKTE
Artefakt suchen...
ALLE LÖSCHEN
ALLE COMPUTER-ARTEFAKTE
ALLE ANSEHEN
PROFIL Alle Artefakte (Vorg
PROFILOPTIONEN
ANWENDUNGSNUTZUNG (7 von 7)
ARBEITSSPEICHER (0 von 21)
BENUTZERDEFINIERTE ARTEFAKTE (4 von 5)
BETRIEBSSYSTEM (66 von 69)
CLOUD SPEICHERUNG (6 von 6)
DOKUMENTE (17 von 17)
E-MAIL UND KALENDER (13 von 14)
FLÜCHTIGE ARTEFAKTE (1 von 1)
KOMMUNIKATION (26 von 39)
MEDIEN (12 von 13)
PEER-TO-PEER (8 von 11)
SOZIALE NETZWERKE (8 von 9)
STANDORT UND REISE (1 von 1)
VERBUNDENE GERÄTE (8 von 8)
VERSCHLÜSSELUNG UND ZUGANGSDATEN (5 von
WEBBEZOGEN (14 von 19)
WEITERE QUELLEN (4 von 4)
$LogFile-Analyse Betriebssystem
360 Safe Browser Webbezogen
Abbildungsinformationen (imageinfo) Arbeitsspeicher
Adium Kommunikation
Adobe Flash Cookies / Lokal geteilte Objekte Webbezogen
AIM Kommunikation
AirDrop Betriebssystem
AmCache Betriebssystem
Android-Backups Weitere Quellen
Anmeldeverlauf Betriebssystem
Anwendungsgenehmigunge Anwendungsnutzung
API-Hooks (apihooks) Arbeitsspeicher OPTIONEN
Apple Accounts Betriebssystem
Apple Contacts Kommunikation
Apple Keychain Verschlüsselung und
Apple Notes Dokumente
ZURÜCK
GEHE ZU BEWEISANALYSE

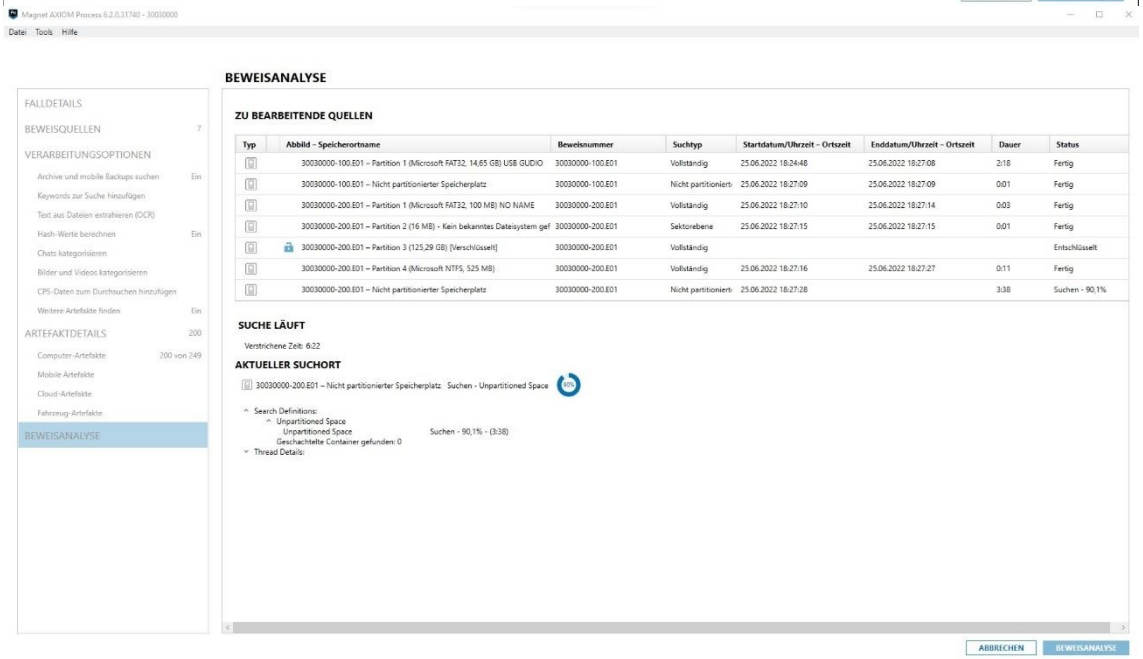

Magnet AXIOM Process 6.2.0.31740
Datei Tools Hilfe
BEWEISANALYSE
FALLDETAILS
BEWEISQUELLEN 7
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
ZU BEARBEITENDE QUELLEN
Typ
Abbild – Speicherortname
Beweisnummer
Suchtyp
Startdatum/Uhrzeit – Or
30030000-100.E01 – Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO 30030000-100.E01 Vollständig
30030000-100.E01 – Nicht partitionierter Speicherplatz 30030000-100.E01 Nicht partitioniert
30030000-200.E01 – Partition 1 (Microsoft FAT32, 100 MB) NO NAME 30030000-200.E01 Vollständig
30030000-200.E01 – Partition 2 (16 MB) - Kein bekanntes Dateisystem gef 30030000-200.E01 Sektorebene
30030000-200.E01 – Partition 3 (125,29 GB) [Verschlüsselt] 30030000-200.E01 Vollständig
30030000-200.E01 – Partition 4 (Microsoft NTFS, 525 MB) 30030000-200.E01 Vollständig
30030000-200.E01 – Nicht partitionierter Speicherplatz 30030000-200.E01 Nicht partitioniert
ZURÜCK
BEWEISANALYSE

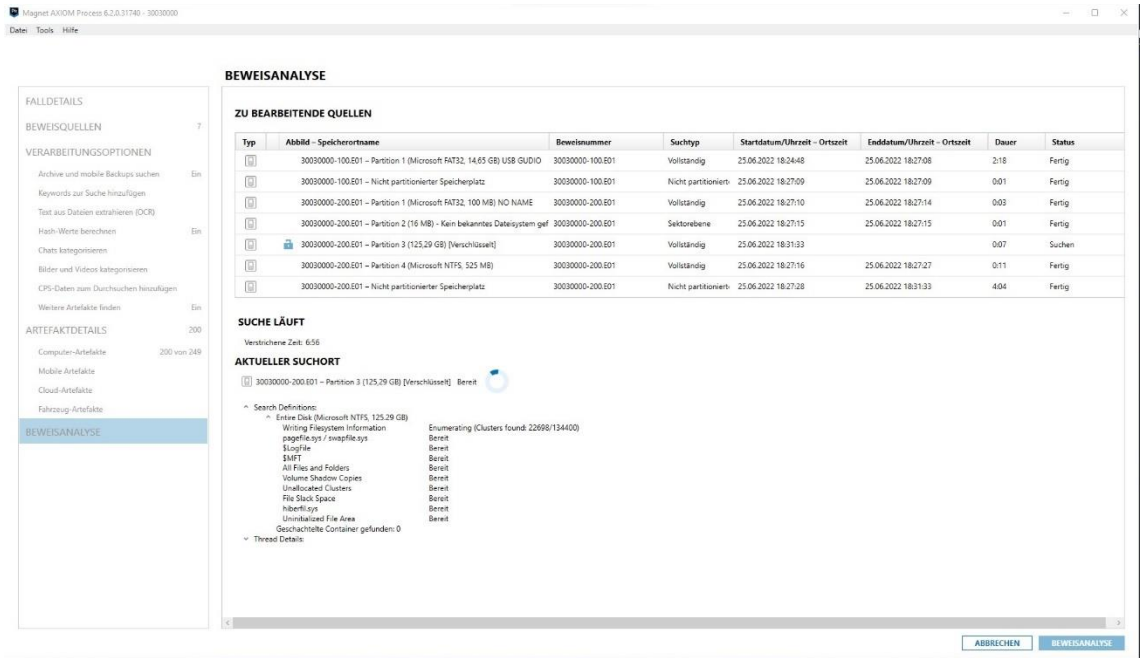

Magnet AXIOM Process 6.2.0.31740 - 30030000
Datei Tools Hilfe
BEWEISANALYSE
FALLDETAILS
BEWEISQUELLEN 7
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
ZU BEARBEITENDE QUELLEN
Typ
Abbild – Speicherortname
Beweisnummer
Suchtyp
Startdatum/Uhrzeit – Or
30030000-100.E01 – Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO 30030000-100.E01 Vollständig
30030000-100.E01 – Nicht partitionierter Speicherplatz 30030000-100.E01 Nicht partitioniert
30030000-200.E01 – Partition 1 (Microsoft FAT32, 100 MB) NO NAME 30030000-200.E01 Vollständig
30030000-200.E01 – Partition 2 (16 MB) - Kein bekanntes Dateisystem gef 30030000-200.E01 Sektorebene
30030000-200.E01 – Partition 3 (125,29 GB) [Verschlüsselt] 30030000-200.E01 Vollständig
30030000-200.E01 – Partition 4 (Microsoft NTFS, 525 MB) 30030000-200.E01 Vollständig
30030000-200.E01 – Nicht partitionierter Speicherplatz 30030000-200.E01 Nicht partitioniert
ENTSCHLÜSSELUNG LÄUFT
30030000-200.E01 – Partition 3 (125,29 GB) [Verschlüsselt]
0%
Entschlüsseln...
Entschlüsselungstyp: Clear Key Bitlocker
ABBRECHEN
BEWEISANALYSE

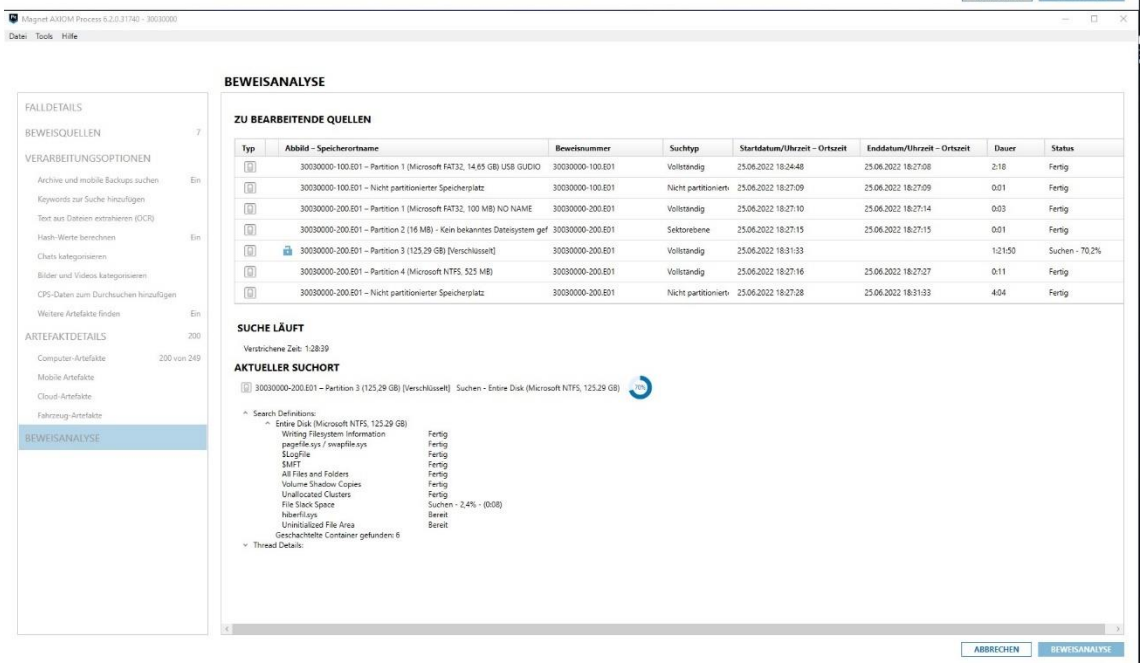

Magnet AXIOM Process 6.2.0.31740 - 30030000
Datei Tools Hilfe
BEWEISANALYSE
FALLDETAILS
BEWEISQUELLEN 7
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
ZU BEARBEITENDE QUELLEN
Typ
Abbild – Speicherortname
Beweisnummer
Suchtyp
Startdatum/Uhrzeit – Or
30030000-100.E01 – Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO 30030000-100.E01 Vollständig 25.06.2022 18:24:48
30030000-100.E01 – Nicht partitionierter Speicherplatz 30030000-100.E01 Nicht partitioniert
30030000-200.E01 – Partition 1 (Microsoft FAT32, 100 MB) NO NAME 30030000-200.E01 Vollständig
30030000-200.E01 – Partition 2 (16 MB) - Kein bekanntes Dateisystem gef 30030000-200.E01 Sektorebene
30030000-200.E01 – Partition 3 (125,29 GB) [Verschlüsselt] 30030000-200.E01 Vollständig
30030000-200.E01 – Partition 4 (Microsoft NTFS, 525 MB) 30030000-200.E01 Vollständig
30030000-200.E01 – Nicht partitionierter Speicherplatz 30030000-200.E01 Nicht partitioniert
SUCHE LÄUFT
Verstrichene Zeit: 0:24
AKTUELLER SUCHORT
30030000-100.E01 – Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO Suchen - Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO 28%
Search Definitions:
Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO
Writing Filesystem Information Fertig
All Files and Folders Suchen - 12,9% - (0:20)
Unallocated Clusters Bereit
File Slack Space Bereit
Geschachtelte Container gefunden: 3
Thread Details:
ABBRECHEN
BEWEISANALYSE

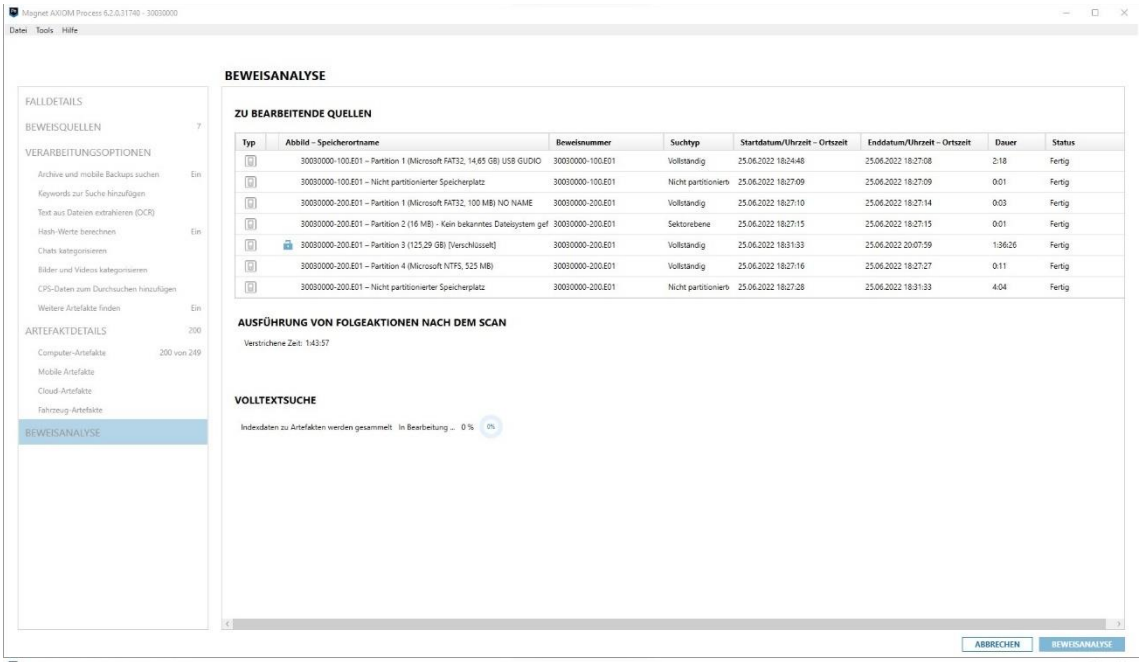

Magnet AXIOM Process 6.2.0.31740 - 30030000
Datei Tools Hilfe
BEWEISANALYSE
FALLDETAILS
BEWEISQUELLEN 7
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
ZU BEARBEITENDE QUELLEN
Typ
Abbild - Speicherortname
Beweisnummer
Suchtyp
Startdatum/Uhrzeit - Ortszeit
Enddatum/Uhrzeit - Ortszeit
Dauer
Status
30030000-100.E01 – Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO 30030000-100.E01 Vollständig 25.06.2022 18:24:48 2:03 Suchen - 67,5%
30030000-100.E01 – Nicht partitionierter Speicherplatz 30030000-100.E01 Nicht partitioniert Bereit
30030000-200.E01 – Partition 1 (Microsoft FAT32, 100 MB) NO NAME 30030000-200.E01 Vollständig Bereit
30030000-200.E01 – Partition 2 (16 MB) - Kein bekanntes Dateisystem gef 30030000-200.E01 Sektorebene Bereit
30030000-200.E01 – Partition 3 (125,29 GB) [Verschlüsselt] 30030000-200.E01 Vollständig Entschlüsselt
30030000-200.E01 – Partition 4 (Microsoft NTFS, 525 MB) 30030000-200.E01 Vollständig Bereit
30030000-200.E01 – Nicht partitionierter Speicherplatz 30030000-200.E01 Nicht partitioniert Bereit
SUCHE LÄUFT
Verstrichene Zeit: 2:06
AKTUELLER SUCHORT
30030000-100.E01 – Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO Suchen - Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO 68%
Search Definitions:
Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO
Writing Filesystem Information Fertig
All Files and Folders Fertig
Unallocated Clusters Suchen - 70,2% - (0:28)
File Slack Space Bereit
Geschachtelte Container gefunden: 3
Thread Details:
ABBRECHEN
BEWEISANALYSE

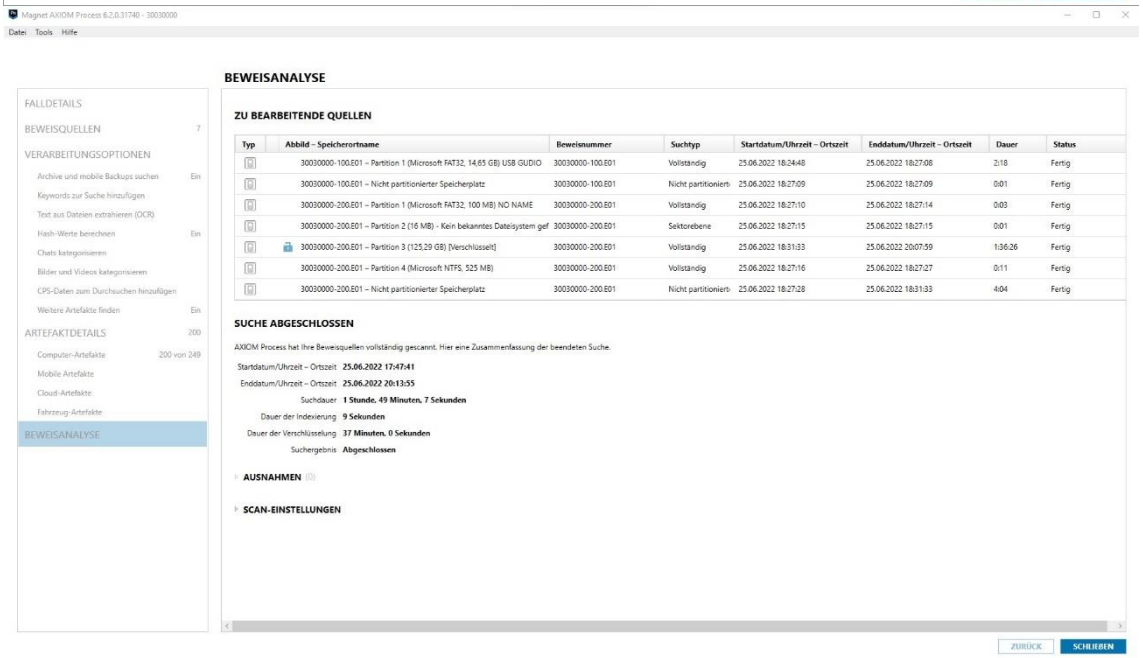

Magnet AXIOM Process 6.2.0.31740 - 30030000
Datei Tools Hilfe
BEWEISANALYSE
FALLDETAILS
BEWEISQUELLEN 7
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
ZU BEARBEITENDE QUELLEN
Typ | Abbild – Speicherortname | Beweisnummer | Suchtyp | Startdatum/Uhrzeit – Ortszeit | Enddatum/Uhrzeit – Ortszeit | Dauer | Status
30030000-100.E01 – Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO | 30030000-100.E01 | Vollständig | 25.06.2022 18:24:48 | 25.06.2022 18:27:08 | 2:18 | Fertig
30030000-100.E01 – Nicht partitionierter Speicherplatz | 30030000-100.E01 | Nicht partitionierb | 25.06.2022 18:27:09 | 25.06.2022 18:27:09 | 0:01 | Fertig
30030000-200.E01 – Partition 1 (Microsoft FAT32, 100 MB) NO NAME | 30030000-200.E01 | Vollständig | 25.06.2022 18:27:10 | 25.06.2022 18:27:14 | 0:03 | Fertig
30030000-200.E01 – Partition 2 (16 MB) - Kein bekanntes Dateisystem gef | 30030000-200.E01 | Sektorebene | 25.06.2022 18:27:15 | 25.06.2022 18:27:15 | 0:01 | Fertig
30030000-200.E01 – Partition 3 (125,29 GB) [Verschlüsselt] | 30030000-200.E01 | Vollständig | | | | Entschlüsselt
30030000-200.E01 – Partition 4 (Microsoft NTFS, 525 MB) | 30030000-200.E01 | Vollständig | 25.06.2022 18:27:16 | 25.06.2022 18:27:27 | 0:11 | Fertig
30030000-200.E01 – Nicht partitionierter Speicherplatz | 30030000-200.E01 | Nicht partitionierb | 25.06.2022 18:27:28 | | 0:08 | Suchen - 3,3%
SUCHE LÄUFT
Verstrichene Zeit: 2:53
AKTUELLER SUCHORT
30030000-200.E01 – Nicht partitionierter Speicherplatz Suchen - Unpartitioned Space 3%
Search Definitions:
Unpartitioned Space
Unpartitioned Space Suchen - 3,3% - (0:08)
Geschachtelte Container gefunden: 0
Thread Details:
ABBRECHEN
BEWEISANALYSE


Magnet AXIOM Process 6.2.0.31740 - 30030000
Datei Tools Hilfe
BEWEISANALYSE
FALLDETAILS
BEWEISQUELLEN 7
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
ZU BEARBEITENDE QUELLEN
Typ | Abbild - Speicherortname | Beweisnummer | Suchtyp | Startdatum/Uhrzeit – Ortszeit | Enddatum/Uhrzeit – Ortszeit | Dauer | Status
30030000-100.E01 – Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO | 30030000-100.E01 | Vollständig | 25.06.2022 18:24:48 | 25.06.2022 18:27:08 | 2:18 | Fertig
30030000-100.E01 – Nicht partitionierter Speicherplatz | 30030000-100.E01 | Nicht partitionierb | 25.06.2022 18:27:09 | 25.06.2022 18:27:09 | 0:01 | Fertig
30030000-200.E01 – Partition 1 (Microsoft FAT32, 100 MB) NO NAME | 30030000-200.E01 | Vollständig | 25.06.2022 18:27:10 | 25.06.2022 18:27:14 | 0:03 | Fertig
30030000-200.E01 – Partition 2 (16 MB) - Kein bekanntes Dateisystem gef | 30030000-200.E01 | Sektorebene | 25.06.2022 18:27:15 | 25.06.2022 18:27:15 | 0:01 | Fertig
30030000-200.E01 – Partition 3 (125,29 GB) [Verschlüsselt] | 30030000-200.E01 | Vollständig | | | | Entschlüsselt
30030000-200.E01 – Partition 4 (Microsoft NTFS, 525 MB) | 30030000-200.E01 | Vollständig | 25.06.2022 18:27:16 | 25.06.2022 18:27:27 | 0:11 | Fertig
30030000-200.E01 – Nicht partitionierter Speicherplatz | 30030000-200.E01 | Nicht partitionierb | 25.06.2022 18:27:28 | | 3:38 | Suchen - 90,1%
SUCHE LÄUFT
Verstrichene Zeit: 6:22
AKTUELLER SUCHORT
30030000-200.E01 – Nicht partitionierter Speicherplatz Suchen - Unpartitioned Space 90%
Search Definitions:
Unpartitioned Space
Unpartitioned Space Suchen - 90,1% - (3:38)
Geschachtelte Container gefunden: 0
Thread Details:
ABBRECHEN
BEWEISANALYSE

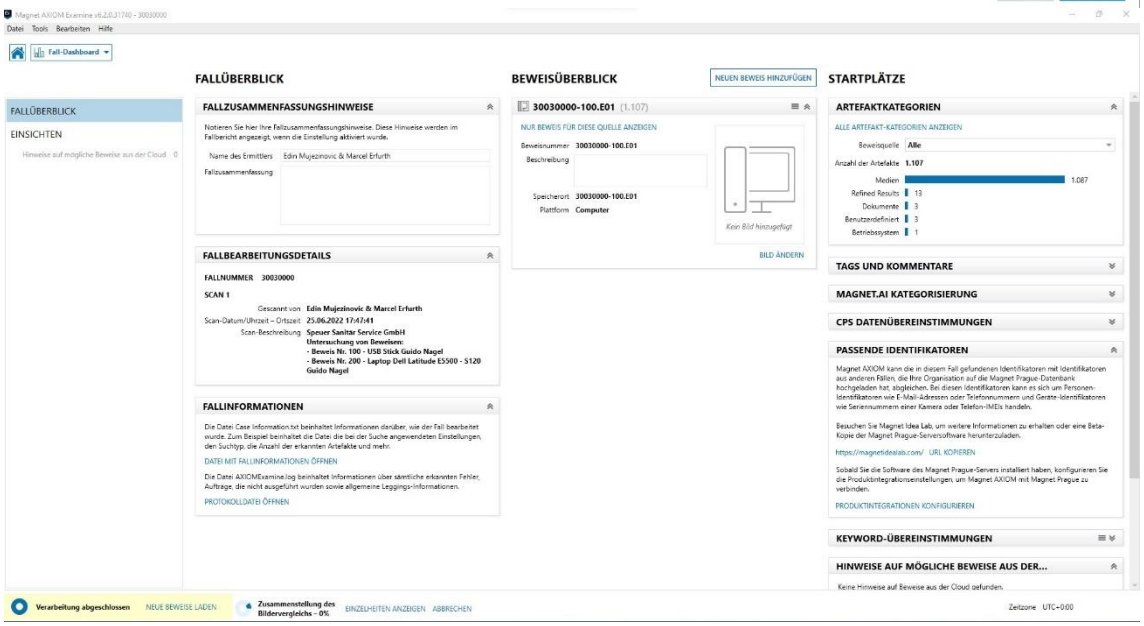

Magnet AXIOM Process 6.2.0.31740 - 30030000
Datei Tools Hilfe
BEWEISANALYSE
FALLDETAILS
BEWEISQUELLEN 7
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
ZU BEARBEITENDE QUELLEN
Typ | Abbild – Speicherortname | Beweisnummer | Suchtyp | Startdatum/Uhrzeit – Ortszeit | Enddatum/Uhrzeit – Ortszeit | Dauer | Status
30030000-100.E01 – Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO | 30030000-100.E01 | Vollständig | 25.06.2022 18:24:48 | 25.06.2022 18:27:08 | 2:18 | Fertig
30030000-100.E01 – Nicht partitionierter Speicherplatz | 30030000-100.E01 | Nicht partitioniert- | 25.06.2022 18:27:09 | 25.06.2022 18:27:09 | 0:01 | Fertig
30030000-200.E01 – Partition 1 (Microsoft FAT32, 100 MB) NO NAME | 30030000-200.E01 | Vollständig | 25.06.2022 18:27:10 | 25.06.2022 18:27:14 | 0:03 | Fertig
30030000-200.E01 – Partition 2 (16 MB) - Kein bekanntes Dateisystem gef | 30030000-200.E01 | Sektorebene | 25.06.2022 18:27:15 | 25.06.2022 18:27:15 | 0:01 | Fertig
30030000-200.E01 – Partition 3 (125,29 GB) [Verschlüsselt] | 30030000-200.E01 | Vollständig | 25.06.2022 18:31:33 | | 0:07 | Suchen
30030000-200.E01 – Partition 4 (Microsoft NTFS, 525 MB) | 30030000-200.E01 | Vollständig | 25.06.2022 18:27:16 | 25.06.2022 18:27:27 | 0:11 | Fertig
30030000-200.E01 – Nicht partitionierter Speicherplatz | 30030000-200.E01 | Nicht partitioniert- | 25.06.2022 18:27:28 | 25.06.2022 18:31:33 | 4:04 | Fertig
SUCHE LÄUFT
Verstrichene Zeit: 6:56
AKTUELLER SUCHORT
30030000-200.E01 – Partition 3 (125,29 GB) [Verschlüsselt] Bereit
Search Definitions:
Entire Disk (Microsoft NTFS, 125,29 GB)
Writing Filesystem Information Enumerating (Clusters found: 22698/134400)
pagefile.sys / swapfile.sys Bereit
$LogFile Bereit
$MFT Bereit
All Files and Folders Bereit
Volume Shadow Copies Bereit
Unallocated Clusters Bereit
File Slack Space Bereit
hiberfil.sys Bereit
Uninitialized File Area Bereit
Geschachtelte Container gefunden: 0
Thread Details:
ABBRECHEN
BEWEISANALYSE

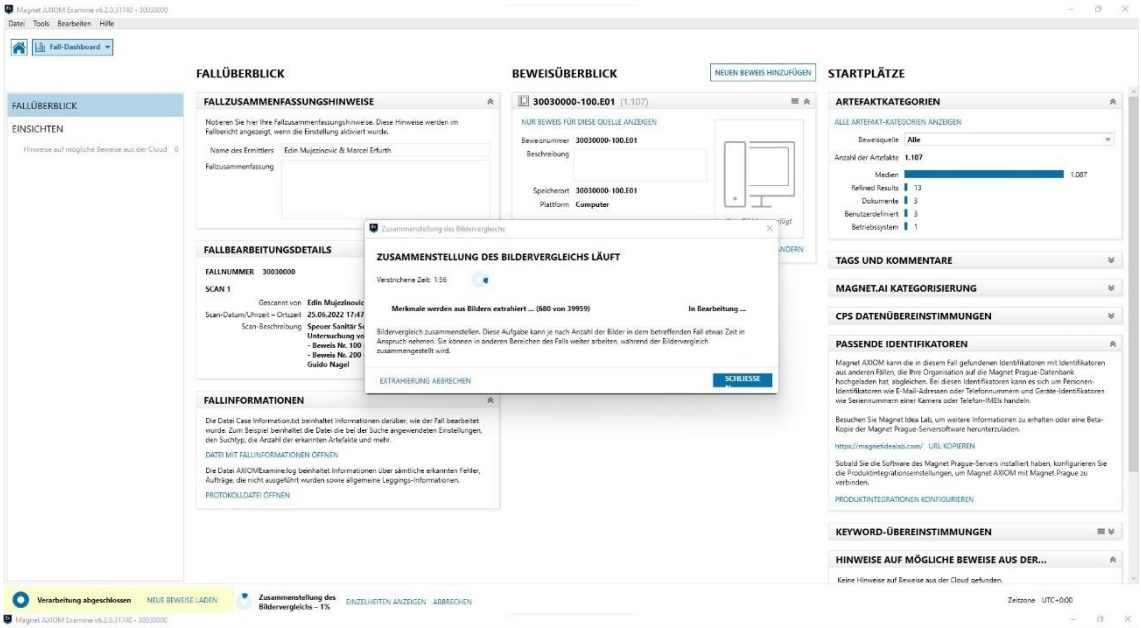

Magnet AXIOM Process 6.2.0.31740 - 30030000
Datei Tools Hilfe
BEWEISANALYSE
FALLDETAILS
BEWEISQUELLEN 7
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
ZU BEARBEITENDE QUELLEN
Typ | Abbild – Speicherortname | Beweisnummer | Suchtyp | Startdatum/Uhrzeit – Ortszeit | Enddatum/Uhrzeit – Ortszeit | Dauer | Status
30030000-100.E01 – Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO | 30030000-100.E01 | Vollständig | 25.06.2022 18:24:48 | 25.06.2022 18:27:08 | 2:18 | Fertig
30030000-100.E01 – Nicht partitionierter Speicherplatz | 30030000-100.E01 | Nicht partitioniert- | 25.06.2022 18:27:09 | 25.06.2022 18:27:09 | 0:01 | Fertig
30030000-200.E01 – Partition 1 (Microsoft FAT32, 100 MB) NO NAME | 30030000-200.E01 | Vollständig | 25.06.2022 18:27:10 | 25.06.2022 18:27:14 | 0:03 | Fertig
30030000-200.E01 – Partition 2 (16 MB) - Kein bekanntes Dateisystem gef | 30030000-200.E01 | Sektorebene | 25.06.2022 18:27:15 | 25.06.2022 18:27:15 | 0:01 | Fertig
30030000-200.E01 – Partition 3 (125,29 GB) [Verschlüsselt] | 30030000-200.E01 | Vollständig | 25.06.2022 18:31:33 | | 1:21:50 | Suchen - 70,2%
30030000-200.E01 – Partition 4 (Microsoft NTFS, 525 MB) | 30030000-200.E01 | Vollständig | 25.06.2022 18:27:16 | 25.06.2022 18:27:27 | 0:11 | Fertig
30030000-200.E01 – Nicht partitionierter Speicherplatz | 30030000-200.E01 | Nicht partitioniert- | 25.06.2022 18:27:28 | 25.06.2022 18:31:33 | 4:04 | Fertig
SUCHE LÄUFT
Verstrichene Zeit: 1:28:39
AKTUELLER SUCHORT
30030000-200.E01 – Partition 3 (125,29 GB) [Verschlüsselt] Suchen - Entire Disk (Microsoft NTFS, 125,29 GB)
Search Definitions:
Entire Disk (Microsoft NTFS, 125,29 GB)
Writing Filesystem Information Fertig
pagefile.sys / swapfile.sys Fertig
$LogFile Fertig
$MFT Fertig
All Files and Folders Fertig
Volume Shadow Copies Fertig
Unallocated Clusters Fertig
File Slack Space Suchen - 2,4% - (0:08)
hiberfil.sys Bereit
Uninitialized File Area Bereit
Geschachtelte Container gefunden: 6
Thread Details:
ABBRECHEN
BEWEISANALYSE

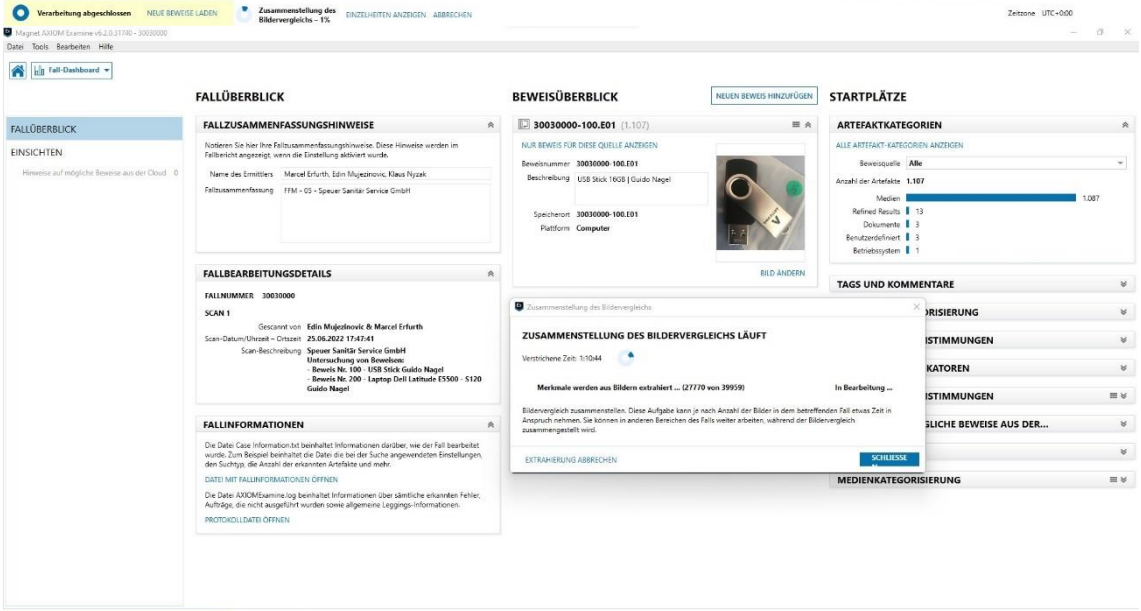

Magnet AXIOM Process 6.2.0.31740 - 30030000
Datei Tools Hilfe
BEWEISANALYSE
FALLDETAILS
BEWEISQUELLEN 7
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
ZU BEARBEITENDE QUELLEN
Typ | Abbild – Speicherortname | Beweisnummer | Suchtyp | Startdatum/Uhrzeit – Ortszeit | Enddatum/Uhrzeit – Ortszeit | Dauer | Status
30030000-100.E01 – Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO | 30030000-100.E01 | Vollständig | 25.06.2022 18:24:48 | 25.06.2022 18:27:08 | 2:18 | Fertig
30030000-100.E01 – Nicht partitionierter Speicherplatz | 30030000-100.E01 | Nicht partitioniert | 25.06.2022 18:27:09 | 25.06.2022 18:27:09 | 0:01 | Fertig
30030000-200.E01 – Partition 1 (Microsoft FAT32, 100 MB) NO NAME | 30030000-200.E01 | Vollständig | 25.06.2022 18:27:10 | 25.06.2022 18:27:14 | 0:03 | Fertig
30030000-200.E01 – Partition 2 (16 MB) - Kein bekanntes Dateisystem gef | 30030000-200.E01 | Sektorebene | 25.06.2022 18:27:15 | 25.06.2022 18:27:15 | 0:01 | Fertig
30030000-200.E01 – Partition 3 (125,29 GB) [Verschlüsselt] | 30030000-200.E01 | Vollständig | 25.06.2022 18:31:33 | 25.06.2022 20:07:59 | 1:36:26 | Fertig
30030000-200.E01 – Partition 4 (Microsoft NTFS, 525 MB) | 30030000-200.E01 | Vollständig | 25.06.2022 18:27:16 | 25.06.2022 18:27:27 | 0:11 | Fertig
30030000-200.E01 – Nicht partitionierter Speicherplatz | 30030000-200.E01 | Nicht partitioniert | 25.06.2022 18:27:28 | 25.06.2022 18:31:33 | 4:04 | Fertig
AUSFÜHRUNG VON FOLGEAKTIONEN NACH DEM SCAN
Verstrichene Zeit: 1:43:57
VOLLTEXTSUCHE
Indexdaten zu Artefakten werden gesammelt In Bearbeitung ... 0 %
ABBRECHEN
BEWEISANALYSE

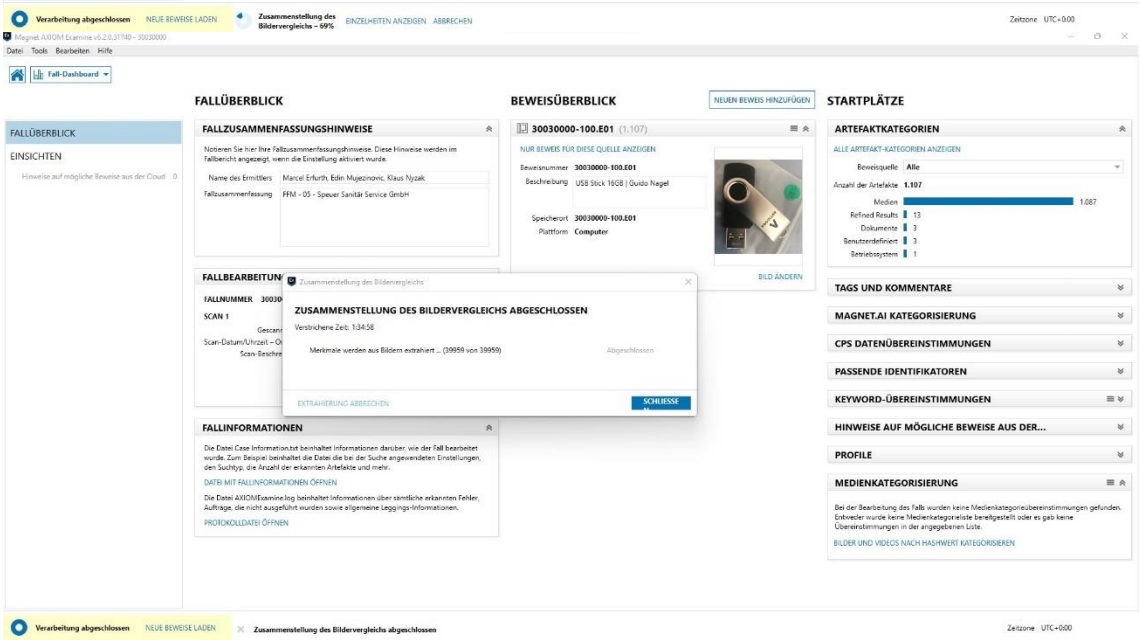

Magnet AXIOM Process 6.2.0.31740 - 30030000
Datei Tools Hilfe
BEWEISANALYSE
FALLDETAILS
BEWEISQUELLEN 7
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
ZU BEARBEITENDE QUELLEN
Typ | Abbild – Speicherortname | Beweisnummer | Suchtyp | Startdatum/Uhrzeit – Ortszeit | Enddatum/Uhrzeit – Ortszeit | Dauer | Status
30030000-100.E01 – Partition 1 (Microsoft FAT32, 14,65 GB) USB GUDIO | 30030000-100.E01 | Vollständig | 25.06.2022 18:24:48 | 25.06.2022 18:27:08 | 2:18 | Fertig
30030000-100.E01 – Nicht partitionierter Speicherplatz | 30030000-100.E01 | Nicht partitioniert | 25.06.2022 18:27:09 | 25.06.2022 18:27:09 | 0:01 | Fertig
30030000-200.E01 – Partition 1 (Microsoft FAT32, 100 MB) NO NAME | 30030000-200.E01 | Vollständig | 25.06.2022 18:27:10 | 25.06.2022 18:27:14 | 0:03 | Fertig
30030000-200.E01 – Partition 2 (16 MB) - Kein bekanntes Dateisystem gef | 30030000-200.E01 | Sektorebene | 25.06.2022 18:27:15 | 25.06.2022 18:27:15 | 0:01 | Fertig
30030000-200.E01 – Partition 3 (125,29 GB) [Verschlüsselt] | 30030000-200.E01 | Vollständig | 25.06.2022 18:31:33 | 25.06.2022 20:07:59 | 1:36:26 | Fertig
30030000-200.E01 – Partition 4 (Microsoft NTFS, 525 MB) | 30030000-200.E01 | Vollständig | 25.06.2022 18:27:16 | 25.06.2022 18:27:27 | 0:11 | Fertig
30030000-200.E01 – Nicht partitionierter Speicherplatz | 30030000-200.E01 | Nicht partitioniert | 25.06.2022 18:27:28 | 25.06.2022 18:31:33 | 4:04 | Fertig
SUCHE ABGESCHLOSSEN
AXIOM Process hat Ihre Beweisquellen vollständig gescannt. Hier eine Zusammenfassung der beendeten Suche.
Startdatum/Uhrzeit – Ortszeit 25.06.2022 17:47:41
Enddatum/Uhrzeit – Ortszeit 25.06.2022 20:13:55
Suchdauer 1 Stunde, 49 Minuten, 7 Sekunden
Dauer der Indexierung 9 Sekunden
Dauer der Verschlüsselung 37 Minuten, 0 Sekunden
Suchergebnis Abgeschlossen
AUSNAHMEN (0)
SCAN-EINSTELLUNGEN
ZURÜCK
SCHLIEßEN

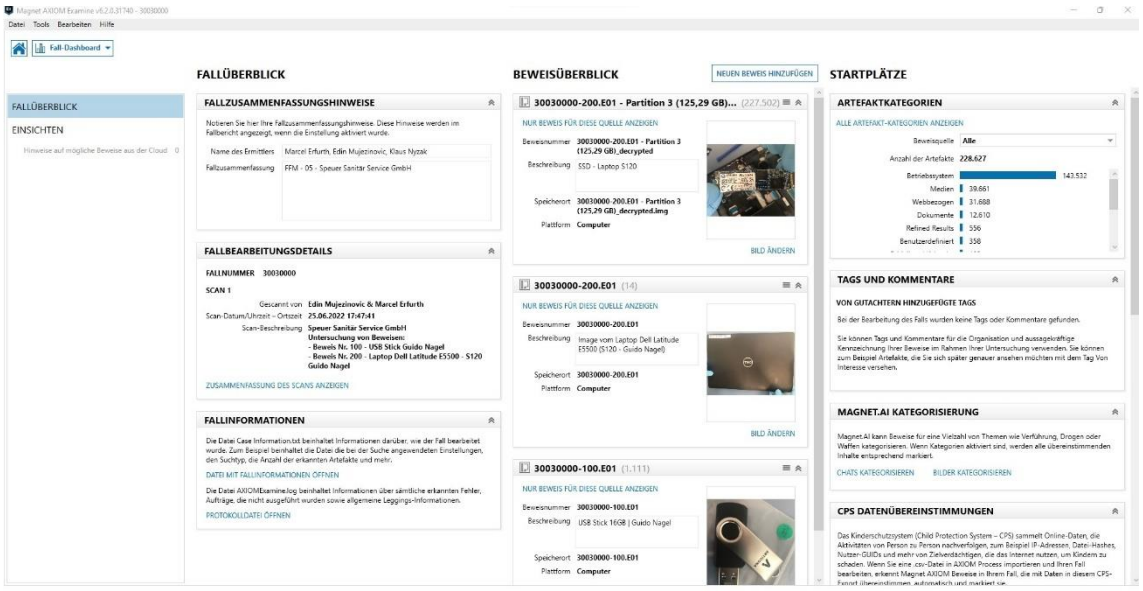

Magnet AXIOM Process 6.2.0.31740 - 30030000
Datei Tools Hilfe
BEWEISANALYSE
FALLDETAILS
BEWEISQUELLEN 7
VERARBEITUNGSOPTIONEN
Archive und mobile Backups suchen Ein
Keywords zur Suche hinzufügen
Text aus Dateien extrahieren (OCR)
Hash-Werte berechnen Ein
Chats kategorisieren
Bilder und Videos kategorisieren
CPS-Daten zum Durchsuchen hinzufügen
Weitere Artefakte finden Ein
ARTEFAKTDETAILS 200
Computer-Artefakte 200 von 249
Mobile Artefakte
Cloud-Artefakte
Fahrzeug-Artefakte
BEWEISANALYSE
30030000-200.E01 – Partition 4 (Microsoft NTFS, 525 MB) 30030000-200.E01 Vollständig 25.06.2022 18:27:16 25.06.2022 18:27:27 0:11 Fertig
30030000-200.E01 – Nicht partitionierter Speicherplatz 30030000-200.E01 Nicht partitioniert 25.06.2022 18:27:28 25.06.2022 18:31:33 4:04 Fertig
SUCHE ABGESCHLOSSEN
AXIOM Process hat Ihre Beweisquellen vollständig gescannt. Hier eine Zusammenfassung der beendeten Suche.
Startdatum/Uhrzeit – Ortszeit 25.06.2022 17:47:41
Enddatum/Uhrzeit – Ortszeit 25.06.2022 20:13:55
Suchdauer 1 Stunde, 49 Minuten, 7 Sekunden
Dauer der Indexierung 9 Sekunden
Dauer der Verschlüsselung 37 Minuten, 0 Sekunden
Suchergebnis Abgeschlossen
AUSNAHMEN (0)
SCAN-EINSTELLUNGEN
VERARBEITUNGSOPTIONEN
AXIOM-Version 6.2.0.31740
Ausgabeordner E:\Axiom Dateien\AXIOM - 30030000 - Speuer Sanitär Service GmbH\
Archive durchsuchen Ein
Mobile Backups suchen Ein
Max. Tiefe der Containerschachtelung 5
Kopien entfernen Ein
Eingegebene Schlüsselwörter 0
Eingegebene reguläre Ausdrücke 0
Text aus Dateien extrahieren (OCR) Aus
Dateien mit bestimmten Hashes überspringen Aus
Tag-Dateien mit übereinstimmenden Hash-Werten Aus
Kategorisierung der Bilder und Videos Aus
Dynamischer App-Finder Ein
ZURÜCK
SCHLIEBEN

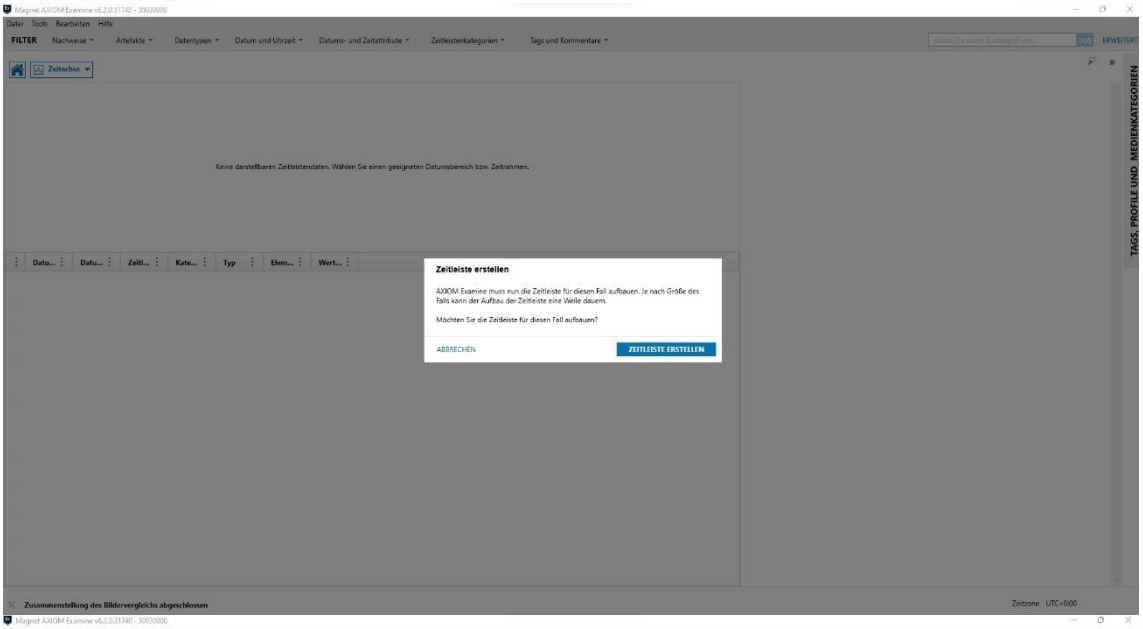

Magnet AXIOM Examine v6.2.0.31740 - 30030000
Datei Tools Bearbeiten Hilfe
Fall-Dashboard
FALLÜBERBLICK
EINSICHTEN
Hinweise auf mögliche Beweise aus der Cloud 0
FALLÜBERBLICK
FALLZUSAMMENFASSUNGSHINWEISE
Notieren Sie hier Ihre Fallzusammenfassungshinweise. Diese Hinweise werden im Fallbericht angezeigt, wenn die Einstellung aktiviert wurde.
Name des Ermittlers Edin Mujezinovic & Marcel Erfurth
Fallzusammenfassung
FALLBEARBEITUNGSDETAILS
FALLNUMMER 30030000
SCAN 1
Gescannt von Edin Mujezinovic & Marcel Erfurth
Scan-Datum/Uhrzeit – Ortszeit 25.06.2022 17:47:41
Scan-Beschreibung Speuer Sanitär Service GmbH
Untersuchung von Beweisen:
- Beweis Nr. 100 - USB Stick Guido Nagel
- Beweis Nr. 200 - Laptop Dell Latitude E5500 - S120 Guido Nagel
FALLINFORMATIONEN
Die Datei Case Information.txt beinhaltet Informationen darüber, wie der Fall bearbeitet wurde. Zum Beispiel beinhaltet die Datei die bei der Suche angewendeten Einstellungen, den Suchtyp, die Anzahl der erkannten Artefakte und mehr.
DATEI MIT FALLINFORMATIONEN ÖFFNEN
Die Datei AXIOMExamine.log beinhaltet Informationen über sämtliche erkannten Fehler, Aufträge, die nicht ausgeführt wurden sowie allgemeine Logging-Informationen.
PROTOKOLLDATEI ÖFFNEN
BEWEISÜBERBLICK
NEUEN BEWEIS HINZUFÜGEN
30030000-100.E01 (1.107)
NUR BEWEIS FÜR DIESE QUELLE ANZEIGEN
Beweisnummer 30030000-100.E01
Beschreibung
Speicherort 30030000-100.E01
Plattform Computer
Kein Bild hinzugefügt
BILD ÄNDERN
STARTPLÄTZE
ARTEFAKTKATEGORIEN
ALLE ARTEFAKT-KATEGORIEN ANZEIGEN
Beweisquelle Alle
Anzahl der Artefakte 1.107
Medien 1.087
Refined Results 13
Dokumente 3
Benutzerdefiniert 3
Betriebssystem 1
TAGS UND KOMMENTARE
MAGNET.AI KATEGORISIERUNG
CPS DATENÜBEREINSTIMMUNGEN
PASSENDE IDENTIFIKATOREN
Magnet AXIOM kann die in diesem Fall gefundenen Identifikatoren mit Identifikatoren aus anderen Fällen, die Ihre Organisation auf die Magnet Prague-Datenbank hochgeladen hat, abgleichen. Bei diesen Identifikatoren kann es sich um Personen-Identifikatoren wie E-Mail-Adressen oder Telefonnummern und Geräte-Identifikatoren wie Seriennummern einer Kamera oder Telefon-IMEIs handeln.
Besuchen Sie Magnet Idea Lab, um weitere Informationen zu erhalten oder eine Beta-Kopie der Magnet Prague-Serversoftware herunterzuladen.
https://magnetidealab.com/ URL KOPIEREN
Sobald Sie die Software des Magnet Prague-Servers installiert haben, konfigurieren Sie die Produktintegrationseinstellungen, um Magnet AXIOM mit Magnet Prague zu verbinden.
PRODUKTINTEGRATIONEN KONFIGURIEREN
KEYWORD-ÜBEREINSTIMMUNGEN
HINWEISE AUF MÖGLICHE BEWEISE AUS DER...
Keine Hinweise auf Beweise aus der Cloud gefunden.
Verarbeitung abgeschlossen NEUE BEWEISE LADEN
Zusammenstellung des Bildervergleichs – 0% EINZELHEITEN ANZEIGEN ABBRECHEN
Zeitzone UTC+0:00

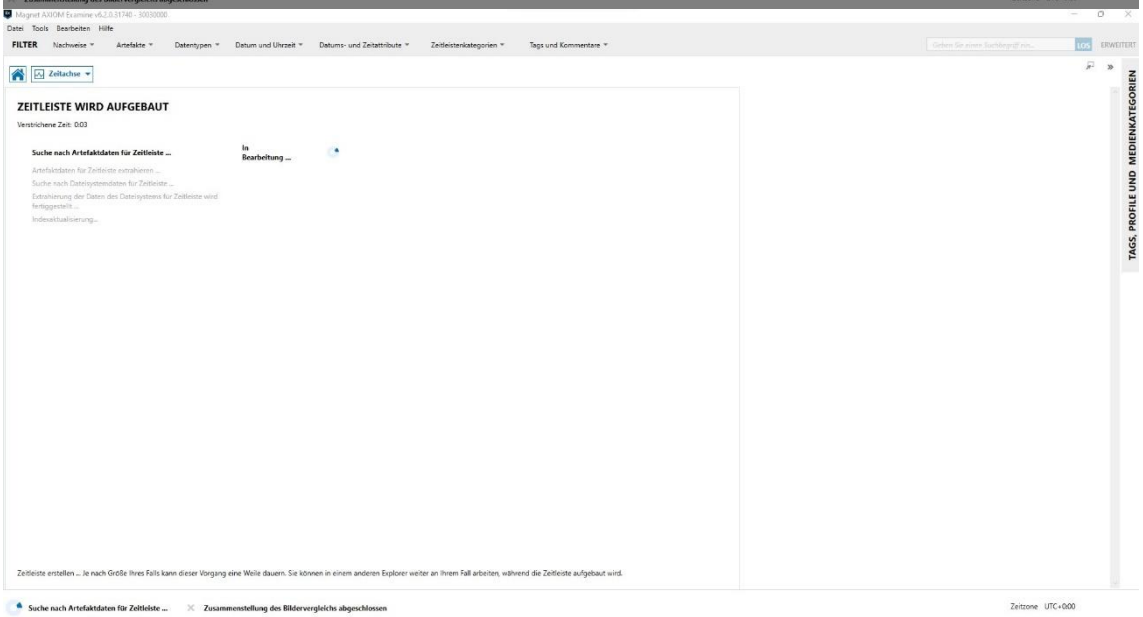

Magnet AXIOM Examine v6.2.0.31740 - 30030000
Datei Tools Bearbeiten Hilfe
Fall-Dashboard
FALLÜBERBLICK
BEWEISÜBERBLICK
NEUEN BEWEIS HINZUFÜGEN
STARTPLÄTZE
FALLÜBERBLICK
EINSICHTEN
Hinweise auf mögliche Beweise aus der Cloud 0
FALLZUSAMMENFASSUNGSHINWEISE
Notieren Sie hier Ihre Fallzusammenfassungshinweise. Diese Hinweise werden im Fallbericht angezeigt, wenn die Einstellung aktiviert wurde.
Name des Ermittlers Edin Mujezinovic & Marcel Erfurth
Fallzusammenfassung
30030000-100.E01 (1.107)
NUR BEWEIS FÜR DIESE QUELLE ANZEIGEN
Beweisnummer 30030000-100.E01
Beschreibung
Speicherort 30030000-100.E01
Plattform Computer
ARTEFAKTKATEGORIEN
ALLE ARTEFAKT-KATEGORIEN ANZEIGEN
Beweisquelle Alle
Anzahl der Artefakte 1.107
Medien 1.087
Refined Results 13
Dokumente 3
Benutzerdefiniert 3
Betriebssystem 1
FALLBEARBEITUNGSDETAILS
FALLNUMMER 30030000
SCAN 1
Gescannt von Edin Mujezinovic
Scan-Datum/Uhrzeit – Ortszeit 25.06.2022 17:47
Scan-Beschreibung Speuer Sanitär S
Untersuchung v
- Beweis Nr. 100
- Beweis Nr. 200
Guido Nagel
Zusammenstellung des Bildervergleichs
ZUSAMMENSTELLUNG DES BILDERVERGLEICHS LÄUFT
Verstrichene Zeit: 1:56
Merkmale werden aus Bildern extrahiert ... (680 von 39959)
In Bearbeitung ...
Bildervergleich zusammenstellen. Diese Aufgabe kann je nach Anzahl der Bilder in dem betreffenden Fall etwas Zeit in Anspruch nehmen. Sie können in anderen Bereichen des Falls weiter arbeiten, während der Bildervergleich zusammengestellt wird.
EXTRAHIERUNG ABBRECHEN
SCHLIESSE
TAGS UND KOMMENTARE
MAGNET.AI KATEGORISIERUNG
CPS DATENÜBEREINSTIMMUNGEN
PASSENDE IDENTIFIKATOREN
Magnet AXIOM kann die in diesem Fall gefundenen Identifikatoren mit Identifikatoren aus anderen Fällen, die Ihre Organisation auf die Magnet Prague-Datenbank hochgeladen hat, abgleichen. Bei diesen Identifikatoren kann es sich um Personen-Identifikatoren wie E-Mail-Adressen oder Telefonnummern und Geräte-Identifikatoren wie Seriennummern einer Kamera oder Telefon-IMEIs handeln.
Besuchen Sie Magnet Idea Lab, um weitere Informationen zu erhalten oder eine Beta-Kopie der Magnet Prague-Serversoftware herunterzuladen.
https://magnetidealab.com/ URL KOPIEREN
Sobald Sie die Software des Magnet Prague-Servers installiert haben, konfigurieren Sie die Produktintegrationseinstellungen, um Magnet AXIOM mit Magnet Prague zu verbinden.
PRODUKTINTEGRATIONEN KONFIGURIEREN
FALLINFORMATIONEN
Die Datei Case Information.txt beinhaltet Informationen darüber, wie der Fall bearbeitet wurde. Zum Beispiel beinhaltet die Datei die bei der Suche angewendeten Einstellungen, den Suchtyp, die Anzahl der erkannten Artefakte und mehr.
DATEI MIT FALLINFORMATIONEN ÖFFNEN
Die Datei AXIOMExamine.log beinhaltet Informationen über sämtliche erkannten Fehler, Aufträge, die nicht ausgeführt wurden sowie allgemeine Leggings-Informationen.
PROTOKOLLDATEI ÖFFNEN
KEYWORD-ÜBEREINSTIMMUNGEN
HINWEISE AUF MÖGLICHE BEWEISE AUS DER...
Keine Hinweise auf Beweise aus der Cloud gefunden.
Verarbeitung abgeschlossen
NEUE BEWEISE LADEN
Zusammenstellung des Bildervergleichs – 1%
EINZELHEITEN ANZEIGEN
ABBRECHEN
Zeitzone UTC+0:00

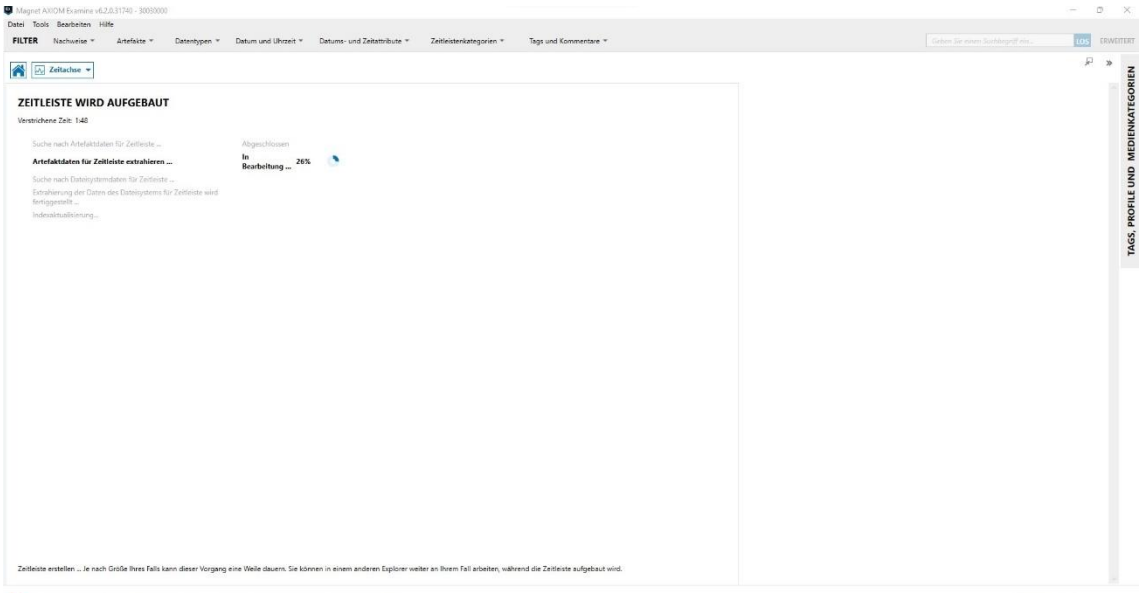

Magnet AXIOM Examine v6.2.0.31740 - 30030000
Datei Tools Bearbeiten Hilfe
Fall-Dashboard
FALLÜBERBLICK
BEWEISÜBERBLICK
NEUEN BEWEIS HINZUFÜGEN
STARTPLÄTZE
FALLÜBERBLICK
EINSICHTEN
Hinweise auf mögliche Beweise aus der Cloud 0
FALLZUSAMMENFASSUNGSHINWEISE
Notieren Sie hier Ihre Fallzusammenfassungshinweise. Diese Hinweise werden im Fallbericht angezeigt, wenn die Einstellung aktiviert wurde.
Name des Ermittlers Marcel Erfurth, Edin Mujezinovic, Klaus Nyzak
Fallzusammenfassung FFM - 05 - Speuer Sanitär Service GmbH
30030000-100.E01 (1.107)
NUR BEWEIS FÜR DIESE QUELLE ANZEIGEN
Beweisnummer 30030000-100.E01
Beschreibung USB Stick 16GB | Guido Nagel
Speicherort 30030000-100.E01
Plattform Computer
BILD ÄNDERN
ARTEFAKTKATEGORIEN
ALLE ARTEFAKT-KATEGORIEN ANZEIGEN
Beweisquelle Alle
Anzahl der Artefakte 1.107
Medien 1.087
Refined Results 13
Dokumente 3
Benutzerdefiniert 3
Betriebssystem 1
FALLBEARBEITUNGSDETAILS
FALLNUMMER 30030000
SCAN 1
Gescannt von Edin Mujezinovic & Marcel Erfurth
Scan-Datum/Uhrzeit – Ortszeit 25.06.2022 17:47:41
Scan-Beschreibung Speuer Sanitär Service GmbH
Untersuchung von Beweisen:
- Beweis Nr. 100 - USB Stick Guido Nagel
- Beweis Nr. 200 - Laptop Dell Latitude E5500 - S120
Guido Nagel
Zusammenstellung des Bildervergleichs
ZUSAMMENSTELLUNG DES BILDERVERGLEICHS LÄUFT
Verstrichene Zeit: 1:10:44
Merkmale werden aus Bildern extrahiert ... (27770 von 39959)
In Bearbeitung ...
Bildervergleich zusammenstellen. Diese Aufgabe kann je nach Anzahl der Bilder in dem betreffenden Fall etwas Zeit in Anspruch nehmen. Sie können in anderen Bereichen des Falls weiter arbeiten, während der Bildervergleich zusammengestellt wird.
EXTRAHIERUNG ABBRECHEN
SCHLIESSE
TAGS UND KOMMENTARE
MEDIENKATEGORISIERUNG
FALLINFORMATIONEN
Die Datei Case Information.txt beinhaltet Informationen darüber, wie der Fall bearbeitet wurde. Zum Beispiel beinhaltet die Datei die bei der Suche angewendeten Einstellungen, den Suchtyp, die Anzahl der erkannten Artefakte und mehr.
DATEI MIT FALLINFORMATIONEN ÖFFNEN
Die Datei AXIOMExamine.log beinhaltet Informationen über sämtliche erkannten Fehler, Aufträge, die nicht ausgeführt wurden sowie allgemeine Leggings-Informationen.
PROTOKOLLDATEI ÖFFNEN
Verarbeitung abgeschlossen
NEUE BEWEISE LADEN
Zusammenstellung des Bildervergleichs – 69%
EINZELHEITEN ANZEIGEN
ABBRECHEN
Zeitzone UTC+0:00

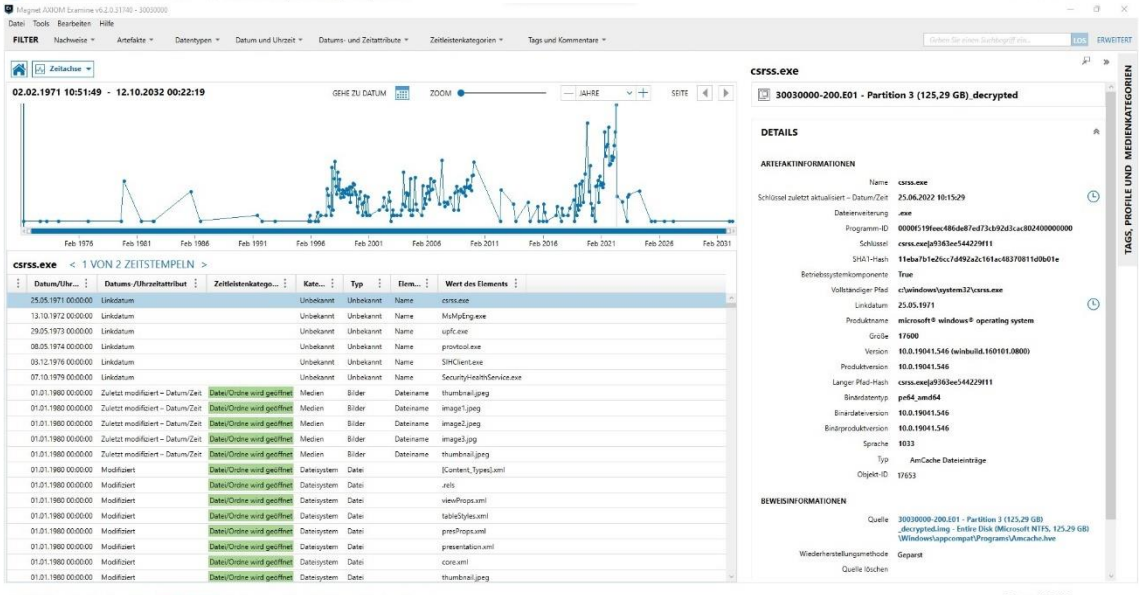

Magnet AXIOM Examine v6.2.0.31740 - 30030000
Datei Tools Bearbeiten Hilfe
Fall-Dashboard
FALLÜBERBLICK
BEWEISÜBERBLICK
NEUEN BEWEIS HINZUFÜGEN
STARTPLÄTZE
FALLÜBERBLICK
EINSICHTEN
Hinweise auf mögliche Beweise aus der Cloud 0
FALLZUSAMMENFASSUNGSHINWEISE
Notieren Sie hier Ihre Fallzusammenfassungshinweise. Diese Hinweise werden im Fallbericht angezeigt, wenn die Einstellung aktiviert wurde.
Name des Ermittlers Marcel Erfurth, Edin Mujezinovic, Klaus Nyzak
Fallzusammenfassung FFM - 05 - Speuer Sanitär Service GmbH
30030000-100.E01 (1.107)
NUR BEWEIS FÜR DIESE QUELLE ANZEIGEN
Beweisnummer 30030000-100.E01
Beschreibung USB Stick 16GB | Guido Nagel
Speicherort 30030000-100.E01
Plattform Computer
BILD ÄNDERN
ARTEFAKTKATEGORIEN
ALLE ARTEFAKT-KATEGORIEN ANZEIGEN
Beweisquelle Alle
Anzahl der Artefakte 1.107
Medien 1.087
Refined Results 13
Dokumente 3
Benutzerdefiniert 3
Betriebssystem 1
Zusammenstellung des Bildervergleichs
ZUSAMMENSTELLUNG DES BILDERVERGLEICHS ABGESCHLOSSEN
Verstrichene Zeit: 1:34:58
Merkmale werden aus Bildern extrahiert ... (39959 von 39959)
Abgeschlossen
EXTRAHIERUNG ABBRECHEN
SCHLIESSE
TAGS UND KOMMENTARE
MAGNET.AI KATEGORISIERUNG
CPS DATENÜBEREINSTIMMUNGEN
PASSENDE IDENTIFIKATOREN
KEYWORD-ÜBEREINSTIMMUNGEN
HINWEISE AUF MÖGLICHE BEWEISE AUS DER...
PROFILE
MEDIENKATEGORISIERUNG
Bei der Bearbeitung des Falls wurden keine Medienkategorieübereinstimmungen gefunden. Entweder wurde keine Medienkategorieliste bereitgestellt oder es gab keine Übereinstimmungen in der angegebenen Liste.
BILDER UND VIDEOS NACH HASHWERT KATEGORISIEREN
FALLINFORMATIONEN
Die Datei Case Information.txt beinhaltet Informationen darüber, wie der Fall bearbeitet wurde. Zum Beispiel beinhaltet die Datei die bei der Suche angewendeten Einstellungen, den Suchtyp, die Anzahl der erkannten Artefakte und mehr.
DATEI MIT FALLINFORMATIONEN ÖFFNEN
Die Datei AXIOMExamine.log beinhaltet Informationen über sämtliche erkannten Fehler, Aufträge, die nicht ausgeführt wurden sowie allgemeine Leggings-Informationen.
PROTOKOLLDATEI ÖFFNEN
Verarbeitung abgeschlossen
NEUE BEWEISE LADEN
Zusammenstellung des Bildervergleichs abgeschlossen
Zeitzone UTC+0:00

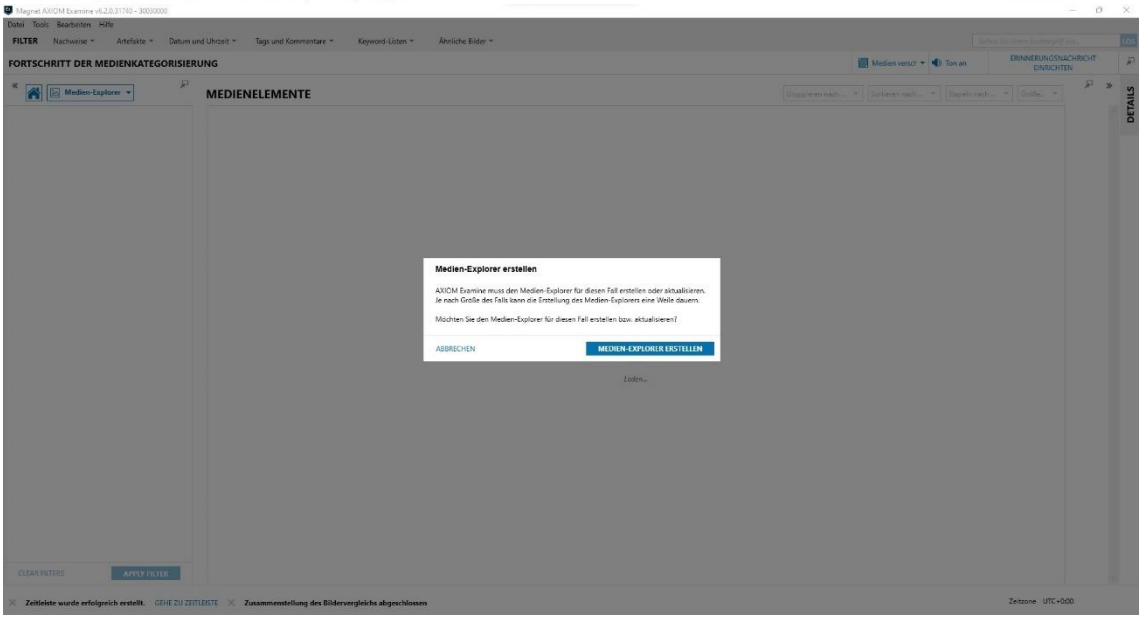

Magnet AXIOM Examine v6.2.0.31740 - 30030000
Datei Tools Bearbeiten Hilfe
Fall-Dashboard
FALLÜBERBLICK
EINSICHTEN
Hinweise auf mögliche Beweise aus der Cloud 0
FALLÜBERBLICK
FALLZUSAMMENFASSUNGSHINWEISE
Notieren Sie hier Ihre Fallzusammenfassungshinweise. Diese Hinweise werden im Fallbericht angezeigt, wenn die Einstellung aktiviert wurde.
Name des Ermittlers Marcel Erfurth, Edin Mujezinovic, Klaus Nyzak
Fallzusammenfassung FFM - 05 - Speuer Sanitär Service GmbH
FALLBEARBEITUNGSDETAILS
FALLNUMMER 30030000
SCAN 1
Gescannt von Edin Mujezinovic & Marcel Erfurth
Scan-Datum/Uhrzeit – Ortszeit 25.06.2022 17:47:41
Scan-Beschreibung Speuer Sanitär Service GmbH
Untersuchung von Beweisen:
- Beweis Nr. 100 - USB Stick Guido Nagel
- Beweis Nr. 200 - Laptop Dell Latitude E5500 - S120 Guido Nagel
ZUSAMMENFASSUNG DES SCANS ANZEIGEN
FALLINFORMATIONEN
Die Datei Case Information.txt beinhaltet Informationen darüber, wie der Fall bearbeitet wurde. Zum Beispiel beinhaltet die Datei die bei der Suche angewendeten Einstellungen, den Suchtyp, die Anzahl der erkannten Artefakte und mehr.
DATEI MIT FALLINFORMATIONEN ÖFFNEN
Die Datei AXIOMExamine.log beinhaltet Informationen über sämtliche erkannten Fehler, Aufträge, die nicht ausgeführt wurden sowie allgemeine Leggings-Informationen.
PROTOKOLLDATEI ÖFFNEN
BEWEISÜBERBLICK
NEUEN BEWEIS HINZUFÜGEN
30030000-200.E01 - Partition 3 (125,29 GB)... (227.502)
NUR BEWEIS FÜR DIESE QUELLE ANZEIGEN
Beweisnummer 30030000-200.E01 - Partition 3 (125,29 GB)_decrypted
Beschreibung SSD - Laptop S120
Speicherort 30030000-200.E01 - Partition 3 (125,29 GB)_decrypted.img
Plattform Computer
BILD ÄNDERN
30030000-200.E01 (14)
NUR BEWEIS FÜR DIESE QUELLE ANZEIGEN
Beweisnummer 30030000-200.E01
Beschreibung Image vom Laptop Dell Latitude E5500 (S120 - Guido Nagel)
Speicherort 30030000-200.E01
Plattform Computer
BILD ÄNDERN
30030000-100.E01 (1.111)
NUR BEWEIS FÜR DIESE QUELLE ANZEIGEN
Beweisnummer 30030000-100.E01
Beschreibung USB Stick 16GB | Guido Nagel
Speicherort 30030000-100.E01
Plattform Computer
STARTPLÄTZE
ARTEFAKTKATEGORIEN
ALLE ARTEFAKT-KATEGORIEN ANZEIGEN
Beweisquelle Alle
Anzahl der Artefakte 228.627
Betriebssystem 143.532
Medien 39.661
Webbezogen 31.688
Dokumente 12.610
Refined Results 556
Benutzerdefiniert 358
TAGS UND KOMMENTARE
VON GUTACHTERN HINZUGEFÜGTE TAGS
Bei der Bearbeitung des Falls wurden keine Tags oder Kommentare gefunden.
Sie können Tags und Kommentare für die Organisation und aussagekräftige Kennzeichnung Ihrer Beweise im Rahmen Ihrer Untersuchung verwenden. Sie können zum Beispiel Artefakte, die Sie sich später genauer ansehen möchten mit dem Tag Von Interesse versehen.
MAGNET.AI KATEGORISIERUNG
Magnet.AI kann Beweise für eine Vielzahl von Themen wie Verführung, Drogen oder Waffen kategorisieren. Wenn Kategorien aktiviert sind, werden alle übereinstimmenden Inhalte entsprechend markiert.
CHATS KATEGORISIEREN
BILDER KATEGORISIEREN
CPS DATENÜBEREINSTIMMUNGEN
Das Kinderschutzsystem (Child Protection System – CPS) sammelt Online-Daten, die Aktivitäten von Person zu Person nachverfolgen, zum Beispiel IP-Adressen, Datei-Hashes, Nutzer-GUIDs und mehr von Zielverdächtigen, die das Internet nutzen, um Kindern zu schaden. Wenn Sie eine .csv-Datei in AXIOM Process importieren und Ihren Fall bearbeiten, erkennt Magnet AXIOM Beweise in Ihrem Fall, die mit Daten in diesem CPS-Export übereinstimmen, automatisch und markiert sie.
Zusammenstellung des Bildervergleichs abgeschlossen
Zeitzone UTC+0:00

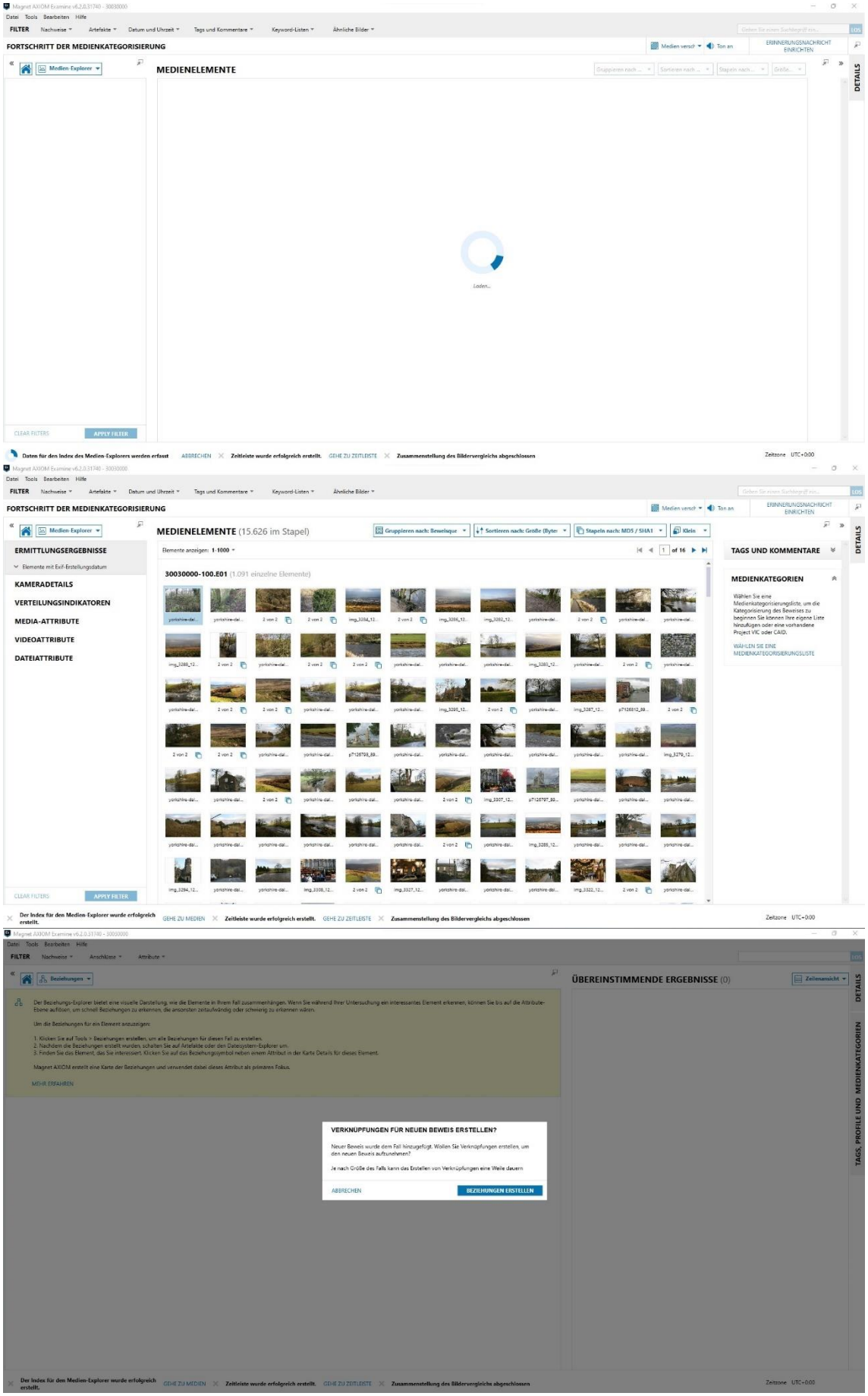

Magnet AXIOM Examine v6.2.0.31740 - 30030000
Datei Tools Bearbeiten Hilfe
FILTER Nachweise Artefakte Datentypen Datum und Uhrzeit Datums- und Zeitattribute Zeitleistenkategorien Tags und Kommentare
ERWEITERT
Zeitachse
Keine darstellbaren Zeitleistendaten. Wählen Sie einen geeigneten Datumsbereich bzw. Zeitrahmen.
Datu... Datu... Zeit... Kate... Typ Elem... Wert...
Zeitleiste erstellen
AXIOM Examine muss nun die Zeitleiste für diesen Fall aufbauen. Je nach Größe des Falls kann der Aufbau der Zeitleiste eine Weile dauern.
Möchten Sie die Zeitleiste für diesen Fall aufbauen?
ABBRECHEN
ZEITLEISTE ERSTELLEN
TAGS, PROFILE UND MEDIENKATEGORIEN
Zusammenstellung des Bildervergleichs abgeschlossen
Zeitzone UTC+0:00

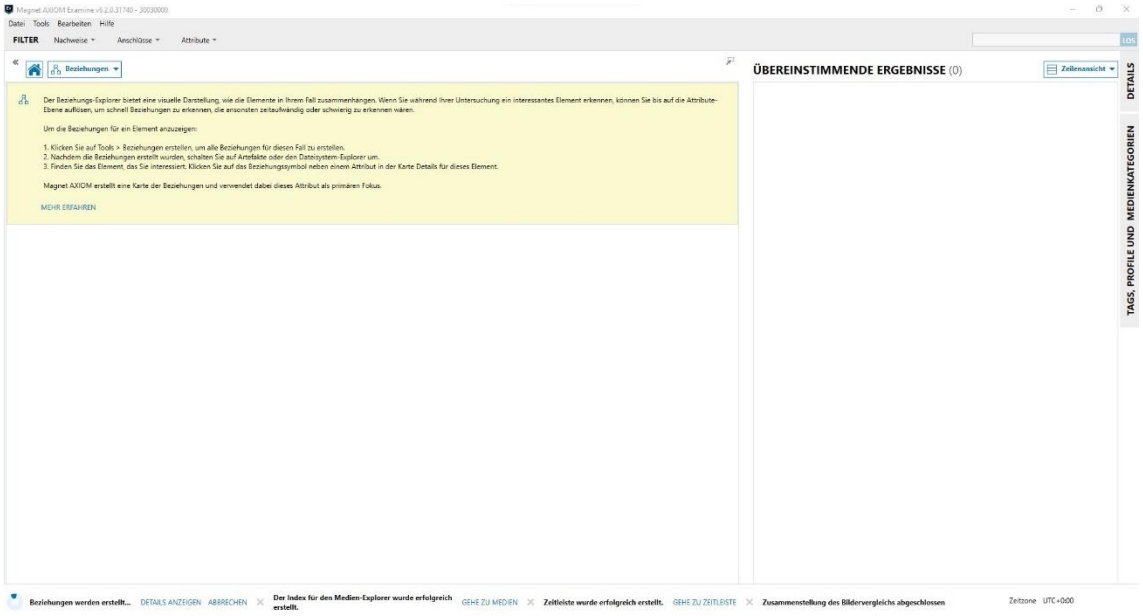

Magnet AXIOM Examine v6.2.0.31740 - 30030000
Datei Tools Bearbeiten Hilfe
FILTER Nachweise Artefakte Datentypen Datum und Uhrzeit Datums- und Zeitattribute Zeitleistenkategorien Tags und Kommentare
ERWEITERT
Zeitachse
ZEITLEISTE WIRD AUFGEBAUT
Verstrichene Zeit: 0:03
Suche nach Artefaktdaten für Zeitleiste ...
In Bearbeitung ...
Artefaktdaten für Zeitleiste extrahieren ...
Suche nach Dateisystemdaten für Zeitleiste ...
Extrahierung der Daten des Dateisystems für Zeitleiste wird fertiggestellt ...
Indexaktualisierung...
Zeitleiste erstellen ... Je nach Größe Ihres Falls kann dieser Vorgang eine Weile dauern. Sie können in einem anderen Explorer weiter an Ihrem Fall arbeiten, während die Zeitleiste aufgebaut wird.
TAGS, PROFILE UND MEDIENKATEGORIEN
Suche nach Artefaktdaten für Zeitleiste ...
Zusammenstellung des Bildervergleichs abgeschlossen
Zeitzone UTC+0:00

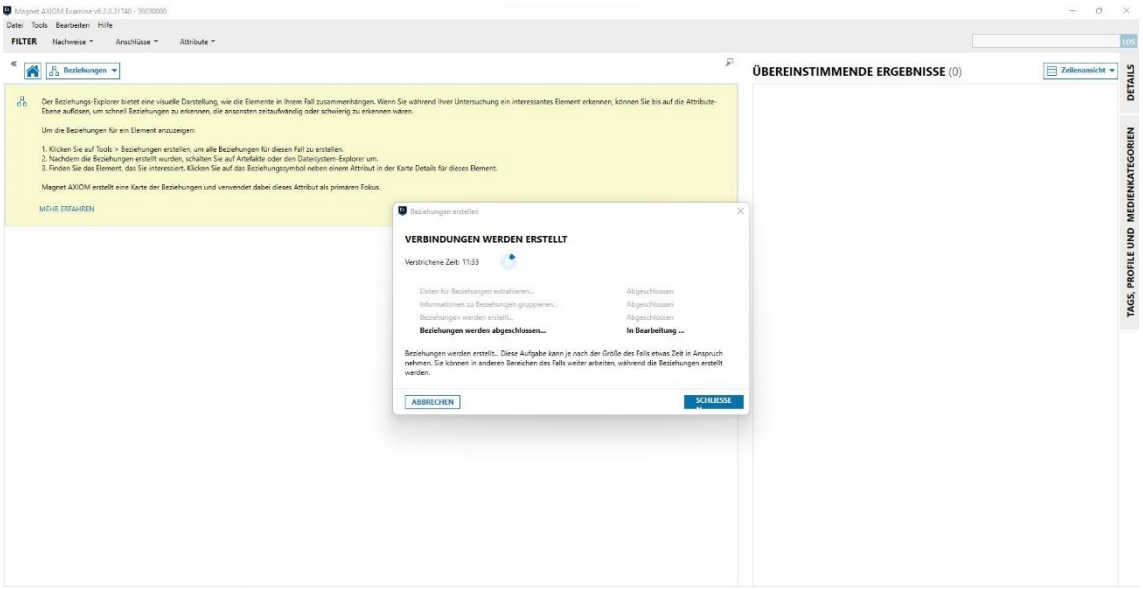

ZEITLEISTE WIRD AUFGEBAUT
Artefaktdaten für Zeitleiste extrahieren ...
Zeitleiste erstellen ... Je nach Größe Ihres Falls kann dieser Vorgang eine Weile dauern. Sie können in einem anderen Explorer weiter an Ihrem Fall arbeiten, während die Zeitleiste aufgebaut wird.

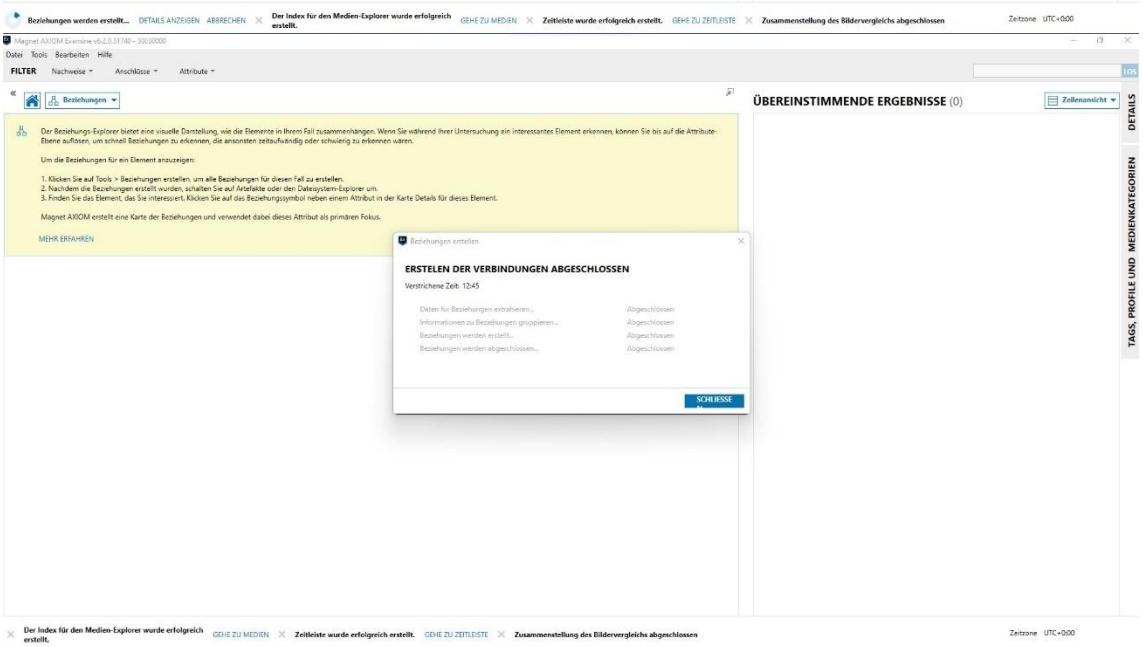

02.02.1971 10:51:49 - 12.10.2032 00:22:19
csrss.exe
30030000-200.E01 - Partition 3 (125,29 GB)_decrypted
DETAILS
ARTEFAKTINFORMATIONEN
BEWEISINFORMATIONEN

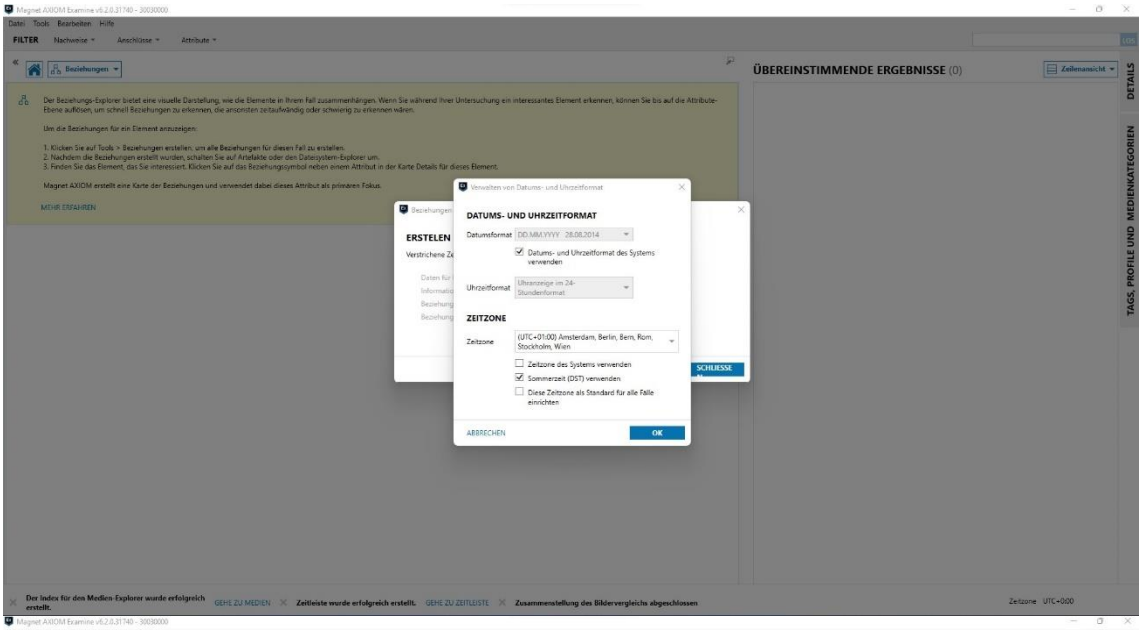

FORTSCHRITT DER MEDIENKATEGORISIERUNG
MEDIENELEMENTE
Medien-Explorer erstellen
AXIOM Examine muss den Medien-Explorer für diesen Fall erstellen oder aktualisieren. Je nach Größe des Falls kann die Erstellung des Medien-Explorers eine Weile dauern.
Möchten Sie den Medien-Explorer für diesen Fall erstellen bzw. aktualisieren?
ABBRECHEN
MEDIEN-EXPLORER ERSTELLEN

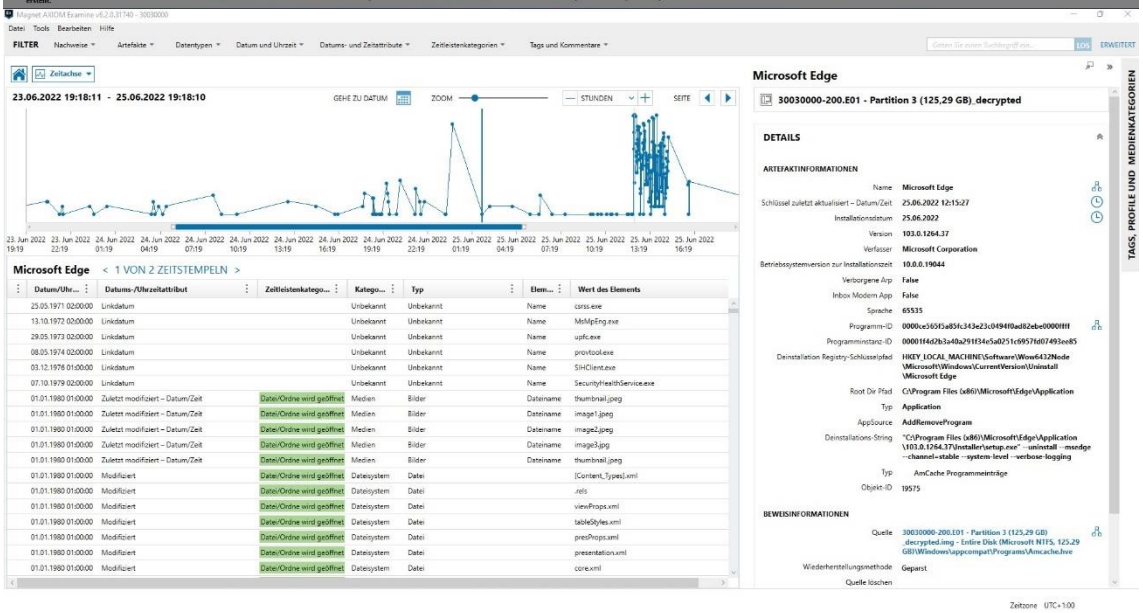

FORTSCHRITT DER MEDIENKATEGORISIERUNG
MEDIENELEMENTE
Medien-Explorer
ERMITTLUNGSERGEBNISSE
KAMERADETAILS
VERTEILUNGSINDIKATOREN
MEDIA-ATTRIBUTE
VIDEOATTRIBUTE
DATEIATTRIBUTE
MEDIENELEMENTE (15.626 im Stapel)
30030000-100.E01 (1.091 einzelne Elemente)
TAGS UND KOMMENTARE
MEDIENKATEGORIEN
ÜBEREINSTIMMENDE ERGEBNISSE (0)
VERKNÜPFUNGEN FÜR NEUEN BEWEIS ERSTELLEN?
ABBRECHEN
BEZIEHUNGEN ERSTELLEN


Magnet AXIOM Examine v6.2.0.31740 - 30030000
Datei Tools Bearbeiten Hilfe
FILTER Nachweise Anschlüsse Attribute
Beziehungen
ÜBEREINSTIMMENDE ERGEBNISSE (0)
Zeilenansicht
DETAILS
TAGS, PROFILE UND MEDIENKATEGORIEN
Der Beziehungs-Explorer bietet eine visuelle Darstellung, wie die Elemente in Ihrem Fall zusammenhängen. Wenn Sie während Ihrer Untersuchung ein interessantes Element erkennen, können Sie bis auf die Attribute-Ebene auflösen, um schnell Beziehungen zu erkennen, die ansonsten zeitaufwändig oder schwierig zu erkennen wären.
Um die Beziehungen für ein Element anzuzeigen:
1. Klicken Sie auf Tools > Beziehungen erstellen, um alle Beziehungen für diesen Fall zu erstellen.
2. Nachdem die Beziehungen erstellt wurden, schalten Sie auf Artefakte oder den Dateisystem-Explorer um.
3. Finden Sie das Element, das Sie interessiert. Klicken Sie auf das Beziehungssymbol neben einem Attribut in der Karte Details für dieses Element.
Magnet AXIOM erstellt eine Karte der Beziehungen und verwendet dabei dieses Attribut als primären Fokus.
MEHR ERFAHREN
Beziehungen werden erstellt... DETAILS ANZEIGEN ABBRECHEN
Der Index für den Medien-Explorer wurde erfolgreich erstellt. GEHE ZU MEDIEN
Zeitleiste wurde erfolgreich erstellt. GEHE ZU ZEITLEISTE
Zusammenstellung des Bildervergleichs abgeschlossen
Zeitzone UTC+0:00

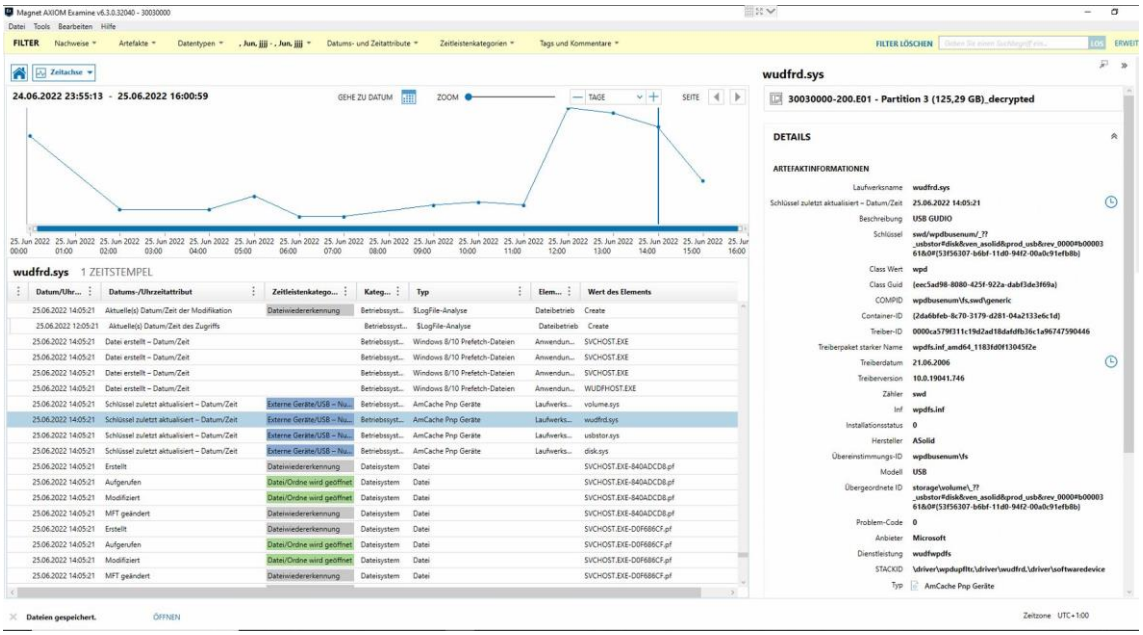

Magnet AXIOM Examine v6.2.0.31740 - 30030000
Datei Tools Bearbeiten Hilfe
FILTER Nachweise Anschlüsse Attribute
Beziehungen
ÜBEREINSTIMMENDE ERGEBNISSE (0)
Zeilenansicht
DETAILS
TAGS, PROFILE UND MEDIENKATEGORIEN
Der Beziehungs-Explorer bietet eine visuelle Darstellung, wie die Elemente in Ihrem Fall zusammenhängen. Wenn Sie während Ihrer Untersuchung ein interessantes Element erkennen, können Sie bis auf die Attribute-Ebene auflösen, um schnell Beziehungen zu erkennen, die ansonsten zeitaufwändig oder schwierig zu erkennen wären.
Um die Beziehungen für ein Element anzuzeigen:
1. Klicken Sie auf Tools > Beziehungen erstellen, um alle Beziehungen für diesen Fall zu erstellen.
2. Nachdem die Beziehungen erstellt wurden, schalten Sie auf Artefakte oder den Dateisystem-Explorer um.
3. Finden Sie das Element, das Sie interessiert. Klicken Sie auf das Beziehungssymbol neben einem Attribut in der Karte Details für dieses Element.
Magnet AXIOM erstellt eine Karte der Beziehungen und verwendet dabei dieses Attribut als primären Fokus.
MEHR ERFAHREN
Beziehungen erstellen
VERBINDUNGEN WERDEN ERSTELLT
Verstrichene Zeit: 11:33
Daten für Beziehungen extrahieren... Abgeschlossen
Informationen zu Beziehungen gruppieren... Abgeschlossen
Beziehungen werden erstellt... Abgeschlossen
Beziehungen werden abgeschlossen... In Bearbeitung ...
Beziehungen werden erstellt... Diese Aufgabe kann je nach der Größe des Falls etwas Zeit in Anspruch nehmen. Sie können in anderen Bereichen des Falls weiter arbeiten, während die Beziehungen erstellt werden.
ABBRECHEN
SCHLIESSE
Beziehungen werden erstellt... DETAILS ANZEIGEN ABBRECHEN
Der Index für den Medien-Explorer wurde erfolgreich erstellt. GEHE ZU MEDIEN
Zeitleiste wurde erfolgreich erstellt. GEHE ZU ZEITLEISTE
Zusammenstellung des Bildervergleichs abgeschlossen
Zeitzone UTC+0:00

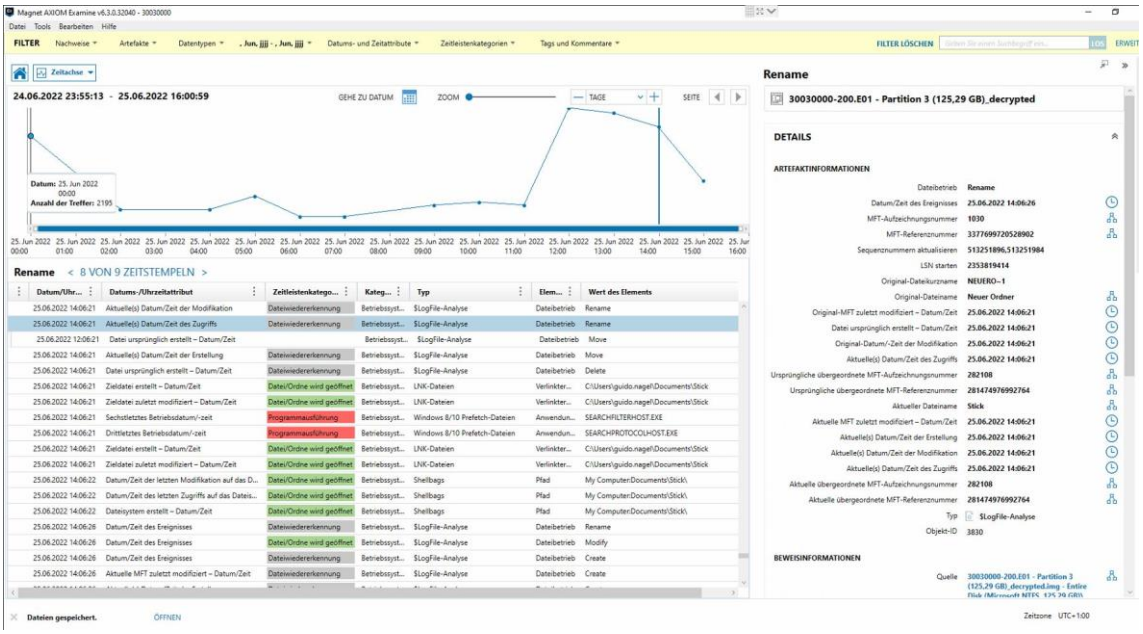

Magnet AXIOM Examine v6.2.0.31740 - 30030000
Datei Tools Bearbeiten Hilfe
FILTER Nachweise Anschlüsse Attribute
Beziehungen
ÜBEREINSTIMMENDE ERGEBNISSE (0)
Zeilenansicht
DETAILS
TAGS, PROFILE UND MEDIENKATEGORIEN
Der Beziehungs-Explorer bietet eine visuelle Darstellung, wie die Elemente in Ihrem Fall zusammenhängen. Wenn Sie während Ihrer Untersuchung ein interessantes Element erkennen, können Sie bis auf die Attribute-Ebene auflösen, um schnell Beziehungen zu erkennen, die ansonsten zeitaufwändig oder schwierig zu erkennen wären.
Um die Beziehungen für ein Element anzuzeigen:
1. Klicken Sie auf Tools > Beziehungen erstellen, um alle Beziehungen für diesen Fall zu erstellen.
2. Nachdem die Beziehungen erstellt wurden, schalten Sie auf Artefakte oder den Dateisystem-Explorer um.
3. Finden Sie das Element, das Sie interessiert. Klicken Sie auf das Beziehungssymbol neben einem Attribut in der Karte Details für dieses Element.
Magnet AXIOM erstellt eine Karte der Beziehungen und verwendet dabei dieses Attribut als primären Fokus.
MEHR ERFAHREN
Beziehungen erstellen
ERSTELEN DER VERBINDUNGEN ABGESCHLOSSEN
Verstrichene Zeit: 12:45
Daten für Beziehungen extrahieren... Abgeschlossen
Informationen zu Beziehungen gruppieren... Abgeschlossen
Beziehungen werden erstellt... Abgeschlossen
Beziehungen werden abgeschlossen... Abgeschlossen
SCHLIESSE
Der Index für den Medien-Explorer wurde erfolgreich erstellt. GEHE ZU MEDIEN
Zeitleiste wurde erfolgreich erstellt. GEHE ZU ZEITLEISTE
Zusammenstellung des Bildervergleichs abgeschlossen
Zeitzone UTC+0:00

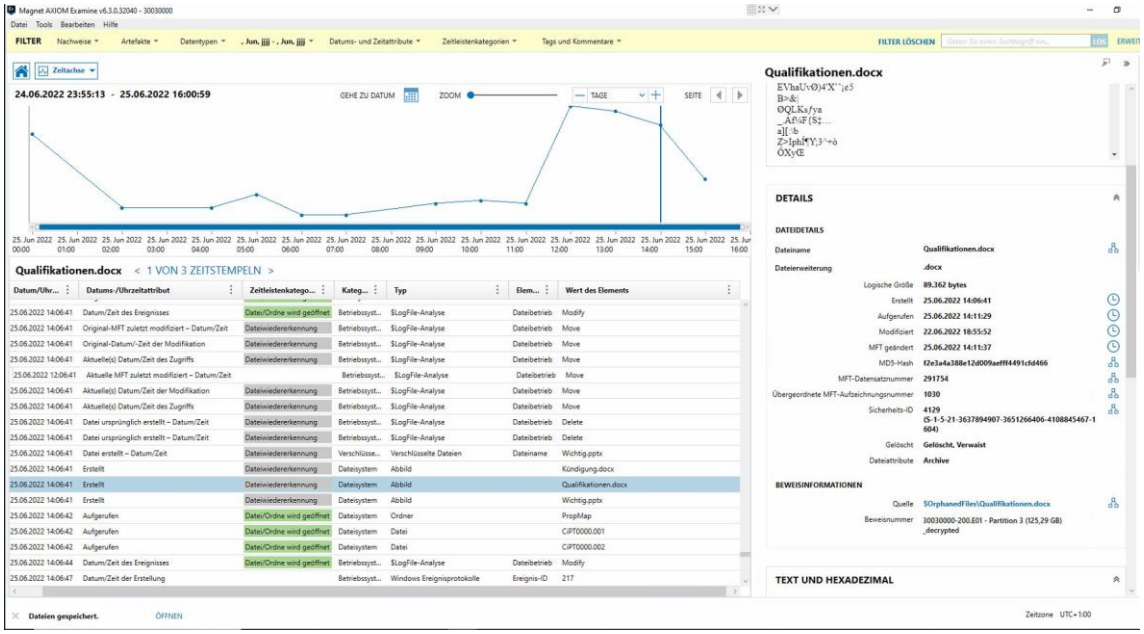

Magnet AXIOM Examine v6.2.0.31740 - 30030000
Datei Tools Bearbeiten Hilfe
FILTER Nachweise Anschlüsse Attribute
Beziehungen
ÜBEREINSTIMMENDE ERGEBNISSE (0)
Zeilenansicht
DETAILS
TAGS, PROFILE UND MEDIENKATEGORIEN
Der Beziehungs-Explorer bietet eine visuelle Darstellung, wie die Elemente in Ihrem Fall zusammenhängen. Wenn Sie während Ihrer Untersuchung ein interessantes Element erkennen, können Sie bis auf die Attribute-Ebene auflösen, um schnell Beziehungen zu erkennen, die ansonsten zeitaufwändig oder schwierig zu erkennen wären.
Um die Beziehungen für ein Element anzuzeigen:
1. Klicken Sie auf Tools > Beziehungen erstellen, um alle Beziehungen für diesen Fall zu erstellen.
2. Nachdem die Beziehungen erstellt wurden, schalten Sie auf Artefakte oder den Dateisystem-Explorer um.
3. Finden Sie das Element, das Sie interessiert. Klicken Sie auf das Beziehungssymbol neben einem Attribut in der Karte Details für dieses Element.
Magnet AXIOM erstellt eine Karte der Beziehungen und verwendet dabei dieses Attribut als primären Fokus.
MEHR ERFAHREN
Verwalten von Datums- und Uhrzeitformat
DATUMS- UND UHRZEITFORMAT
Datumsformat DD.MM.YYYY 28.08.2014
Datums- und Uhrzeitformat des Systems verwenden
Uhrzeitformat Uhrzeanzeige im 24-Stundenformat
ZEITZONE
Zeitzone (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
Zeitzone des Systems verwenden
Sommerzeit (DST) verwenden
Diese Zeitzone als Standard für alle Fälle einrichten
ABBRECHEN
OK
ERSTELEN
SCHLIESSE
Der Index für den Medien-Explorer wurde erfolgreich erstellt.
GEHE ZU MEDIEN
Zeitleiste wurde erfolgreich erstellt.
GEHE ZU ZEITLEISTE
Zusammenstellung des Bildervergleichs abgeschlossen
Zeitzone UTC+000

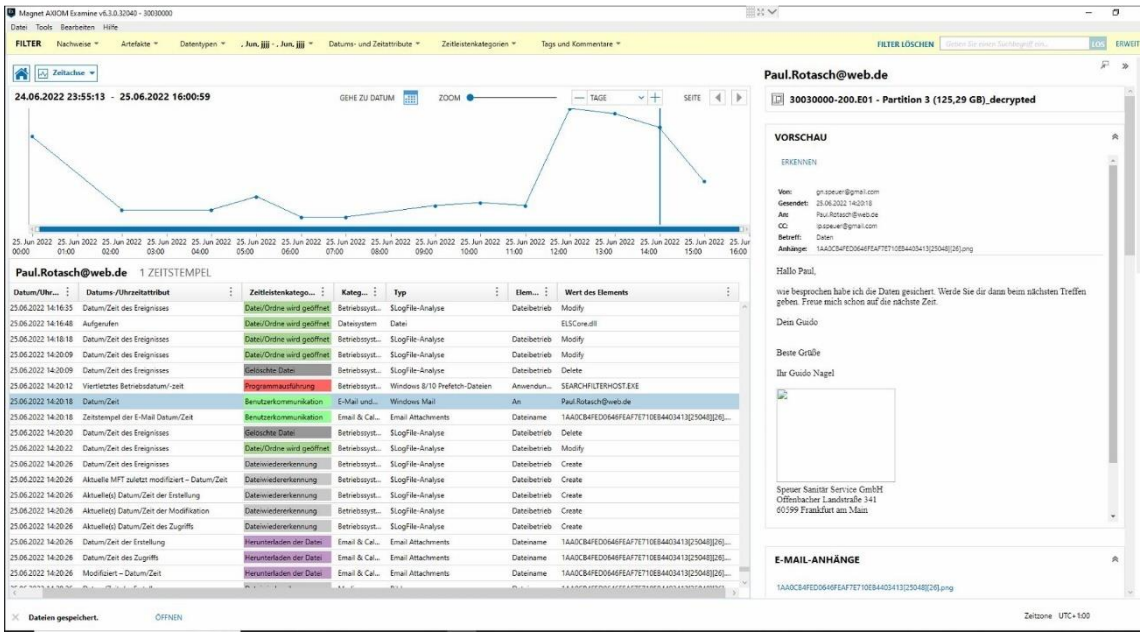

Magnet AXIOM Examine v6.2.0.31740 - 30030000
Datei Tools Bearbeiten Hilfe
FILTER Nachweise Artefakte Datentypen Datum und Uhrzeit Datums- und Zeitattribute Zeitleistenkategorien Tags und Kommentare
ERWEITERT
Zeitachse
23.06.2022 19:18:11 - 25.06.2022 19:18:10
GEHE ZU DATUM
ZOOM
STUNDEN
SEITE
Microsoft Edge
< 1 VON 2 ZEITSTEMPELN >
Datum/Uhr... Datums-/Uhrzeitattribut Zeitleistenkatego... Katego... Typ Elem... Wert des Elements
25.05.1971 02:00:00 Linkdatum Unbekannt Unbekannt Name csrss.exe
13.10.1972 02:00:00 Linkdatum Unbekannt Unbekannt Name MsMpEng.exe
29.05.1973 02:00:00 Linkdatum Unbekannt Unbekannt Name upfc.exe
08.05.1974 02:00:00 Linkdatum Unbekannt Unbekannt Name provtool.exe
03.12.1976 01:00:00 Linkdatum Unbekannt Unbekannt Name SIHClient.exe
07.10.1979 02:00:00 Linkdatum Unbekannt Unbekannt Name SecurityHealthService.exe
01.01.1980 01:00:00 Zuletzt modifiziert – Datum/Zeit Datei/Ordne wird geöffnet Medien Bilder Dateiname thumbnail.jpeg
01.01.1980 01:00:00 Zuletzt modifiziert – Datum/Zeit Datei/Ordne wird geöffnet Medien Bilder Dateiname image1.jpeg
01.01.1980 01:00:00 Zuletzt modifiziert – Datum/Zeit Datei/Ordne wird geöffnet Medien Bilder Dateiname image2.jpeg
01.01.1980 01:00:00 Zuletzt modifiziert – Datum/Zeit Datei/Ordne wird geöffnet Medien Bilder Dateiname image3.jpg
01.01.1980 01:00:00 Zuletzt modifiziert – Datum/Zeit Datei/Ordne wird geöffnet Medien Bilder Dateiname thumbnail.jpeg
01.01.1980 01:00:00 Modifiziert Datei/Ordne wird geöffnet Dateisystem Datei [Content_Types].xml
01.01.1980 01:00:00 Modifiziert Datei/Ordne wird geöffnet Dateisystem Datei .rels
01.01.1980 01:00:00 Modifiziert Datei/Ordne wird geöffnet Dateisystem Datei viewProps.xml
01.01.1980 01:00:00 Modifiziert Datei/Ordne wird geöffnet Dateisystem Datei tableStyles.xml
01.01.1980 01:00:00 Modifiziert Datei/Ordne wird geöffnet Dateisystem Datei presProps.xml
01.01.1980 01:00:00 Modifiziert Datei/Ordne wird geöffnet Dateisystem Datei presentation.xml
01.01.1980 01:00:00 Modifiziert Datei/Ordne wird geöffnet Dateisystem Datei core.xml
30030000-200.E01 - Partition 3 (125,29 GB)_decrypted
DETAILS
ARTEFAKTINFORMATIONEN
Name Microsoft Edge
Schlüssel zuletzt aktualisiert – Datum/Zeit 25.06.2022 12:15:27
Installationsdatum 25.06.2022
Version 103.0.1264.37
Verfasser Microsoft Corporation
Betriebssystemversion zur Installationszeit 10.0.0.19044
Verborgene Arp False
Inbox Modern App False
Sprache 65535
Programm-ID 0000ce565f5a85fc343e23c0494f0ad82ebe0000ffff
Programminstanz-ID 0000ff4d2b3a40a291f34e5a0251c6957fd07493ee85
Deinstallation Registry-Schlüsselpfad HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Microsoft Edge
Root Dir Pfad C:\Program Files (x86)\Microsoft\Edge\Application
Typ Application
AppSource AddRemoveProgram
Deinstallations-String "C:\Program Files (x86)\Microsoft\Edge\Application\103.0.1264.37\Installer\setup.exe" --uninstall --msedge --channel=stable --system-level --verbose-logging
Typ AmCache Programmeinträge
Objekt-ID 19575
BEWEISINFORMATIONEN
Quelle 30030000-200.E01 - Partition 3 (125,29 GB)_decrypted.img - Entire Disk (Microsoft NTFS, 125,29 GB)\Windows\appcompat\Programs\Amcache.hve
Wiederherstellungsmethode Geparst
Quelle löschen
Zeitzone UTC+1:00

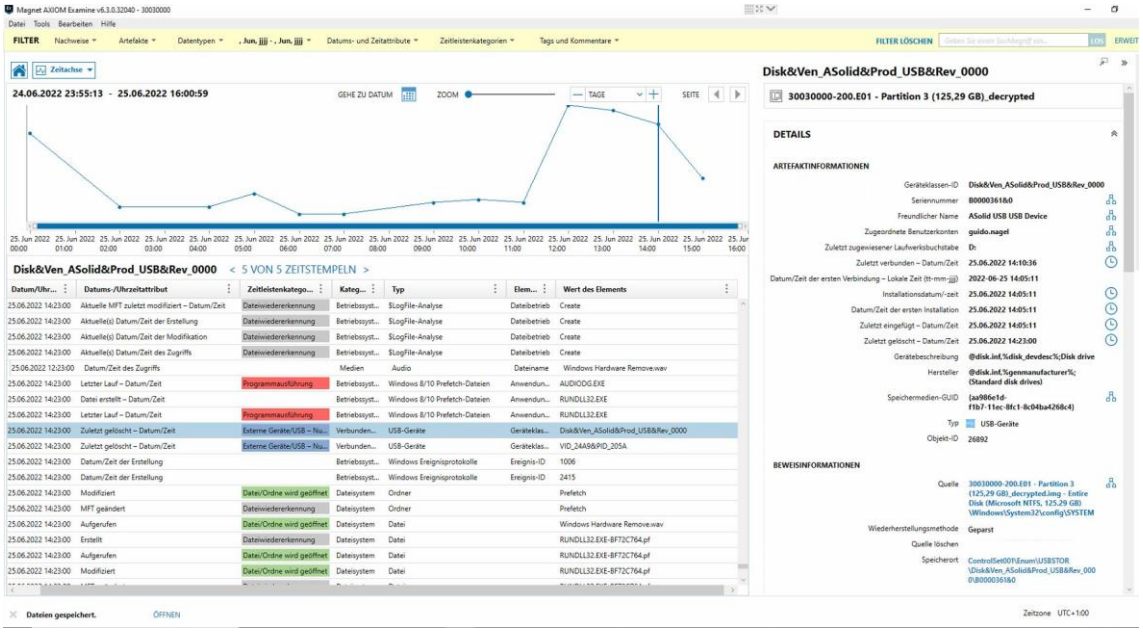
Timeline (Axiom)

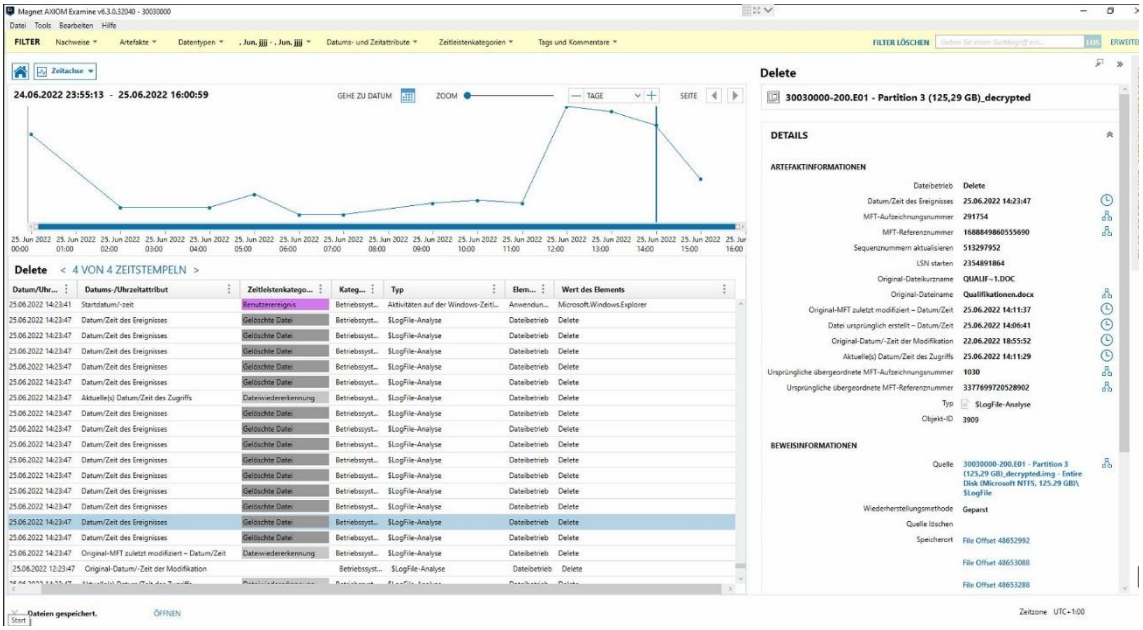


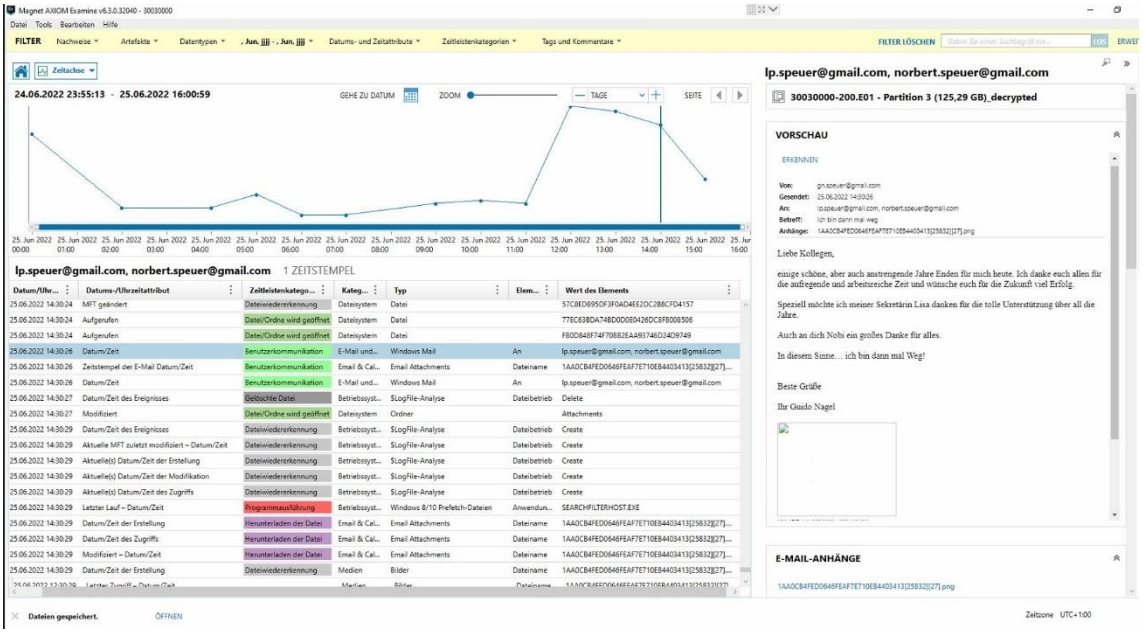


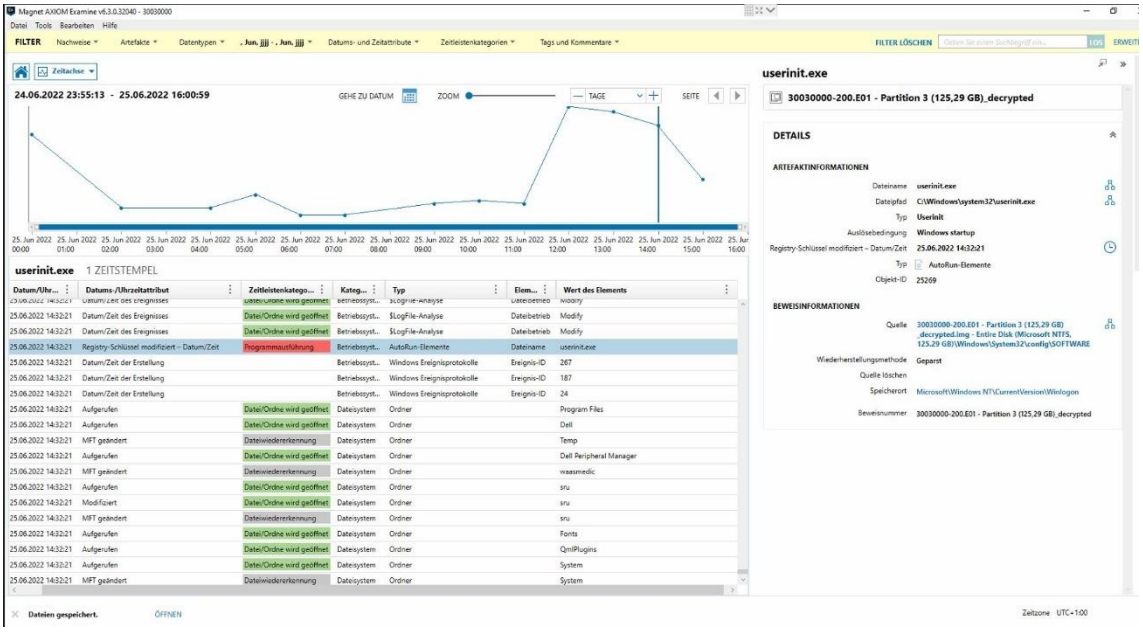

Magnet AXIOM Examine v6.3.0.32040 - 30030000
Datei Tools Bearbeiten Hilfe
FILTER
Zeitachse
24.06.2022 23:55:13 - 25.06.2022 16:00:59
Qualifikationen.docx
< 1 VON 3 ZEITSTEMPELN >
Qualifikationen.docx
DETAILS
DATEIDETAILS
Dateiname
Dateierweiterung
Logische Größe
Erstellt
Aufgerufen
Modifiziert
MFT geändert
MD5-Hash
MFT-Datensatznummer
Übergeordnete MFT-Aufzeichnungsnummer
Sicherheits-ID
Gelöscht
Dateiattribute
BEWEISINFORMATIONEN
Quelle
Beweisnummer
TEXT UND HEXADEZIMAL
Dateien gespeichert.
ÖFFNEN
Zeitzone UTC+1:00


Magnet AXIOM Examine v6.3.0.32040 - 30030000
Datei Tools Bearbeiten Hilfe
FILTER
Zeitachse
24.06.2022 23:55:13 - 25.06.2022 16:00:59
Paul.Rotasch@web.de
30030000-200.E01 - Partition 3 (125,29 GB)_decrypted
VORSCHAU
ERKENNEN
Hallo Paul,
Beste Grüße
E-MAIL-ANHÄNGE
Dateien gespeichert.
ÖFFNEN
Zeitzone UTC+1:00


Magnet AXIOM Examine v6.3.0.32040 - 30030000
Datei Tools Bearbeiten Hilfe
FILTER Nachweise Artefakte Datentypen Datums- und Zeitattribute Zeitleistenkategorien Tags und Kommentare
FILTER LÖSCHEN
Zeitachse
24.06.2022 23:55:13 - 25.06.2022 16:00:59
GEHE ZU DATUM
ZOOM
TAGE
SEITE
Disk&Ven_ASolid&Prod_USB&Rev_0000
< 5 VON 5 ZEITSTEMPELN >
Datum/Uhr... Datums-/Uhrzeitattribut Zeitleistenkatego... Kateg... Typ Elem... Wert des Elements
Disk&Ven_ASolid&Prod_USB&Rev_0000
30030000-200.E01 - Partition 3 (125,29 GB)_decrypted
DETAILS
ARTEFAKTINFORMATIONEN
Geräteklassen-ID Disk&Ven_ASolid&Prod_USB&Rev_0000
Seriennummer B00003618&0
Freundlicher Name ASolid USB USB Device
Zugeordnete Benutzerkonten guido.nagel
Zuletzt zugewiesener Laufwerksbuchstabe D:
Zuletzt verbunden – Datum/Zeit 25.06.2022 14:10:36
Datum/Zeit der ersten Verbindung – Lokale Zeit (tt-mm-jjjj) 2022-06-25 14:05:11
Installationsdatum/-zeit 25.06.2022 14:05:11
Datum/Zeit der ersten Installation 25.06.2022 14:05:11
Zuletzt eingefügt – Datum/Zeit 25.06.2022 14:05:11
Zuletzt gelöscht – Datum/Zeit 25.06.2022 14:23:00
Gerätebeschreibung @disk.inf,%disk_devdesc%;Disk drive
Hersteller @disk.inf,%genmanufacturer%;(Standard disk drives)
Speichermedien-GUID {aa986e1d-f1b7-11ec-8fc1-8c04ba4268c4}
Typ USB-Geräte
Objekt-ID 26892
BEWEISINFORMATIONEN
Quelle 30030000-200.E01 - Partition 3 (125,29 GB)_decrypted.img - Entire Disk (Microsoft NTFS, 125.29 GB) \Windows\System32\config\SYSTEM
Wiederherstellungsmethode Geparst
Quelle löschen
Speicherort ControlSet001\Enum\USBSTOR \Disk&Ven_ASolid&Prod_USB&Rev_0000\B00003618&0
Dateien gespeichert.
ÖFFNEN
Zeitzone UTC+1:00


Magnet AXIOM Examine v6.3.0.32040 - 30030000
Datei Tools Bearbeiten Hilfe
FILTER Nachweise Artefakte Datentypen Datums- und Zeitattribute Zeitleistenkategorien Tags und Kommentare
FILTER LÖSCHEN
Zeitachse
24.06.2022 23:55:13 - 25.06.2022 16:00:59
GEHE ZU DATUM
ZOOM
TAGE
SEITE
Delete
< 4 VON 4 ZEITSTEMPELN >
Datum/Uhr... Datums-/Uhrzeitattribut Zeitleistenkatego... Kateg... Typ Elem... Wert des Elements
Delete
30030000-200.E01 - Partition 3 (125,29 GB)_decrypted
DETAILS
ARTEFAKTINFORMATIONEN
Dateibetrieb Delete
Datum/Zeit des Ereignisses 25.06.2022 14:23:47
MFT-Aufzeichnungsnummer 291754
MFT-Referenznummer 1688849860555690
Sequenznummern aktualisieren 513297952
LSN starten 2354891864
Original-Dateikurzname QUALIF~1.DOC
Original-Dateiname Qualifikationen.docx
Original-MFT zuletzt modifiziert – Datum/Zeit 25.06.2022 14:11:37
Datei ursprünglich erstellt – Datum/Zeit 25.06.2022 14:06:41
Original-Datum/-Zeit der Modifikation 22.06.2022 18:55:52
Aktuelle(s) Datum/Zeit des Zugriffs 25.06.2022 14:11:29
Ursprüngliche übergeordnete MFT-Aufzeichnungsnummer 1030
Ursprüngliche übergeordnete MFT-Referenznummer 337769972052890 2
Typ $LogFile-Analyse
Objekt-ID 3909
BEWEISINFORMATIONEN
Quelle 30030000-200.E01 - Partition 3 (125,29 GB)_decrypted.img - Entire Disk (Microsoft NTFS, 125.29 GB)\ $LogFile
Wiederherstellungsmethode Geparst
Quelle löschen
Speicherort File Offset 48652992
File Offset 48653088
File Offset 48653288
Dateien gespeichert.
ÖFFNEN
Zeitzone UTC+1:00


Magnet AXIOM Examine v6.3.0.32040 - 30030000
Datei Tools Bearbeiten Hilfe
FILTER Nachweise Artefakte Datentypen Datums- und Zeitattribute Zeitleistenkategorien Tags und Kommentare
FILTER LÖSCHEN
Zeitachse
24.06.2022 23:55:13 - 25.06.2022 16:00:59
GEHE ZU DATUM
ZOOM
TAGE
SEITE
lp.speuer@gmail.com, norbert.speuer@gmail.com
30030000-200.E01 - Partition 3 (125,29 GB)_decrypted
VORSCHAU
ERKENNEN
Von: gn.speuer@gmail.com
Gesendet: 25.06.2022 14:30:26
An: lp.speuer@gmail.com, norbert.speuer@gmail.com
Betreff: Ich bin dann mal weg
Anhänge: 1AA0CB4FED0646FEAF7E710EB4403413[25832][27].png
Liebe Kollegen,
einige schöne, aber auch anstrengende Jahre Enden für mich heute. Ich danke euch allen für die aufregende und arbeitsreiche Zeit und wünsche euch für die Zukunft viel Erfolg.
Speziell möchte ich meiner Sekretärin Lisa danken für die tolle Unterstützung über all die Jahre.
Auch an dich Nobi ein großes Danke für alles.
In diesem Sinne… ich bin dann mal Weg!
Beste Grüße
Ihr Guido Nagel
E-MAIL-ANHÄNGE
1AA0CB4FED0646FEAF7E710EB4403413[25832][27].png
lp.speuer@gmail.com, norbert.speuer@gmail.com 1 ZEITSTEMPEL
Datum/Uhr... Datums-/Uhrzeitattribut Zeitleistenkatego... Kateg... Typ Elem... Wert des Elements
25.06.2022 14:30:24 MFT geändert Dateiwiedererkennung Dateisystem Datei 57C8ED895DF3F0AD4EE2DC2B6CFD4157
25.06.2022 14:30:24 Aufgerufen Datei/Ordne wird geöffnet Dateisystem Datei 77EC638DA74BD0D0E0426DC8F8008506
25.06.2022 14:30:24 Aufgerufen Datei/Ordne wird geöffnet Dateisystem Datei F80D848F74F708B2EAA93746D24D9749
25.06.2022 14:30:26 Datum/Zeit Benutzerkommunikation E-Mail und... Windows Mail An lp.speuer@gmail.com, norbert.speuer@gmail.com
25.06.2022 14:30:26 Zeitstempel der E-Mail Datum/Zeit Benutzerkommunikation Email & Cal... Email Attachments Dateiname 1AA0CB4FED0646FEAF7E710EB4403413[25832][27]...
25.06.2022 14:30:26 Datum/Zeit Benutzerkommunikation E-Mail und... Windows Mail An lp.speuer@gmail.com, norbert.speuer@gmail.com
25.06.2022 14:30:27 Datum/Zeit des Ereignisses Gelöschte Datei Betriebssyst... $LogFile-Analyse Dateibetrieb Delete
25.06.2022 14:30:27 Modifiziert Datei/Ordne wird geöffnet Dateisystem Ordner Attachments
25.06.2022 14:30:29 Datum/Zeit des Ereignisses Dateiwiedererkennung Betriebssyst... $LogFile-Analyse Dateibetrieb Create
25.06.2022 14:30:29 Aktuelle MFT zuletzt modifiziert – Datum/Zeit Dateiwiedererkennung Betriebssyst... $LogFile-Analyse Dateibetrieb Create
25.06.2022 14:30:29 Aktuelle(s) Datum/Zeit der Erstellung Dateiwiedererkennung Betriebssyst... $LogFile-Analyse Dateibetrieb Create
25.06.2022 14:30:29 Aktuelle(s) Datum/Zeit der Modifikation Dateiwiedererkennung Betriebssyst... $LogFile-Analyse Dateibetrieb Create
25.06.2022 14:30:29 Aktuelle(s) Datum/Zeit des Zugriffs Dateiwiedererkennung Betriebssyst... $LogFile-Analyse Dateibetrieb Create
25.06.2022 14:30:29 Letzter Lauf – Datum/Zeit Programmausführung Betriebssyst... Windows 8/10 Prefetch-Dateien Anwendun... SEARCHFILTERHOST.EXE
25.06.2022 14:30:29 Datum/Zeit der Erstellung Herunterladen der Datei Email & Cal... Email Attachments Dateiname 1AA0CB4FED0646FEAF7E710EB4403413[25832][27]...
25.06.2022 14:30:29 Datum/Zeit des Zugriffs Herunterladen der Datei Email & Cal... Email Attachments Dateiname 1AA0CB4FED0646FEAF7E710EB4403413[25832][27]...
25.06.2022 14:30:29 Modifiziert – Datum/Zeit Herunterladen der Datei Email & Cal... Email Attachments Dateiname 1AA0CB4FED0646FEAF7E710EB4403413[25832][27]...
25.06.2022 14:30:29 Datum/Zeit der Erstellung Dateiwiedererkennung Medien Bilder Dateiname 1AA0CB4FED0646FEAF7E710EB4403413[25832][27]...
Dateien gespeichert.
ÖFFNEN
Zeitzone UTC+1:00


Magnet AXIOM Examine v6.3.0.32040 - 30030000
Datei Tools Bearbeiten Hilfe
FILTER Nachweise Artefakte Datentypen Datums- und Zeitattribute Zeitleistenkategorien Tags und Kommentare
FILTER LÖSCHEN
Zeitachse
24.06.2022 23:55:13 - 25.06.2022 16:00:59
GEHE ZU DATUM
ZOOM
TAGE
SEITE
userinit.exe
30030000-200.E01 - Partition 3 (125,29 GB)_decrypted
DETAILS
ARTEFAKTINFORMATIONEN
Dateiname userinit.exe
Dateipfad C:\Windows\system32\userinit.exe
Typ Userinit
Auslösebedingung Windows startup
Registry-Schlüssel modifiziert – Datum/Zeit 25.06.2022 14:32:21
Typ AutoRun-Elemente
Objekt-ID 25269
BEWEISINFORMATIONEN
Quelle 30030000-200.E01 - Partition 3 (125,29 GB) _decrypted.img - Entire Disk (Microsoft NTFS, 125,29 GB)\Windows\System32\config\SOFTWARE
Wiederherstellungsmethode Geparst
Quelle löschen
Speicherort Microsoft\Windows NT\CurrentVersion\Winlogon
Beweisnummer 30030000-200.E01 - Partition 3 (125,29 GB)_decrypted
userinit.exe 1 ZEITSTEMPEL
Datum/Uhr... Datums-/Uhrzeitattribut Zeitleistenkatego... Kateg... Typ Elem... Wert des Elements
25.06.2022 14:32:21 Datum/Zeit des Ereignisses Datei/Ordne wird geöffnet Betriebssyst... $LogFile-Analyse Dateibetrieb Modify
25.06.2022 14:32:21 Datum/Zeit des Ereignisses Datei/Ordne wird geöffnet Betriebssyst... $LogFile-Analyse Dateibetrieb Modify
25.06.2022 14:32:21 Registry-Schlüssel modifiziert – Datum/Zeit Programmausführung Betriebssyst... AutoRun-Elemente Dateiname userinit.exe
25.06.2022 14:32:21 Datum/Zeit der Erstellung Betriebssyst... Windows Ereignisprotokolle Ereignis-ID 267
25.06.2022 14:32:21 Datum/Zeit der Erstellung Betriebssyst... Windows Ereignisprotokolle Ereignis-ID 187
25.06.2022 14:32:21 Datum/Zeit der Erstellung Betriebssyst... Windows Ereignisprotokolle Ereignis-ID 24
25.06.2022 14:32:21 Aufgerufen Datei/Ordne wird geöffnet Dateisystem Ordner Program Files
25.06.2022 14:32:21 Aufgerufen Datei/Ordne wird geöffnet Dateisystem Ordner Dell
25.06.2022 14:32:21 MFT geändert Dateiwiedererkennung Dateisystem Ordner Temp
25.06.2022 14:32:21 Aufgerufen Datei/Ordne wird geöffnet Dateisystem Ordner Dell Peripheral Manager
25.06.2022 14:32:21 MFT geändert Dateiwiedererkennung Dateisystem Ordner waasmedic
25.06.2022 14:32:21 Aufgerufen Datei/Ordne wird geöffnet Dateisystem Ordner sru
25.06.2022 14:32:21 Modifiziert Datei/Ordne wird geöffnet Dateisystem Ordner sru
25.06.2022 14:32:21 MFT geändert Dateiwiedererkennung Dateisystem Ordner sru
25.06.2022 14:32:21 Aufgerufen Datei/Ordne wird geöffnet Dateisystem Ordner Fonts
25.06.2022 14:32:21 Aufgerufen Datei/Ordne wird geöffnet Dateisystem Ordner QmlPlugins
25.06.2022 14:32:21 Aufgerufen Datei/Ordne wird geöffnet Dateisystem Ordner System
25.06.2022 14:32:21 MFT geändert Dateiwiedererkennung Dateisystem Ordner System
Dateien gespeichert.
ÖFFNEN
Zeitzone UTC+1:00

Bericht Asservat-100 USB-Stick (Axiom)

Der vollständige Bericht des USB-Sticks (Asservat-100) umfasst 1213 Seiten und wird aus Gründen der Übersichtlichkeit in diesem Dokument nur verlinkt.

https://cloud.hs-wismar.de/getlink/fiNhpSMFofUDbbTkeNYfJqRv/

Bericht Asservat-200 Notebook (Axiom)

Der vollständige Bericht des Notebooks (Asservat-200) umfasst 9460 Seiten und wird aus Gründen der Übersichtlichkeit in diesem Dokument nur verlinkt.

https://cloud.hs-wismar.de/getlink/fiNhpSMFofUDbbTkeNYfJqRv/