Hochschule Wismar
University of Applied Sciences: Technology, Business and Design
Fachrichtung IT-Forensik
Sommersemster 2023
Modul: IT-Forensik Projekt II
Dozentin: Frau Prof. Dr. Antje Raab-Düsterhöft

Projektarbeit II im Studiengang IT-Forensik

zum Thema

Vergleich der beiden Forensik-Programme X-Ways Forensics und Autopsy im Bereich der Smartphone-Forensik

Vorgelegt von

Michael Krimplstötter

Matrikelnummer 360485

6. Semester

am

15.10.2023

Abstract

Heutzutage sind Smartphones aus dem Alltag nicht mehr wegzudenken. Aufgrund ihrer immer größeren Speicherkapazitäten, leistungsstarker Hardware und permanenter Datenverbindung, bieten uns Smartphones eine Vielzahl an Verwendungsmöglichkeiten. Fast jeder besitzt heutzutage ein Smartphone welches als ständiger Begleiter mitgeführt wird, weshalb oft auf diesen unser ganzer Alltag gespeichert (z. B. Bilder, Videos) und daher freiwillig oder auch unfreiwillig unser Leben dokumentiert wird (z. B. Speicherung der Standortdaten). Somit ist es absolut nachvollziehbar, dass vor allem im Rahmen von behördlichen Ermittlungsverfahren das sicherstellen von Smartphones von großem Interesse ist, da dort gespeicherte Daten als mögliche Beweise zur Aufklärung von Verbrechen dienen können.

In der nachfolgenden Projektarbeit soll die Effektivität sowie die Leistungsfähigkeit der beiden Forensik-Programme X-Ways und Autopsy in bestimmten Bereichen analysiert und verglichen werden. Hierbei werden die Kriterien wie Benutzerfreundlichkeit, Datenextraktion Analysemöglichkeiten und Berichterstellung herangezogen um die Stärken und Schwächen der beiden Tools festzustellen. Ziel dieser Projektarbeit soll es daher sein, die für die Smartphone-Forensik geeignetere Software zu finden um somit die besten Ergebnisse erzielen zu können.

1. Einleitung

Als erstes wird auf den Hintergrund und die Bedeutung der Smartphone-Forensik und die Zielsetzung der Arbeit hingewiesen. Danach werden die beiden Forensik-Programme X-Ways und Autopsy anhand ihrer Möglichkeiten vorgestellt. Anschließend soll eine Analyse und Auswertung der beiden Programme erfolgen.

1.1 Hintergrund und Bedeutung der Smartphone-Forensik

Die Anzahl der Nutzer von Smartphones in Deutschland ist in den letzten Jahren stetig gestiegen. Im Kalenderjahr 2021 beläuft sich die Anzahl der Smartphone-Nutzer in Deutschland auf rund 62,6 Millionen Menschen. Besonders hoch ist der Nutzeranteil von Smartphones in der Altersgruppe der 14 – 49 jährigen. Dort liegt dieser bei über 95 Prozent. Neben der Möglichkeit Telefonate zu führen oder SMS zu versenden, erlauben Smartphones heutzutage Fotos in hoher Qualität aufzunehmen, Musik zu hören, ständig die neuesten Informationen zu erhalten, die Verwaltung von E-Mails, Terminen oder Kontakten vorzunehmen oder die Navigation anhand ausgewählter Routen durchzuführen. Mobile Daten sichern dabei die andauernde Synchronisation sämtlicher Daten. Da Smartphones auch in Zukunft immer mehr Geräte ersetzen werden und Hersteller immer neue Funktionen hinzufügen, wird die Bedeutung der Smartphones auch in Zukunft weiter steigen.[1]

Dies heißt jedoch auch, dass die Bedeutung von Smartphones bei zukünftigen Ermittlungen für Strafverfolgungsbehörden eine noch größere Rolle spielen wird. Smartphones bieten vor allem aufgrund von Daten wie des gespeicherten Verlaufs besuchter Internetseiten, Fotos, Chatverläufen oder E-Mails für die Strafverfolgungsbehörden eine Vielfalt von Informationen und somit oftmals auch Aufschluss über die Tat oder Täter. Auch über die auf dem Smartphone gespeicherten Apps können Informationen wie Bewegungsaktivitäten oder den Standort des Gerätes entnommen werden und somit zur Aufklärung einer Straftat hilfreich sein. Somit existiert heutzutage kaum ein vergleichbares Objekt, welches über seinen Besitzer in solch einem Umfang Informationen speichert und daher eine Auswertung über sein soziales Verhalten, seine sozialen Kontakte und gegebenenfalls auch zu seinen Gedanken ermöglicht.[2]

[1] (F.Tenzer, 2022)
[2] (Stephan Ludewig, 2019)

Je nach Anforderung kann die Auswertung eines Smartphones auf verschiedene Weise erfolgen. Dies kann zum Beispiel durch Abfotografieren des Displays über die Verwendung einer Forensik-Software bis hin zum „Chip-Off“-Verfahren, bei dem beispielsweise ein Flash-Speicher physisch von der Hauptplatine entfernt wird und anschließend mit einer speziellen Hardware ausgewertet wird, erfolgen.[3]

Aber nicht nur für Strafverfolgungsbehörden ist die forensische Untersuchung von Smartphones wichtig. Auch in Unternehmen, wo der Datenschutz einer immer größere Rolle spielt, ist im Falle von Sicherheitsvorfällen eine forensische Untersuchung notwendig, um die Integrität von Daten zu gewährleisten und die Einhaltung von Vorschriften und Richtlinien sicherzustellen.

Somit gewinnt die Bedeutung der Smartphone-Forensik für Strafverfolgungsbehörden als auch für Unternehmen immer mehr an Bedeutung. Nur mit der forensischen Untersuchung lassen sich Beweismittel aus Smartphones sichern um Straftaten aufzuklären. Aber auch für die Unternehmen spielt die Smartphone-Forensik zukünftig eine Rolle, um die Sicherheit der Unternehmensdaten zu gewährleisten.

1.2 Zielsetzung der Arbeit

Zielsetzung dieser Hausarbeit ist, die beiden Forensik-Programme X-Ways und Autopsy hinsichtlich ihrer Anwendungsmöglichkeiten und Funktionen im Bereich der Smartphone-Forensik zu vergleichen um somit die jeweiligen Stärken und Schwächen sowie Unterschiede erkennbar zu machen.

Innerhalb der Funktionen soll sich ein Überblick über Faktoren wie Datenextraktion, Analysemöglichkeiten, Benutzerfreundlichkeit und Berichterstellung verschafft werden. Dies soll dazu führen, dass bei einer zukünftigen forensischen Untersuchung die geeignetste Software ausgewählt werden kann.

1.3 Abgrenzung

In dieser Projektarbeit werden nur die beiden Forensik-Programme X-Ways Forensics und Autopsy untersucht. Da es mit diesen Programmen bereits in anderen Modulen des Studiums Berührungspunkte gab, hatte ich mich für diese beiden Forensik-Programme entschieden. Andere forensische Tools werden nicht herangezogen. Des Weiteren wird sich, wie unter Punkt 1.2 bereits aufgeführt, auf

[3] (Stephan Ludewig, 2019)

die Faktoren Datenextraktion, Analysemöglichkeiten, Benutzerfreundlichkeit und Berichterstellung beschränkt, da die vorgestellten Forensik-Programme eine Vielzahl von Funktionen und Tools bereitstellen und eine Berücksichtigung aller Funktionen den Umfang der Projektarbeit übersteigen würden.

1.4 Evaluation

Um eine Überprüfung der vor allem in den Benutzerhandbüchern dargestellten Funktionen der beiden Forensik-Programme vornehmen zu können, wurde freundlicherweise durch die Firma X-Ways Software Technology AG eine Probe-Lizenz von X-Ways Forensics zur Verfügung gestellt. Bei der Software Autopsy war dies nicht notwendig, da diese frei verfügbar ist. Für die Überprüfung der Faktoren Benutzerfreundlichkeit, Analyse- und Datenextraktionsmöglichkeiten sowie Berichterstellung wurde ein Smartphone-Image eines Samsung Galaxy S3 mit einem Android-Betriebssystem 6.0 (Marshmallow) verwendet, welches bereits im Modul Computerforensik I für forensische Arbeiten vom Dozenten Hans-Peter Merkel zur Verfügung gestellt wurde.

2. Forensik-Programm X-Ways

Im Folgenden wird das Forensik-Tool X-Ways Forensics mit seinen beworbenen Eigenschaften vorgestellt. Hierbei wurde die X-Ways Forensics Version 20.9 verwendet.

2.1 Einführung in X-Ways

X-Ways Forensics ist ein Forensik-Programm welches weltweit verbreitet und im Bereich der Digital-Forensik auch anerkannt ist. Stefan Fleischmann gründetet 2002 als Student ein Softwareentwicklungsunternehmen Namens X-Ways Corporation. Am 21. Juni 2004 stellte er die erste Version von X-Way Forensics vor. Im Jahr 2005 erfolgten zu X-Way Forensics die ersten Schulungen in Seattle, Washington. Seit diesem Zeitpunkt wurde X-Ways Forensics ständig weiterentwickelt und erhielt hunderte neuer Funktionen. Anwender von X-Ways Forensics sind sowohl Strafverfolgungsbehörden als auch private Unternehmen und alles, was dazwischen liegt.[4] Auf der Internetseite von X-Ways Forensics wird das Tool vor allem damit beworben, dass dieses unter anderem sehr effizient zu bedienen ist, weniger

[4] (Shavers & Zimmerman, 2014, S. xviii)

ressourcenhungrig wie andere Forensik-Programme ist, kaum Speicher benötigt und schneller gelöschte Dateien und Suchbegriffe findet. Des Weiteren wird es als kostengünstiger (Zeitlich unbegrenzte Lizenz für 2.639 €) beworben wie vergleichbare Programme. X-Ways Forensics entwickelte sich aus dem Hexadezimal- und Datenträgereditor WinHex, welches Teil eines Workflow-Models ist, wo IT-Forensiker mit Ermittlern zusammenarbeiten können, die X-Ways Investigator verwenden.[5]

2.2 Funktionen und Tools

X-Ways Forensics beinhaltet eine Vielzahl an Funktionen und Tools welche für die forensische Untersuchung von Smartphones verwendet werden können. Dies ist vor allem auf der Internetseite von X-Ways Forensics gut erkennbar (Abbildung 1).

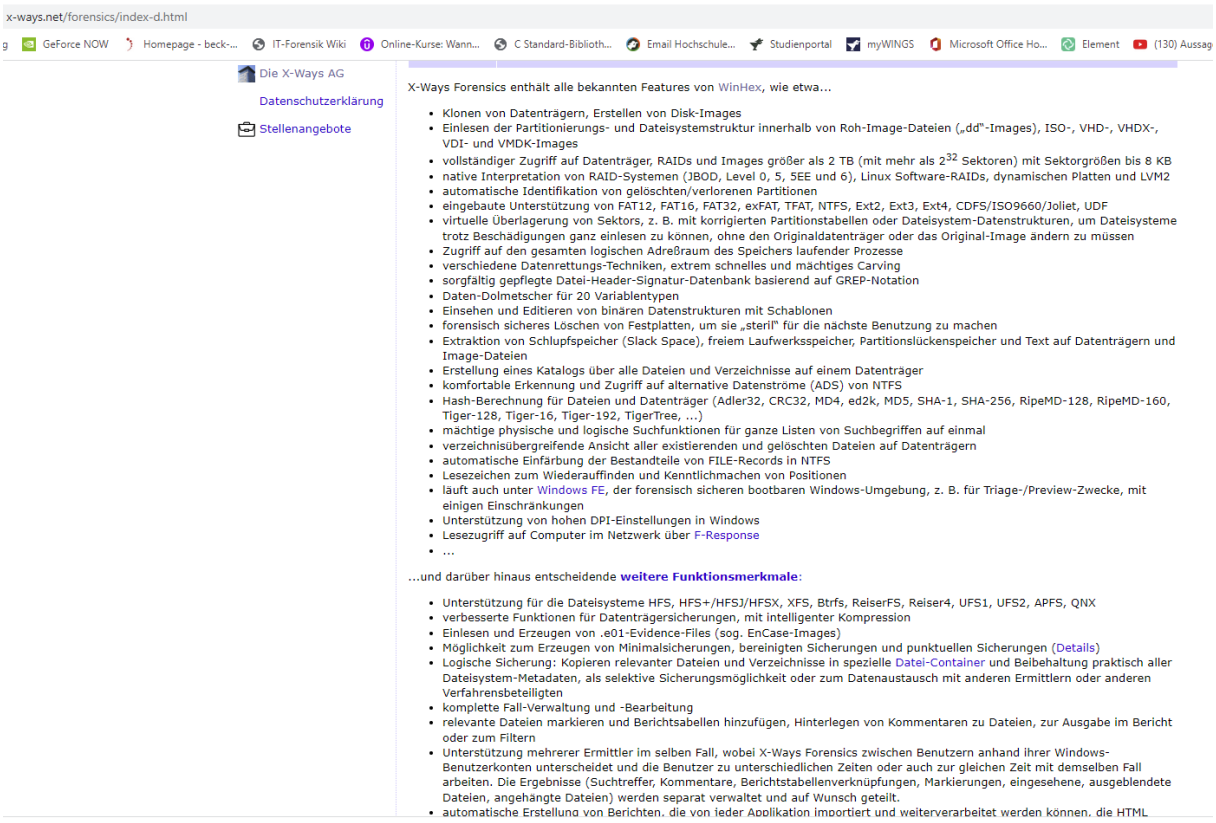


Abbildung 1: Übersicht Funktionen X-Ways Forensics[6]

Hier werden eine große Anzahl von Funktionen von X-Ways aufgeführt. Die Liste ist jedoch nicht abschließend. Im Rahmen der Projektarbeit soll sich jedoch, wie bereits im Punkt 1.2 geschildert, auf die Funktionen Datenextraktion, Analysemöglichkeiten,

[5] (X-Ways Software Technology AG, www.x-ways.net, 2023)
[6] (X-Ways Software Technology AG, www.x-ways.net, 2023)

Benutzerfreundlichkeit und Berichterstellung beschränkt werden, da nicht alle Funktionen in der Projektarbeit berücksichtigt werden können.

Für die Datenextraktion unterstützt X-Ways zum Beispiel Dateiformate wie Ext4, Ext3 oder Ext2. Ext4 wird beispielsweise von Google für Android-Smartphones benutzt. Des Weiteren gibt es die Möglichkeit Bilder aus Video-Dateien mittels dem Tool MPlayer oder Forensic Framer zu extrahieren, was die Durchsuchung von Filmen auf illegale oder unangemessene Inhalte wesentlich beschleunigt. Auch ermöglicht X-Ways Forensics das extrahieren von Metadaten und Erzeugungszeitstempel aus verschiedenen Dateitypen.[7] Aufgrund dessen, das X-Ways Forensics sich aus dem Hex-Editor WinHex weiterentwickelt hat, bietet X-Ways die Möglichkeit, Daten aus unterschiedlichsten Ebenen zu extrahieren.[8] Dies bietet IT-Forensikern und Experten die Chance, Smartphones ausführlich und umfassend zu untersuchen. X-Ways Forensics bietet somit eine große Anzahl von Datenextraktionsmöglichkeiten um eine Vielzahl von Informationen aus zu untersuchenden Android-Smartphones zu erhalten.

Die Analysemöglichkeit von X-Ways Forensics bietet Möglichkeiten um verschiedene Artefakte auf Smartphones zu untersuchen. Dazu gehören unter anderem Ereignislisten welche auf den Zeitstempeln beruhen, Event-Logs und Registrys in Betriebssystemen, Datei-Inhalte wie beispielsweise E-Mail-Header, GPS-Zeitstempel, Skype-Chats, Anrufprotokolle und vieles mehr. Auch bietet X-Ways Forensics die Möglichkeit zur Erkennung verschlüsselter MS-Office und PDF-Dokumente, das automatische Auffinden von eingebetteten Bildern in Dokumenten und eine Hautfarbenerkennung, welche die Suche nach Spuren von Kinderpornographie wesentlich beschleunigt.[9] Aufgrund der umfassenden Analysemöglichkeiten von X-Ways-Forensic ist es für IT-Forensiker möglich, Artefakte auf Smartphones intensiv zu untersuchen um wichtige Informationen zu erhalten, die Rückschlüsse auf die Nutzung sowie die Kommunikation der betreffenden Person zulassen.

Bezüglich der Benutzerfreundlichkeit bietet X-Ways Forensics verschiedene Einstellungsmöglichkeiten um den Anwender die Benutzung zu erleichtern. X-Ways Software Technology AG bietet den Anwendern auch Anleitungsvideos, welche den

[7] (X-Ways Software Technology AG, www.x-ways.net, 2023)
[8] (Shavers & Zimmerman, 2014, S. xviii)
[9] (X-Ways Software Technology AG, www.x-ways.net, 2023)

Einstieg in X-Ways Forensics erleichtern sollen. Des Weiteren findet sich auch auf der Internetseite von X-Ways Software Technology AG ein Benutzerhandbuch, auf welches Personen, die erstmalig mit X-Ways Forensics arbeiten, zurückgreifen können.

Für Experten ist bei der Berichtserstellung von entscheidender Bedeutung, dass die gefundenen Informationen auf dem Smartphone in einem leicht verständlichen und leicht zu erstellenden Bericht übermittelt werden können. Die Berichtsfunktion von X-Ways Forensics basiert auf Berichtstabellen, die als eine Art Lesezeichen oder Kategorie angesehen werden kann. Die Berichtstabellen ermöglichen es, die Ergebnisse der Überprüfung für Staatsanwälte, Kunden und Kollegen logisch zu organisieren. X-Ways Forensics erzeugt Berichte auf HTML-Basis, sodass diese sich mit einem einfachen Texteditor oder beispielsweise Word bearbeiten lassen.[10]

2.3 Benutzerfreundlichkeit

Im Folgenden wurde die Benutzerfreundlichkeit in den Bereichen Installationsaufwand/Systemvoraussetzungen, Anwendersupport und Benutzeroberfläche, welche X-Ways Forensik bietet, untersucht.

2.3.1 Installationsaufwand / Systemvoraussetzungen

Der Installationsaufwand bei X-Ways Forensics ist sehr gering. Aufgrund der niedrigen Systemanforderungen (benötigter Speicherplatz ca. 746 MB) kann X-Ways Forensics heutzutage auf jeden modernen Computer installiert werden. Eigentlich kann gesagt werden, das X-Ways Forensics sogar ohne eine Installation auskommt, da die benötigten Dateien einfach nur aus der Zip-Datei extrahiert werden müssen. X-Ways Forensics liefert zwar einen sogenannten „Installer“ mit, dieser wird aber grundsätzlich nicht benötigt. Mit der in der E-Mail enthaltenen Installationsanleitung sowie den jeweiligen Verlinkungen zu den benötigten Dateien, sollte es für die meisten Benutzer möglich sein, die Installation ohne größere Probleme durchzuführen.

Zuerst erfolgte mit Übersendung der E-Mail vom Support die zur Verfügungstellung alle benötigen Informationen wie Benutzerkennung und Passwort für den Login auf der Herstellerseite, Link zur Lizenzvergabe, Link zur Download-Datei sowie zu

[10] (Shavers & Zimmerman, 2014, S. 181)

zusätzlichen Erweiterungen (Abbildung 2). Leider funktionierten die Links für die Erweiterungen von Excire und Tesseract nicht. Jedoch konnte durch selbständige Abänderung der Links doch noch der Zugriff auf die Erweiterungen erfolgen (Abbildung 3). Hätte dies keinen Erfolg gehabt, hätte hierzu nochmaliger Kontakt mit dem Support erfolgen müssen.

RE: RE: Probeversion X-Ways-Forensics für Projektarbeit im Studium

XN **X-Ways Sales / [redacted] <sales@x-ways.com>**
10.07.2023 10:45

An: 'Michael Krimplstötter'

Sehr geehrter Herr Krimplstötter,

bitte entschuldigen Sie vielmals, das war mein Versäumnis. Hier kommen die benötigten Anweisungen.

Sie können sich die neueste Version sowie ältere Versionen herunter-
laden von https://www.x-ways.com/xwb/.
(BYOD-Version, nicht identisch zur Dongle-Version!)

Zugangsdaten für passwortgeschützte Downloads und Web-Bereiche:
Benutzername : [redacted]
Passwort : [redacted]

Instruktionen zum Download von Updates werden Sie künftig immer
unter https://www.x-ways.net/winhex/license-d.html durch Eingabe
Ihrer E-Mail-Adresse abfragen können. Dort erhalten Sie auch
aktuelle Zugangsdaten, da die o. g. sich ändern könnten.

Die Funktionsweise von BYOD ist beschrieben unter
www.x-ways.net/BYOD-d.html und www.x-ways.com/xwb/Q&A.html.

Unter folgender Adresse können Sie Ihre Lizenzdatei abrufen:
[redacted]

Ihre Lizenz ist gültig bis zum 10.09.23.

Die Viewer-Komponente ist verfügbar von
https://www.x-ways.com/res/viewer/xw_viewer.zip und sollte am
besten in dasselbe Verzeichnis entpackt werden, in dem Sie X-Ways
Forensics ausführen. Unter Optionen | Externe Programme können Sie
im Programm sicherstellen, dass die Viewer-Komponente aktiv ist.

Tesseract, eine separate Komponente für OCR (grafische Texterkennung)
in Stichwort-Suchen, erhalten Sie unter www.x-ways.net/res/Tesseract.zip.

Excire, eine separate Komponente für automatische Bildinhalts-
analyse mit künstlicher Intelligenz, können Sie herunterladen
von https://www.x-ways.com/res/Excire.zip.

MPlayer, eine separate Komponente zum Abspielen von Videos und
Extrahieren von einzelnen Frames in Videos, ist verfügbar unter
https://www.x-ways.net/res/mplayer/.

Abbildung 2 - E-Mail mit Installationsanleitung X-Ways Forensics

Abbildung 3 - Download Erweiterung Excire und Tesseract

Danach erfolgt die Installation von X-Ways Forensics entweder durch das extrahieren der Zip-Datei oder durch den Setup-Installer (welcher ebenfalls in der Zip-Datei enthalten ist) (Abbildung 4). Nachdem die Installation durchgeführt wurde, wird durch den BYDO-Kopierschutz (BYDO = **B**ring **y**our **o**wn **d**evice/**d**isk/**d**ongle) die Lizenz geprüft, welche benötigt wird, um die Software freizuschalten. Das benutzte Gerät dient als Freischaltgerät für eine Lizenz. Hierbei wird eine Device-ID ermittelt welche dann übermittelt wird (Abbildung 5). Erst dann wird die Lizenz erstellt (Abbildung 6). Mit dieser wird dann X-Ways Forensics freigeschaltet und kann ab diesem Zeitpunkt genutzt werden (Abbildung 7).[11]

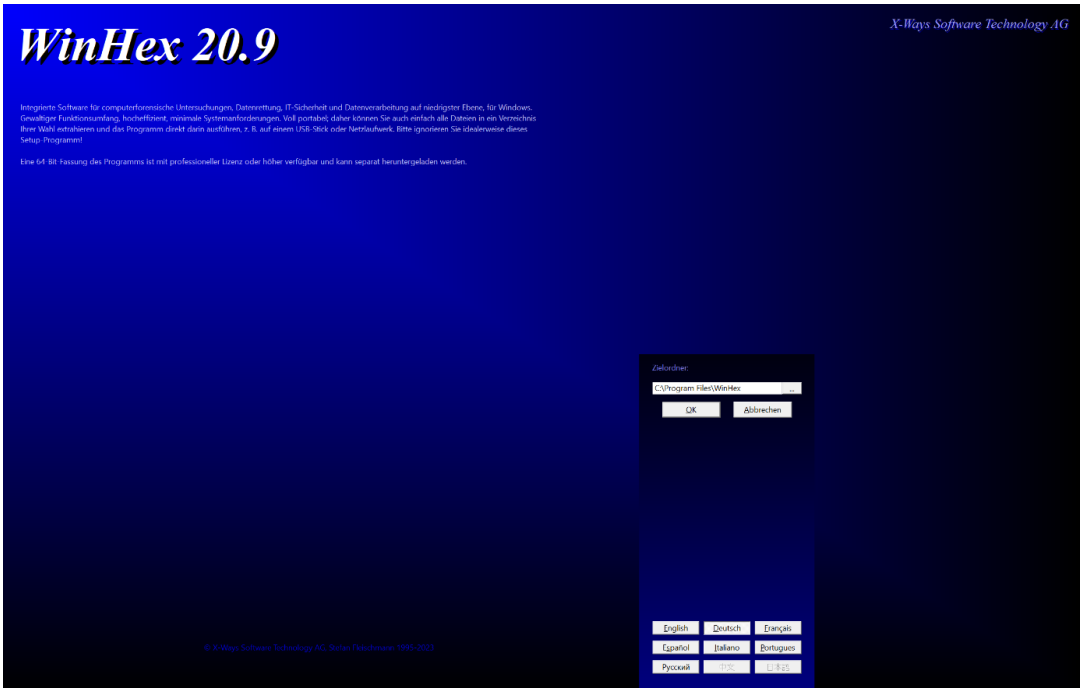


Abbildung 4 - Setup Installer X-Ways Forensics

[11] (X-Ways Software Technology AG, http://www.x-ways.net/BYOD-d.html, 2023)

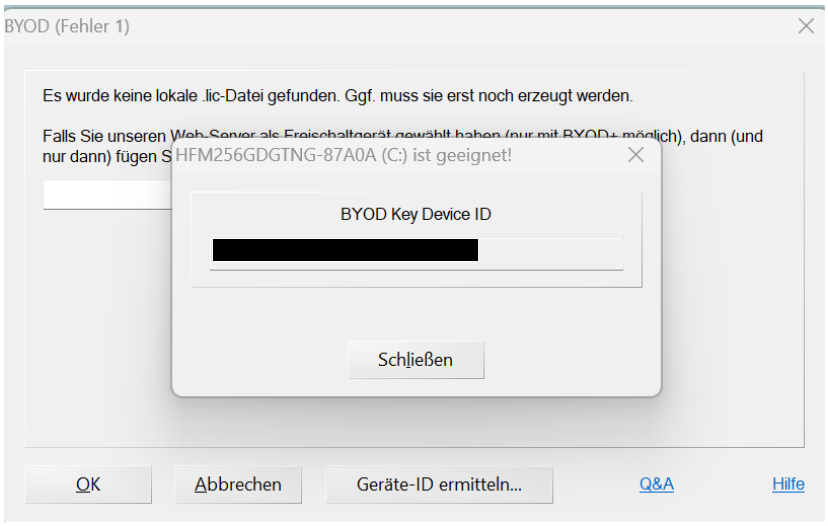


Abbildung 5 - BYOD-Kopierschutz

Abbildung 6 - Lizenz-Datei X-Ways Forensic

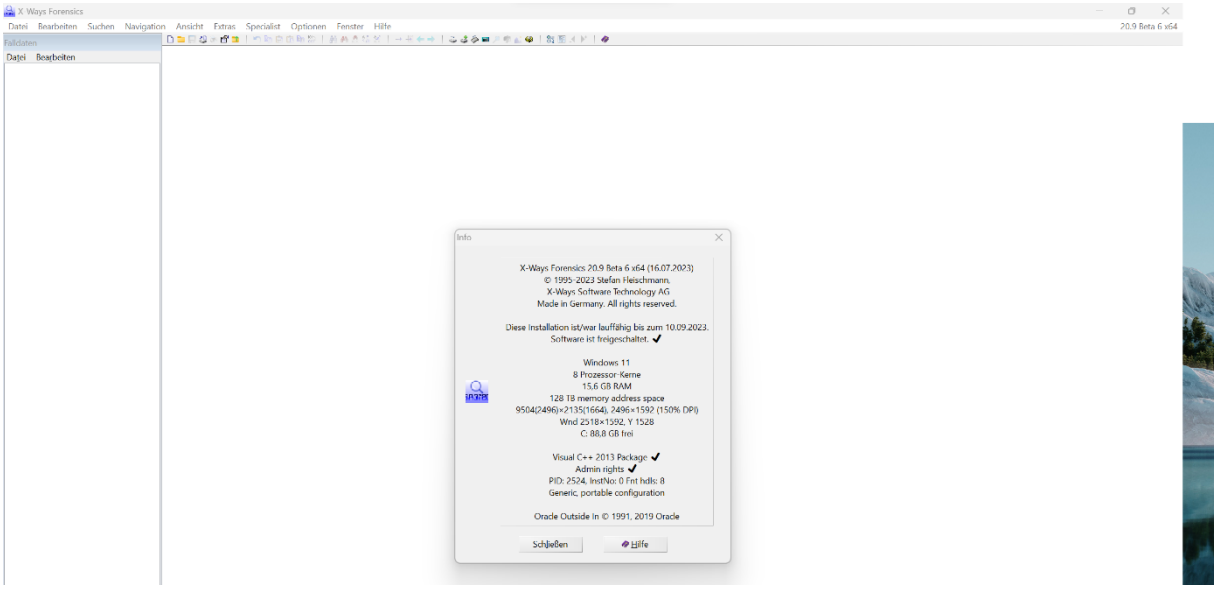


Abbildung 7 - Freischaltung X-Ways Forensic

2.3.2 Anwendersupport

Aufgrund einer fehlenden Lizenz, wurde über die Internetseite Kontakt zu X-Ways Software Technology AG aufgenommen. Der Anwendersupport meldete sich nach Kontaktaufnahme über das Kontaktformular[12] schnell und zuverlässig. Die Rückmeldung erfolgte meist innerhalb der ersten 24 Stunden. Dies sollte für Kunden,

[12] (X-Ways Software Technology AG, https://www.x-ways.net/corporate/contact-d.html, 2023)

welche die Software aus dem Hause X-Ways Software Technology AG verwenden, in jedem Fall ausreichend sein, falls Probleme oder Hilfestellungen nötig sind. Ebenfalls wird ein Forum[13] betrieben, wo Benutzer einen Beitrag erstellen und sich somit austauschen können. Eine Kontaktaufnahme per Hotline ist jedoch nicht möglich.

Des Weiteren wird auf der Internetseite von X-Ways Software Technology AG sowohl ein Benutzerhandbuch[14] zur Verfügung gestellt sowie Videos auf YouTube[15], welche den Einstieg für neue Benutzer erleichtert. Ebenfalls bietet X-Ways Forensics selbst im Programm über den Reiter „Hilfe“ Informationen für Benutzer.

2.3.3 Benutzeroberfläche

Die Benutzeroberfläche in X-Ways Forensic selbst bietet ebenfalls eine Vielzahl von Einstellungsmöglichkeiten für den Benutzer. Auf alle Einstellungsmöglichkeiten einzugehen würde jedoch den Rahmen der Projektarbeit übersteigen. Deshalb sollen die Einstellungsmöglichkeiten innerhalb von X-Ways Forensics nur kurz angeschnitten werden. So kann der Benutzer Sicherheitsoptionen einstellen wie zum Beispiel das die Software Infos bei einem Absturz sammelt oder ob die Software den Benutzer vor Ausführung von Skripten erst fragen soll (Abbildung 8). Ebenfalls können allgemeine Optionen wie die Beibehaltung der Fensteranordnung oder verschiedene Farben für verschiedene Attribute eingestellt werden (Abbildung 9). Eine weitere Einstellung ist auch, wie dem Benutzer die gefundenen Dateien angezeigt werden sollen. Hier kann beispielsweise eingestellt werden, wie die bevorzugte Größe der Thumbnail-Anzeige in X-Ways aussehen soll (Abbildung 10)[16]. Mehr Informationen zu den einzelnen Einstellungsmöglichkeiten werden jedoch in dem Buch „X-Ways Forensics Practitioner´s Guide von Brett Shavers und Eric Zimmermann aufgezeigt.

[13] (X-Ways Software Technology AG, http://www.winhex.net/, 2023)
[14] (X-Ways Software Technology AG, https://www.x-ways.net/winhex/manual-d.pdf, 2023)
[15] (X-Ways Software Technology AG, https://www.youtube.com/playlist?list=PLB0pU0wP67A-_DeVFfswVlZuRTH4cWswQ, 2023)
[16] (X-Ways Software Technology AG, https://www.youtube.com/watch?v=OuT33vh8ZoM, 2023)

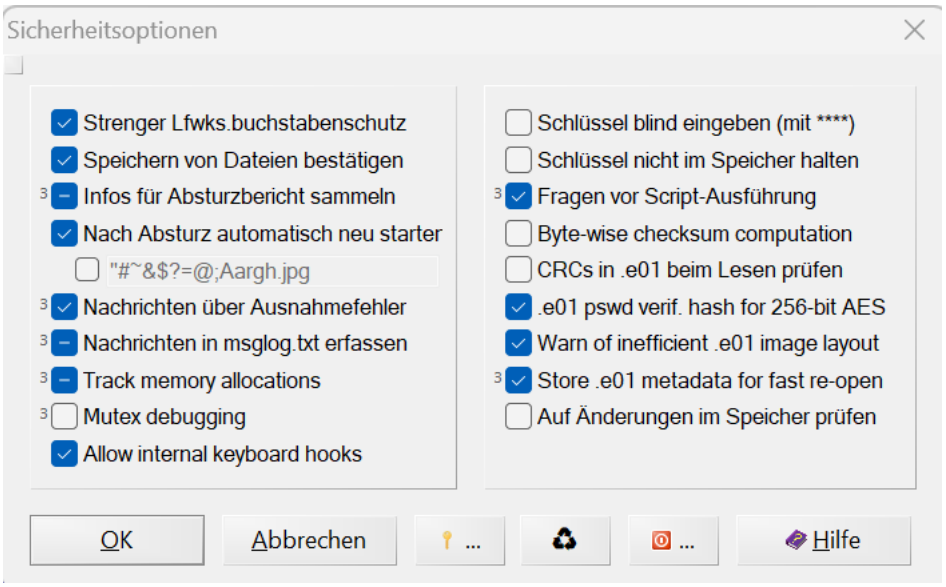


Abbildung 8 – Einstellungsmöglichkeiten Sicherheitsoptionen

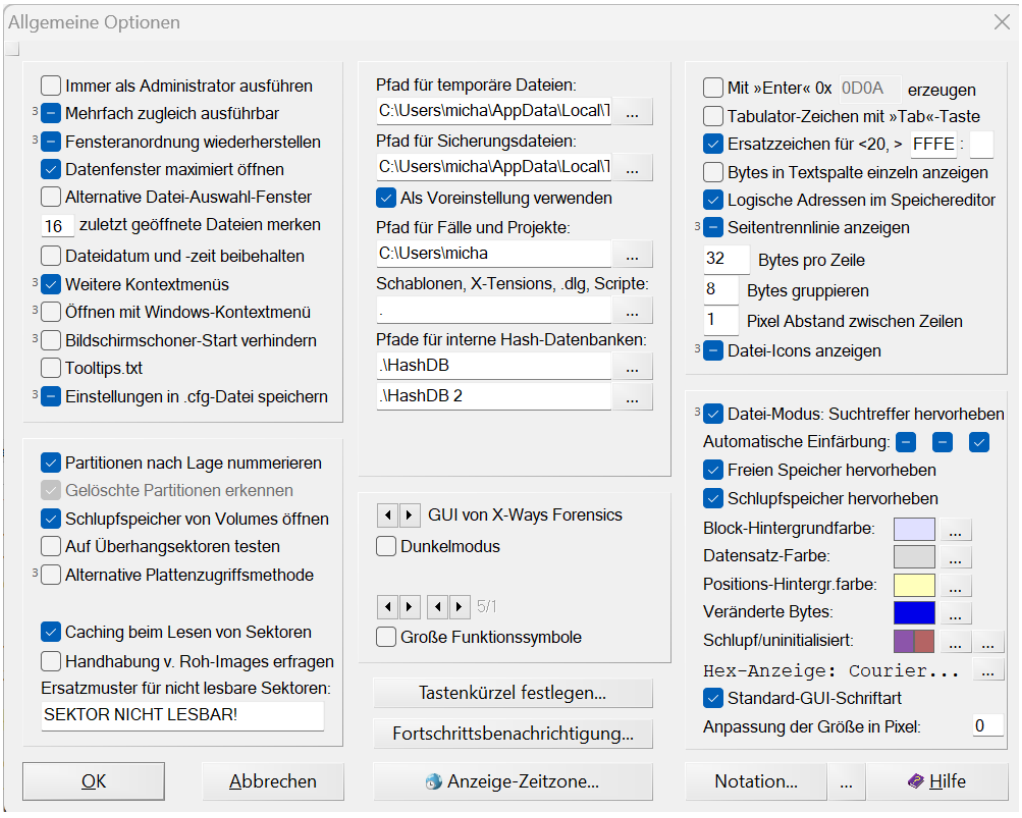


Abbildung 9 – Einstellungsmöglichkeiten Allgemeine Optionen

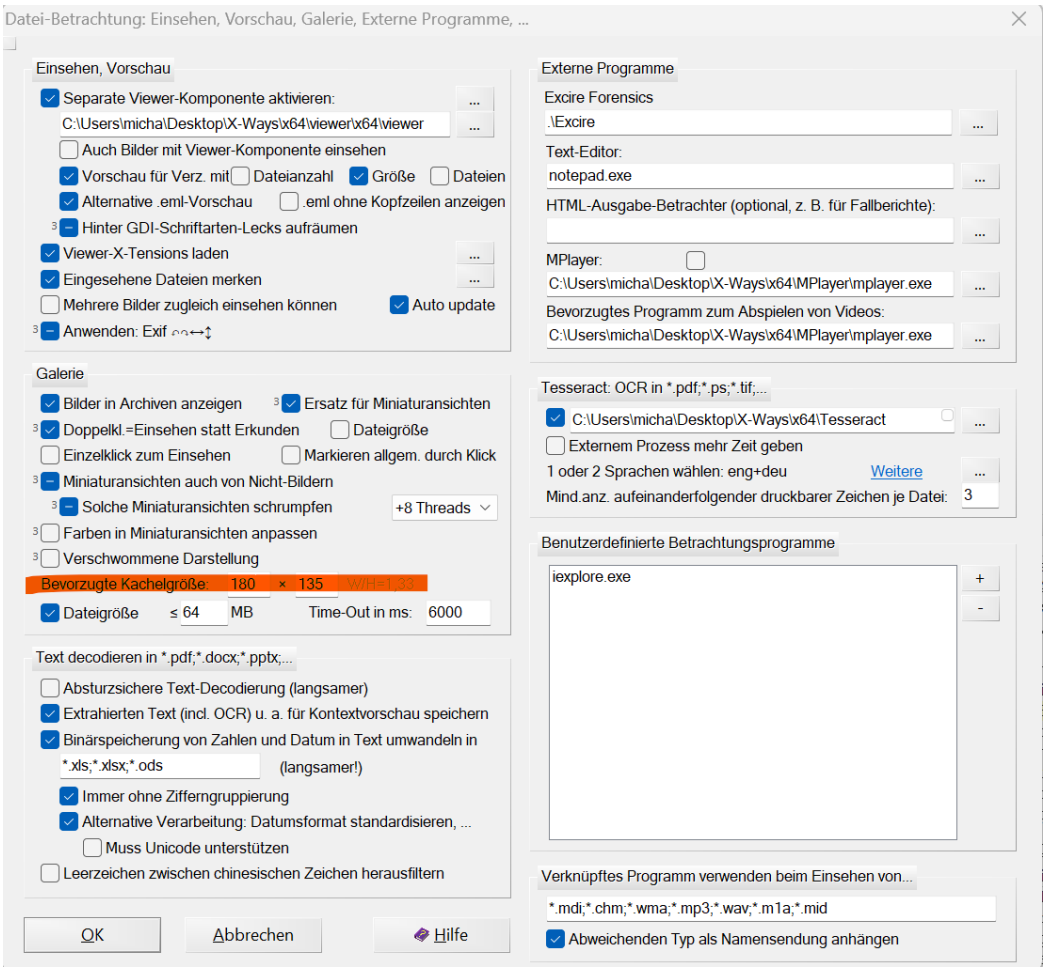


Abbildung 10 – Einstellungsmöglichkeit Datei-Betrachtung

2.4 Analysemöglichkeiten

Im Folgenden werden einige Analysemöglichkeiten, welche X-Ways Forensik bietet, vorgestellt. Eine vollständige Untersuchung aller Analysemöglichkeiten von X-Ways Forensik ist jedoch aufgrund des Umfangs nicht möglich, da dies den Umfang der Projektarbeit übersteigen würde.

2.4.1 Unterstützung von Dateisystemen

X-Ways Forensics unterstützt für die Smartphone-Forensik sowohl das Dateisystem Ext4 welches vor allem bei aktuellen Android-Smartphones vorliegt, als auch Ext2 und Ext3, welche vor allem bei älteren Smartphones verwendet werden. Ebenfalls unterstütz X-Ways Forensics APFS-Dateisysteme, welches bei neueren Geräten mit iOS von Apple verwendet wird. Aber auch die älteren Datei-Formate von Apple wie HFS+ oder HFSJ/HFSX werden unterstützt. Das verwendete Smartphone-Image

verwendet das Dateisystem Ext4 welches ohne Probleme in X-Ways Forensics untersucht werden konnte (Abbildung 11).[17]

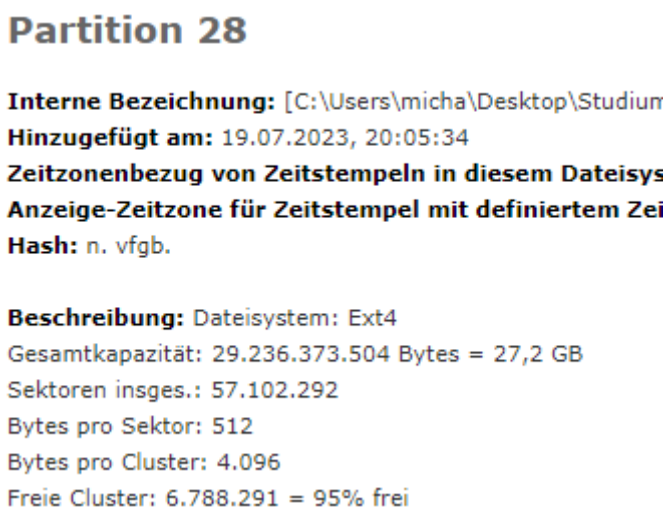


Abbildung 11 - Angabe zum verwendeten Dateisystem

2.4.2 Unterstützung von Image-Dateien

Mit X-Ways Forensics lässt sich auch das Erstellen von Smartphones-Images vollziehen. Dabei werden Roh-Image-Dateien (dd-Images) als auch Formate wie das EWF-Format (Expert Witness Compression Format oder .E01-Evidence-Files) unterstützt, um anhand dieser dann die forensische Untersuchungen durchführen zu können. Das verwendete Smartphone-Image wurde hier im Format EWF genutzt und konnte ohne Problem untersucht werden (Abbildung 12).[18] [19]

Abbildung 12 - EnCase-Format des verwendeten Images

[17] (X-Ways Software Technology AG, http://www.x-ways.net/forensics/index-d.html, 2023)
[18] (X-Ways Software Technology AG, http://www.x-ways.net/forensics/index-d.html, 2023)
[19] (X-Ways Software Technology AG, https://www.x-ways.net/winhex/manual-d.pdf, 2023, S. 94)

2.4.3 Einbinden von Partitionen/Ordnern

X-Ways Forensics bietet eine schnelle und einfache Möglichkeit Partitionen im eigenen Windows-System als Laufwerkbuchstaben einzubinden (Abbildung 13) und anschließend zu durchsuchen. Dies kann sowohl vollständig (Abbildung 14) als auch ausschnitthaft erfolgen. So kann mit externen Programmen einfach und schnell auf alle relevanten Dateien zugegriffen werden, ohne diese herauskopieren zu müssen. Diese Methode bietet sich auch dann an, wenn ein Verzeichnis oder eine Partition auf Viren untersucht werden sollen. Das kann für alle unterstützten Image-Typen (Datei-Container, VDI, VMDK, VHD, Roh-Images, .e01), alle unterstützten Partitionierungsmethoden sowie für alle unterstützten Dateisysteme erfolgen. Der Zugriff erfolgt vollständig schreibgeschützt, sodass keine Änderungen am Image vorgenommen werden.[20] Für das Einbinden von Partitionen als Laufwerk muss jedoch zuerst das Microsoft Visual C++ 2013 Redistributable Package installiert werden sowie der Dokan-Treiber. Hierzu bietet es sich an die Anleitung auf YouTube anzusehen.[21]

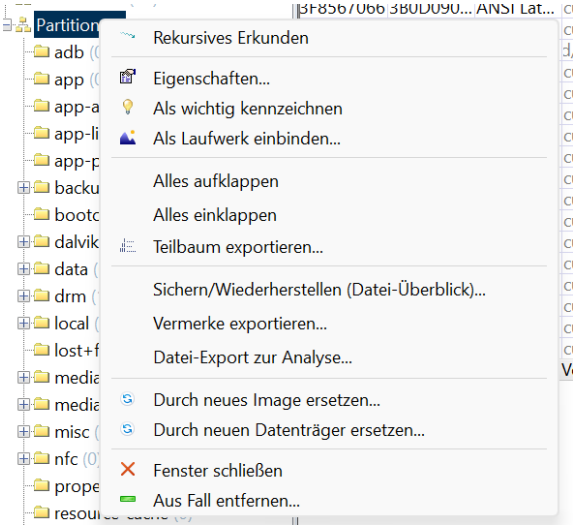


Abbildung 13 – Partition als Laufwerk einbinden

[20] (X-Ways Software Technology AG, https://www.x-ways.net/winhex/manual-d.pdf, 2023, S. 133)
[21] (X-Ways Software Technology AG, https://www.youtube.com/watch?v=Vbz9-GLiCOY&list=PLB0pU0wP67A-_DeVFfswVlZuRTH4cWswQ&index=3&t=17s, 2023)

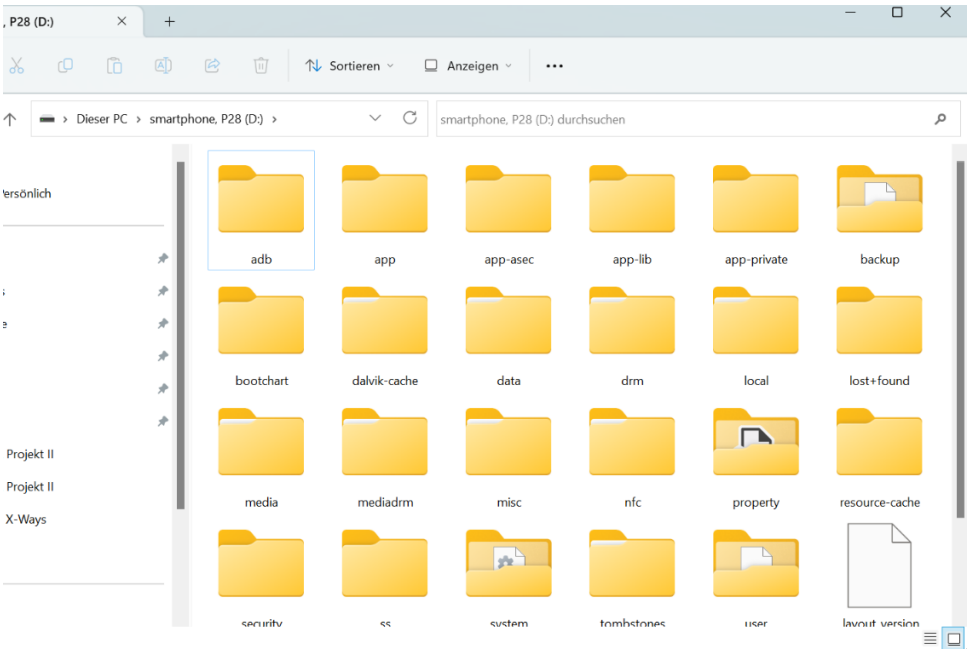


Abbildung 14 – Partition vollständig eingebunden

2.4.4 Hashwertanwendung auf Bilder/PhotoDNA-Funktion

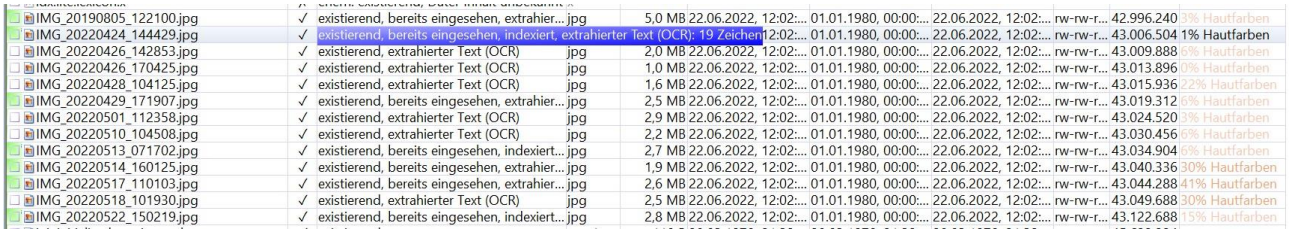
X-Ways Forensics bietet Strafverfolgungsbehörden die Möglichkeit, eine PhotoDNA-Funktionalität zu nutzen, welche das Ziel hat, die Verbreitung und den Besitz von Kindesmissbrauchsinhalten zu stoppen. X-Ways Forensics kann diesen PhotoDNA-Hash-Algorithmus auf Fotos anwenden um Fotos, welche Kindesmissbrauchsinhalte darstellen, wieder zu erkennen. Dabei wird eine Hash-Datenbank mit PhotoDNA-Hash-Werten von Fotos erzeugt, welche diese Inhalte darstellen. Somit können Bilddateien mit dieser Hash-Datenbank abgeglichen werden, um einen automatische Identifizierung dieser Inhalte zu ermöglichen.[22] Diese Funktion ist jedoch den Strafverfolgungsbehörden vorbehalten und steht somit standardmäßig nicht zur Verfügung.

2.4.5 OCR-Funktion/Tesseract-Packet

Das Tesseract-Packet beinhaltet eine OCR-Funktion (OCR = Optical Character Recognition) die als Teil der logischen Indexierung oder Suche auf geeignete Dateien angewendet werden kann (beispielsweise Dokumentenscans) um nach Begriffen zu suchen. Standardmäßig werden auch alle .jpg-Dateien berücksichtigt, was jedoch sehr viel Zeit in Anspruch nehmen kann. X-Ways Forensics bietet die Möglichkeit die Suche mit zwei Sprachen gleichzeitig durchzuführen. Einige

[22] (X-Ways Software Technology AG, https://www.x-ways.net/winhex/manual-d.pdf, 2023, S. 138, 139)

Datentypen die Tesseract unterstützt sind beispielsweise PDF, PS (PostScript) JPEG, HEIC, TIFF, PNG, BMP, GIF, nicht animierte WEBP, AutoCAD DXF, Photoshop PSP. Wurde ein OCR-Scan durchgeführt und konnte dabei ein Text extrahiert werden, so wird dies unter Beschreibung angezeigt. Jedoch erfolgte die Texterkennung bei Bildern nicht immer zuverlässig. (Abbildung 15). [23]



IMG_20190805_122100.jpg	✓	existierend, bereits eingesehen, extrahier...	jpg	5,0 MB	22.06.2022, 12:02:...	01.01.1980, 00:00:...	22.06.2022, 12:02:...	rw-rw-r...	42.996.240
IMG_20220424_144429.jpg	✓	existierend, bereits eingesehen, indexiert, extrahierter Text (OCR): 19 Zeichen	jpg	1,2 MB	22.06.2022, 12:02:...	01.01.1980, 00:00:...	22.06.2022, 12:02:...	rw-rw-r...	43.006.504
IMG_20220426_142853.jpg	✓	existierend, extrahierter Text (OCR)	jpg	2,0 MB	22.06.2022, 12:02:...	01.01.1980, 00:00:...	22.06.2022, 12:02:...	rw-rw-r...	43.009.888
IMG_20220426_170425.jpg	✓	existierend, extrahierter Text (OCR)	jpg	1,0 MB	22.06.2022, 12:02:...	01.01.1980, 00:00:...	22.06.2022, 12:02:...	rw-rw-r...	43.013.896
IMG_20220428_104125.jpg	✓	existierend, extrahierter Text (OCR)	jpg	1,6 MB	22.06.2022, 12:02:...	01.01.1980, 00:00:...	22.06.2022, 12:02:...	rw-rw-r...	43.015.936
IMG_20220429_171907.jpg	✓	existierend, bereits eingesehen, extrahier...	jpg	2,5 MB	22.06.2022, 12:02:...	01.01.1980, 00:00:...	22.06.2022, 12:02:...	rw-rw-r...	43.019.312
IMG_20220501_112358.jpg	✓	existierend, extrahierter Text (OCR)	jpg	2,9 MB	22.06.2022, 12:02:...	01.01.1980, 00:00:...	22.06.2022, 12:02:...	rw-rw-r...	43.024.520
IMG_20220510_104508.jpg	✓	existierend, extrahierter Text (OCR)	jpg	2,2 MB	22.06.2022, 12:02:...	01.01.1980, 00:00:...	22.06.2022, 12:02:...	rw-rw-r...	43.030.456
IMG_20220513_071702.jpg	✓	existierend, bereits eingesehen, indexiert...	jpg	2,7 MB	22.06.2022, 12:02:...	01.01.1980, 00:00:...	22.06.2022, 12:02:...	rw-rw-r...	43.034.904
IMG_20220514_160125.jpg	✓	existierend, bereits eingesehen, extrahier...	jpg	1,9 MB	22.06.2022, 12:02:...	01.01.1980, 00:00:...	22.06.2022, 12:02:...	rw-rw-r...	43.040.336
IMG_20220517_110103.jpg	✓	existierend, bereits eingesehen, extrahier...	jpg	2,6 MB	22.06.2022, 12:02:...	01.01.1980, 00:00:...	22.06.2022, 12:02:...	rw-rw-r...	43.044.288
IMG_20220518_101930.jpg	✓	existierend, extrahierter Text (OCR)	jpg	2,5 MB	22.06.2022, 12:02:...	01.01.1980, 00:00:...	22.06.2022, 12:02:...	rw-rw-r...	43.049.688
IMG_20220522_150219.jpg	✓	existierend, bereits eingesehen, indexiert...	jpg	2,8 MB	22.06.2022, 12:02:...	01.01.1980, 00:00:...	22.06.2022, 12:02:...	rw-rw-r...	43.122.688

Abbildung 15 - Anzeige unter der Tabelle Beschreibung ob ein Text mit der OCR-Funktion extrahiert wurde

2.4.6 Objekterkennung/Excire Forensics

Excire Forensics ist eine Erweiterung für X-Ways Forensics die sich der Bildanalyse mittels KI (KI = Künstliche Intelligenz) bedient. Dabei weist Excire Forensics folgende drei Fähigkeiten auf:

1. Automatische Analyse von Fotos auf Ihren Inhalt wie zum Beispiel Objekte (Gebäude, Fahrzeuge, Menschen usw.), Nacktheit und Pornographie, Drogen, Waffen und noch vieles mehr (Abbildung 16). Eine vollständige Liste findet sich unter https://www.x-ways.net/Excire_Erkannte_Objekte.txt[24]. Mögliche Ergebnisse werden in Form von Kommentaren oder Vermerken ausgegeben, sodass sich auf die Fotos mit relevanten Inhalten konzentriert werden kann. Erfolgt die Ausgabeform anhand von Vermerken, erhalten auch Videos ein Label, wenn aus ihnen die extrahierten Einzelbilder verarbeitet werden.
2. Eine weitere Fähigkeit von Excire Forensics ist das Auffinden von ähnlichen Bildern aus Sicht der künstlichen Intelligenz, mit der vom Benutzer zur Verfügung gestellten Auswahl an relevanten Bildern.
3. Des Weiteren können durch Excire Forensics Gesichter bestimmter Personen erkannt werden. Dabei werden vom Benutzer bestimmte Gesichter beispielsweise in JPEG Dateien gespeichert, die dann mit neuen Bildern abgeglichen werden. Ebenfalls ist eine Kategorisierung von Objekten möglich bzw. werden auch logische UND-Kombinationen (Abbildung 17) unterstützt. Einige UND-

[23] (X-Ways Software Technology AG, https://www.x-ways.net/winhex/manual-d.pdf, 2023, S. 142, 143)
[24] (X-Ways Software Technology AG, https://www.x-ways.net/Excire_Erkannte_Objekte.txt, 2023)

Kombinationen sind bereits vordefiniert um bei der Ermittlung von Kinderpornographie zu unterstützen.[25]

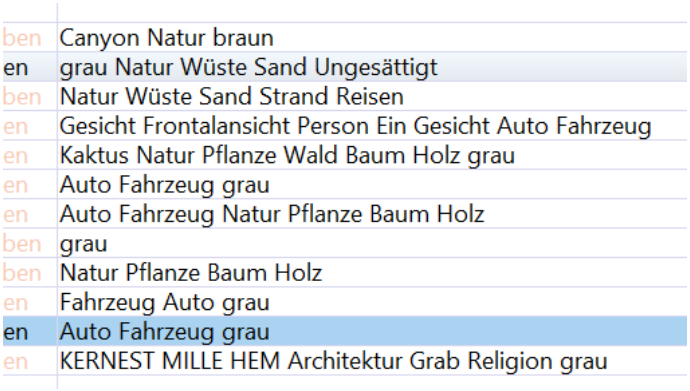


Abbildung 16 - Automatische Kategorisierung von Bildern durch X-Ways Forensics

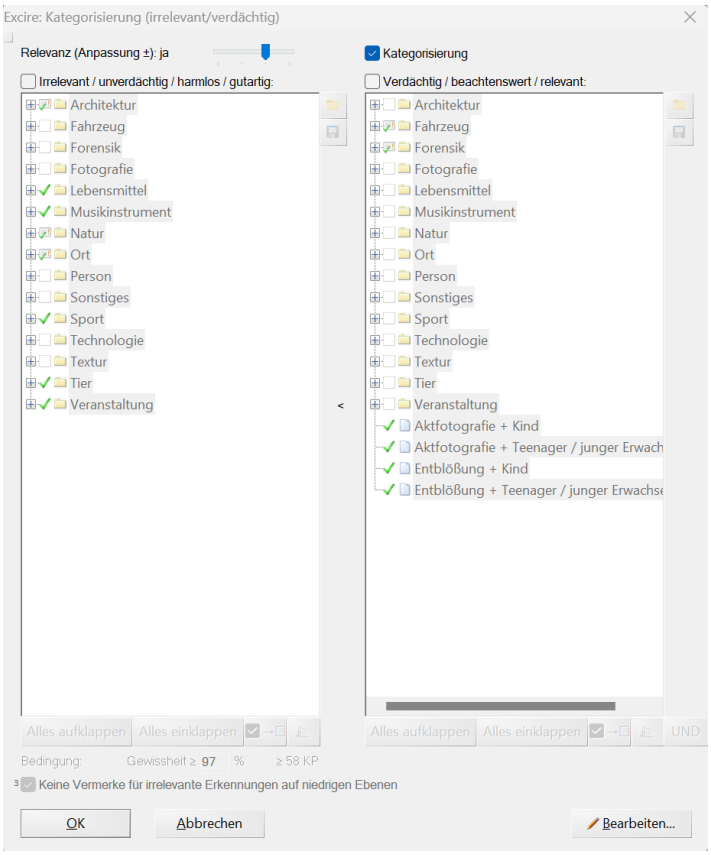


Abbildung 17 - Kategorisierungsmöglichkeiten und logische UND-Kombinationsmöglichkeiten

2.4.7 Bildanalyse Hautfarbenanteil

X-Ways Forensik ermöglicht bei der Analyse von Bildern den Hautfarbenanteil (Abbildung 18) des einzelnen Fotos in Prozent zu bestimmen sowie Schwarz-Weiß Fotos zu erkennen. Dies kann die Arbeit vor allem für Ermittler, die nach Spuren von Kinderpornographie auf Smartphones suchen, wesentlich beschleunigen. Jedoch

[25] (X-Ways Software Technology AG, https://www.x-ways.net/winhex/manual-d.pdf, 2023, S. 144, 145)

kann es hierzu auch zu falschen Treffern kommen, wenn beispielsweise Bilder hautähnliche Farben besitzen, jedoch keine Haut darstellen. In Kombination mit der Objekterkennung lassen sich jedoch falsche Treffer schnell erkennen.

Die Schwarz-Weiß- und Graustufenerkennung ist für Forensiker vor allem nützlich, wenn diese nach eingescannten Dokumenten suchen oder nach Faxen. Bilder deren Höhe und Breite nicht größer als 8 Pixel sind werden als unwichtig klassifiziert, da hier davon ausgegangen wird, dass diese weder ein Dokument sein können noch pornographischen Inhalt besitzen.[26]

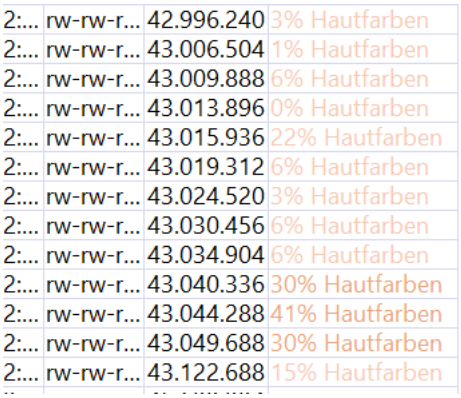


Abbildung 18 - Bildanalyse Hautfarbenanteil

2.5 Datenextraktion

Im Folgenden werden einige Datenextraktionsmöglichkeiten, welche X-Ways Forensik bietet, vorgestellt.

2.5.1 Rekonstruktion gelöschter Daten

Gelöschte Dateien werden automatisch in der Übersicht mit angezeigt. Gelöschte Dateien und Verzeichnisse werden mit einem farblich schwächeren Icon dargestellt als noch verfügbare Dateien und Verzeichnisse. Gelöschte Dateien und Verzeichnisse auf die nicht mehr zugreifbar ist, weil deren Cluster unbekannt bzw. anderweitig verwendet wurde oder sie eine Größe von 0 Bytes besitzen, enthalten im Icon ein rotes X. Von Icons, welche ein blaues Fragezeichen besitzen, kann davon ausgegangen werden, dass diese noch immer verfügbar sind. Es gibt noch einige weitere Icons, welche noch andere Zustände von gelöschten Dateien oder Verzeichnissen abbilden (Abbildung 19). Dadurch ist für den Benutzer schnell

[26] (X-Ways Software Technology AG, https://www.x-ways.net/winhex/manual-d.pdf, 2023, S. 171)

erkennbar, ob gelöschte Daten wiederhergestellt werden können oder für die weitere Bearbeitung nicht mehr relevant sind.[27]

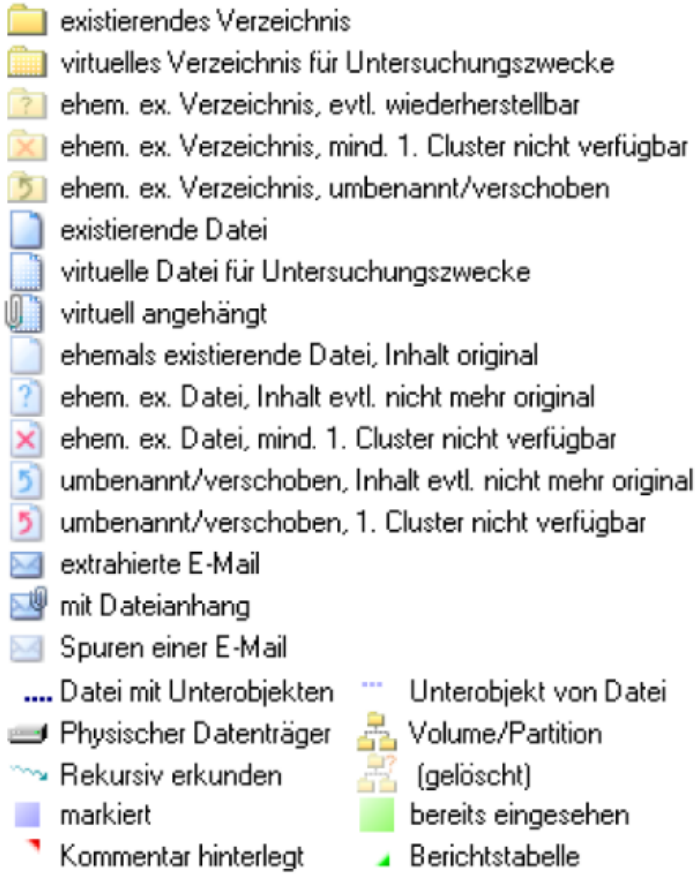


Abbildung 19 - Legende Löschzustände – Quelle Bild: (X-Ways Software Technology AG, https://www.x-ways.net/winhex/manual-d.pdf, 2023)

2.5.2 Extraktion von Metadaten

Die Extraktion von Metadaten ist für Benutzer ein wichtige Methode um essentielle Informationen beispielsweise über GPS-Daten von auf dem Smartphone gefundenen Bildern zu erhalten, um die Bewegungsabläufe von Verdächtigen nachvollziehen zu können (Abbildung 20). X-Ways Forensics ermöglicht daher auch das Extrahieren von Metadaten wie beispielsweise Zeitstempel und GPS-Daten aus Dateien wie PDF, MOV, JPEG und noch einige mehr. Ebenfalls kann auch wenn gewünscht, eine Einschätzung einer generischen Relevanz von Dateien durch X-Ways Forensics vorgenommen werden (Abbildung 21). Beispielsweise ist der Wert 3.9 = Soziale Medien oder der Wert 4.1 = Webcam. Hiermit ist es möglich, für den Benutzer eine für ihn relevante Sortierung vornehmen zu können.[28]

[27] (X-Ways Software Technology AG, https://www.x-ways.net/winhex/manual-d.pdf, 2023, S. 18, 19)
[28] (X-Ways Software Technology AG, https://www.x-ways.net/winhex/manual-d.pdf, 2023, S. 160, 163)

Date original	2022:05:22 15:02:20.151805 (OZ)
Date digitized	2022:05:22 15:02:20.151805 (OZ)
Content modified	2022:05:22 15:02:20.151805 (OZ)
GPS version	*
GPS timestamp	22.05.2022, 23:02:15 +2
Altitude	1733,00 m
Latitude	43° 41' 13,44" N
Longitude	114° 21' 58,59" W

Abbildung 20 - Metadaten aus einem Bild mit Latitude und Longitude Informationen

Kommentare	Metadaten	Relevanz
Auto Fahrzeug Natur Pflanze Baum Holz	Condition: Embedded Bearbeitungszustand: Scaled	3,90
Auto Fahrzeug grau		
Auto Fahrzeug grau	Condition: Embedded Bearbeitungszustand: Scaled	3,90
Canyon Natur braun		
Fahrzeug Auto grau	Condition: Embedded Bearbeitungszustand: Scaled	3,89
Gesicht Frontalansicht Person Ein Gesicht Auto Fahrzeug	Condition: Embedded Bearbeitungszustand: Scaled	3,39
KERNEST MILLE HEM Architektur Grab Religion grau		
Kaktus Natur Pflanze Wald Baum Holz grau		
Natur Pflanze Baum Holz		
Natur Wüste Sand Strand Reisen		
grau		
grau Natur Wüste Sand Ungesättigt		3,84

Abbildung 21 - Bildung einer generische Relevanz in der Spalte „Relevanz“

2.5.3 Extraktion von Standbildern aus Videos

Eine weitere Funktion zur Datenextraktion in X-Ways Forensics ermöglicht es, Standbilder aus einer Video-Datei zu erzeugen und zu extrahieren. Dies kann in einem vorher festgelegten Zeitabstand erfolgen oder durch Angabe einer festen Anzahl von Standbildern (Abbildung 22, Abbildung 23) in einem Video. Während Intervalle mit fester Länge zu einer Anzahl von Standbildern führen, die proportional mit der Videodauer wächst, begrenzt die feste Angabe von Standbildern den Arbeitsaufwand. Letzteres führt jedoch dazu, wichtige Inhalte in einem Video zu übersehen. Für diese Funktion wird die Erweiterung „MPlayer“ benötigt. Bilder können aus allen Video-Formaten und Codecs extrahiert werden, die von MPlayer unterstützt werden. Die Extraktion von Standbildern ist vor allem bei Videos hilfreich, die illegale Inhalte wie beispielsweise Kinderpornographie, terroristische Inhalte oder ideologische Hetze beinhalten.[29]

[29] (X-Ways Software Technology AG, https://www.x-ways.net/winhex/manual-d.pdf, 2023, S. 170)

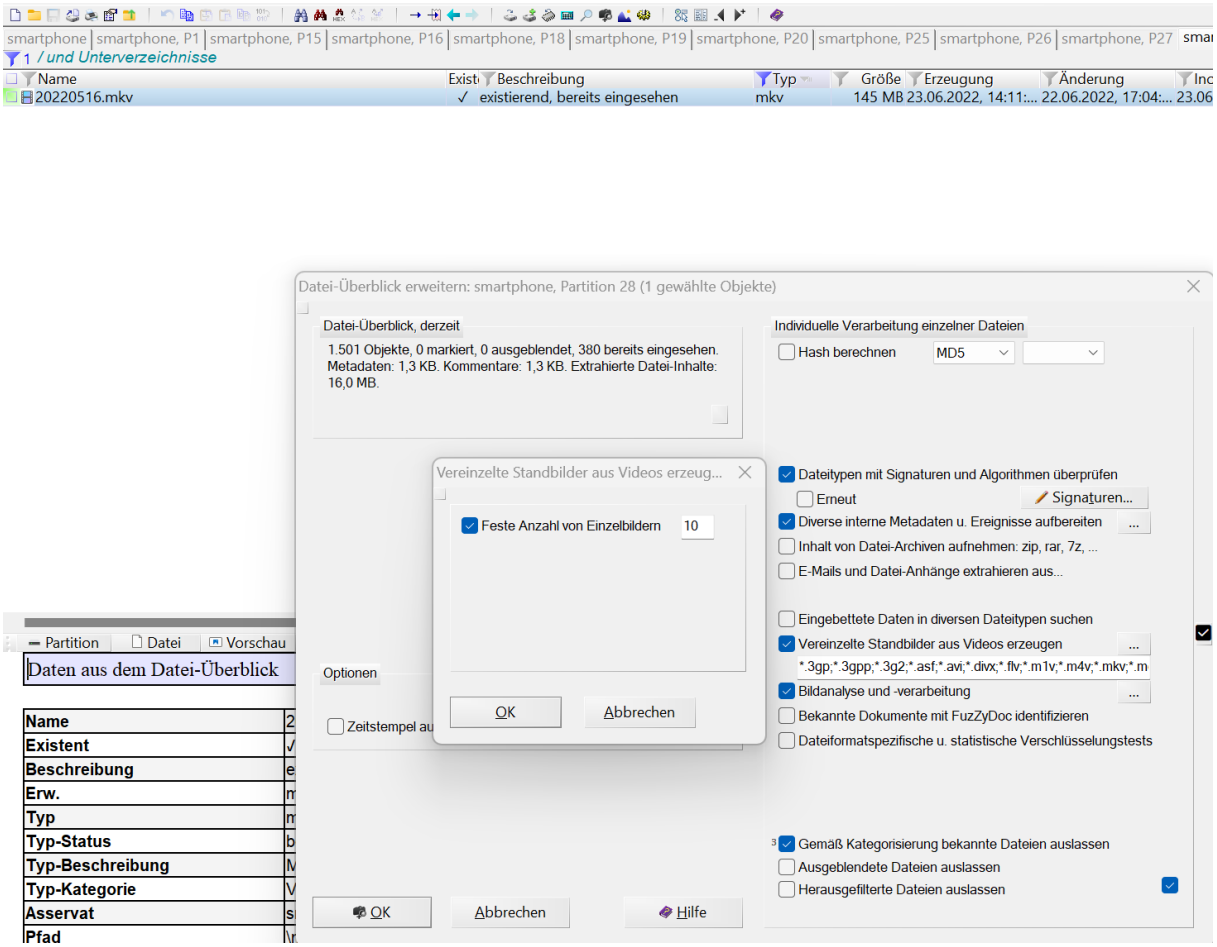


Abbildung 22 - Erstellung von Einzelbildern aus einem Video

Abbildung 23 - Erzeugte Standbilder aus einem Video

2.6 Berichterstellung

X-Ways Forensics bietet auch die Möglichkeit einen Fallbericht zu erzeugen, um später eine Überprüfung der Ergebnisse durch Staatsanwälte, Richter, Kunden usw. zu ermöglichen. X-Ways Forensics verwendet für die Berichtsfunktion sogenannte Berichtstabellen (Abbildung 24), denen verschiedene Elemente, wie beispielsweise Fotos oder Dokumente, zugewiesen werden können (Abbildung 25). In X-Ways-Forensics werden die Berichte in einer HTML-Datei erzeugt, sodass diese sich auf den meisten Geräten mit einem Webbrowser öffnen lassen und bearbeitet werden

können. Auch das Layouts sowie der Inhalt der Berichte können je nach Wunsch angepasst werden.[30]

Smartphone-Forensik

Dieser Bericht wird für die Projektarbeit erstellt

Android_Smartphone_Xways

Bez./Nr. des Falls: Android_Smartphone_Xways
Erzeugung: 19.07.2023, 20:03:43
Falldatei: C:\Users\micha\Android_Smartphone_Xways.xfc
Bericht erzeugt mit X-Ways Forensics BYOD 20.9 Beta 6, 08.08.2023, 19:52:49
Protokollzeitzone: +02:00 Mitteleuropäische Sommerzeit
Anzeige-Zeitzone für Zeitstempel mit definiertem Zeitzonenbezug, für Berichtstabellen: UTC +01:00 Berlin, Vienna, Rome

Asservate:
smartphone
Partition 1
Partition 15
Partition 16
Partition 18
Partition 19
Partition 20
Partition 25
Partition 26
Partition 27
Partition 28

Berichtstabellen:
Wichtige Fotos (2 Einträge)

Abbildung 24 - Bericht mit einer Berichtstabelle

Last write time: 28.03.1970, 22:12:39 +1

Partition 28

Interne Bezeichnung: [C:\Users\micha\Desktop\Studium\6. Semester\IT-Forensik Projekt II\Image\smartphone.E01], Partition 28
Hinzugefügt am: 19.07.2023, 20:05:34
Zeitzonenbezug von Zeitstempeln in diesem Dateisystem: UTC
Anzeige-Zeitzone für Zeitstempel mit definiertem Zeitzonenbezug, für Berichtstabellen: UTC +01:00 Berlin, Vienna, Rome
Hash: n. vfgb.

Beschreibung: Dateisystem: Ext4
Gesamtkapazität: 29.236.373.504 Bytes = 27,2 GB
Sektoren insges.: 57.102.292
Bytes pro Sektor: 512
Bytes pro Cluster: 4.096
Freie Cluster: 6.788.291 = 95% frei
Cluster insgesamt: 7.137.786
Number of Inodes: 1.785.856
Number of free Inodes: 1.784.662
Number of block groups: 218
Blocks per group: 32.768
Inodes per group: 8.192
Inode size: 256
Uses sparse superblocks: Ja
Uses Flexible Block Groups: Nein
Uses Meta Block Groups: Nein
Last mount time: 23.06.2022, 14:14:10 +2
Last write time: 23.06.2022, 14:15:44 +2

Wichtige Fotos (2 Einträge)

Dateien asservatweise nach int. ID sortiert

1

Name: **20220516.mkv 0m 06s.jpg**
Existent: Ja
Typ: jpg
Asservat: smartphone, P28
Pfad: \media\0\Movies\20220516.mkv
Größe: 1,1 MB
Generator-Signatur: 60D7DE6D (U:Standard 76 Minimized, up)
Gerätetyp: unbekannt

2

Name: **20220516.mkv 0m 12s.jpg**
Existent: Ja
Typ: jpg
Asservat: smartphone, P28
Pfad: \media\0\Movies\20220516.mkv
Größe: 1,0 MB
Generator-Signatur: 60D7DE6D (U:Standard 76 Minimized, up)
Gerätetyp: unbekannt

Abbildung 25 - Zugewiesene Fotos zur Berichtstabelle "Wichtige Fotos"

[30] (Shavers & Zimmerman, 2014, S. 180)

3. Forensik-Programm Autopsy/Sleuthkit

Im Folgenden wird das Forensik-Tool Autopsy mit seinen beworbenen Eigenschaften vorgestellt. Hierbei wurde die Autopsy-Version 4.20 verwendet.

3.1 Einführung in Autopsy

Sleuthkit ist eine Sammlung von Kommandozeilen-Tools, welches zur Analyse von Festplattenimages von Brian Carrier entwickelt wurde. Autopsy verwendet zum großen Teil die Tools von Sleuthkit, jedoch enthält Autopsy auch eine große Anzahl von zusätzlichen Programmen und bietet den Vorteil für Benutzer, die wenig oder keine Kommandozeilenerfahrung besitzen, sich aufgrund der GUI (Graphical User Interface) leichter zurecht zu finden. Des Weiteren handelt es sich bei Autopsy um eine Open-Source-Forensikplattform, welche alle Arten von digitalen Medien und Mobilgeräten analysieren kann. Aufgrund der Plug-in-Architektur kann Autopsy jederzeit durch individuell erstelle Module oder Entwicklungen der Community erweitert werden. Ein Support erfolgt durch die Firma Basis Technology.[31]

3.2 Funktionen und Tools

Wie bereits erwähnt, bietet Autopsy aufgrund seiner Open-Source-Plattform eine Vielzahl von Funktionen, welche beispielsweise bei der Anlage eines Falls ausgewählt werden können. Des Weiteren können Erweiterungen und Plugins, welche es dem Benutzer ermöglicht, seine Anforderungen in Autopsy anzupassen, hinzugefügt werden. Zusatzmodule werden auf der Seite von Github[32] angeboten.

Im Rahmen der Projektarbeit soll sich jedoch, wie bereits bei der Software X-Ways Forensics, auf die Funktionen Datenextraktion, Analysemöglichkeiten, Benutzerfreundlichkeit und Berichterstellung beschränkt werden, da nicht alle Funktionen von Autopsy in der Projektarbeit berücksichtigt werden.

Autopsy unterstütz für die Datenextraktion ebenfalls Dateiformate wie Ext2, Ext3 oder Ext4. Letzteres wird, wie bereits unter X-Ways Forensic erwähnt bei vielen Android-Smartphones verwendet. Ebenfalls unterstützt Autopsy das Erstellen von Bildern aus Video-Dateien mittels der Software Video-Triage, was die Durchsuchung von Filmen auf illegale oder unangemessene Inhalte unterstützen und beschleunigen soll. Des Weiteren bietet Autopsy Module für die Dateiextraktion für Archive (ZIP, RAR usw.), ein Bildanalysemodul für die Extraktion von Bildmetadaten, ein spezielles Android-

[31] (Basis Technology, www.autopsy.com, 2023)
[32] (Github, 2023)

und iOS-Analysemodul für Smartphones und noch viele andere Module für die IT-Forensik. Alle diese Module bieten die Möglichkeit, mit Autopsy Smartphones ausführlich und umfassend zu untersuchen, damit Experten so viele Informationen wie möglich erhalten.[33]

Autopsy bietet Möglichkeiten um verschiedene Artefakte auf Smartphones zu analysieren. Dazu gehören beispielsweise ein E-Mail-Parser-Modul um die E-Mail-basierte Kommunikation in dem zu untersuchenden System zu identifizieren, ein Datenquellenintegritätsmodul um Hash-Werte zu überprüfen oder zu berechnen, einen GPX-Analysator-Modul um GPS-Daten in einer GPX-Datei zu finden und noch einige Module mehr. Auch die Erkennung verschlüsselter Dateien sowie die Untersuchung von bestimmten DJI-Drohnen kann mit Autopsy durchgeführt werden.[34]

Bezüglich der Benutzerfreundlichkeit bietet Autopsy ebenfalls verschiedene Einstellungsmöglichkeiten um den Anwender die Benutzung zu erleichtern. Ein Benutzerhandbuch wird auf der Webseite von Sleuthkit zur Verfügung gestellt. Des Weiteren bietet Basis Technology auch eine Grundlagenschulung[35] gegen Gebühr an. Kostenlose Anleitungsvideos werden von Basis Technology jedoch nicht zur Verfügung gestellt.

Autopsy stellt ebenfalls eine Berichtsfunktion für den Benutzer bereit. Somit können auch in Autopsy wichtige Informationen durch den Benutzer gesammelt und extrahiert werden. Autopsy bietet eine Auswahl aus verschiedenen Dateiformaten an in welchem der Bericht erstellt und ausgegeben werden kann wie beispielsweise HTML, Excel, CSV oder KML um gefundene Koordinaten in Google-Earth laden und darstellen zu können.[36]

3.3 Benutzerfreundlichkeit

Im Folgenden wurde die Benutzerfreundlichkeit in den Bereichen Installationsaufwand/Systemvoraussetzungen, Anwendersupport und Benutzeroberfläche, welche Autopsy bietet, untersucht.

[33] (Basis Technology, http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/, 2023)
[34] (Basis Technology, http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/, 2023)
[35] (Basis Technology, https://www.autopsy.com/support/training/, 2023)
[36] (Basis Technology, http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/reporting_page.html, 2023)

3.3.1 Installationsaufwand / Systemvoraussetzungen

Der Installationsaufwand bei Autopsy ist ebenfalls gering. Jedoch ist die Installationsdatei wesentlich größer (benötigter Speicherplatz ca. 1,58 GB) und die Anforderungen an das Betriebssystem sind ebenfalls höher. Der „Installer“ führt den Benutzer durch die Installation, sodass diese auch für unerfahrene Benutzer kein Problem darstellt. Auch im Benutzerhandbuch kann sich der Benutzer informieren, falls Unsicherheiten bei der Installation auftreten.

Eine Lizenz wie bei X-Ways Forensic ist nicht notwendig um die Software nutzen zu können. Es handelt sich hier um eine kostenlose Software. Somit entfällt dieser Schritt bei der Installation von Autopsy. Während der Installation kann der Benutzer bereits auswählen, welche Module dieser benötigt (Abbildung 26). Weitere Module können über Github noch ergänzt werden.[37]

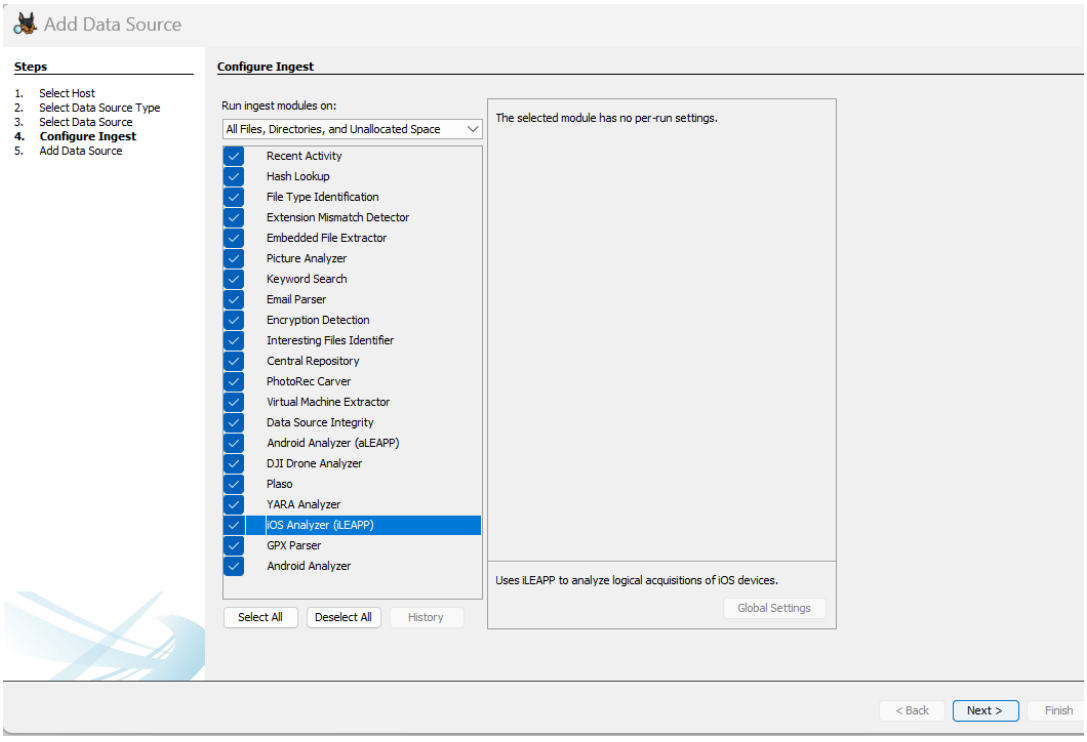


Abbildung 26 - Modulauswahl bei der Installation von Autopsy

3.3.2 Anwendersupport

Eine Kontaktaufnahme bei Autopsy zum Anwendersupport war nicht notwendig, da es sich um eine kostenlose Software handelt und keine Lizenz für die Nutzung notwendig war. Sollten Benutzer Fehler bemerken, so kann die Meldung auf der

[37] (Github, 2023)

Support-Seite erfolgen. Einen kommerziellen Support- und ein Wartungsabonnement bietet Basis Technologie jedoch nur auf Unternehmensebene sowie für Organisationen an. Private Nutzer müssen sich in solchen Fällen mit anderen Benutzern in Verbindung setzen, beispielsweise über das Sleuthkit-Forum[38].[39]

Des Weiteren wird auf der Internetseite von Basis Technology ein Benutzerhandbuch zur Verfügung gestellt, was Benutzern bei Fragen ebenfalls Hilfe bieten sollte. Auch in Autopsy selbst findet sich unter dem Reiter „Hilfe“ das Benutzerhandbuch in Offline-Form, falls kein Internetzugang zur Verfügung stehen würde (Abbildung 27). Wie bereits erwähnt, gibt es eine Grundlagenschulung welche jedoch nur gegen eine Gebühr durchgeführt werden kann. Kostenlose Anleitungsvideos werden leider nicht zur Verfügung gestellt.

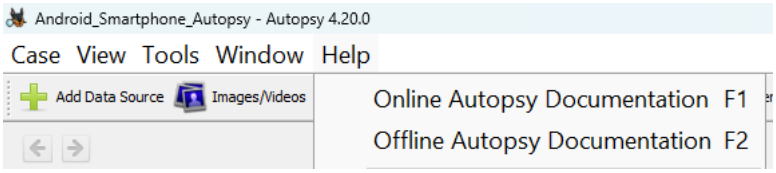


Abbildung 27 - Auswahl Offline-Benutzerhandbuch in Autopsy

3.3.3 Benutzeroberfläche

Die Benutzeroberfläche in Autopsy selbst bietet ebenfalls eine große Möglichkeit von Einstellungsmöglichkeiten für den Anwender. Auf alle Einstellungsmöglichkeiten kann jedoch im Rahmen der Projektarbeit nicht eingegangen werden. Deshalb sollen ein paar Einstellungsmöglichkeiten innerhalb von Autopsy nur kurz angeschnitten werden. Der Benutzer kann beispielsweise unter dem Reiter „Application“ die Anpassung vornehmen, wieviel Speicher von Autopsy verwendet werden darf, sowie die Anzahl der Protokolldateien, die Autopsy aufbewahren darf. Auch die Angabe, wo Autopsy temporäre Dateien speichern darf, kann hier eingestellt werden (Abbildung 28). Im Reiter „External Viewer“ kann eingestellt werden, welche Arten von Dateien mit welchem Editor geöffnet werden sollen (Abbildung 29). Im Reiter „General“ können Proxy-Einstellungen durch den Anwender vorgenommen werden (Abbildung 30). Eine Änderung der Menüsprache auf Deutsch ist in Autopsy leider nicht möglich.

[38] (Sleuthkit, 2023)
[39] (Basis Technology, https://sleuthkit.org/support.php, 2023)

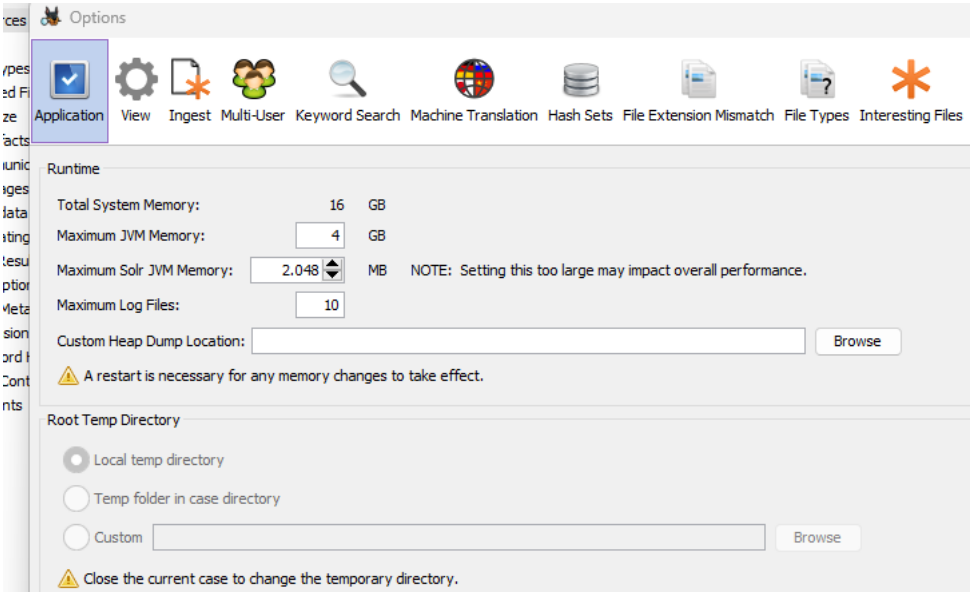


Abbildung 28 - Einstellungsmöglichkeiten im Reiter "Application"

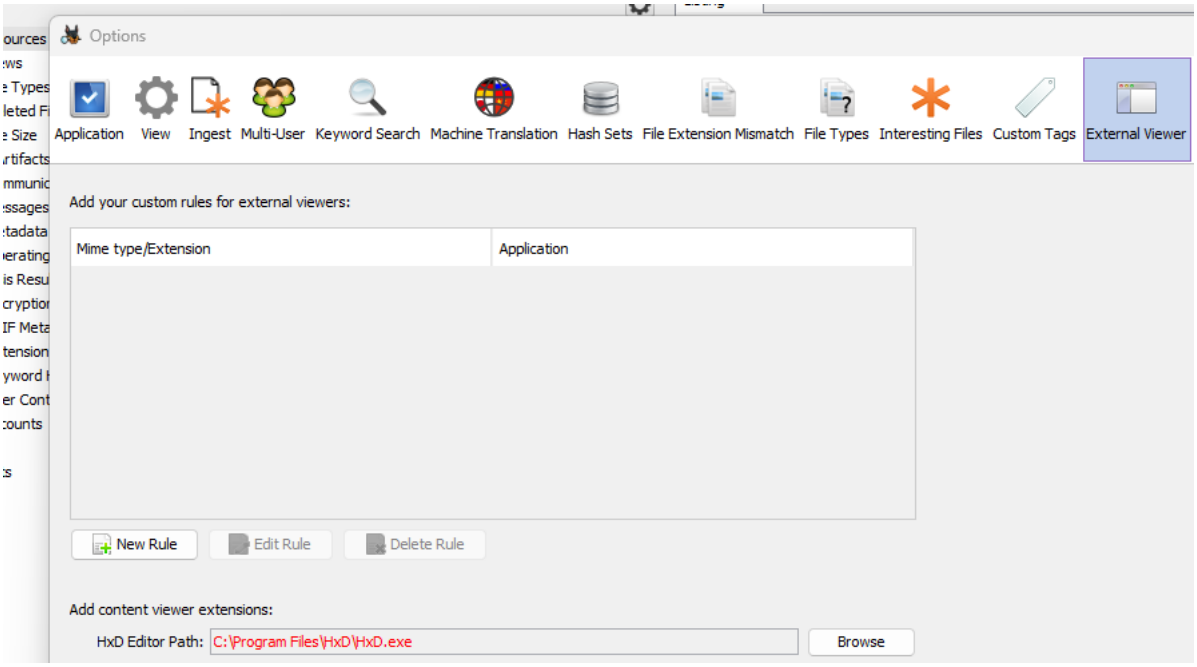


Abbildung 29 - Einstellungsmöglichkeiten im Reiter "External Viewer"

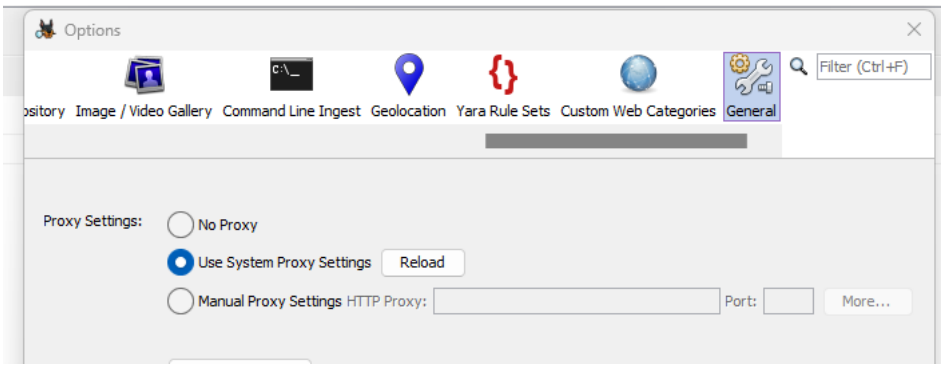


Abbildung 30 - Einstellungsmöglichkeiten im Reiter "General"

3.4 Analysemöglichkeiten

Im Folgenden werden einige Analysemöglichkeiten, welche Autopsy bietet, vorgestellt. Eine vollständige Aufzählung aller Analysemöglichkeiten von Autopsy ist jedoch aufgrund des Umfangs nicht möglich, da dies den Umfang der Projektarbeit übersteigen würde.

3.4.1 Unterstützung von Dateisystemen

Autopsy unterstützt ebenfalls für die Smartphone-Forensik sowohl das Dateisystem Ext4 welches vor allem bei aktuellen Android-Smartphones vorliegt, als auch Ext2 und Ext3 welches vor allem bei älteren Smartphones eingesetzt wurde. Des Weiteren wird auch das Dateisystem FAT unterstützt, welches von SD-Karten verwendet wird. Auch das APFS-Dateisystem, welches von Apple bei Smartphones seit dem iOS-Betriebssystemversion 10.3 eingesetzt wird, wird unterstützt. Ältere Datei-Formate von Apple wie HFS+ oder HFSJ/HFSX werden ebenfalls unterstützt. Bei Fallanlagen kann durch den Benutzer ausgewählt werden, ob er die Module „iOS-Analysator“ oder „Android Analyzer Module“ benötigt, die speziell für die Smartphone-Forensik Unterstützung bieten (Abbildung 31). Das verwendete Smartphone-Image verwendet das Dateisystem Ext4 welches ohne Probleme auch in Autopsy verwendet werden konnte.[40] [41] [42]

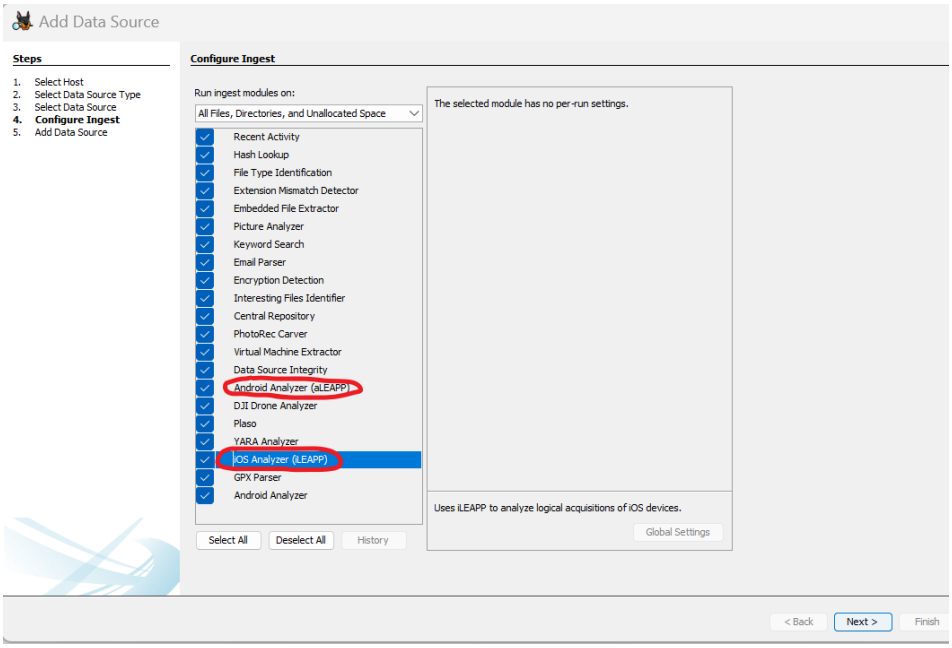


Abbildung 31 - Auswahlmöglichkeit "Android Analyzer Modul sowie "iOS Analyzer"

[40] (wikipedia.org, 2023)
[41] (Basis Technology, http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/android_analyzer_page.html, 2023)
[42] (Basis Technology, http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/ileapp_page.html, 2023)

3.4.2 Unterstützung von Image-Dateien

Das Erstellen von Smartphones-Images lässt sich mit Autopsy ebenfalls durchführen. Es werden unter anderem die Formate wie Raw Single (*.dd), virtuelle Maschinen (*.vmdk), virtuelle Festplatten (*.vhd) oder das Format EnCase (*.e01) unterstützt um dann anschließend die forensischen Untersuchungen durchzuführen. Das verwendete Smartphone-Image wurde auch hier im EWF-Format (Expert Witness Compression Format) genutzt und konnte ohne Problem untersucht werden (Abbildung 32).[43]

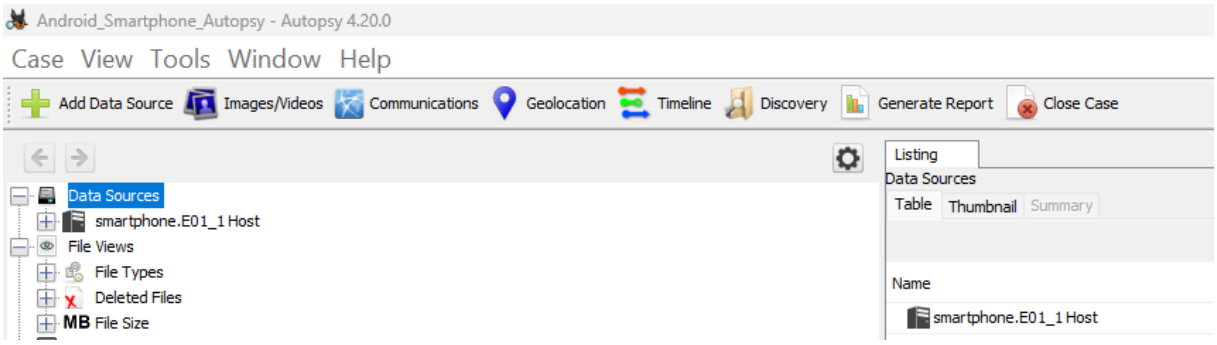


Abbildung 32 - EnCase-Format des Images

3.4.3 Einbinden von Partitionen/Ordnern

Für das Einbinden einer Partition in das eigene Windows-System bietet Autopsy die Möglichkeit, die jeweilige Partition/Ordner zu extrahieren (Abbildung 33), zu speichern und um anschließend eine Untersuchung vorzunehmen (Abbildung 34). Somit kann die jeweilige Partition mit externen Programmen ebenfalls schnell und einfach durchsucht sowie auf alle relevanten Dateien zugegriffen werden. Dieses ist bei allen unterstützten Image-Typen und Dateisystemen möglich.

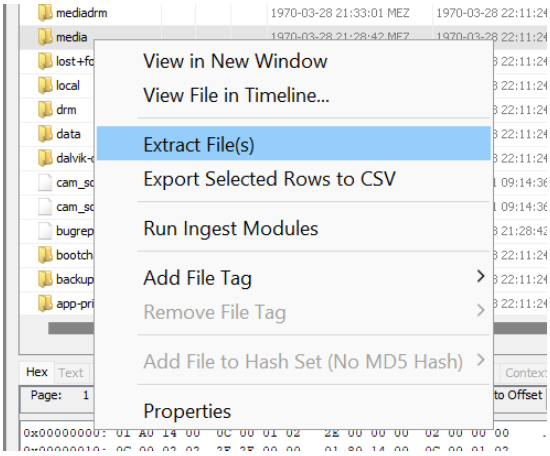


Abbildung 33 - Extrahieren des Ordners „media“ in Autopsy

[43] (Basis Technology, http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/ds_page.html, 2023)

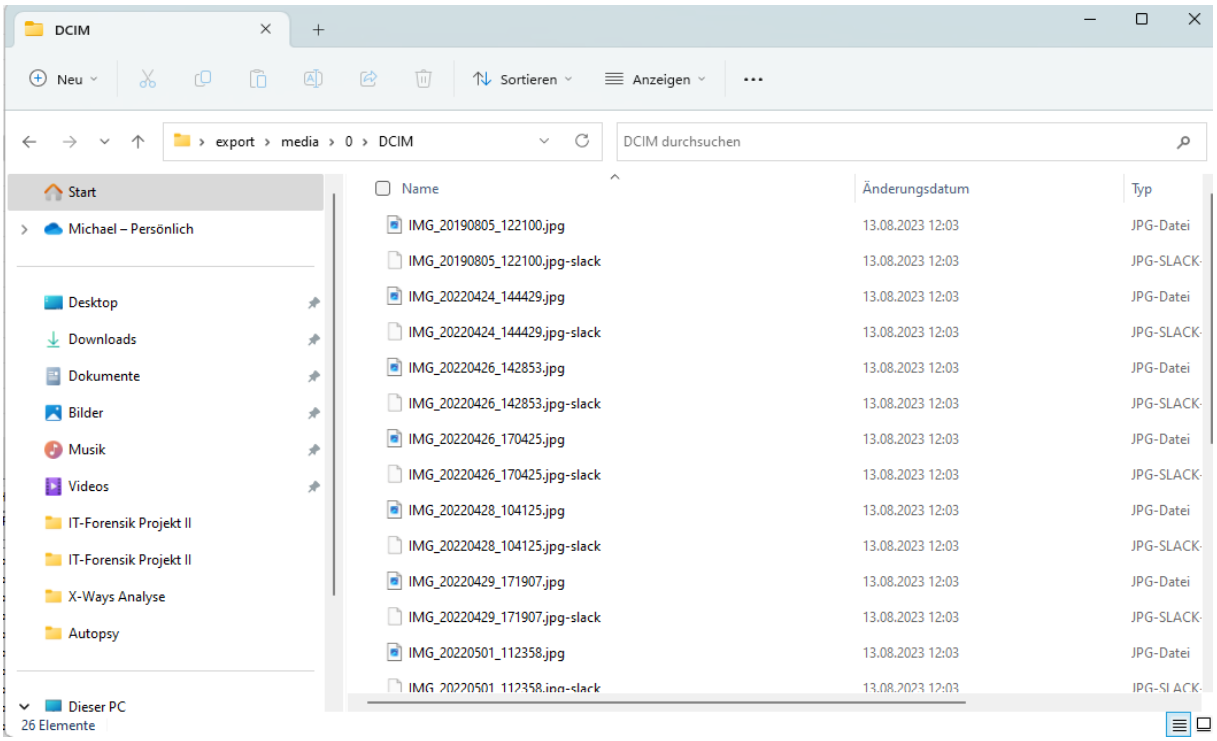


Abbildung 34 – Zugriff auf den extrahierten Ordners "media"

3.4.4 Hashwertanwendung auf Bilder/C4P-Funktion/Projekt VIC

Autopsy bietet ebenfalls mit dem Modul C4P/All eine Möglichkeit, Filme und Bilder von bereits bearbeiteten Fällen im Bereich Kindesmissbrauch, durch eine zentralisierte Hash-Datenbank verwalten zu können. Anhand der Hashwerte und der Kategorisierung der Bilder kann bei neu gefundenen Video- und Bildmaterial nach passenden Hashes in der Datenbank gesucht werden. Des Weiteren wird mit dem Projekt VIC (hierzu gehören Technologien wie VICS Data Model, PhotoDNA, VIC Safer, VIC Point, Katalys, Logo Matcher) eine Funktion angewendet, welches die Datensilos nationaler und internationaler Strafverfolgungsbehörden aufbricht. Dabei werden die Bilddaten in Form robuster Bild-Hash-Werte aggregiert. Dadurch soll ein System entstehen, welches den Daten- und Informationsaustausch beschleunigt und Täter und Opfer schneller und effektiver identifiziert. Diese Funktionen stehen jedoch nur Strafverfolgungsbehörden zur Verfügung.[44] [45]

3.4.5 OCR-Funktion/Tesseract-Packet

Autopsy kann zudem die Funktion der optischen Zeichenerkennung (OCR-Funktion (OCR = Optical Character Recognition)) nutzen, um Text aus unterstützten Bildtypen zu extrahieren. Hierzu greift Autopsy ebenfalls auf das Tesseract-Modul zurück wie

[44] (Basis Technology, https://www.autopsy.com/add-on-modules/law-enforcement-bundle/, 2023)
[45] (Project VIC International, 2023)

X-Ways Forensics. Die OCR-Funktion ist standardmäßig deaktiviert (Abbildung 35). Jedoch kann diese einfach über die Schlüsselwortsuche aktiviert werden. Autopsy ist werkseitig nur für englischen Text konfiguriert. Weitere Sprachen können jedoch jederzeit über Sprachdateien bei Github heruntergeladen und hinzugefügt werden. Jedoch erfolgte auch bei Autopsy die Texterkennung in Bildern nicht immer zuverlässig (Abbildung 36, Abbildung 37)

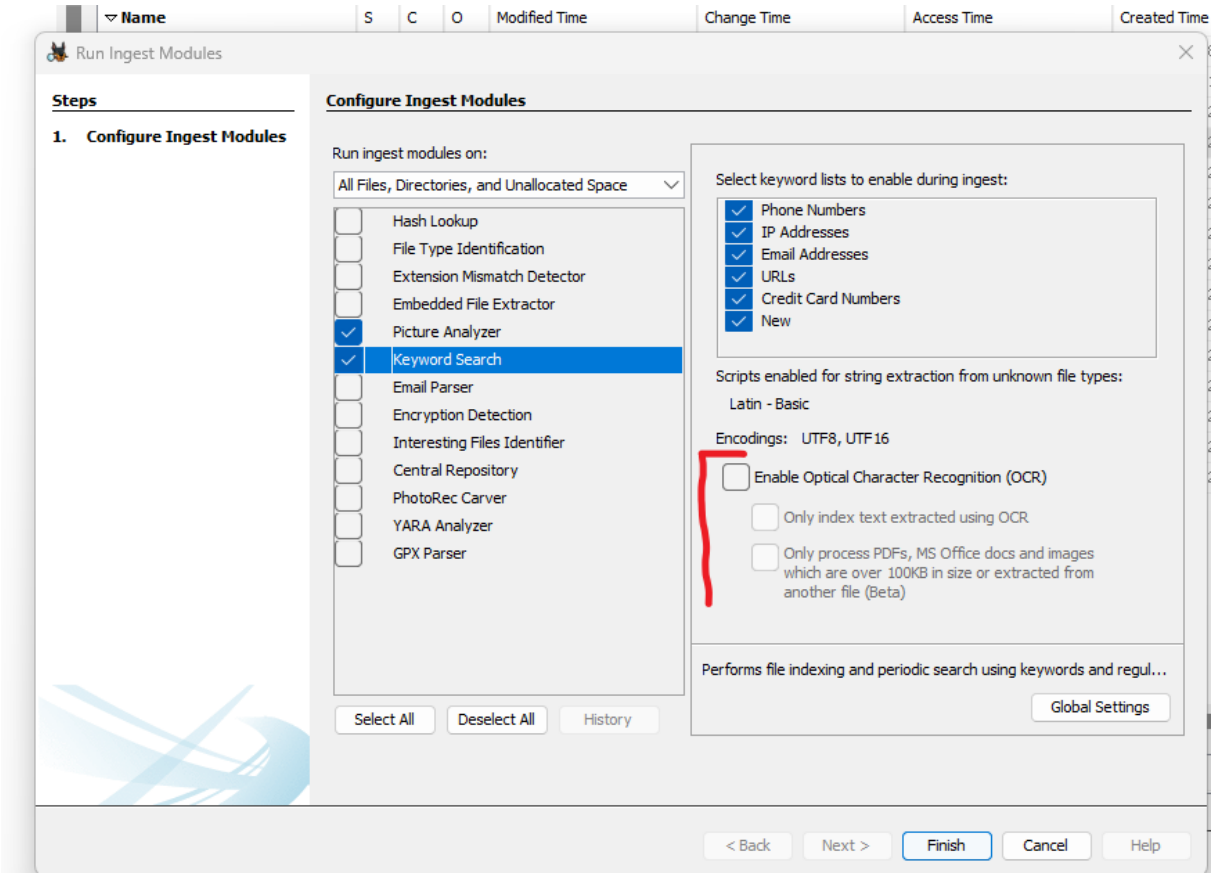


Abbildung 35 - Aktivierung der OCR-Funktion in Autopsy

Abbildung 36 - Bild welches mit OCR-Funktion untersucht wurde

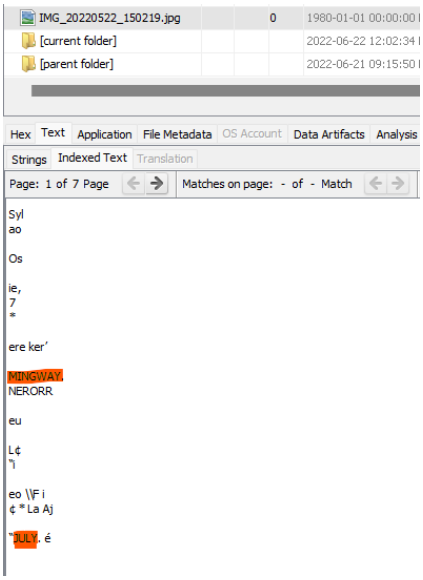


Abbildung 37 - Erkannte Texte: MINGWAY; JULY

3.4.6 Objekterkennung/OpenCV

Autopsy verfügt ebenfalls über ein Objekterkennungsmodul welches OpenCV verwendet um die Erkennung von Objekten in Bildern durchzuführen. Hierbei ist jedoch die Ausführung des Experimentalmoduls in Autopsy notwendig. Des Weiteren werden Klassifikatioren benötigt, da Autopsy diese nicht erstellen kann. Somit ist es durch den Benutzer notwendig, diese OpenCV-Klassifikatoren zu trainieren beziehungsweise zu erstellen. Es gibt jedoch auch bereits von OpenCV bereitgestellte Klassifikatoren. Durch das Herunterladen sowie installieren von

OpenCV können diese unter dem Ordner „haarcascades_cuda“ (Abbildung 38) für Autopsy entnommen werden. Diese sind dann in den Ordner „object_detection_classifiers“ von Autopsy einzufügen (Abbildung 39). Danach kann das Objekterkennungsmodul mit den Klassifikatoren von OpenCV in Autopsy ausgeführt werden und es wird in der Spalte „Description“ angezeigt, welche Objekte erkannt wurden (Abbildung 40).[46]

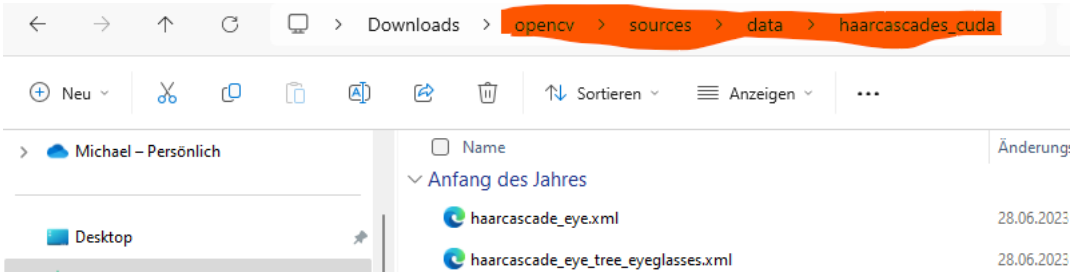


Abbildung 38 - Fertige Klassifikatoren von OpenCV

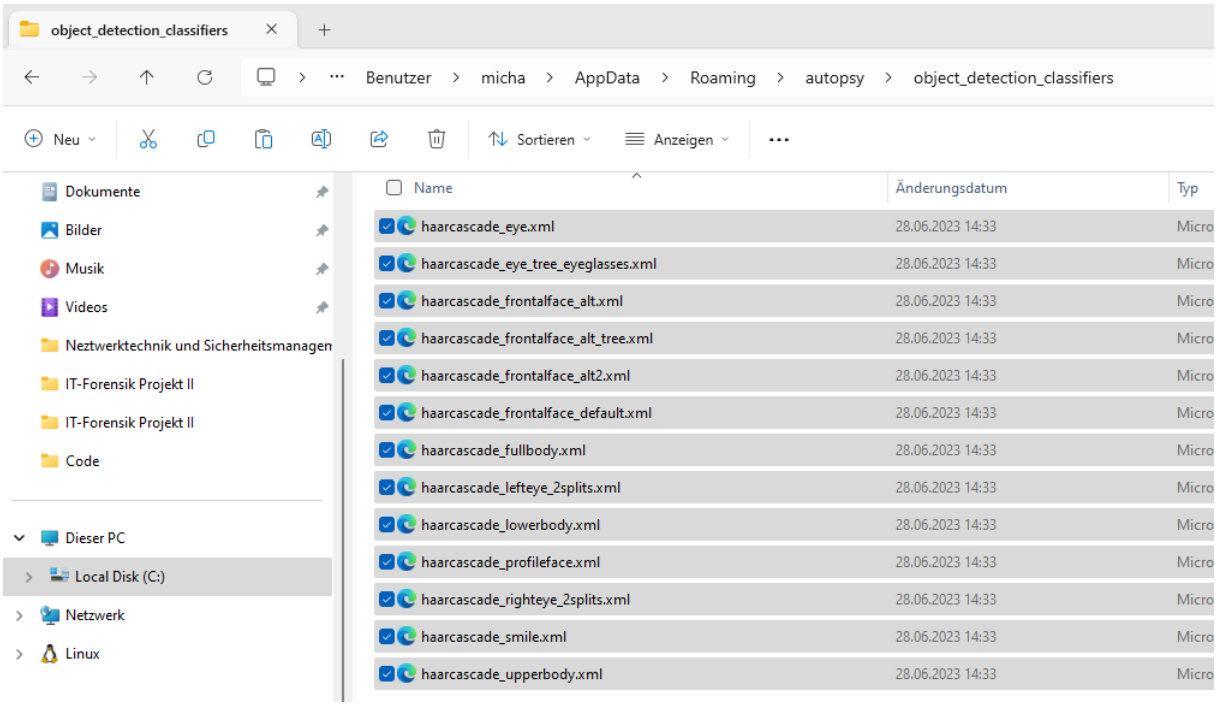


Abbildung 39 - Einfügen der fertigen Klassifikatoren von OpenCV in Autopsy

[46] (Basis Technology, http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/object_detection_page.html, 2023)

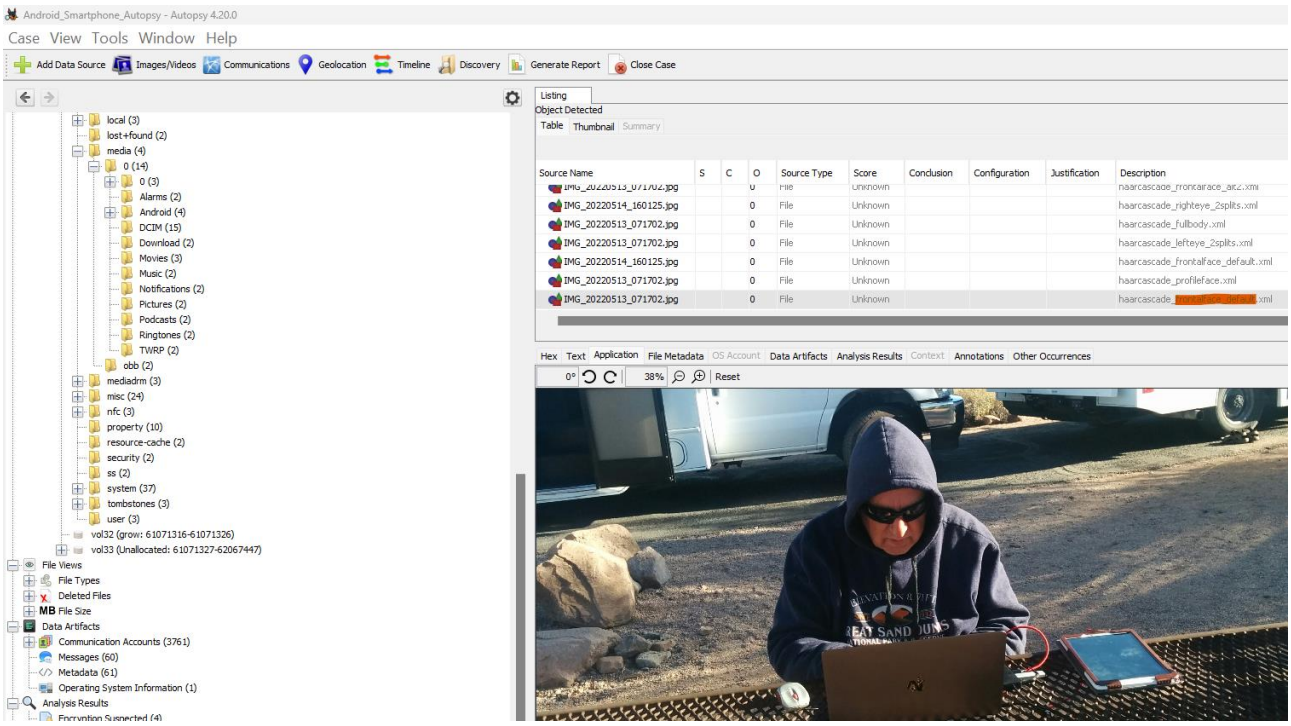


Abbildung 40 - Gesichtserkennung durch den Klassifikator "haarcascade_frontalface_default.xml"

3.4.7 Bildanalyse Hautfarbenanteil

Eine Analyse, ob und wieviel Prozent an Hautfarbenanteilen in einem Bild enthalten ist, ist standardmäßig in Autopsy nicht möglich. Erst die Erweiterung durch das Modul „SmutDetect_Skintone“ (Abbildung 41), welches auf Github heruntergeladen werden kann, ermöglicht auch die Durchführung eines Scans, um die Hautfarbanteile auch in Autopsy anzeigen zu können. Das Modul wird in Autopsy über „Plugins“ hinzugefügt. Dabei wird jeweils in 10er-Schritten der Hautton-Prozentsatz angegeben (Abbildung 42).

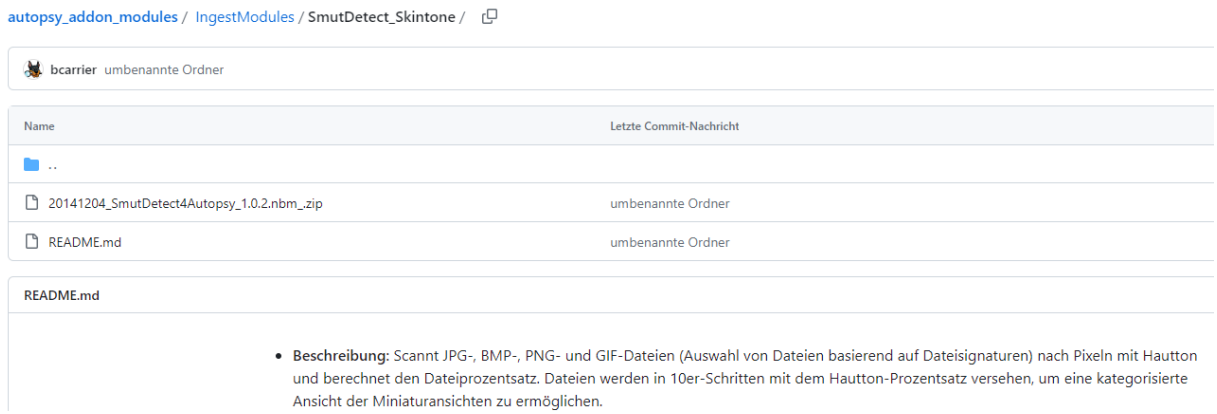


Abbildung 41 – Modul „SmutDetect_Skintone“ auf Github

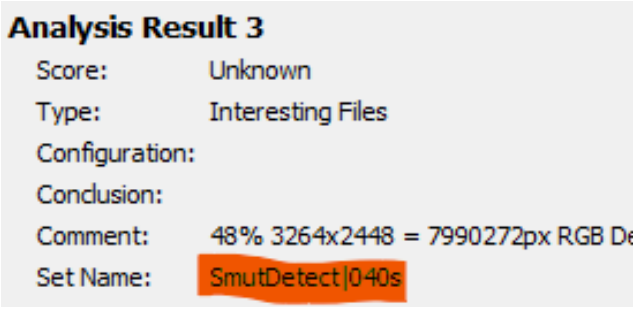


Abbildung 42 – Angabe des Hauttonprozentsatzes in Prozent

3.5 Datenextraktion

3.5.1 Rekonstruktion gelöschter Daten

Autopsy erfasst gelöschte Dateien auf Smartphones automatisch und zeigt diese in der Übersicht mit an (Abbildung 43). Gelöschte Dateien und Verzeichnisse werden mit einem roten X im Icon dargestellt. Gelöschte Daten können über das Kontextmenü wiederhergestellt und exportiert werden. Ebenfalls kann über den Timeline-Button Informationen über den Löschzeitpunkt sowie weiteren Informationen abgerufen werden, was für Ermittler wichtige Anhaltspunkte bei weiteren Ermittlungen darstellen können (Abbildung 44).

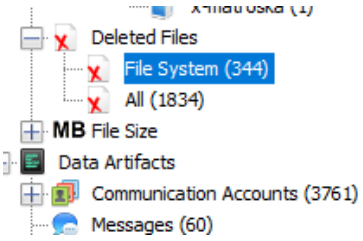


Abbildung 43 - Gefundene gelöschte Dateien in Autopsy

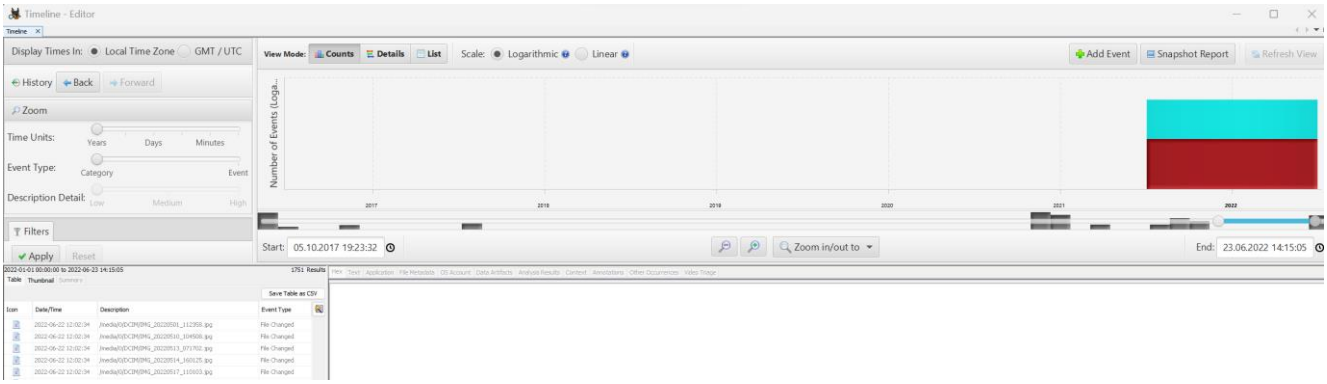


Abbildung 44 - Nutzung der Timline-Funktion in Autopsy

3.5.2 Extraktion von Metadaten

Für die Extraktion von Metadaten verwendet Autopsy ein Bildanalysator-Modul welches EXIF-Informationen (EXIF = Exchangable Image File Format). Damit ist es

möglich die für Ermittler wichtigen Informationen wie beispielsweise Uhrzeit, Kameramodell, Datum und Geolokalisierungsinformationen aus Bildern zu erhalten, die mit dem Smartphone aufgenommen wurden (Abbildung 45). Außerdem ist es möglich, auch bei Konvertierung von HEIC/HEIF-Bildern (welche von dem Betriebssystem iOS verwendet werden) in das JPG-Format, die Metadaten beizubehalten und diese somit ebenfalls extrahieren zu können.[47] Ebenfalls ist es in Autopsy über den Button „Geolocation“ möglich, anhand gefundener Artefakte mit Längen- und Breitengradattributen, diese sich auf einer Karte anzeigen zu lassen. So ist es für Ermittler möglich, schnell und einfach die zurück gelegte Strecke eines Smartphones/Verdächtigen rekonstruieren zu können (Abbildung 46).[48]

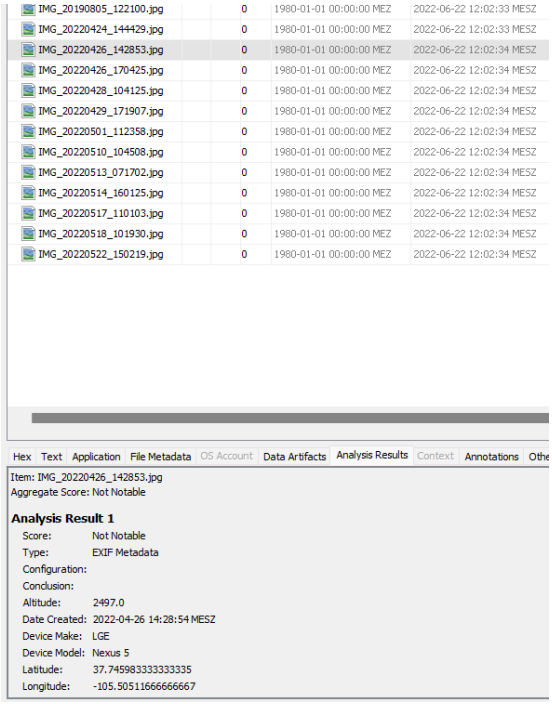


Abbildung 45 - Auslesen von Metadaten eines Bildes in Autopsy

[47] (Basis Technology, http://sleuthkit.org/autopsy/docs/user-docs/4.20.0/_e_x_i_f_parser_page.html, 2023)
[48] (Basis Technology, http://sleuthkit.org/autopsy/docs/user-docs/4.20.0/geolocation_page.html, 2023)

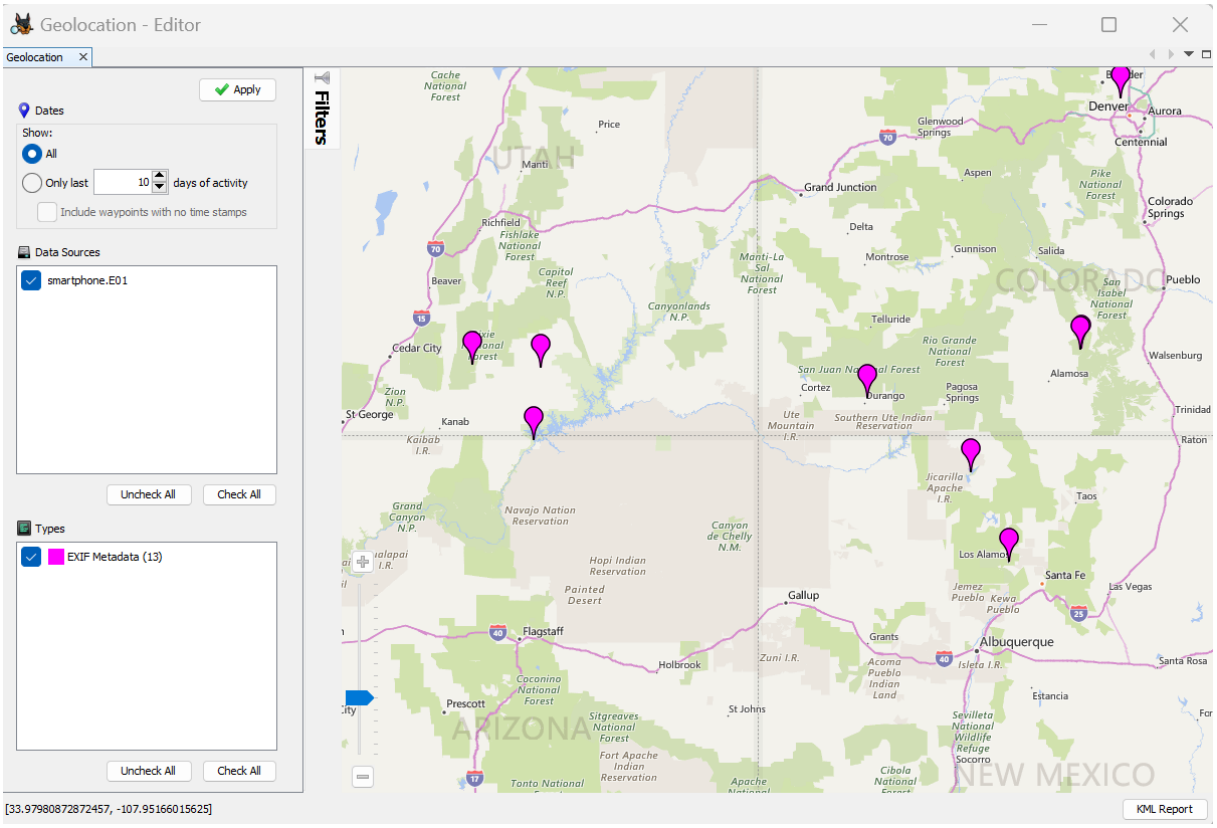


Abbildung 46 - Darstellung der Standorte anhand gefundener Längen- und Breitengradattributen in Autopsy

3.5.3 Extraktion von Standbildern aus Videos

Autopsy stellt für die Extraktion von Standbildern aus Videos das „Video Triage-Modul“ zur Verfügung, dass eine Videodatei in Miniaturbilder (Keyframes) aufteilt, welche Geheimdiensten oder Strafverfolgungsbehörden die Möglichkeit bietet, Videomaterial schnell und effizient nach wichtigen Stellen wie beispielsweise extremistisches Material zu durchsuchen.[49] Da diese Funktion nicht Standardmäßig in Autopsy enthalten ist, muss diese Erweiterung über das Modul „Video Triage“ erfolgen. Hierbei ist eine einmalige Registrierung auf der Internetseite von Autopsy notwendig. Danach kann der Download erfolgen (Abbildung 47). Hierbei ist die Erweiterung ebenfalls über Plugins in Autopsy hinzuzufügen (Abbildung 48). Nach der Installation ist die Erweiterung „Video Triage“ direkt in Autopsy eingebunden, welches beim Öffnen des Media-Viewers ausgewählt werden kann (Abbildung 49). Eine Angabe einer festen Anzahl von Standbildern oder eines festgelegten Zeitabstandes in dem die Standbilder erstellt werden sollen, ist jedoch nicht auswählbar.

[49] (Basis Technology, https://www.autopsy.com/add-on-modules/video-triage/, 2023)

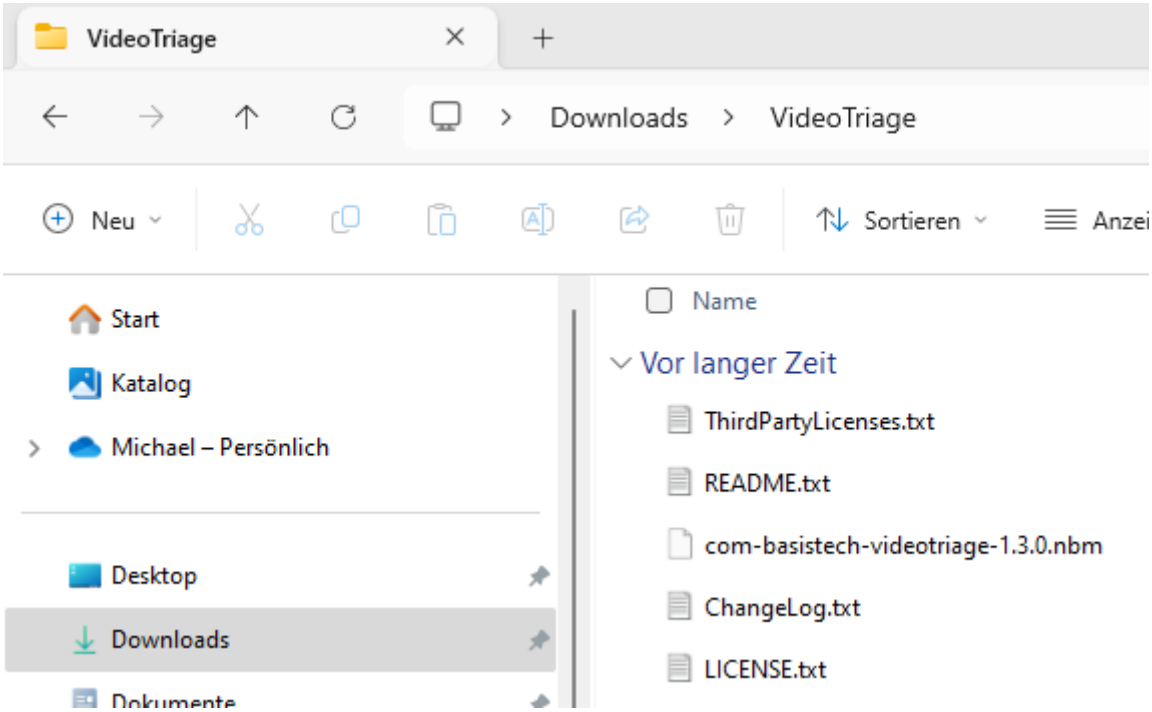


Abbildung 47 - Modulerweiterung "Video Triage"

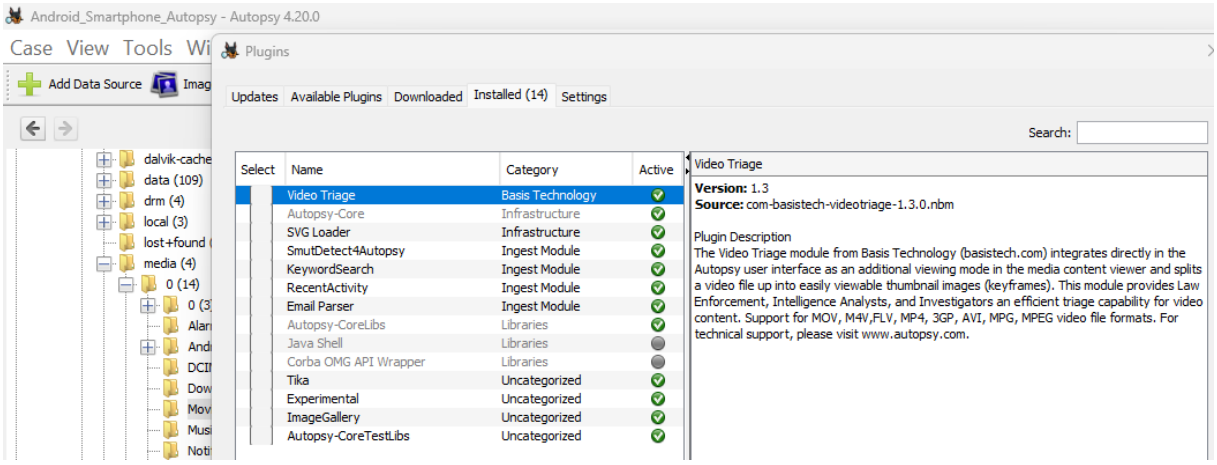


Abbildung 48 - Installation der Erweiterung "Video Triage" über Plugins in Autopsy

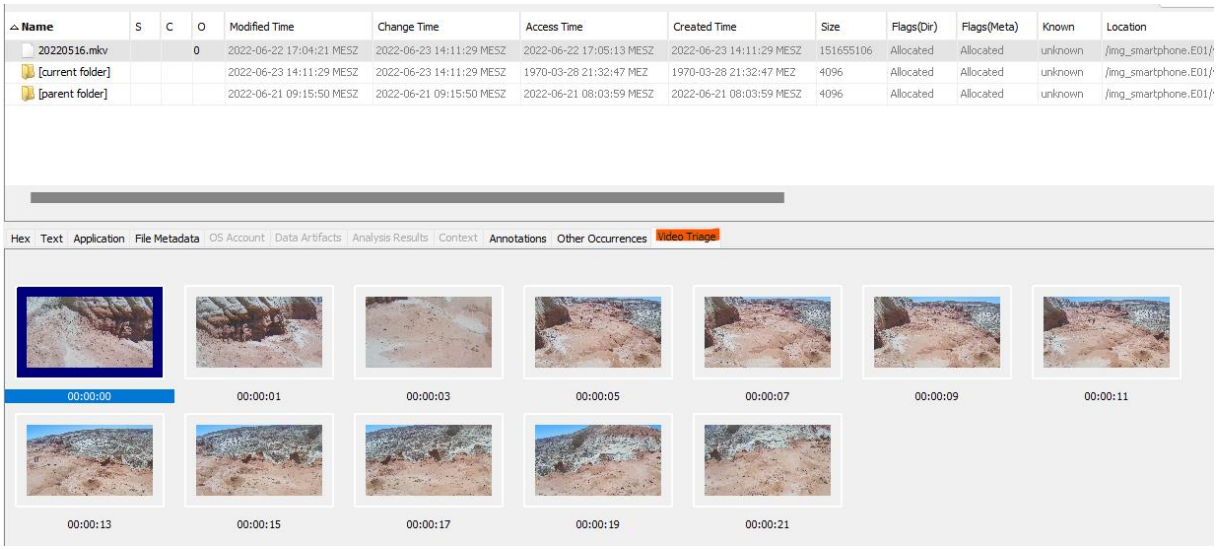


Abbildung 49 - Erstellung von Standbildern eines Videos in Autopsy

3.6 Berichterstellung

Autopsie bietet anhand der Berichtsmodule dem Benutzer auch die Möglichkeit, die wichtigsten Informationen aus dem jeweiligen Fall in verschiedenen Formaten zu extrahieren. Es werden Formate wie beispielsweise HTML oder Excel unterstützt. Des Weiteren kann der Benutzer auswählen, welche für ihn notwendigen Informationen im Bericht enthalten sein sollen (Abbildung 50, Abbildung 51, Abbildung 52, Abbildung 53). Es kann jedoch auch für gefundene Koordinaten das KML-Format ausgewählt werden um diese später in Google Earth zu importieren. Enthält der Berichtstyp einen Viewer, so kann beispielsweise bei einem HTML-Bericht dieser später in einer externen Anwendung geöffnet werden.[50]

[50] (Basis Technology, http://sleuthkit.org/autopsy/docs/user-docs/4.20.0/reporting_page.html, 2023)

Abbildung 50 - HTML-Bericht in Autopsy

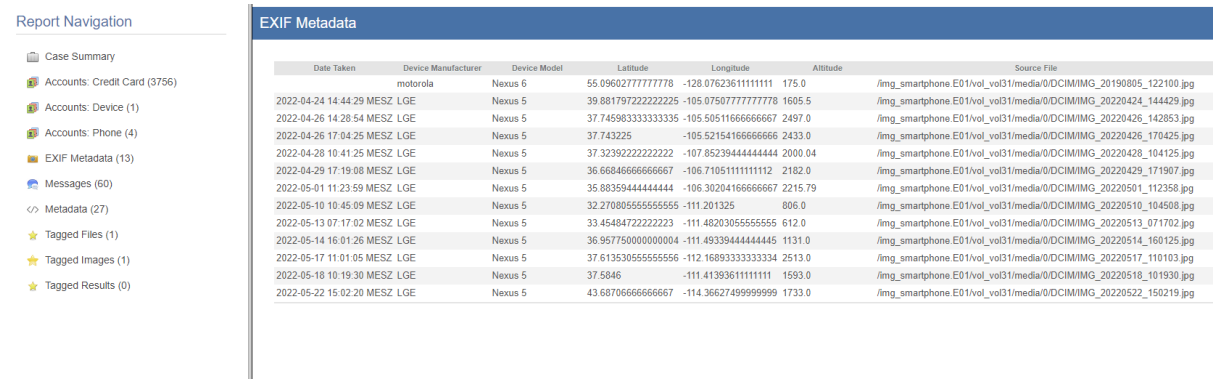


Abbildung 51 - Darstellung Metadaten im Bericht (Autopsy)

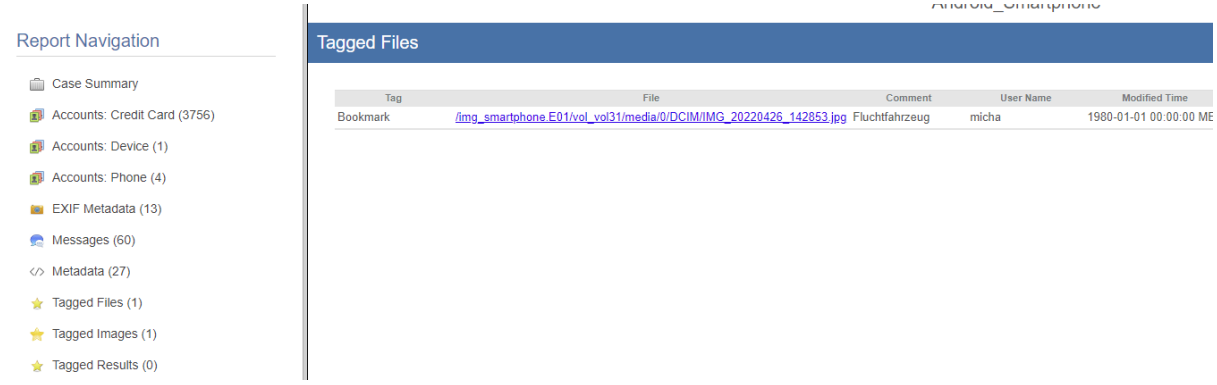


Abbildung 52 - Darstellung vorgenommener Vermerke im Bericht (Autopsy)

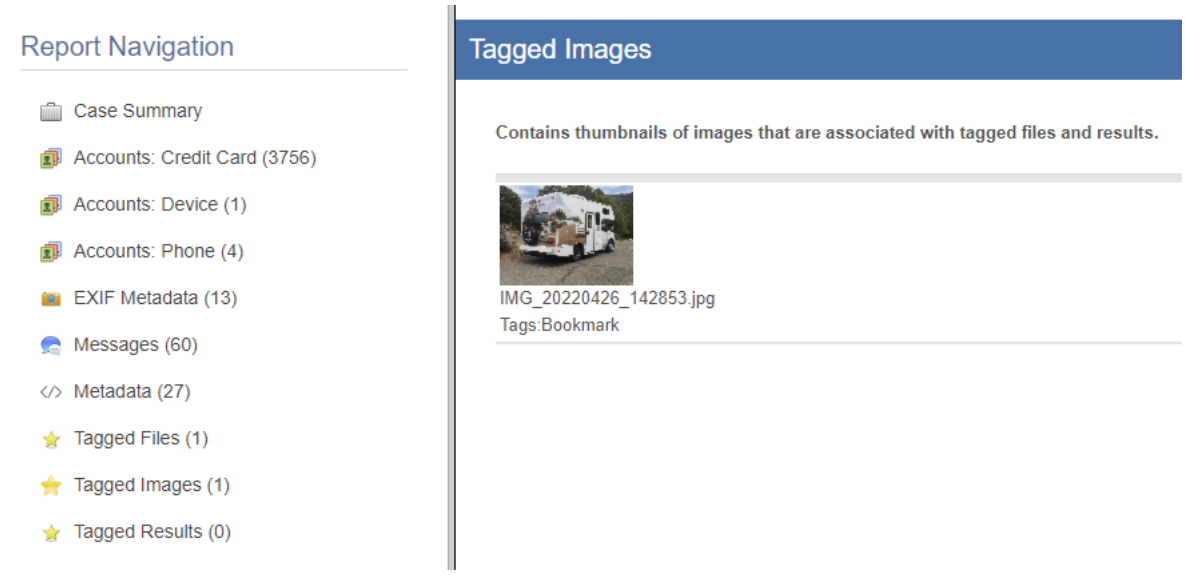


Abbildung 53 - Darstellung von Bildern im Bericht (Autopsy)

4. Vergleich der Funktionen

Bei dem Vergleich der beiden Programme wurde wie folgt vorgegangen:

Einteilung in folgende Kriterien:

Erfüllung des Kriteriums	**Gewichtung**
Kriterium wird voll erfüllt	4
Kriterium wird zum größten Teil erfüllt	3
Kriterium wird kaum erfüllt	2
Kriterium wird nicht erfüllt	1

Des Weiteren erfolgte in der Zusammenfassung noch eine Einstufung der Relevanz

Einstufung der Relevanz	**Kategorie**
Äußerst wichtig	4
Sehr wichtig	3
Wichtig	2
Kaum wichtig	1

4.1 Benutzerfreundlichkeit

X-Ways Forensics	**Erfüllung des Kriteriums**	**Gewichtung**	**Bemerkung**
Installationsaufwand / Systemvoraussetzungen	Kriterium wird voll erfüllt	4	Keine
Anwendersupport	Kriterium wird voll erfüllt	4	Keine
Benutzeroberfläche	Kriterium wird voll erfüllt	4	Keine
Gesamtbewertung		**4**	

Autopsy	Erfüllung des Kriteriums	Gewichtung	Bemerkung
Installationsaufwand / Systemvoraussetzungen	Kriterium wird zum größten Teil erfüllt	3	Benötigt doppelt so viel Speicher wie X-Ways-Forensics
Anwendersupport	Kriterium wird zum größten Teil erfüllt	3	Keine Anleitungs- oder Einführungsvideos / Grundlagenschulung nur gegen Gebühr / Kein Anwendersupport für private Nutzer möglich
Benutzeroberfläche	Kriterium wird voll erfüllt	4	Keine
Gesamtbewertung		**3,33**	

4.2 Analysemöglichkeiten

X-Ways Forensics	Erfüllung des Kriteriums	Gewichtung	Bemerkung
Unterstützung von Dateisystemen	Kriterium wird voll erfüllt	4	Keine
Unterstützung von Image-Dateien	Kriterium wird voll erfüllt	4	Keine
Einbinden Partitionen/Ordnern	Kriterium wird voll erfüllt	4	Keine
Hashwertanwendung auf Bilder/PhotoDNA-Funktion	Kriterium wird voll erfüllt	4	Keine

OCR-Funktion/Tesseract-Packet	Kriterium wird zum größten Teil erfüllt	3	Texterkennung erfolgte in Bilddateien nicht immer bzw. korrekt
Objekterkennung/Excire Forensics	Kriterium wird voll erfüllt	4	Keine
Bildanalyse Hautfarbenanteil	Kriterium wird voll erfüllt	4	Keine
Gesamtbewertung		**3,85**	

Autopsy	**Erfüllung des Kriteriums**	**Gewichtung**	**Bemerkung**
Unterstützung von Dateisystemen	Kriterium wird voll erfüllt	4	Keine
Unterstützung von Image-Dateien	Kriterium wird voll erfüllt	4	Keine
Einbinden Partitionen/Ordnern	Kriterium wird voll erfüllt	4	Keine
Hashwertanwendung auf Bilder/ C4P-Funktion/Projekt VIC	Kriterium wird voll erfüllt	4	Keine
OCR-Funktion/Tesseract-Packet	Kriterium wird zum größten Teil erfüllt	3	Texterkennung erfolgte in Bilddateien nicht immer bzw. korrekt
Objekterkennung/OpenCV	Kriterium wird zum größten Teil erfüllt	3	Objekte müssen über OpenCV zuerst klassifiziert werden damit eine Objekterkennung

			durchgeführt werden kann
Bildanalyse Hautfarbenanteil	Kriterium wird voll erfüllt	4	Keine
Gesamtbewertung		**3,71**	

4.3 Datenextraktion

X-Ways Forensics	**Erfüllung des Kriteriums**	**Gewichtung**	**Bemerkung**
Rekonstruktion gelöschter Daten	Kriterium wird voll erfüllt	4	Keine
Extraktion von Metadaten	Kriterium wird voll erfüllt	4	Keine
Extraktion von Standbildern aus Videos	Kriterium wird voll erfüllt	4	Keine
Gesamtbewertung		**4**	

Autopsy	**Erfüllung des Kriteriums**	**Gewichtung**	**Bemerkung**
Rekonstruktion gelöschter Daten	Kriterium wird voll erfüllt	4	Keine
Extraktion von Metadaten	Kriterium wird voll erfüllt	4	Keine
Extraktion von Standbildern aus Videos	Kriterium wird voll erfüllt	4	Keine
Gesamtbewertung		**4**	

4.4 Berichterstellung

X-Ways Forensics	Erfüllung des Kriteriums	Gewichtung	Bemerkung
Berichtserstellung	Kriterium wird voll erfüllt	4	Keine
Gesamtbewertung		**4**	

Autopsy	Erfüllung des Kriteriums	Gewichtung	Bemerkung
Berichtserstellung	Kriterium wird voll erfüllt	4	Keine
Gesamtbewertung		**4**	

4.5 Zusammenfassung der Bewertung

Relevanz	Titel	X-Ways Forensics	Autopsy
	Benutzerfreundlichkeit	**4**	**3,33**
1	Anwendersupport	4	3
2	Installationsaufwand / Systemvoraussetzungen	4	3
	Benutzeroberfläche	4	4
3	**Berichtserstellung**	**4**	**4**
4	**Analysemöglichkeiten**	**3,85**	**3,71**
	Unterstützung von Dateisystemen	4	4
	Unterstützung von Image-Dateien	4	4

	Einbinden Partitionen/Ordnern	4	4
	Hashwertanwendung auf Bilder/PhotoDNA-Funktion	4	4
	OCR-Funktion/Tesseract-Packet	3	3
	Objekterkennung/Excire Forensics	4	3
	Bildanalyse Hautfarbenanteil	4	4
	Datenextraktion	**4**	**4**
	Rekonstruktion gelöschter Daten	4	4
	Extraktion von Metadaten	4	4
	Extraktion von Standbildern aus Videos	4	4
	Gesamtbewertung	**3,96**	**3,76**

5. Zusammenfassung der Ergebnisse

X-Ways Forensics erreicht eine Gesamtbewertung von 3,96 von möglichen 4 Punkten. Autopsy erreicht 3,76 von möglichen 4 Punkten. Anhand der ausgewählten vier zu untersuchenden Bereiche Benutzerfreundlichkeit, Analysemöglichkeit, Datenextraktion sowie Berichterstellung konnte festgestellt werden, dass X-Ways Forensics nach Punkten das etwas bessere Werkzeug für die Smartphone-Forensik darstellt.

Grundsätzlich bieten beide Forensik-Programme in allen Bereichen Funktionen, welche für Forensiker notwendig sind, um Smartphones auswerten zu können. Allerdings bietet X-Way Forensics das besser Gesamtpaket. In Bereichen wie der Bildanalyse Hautfarbenanteil bietet X-Ways Forensics beispielsweise eine bessere Abstufung der Prozentangaben im Gegensatz zu Autopsy. Bei der Objekterkennung erreicht Autopsy beispielsweise nur die Gewichtung 3, da zwar die Funktion verfügbar ist, diese jedoch durch den Benutzer mit OpenCV sozusagen erst angelernt werden muss, was für Benutzer, die keine OpenCV-Erfahrung besitzen, erstmal eine Hürde darstellt. Jedoch kann auf bereits von OpenCV bereitgestellte

Klassifikationen zurück gegriffen werden. X-Ways Forensics stellt hier dann jedoch für die Objekterkennung ein vollständigeres Paket zur Verfügung, welches vom Benutzer nach einer kurzen Installation sofort verwendet werden kann.

Was sowohl bei X-Ways Forensics als auch Autopsy gleichermaßen nicht ganz zuverlässig funktionierte, war die OCR-Funktion, da in einigen Bildern die darin vorkommenden Texte nicht erkannt wurden.

Ansonsten besitzen beide Forensik-Programme keine nennenswerten Schwächen in den jeweiligen Kategorien, die in dieser Projektarbeit dargestellt wurden.

6. Fazit

In der durchgeführten Projektarbeit wurden die beiden Forensik-Programme X-Ways Forensics sowie Autopsy auf ihre Verwendbarkeit in der Smartphone-Forensik untersucht.

Dabei wurde ein Smartphone-Image eines Samsung Galaxy S3 verwendet, welches bereits in einem früheren Modul des Studiums durch den Dozenten für forensische Analysen präpariert wurde. Es wurde in der Projektarbeit festgestellt, dass sowohl X-Ways Forensics als auch Autopsy grundsätzlich alle grundlegenden Methoden für die Smartphone-Forensik beherrschen. Somit lässt sich sagen, dass beide Forensik-Programme gleichermaßen für die Smartphone-Forensik geeignet sind.

Jedoch muss auch beachtet werden, dass diese beiden Forensik-Programme eine große Anzahl von Funktionen bieten, die in dieser Projektarbeit nicht alle berücksichtigt werden konnten. Eine vollständiger Vergleich aller Funktionen wäre ein zeitlich sehr hoher Aufwand. Dies trifft vor allem auch dann zu, wenn bisher keine Erfahrungen des Benutzers mit einem der beiden Forensik-Programme vorliegen.

Literaturverzeichnis

Basis Technology. (2023). *http://sleuthkit.org/autopsy/docs/user-docs/4.20.0/_e_x_i_f_parser_page.html*. Abgerufen am 30. Augsut 2023 von http://sleuthkit.org/autopsy/docs/user-docs/4.20.0/_e_x_i_f_parser_page.html

Basis Technology. (2023). *http://sleuthkit.org/autopsy/docs/user-docs/4.20.0/embedded_file_extractor_page.html*. Abgerufen am 30. August 2023 von http://sleuthkit.org/autopsy/docs/user-docs/4.20.0/embedded_file_extractor_page.html

Basis Technology. (2023). *http://sleuthkit.org/autopsy/docs/user-docs/4.20.0/geolocation_page.html*. Abgerufen am 30. August 2023 von http://sleuthkit.org/autopsy/docs/user-docs/4.20.0/geolocation_page.html

Basis Technology. (2023). *http://sleuthkit.org/autopsy/docs/user-docs/4.20.0/reporting_page.html*. Abgerufen am 30. August 2023 von http://sleuthkit.org/autopsy/docs/user-docs/4.20.0/reporting_page.html

Basis Technology. (2023). *http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/*. Abgerufen am 10. August 2023 von http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/

Basis Technology. (2023). *http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/_e_x_i_f_parser_page.html*. Abgerufen am 13. August 2023 von http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/_e_x_i_f_parser_page.html

Basis Technology. (2023). *http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/android_analyzer_page.html*. Abgerufen am 13. August 2023 von http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/android_analyzer_page.html

Basis Technology. (2023). *http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/ds_page.html*. Abgerufen am 13. August 2023 von http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/ds_page.html

Basis Technology. (2023). *http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/ileapp_page.html*. Abgerufen am 13. August 2023 von http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/ileapp_page.html

Basis Technology. (2023). *http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/object_detection_page.html*. Abgerufen am 13. August 2023 von http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/object_detection_page.html

Basis Technology. (2023). *http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/reporting_page.html*. Abgerufen am 12. August 2023 von http://sleuthkit.org/autopsy/docs/user-docs/4.21.0/reporting_page.html

Basis Technology. (2023). *https://sleuthkit.org/autopsy/docs/user-docs/3.1/photorec_carver_page.html*. Abgerufen am 30. August 2023 von https://sleuthkit.org/autopsy/docs/user-docs/3.1/photorec_carver_page.html

Basis Technology. (2023). *https://sleuthkit.org/support.php*. Abgerufen am 12. August 2023 von https://sleuthkit.org/support.php

Basis Technology. (2023). *https://www.autopsy.com/add-on-modules/law-enforcement-bundle/*. Abgerufen am 13. August 2023 von https://www.autopsy.com/add-on-modules/law-enforcement-bundle/

Basis Technology. (2023). *https://www.autopsy.com/add-on-modules/video-triage/*. Abgerufen am 30. August 2023 von https://www.autopsy.com/add-on-modules/video-triage/

Basis Technology. (2023). *https://www.autopsy.com/support/training/*. Abgerufen am 12. August 2023 von https://www.autopsy.com/support/training/

Basis Technology. (2023). *www.autopsy.com*. Abgerufen am 07. Juli 2023 von https://www.autopsy.com/about/

F.Tenzer. (28. 11 2022). *www.statista.com*. Abgerufen am 30. Juni 2023 von https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/

Github. (2023). *https://github.com/sleuthkit/autopsy_addon_modules*. Abgerufen am 10. August 2023 von https://github.com/sleuthkit/autopsy_addon_modules

https://www.sit.fraunhofer.de/de/itforensics/file-carving/. (2023). *Frauenhoferinstitut*. Abgerufen am 06. August 2023 von https://www.sit.fraunhofer.de/de/itforensics/file-carving/

Project VIC International. (2023). *https://www.projectvic.org/technologies*. Abgerufen am 13. August 2023 von https://www.projectvic.org/technologies

Shavers, B., & Zimmerman, E. (2014). *X-Ways Forensics Practitioner´s Guide.*

Sleuthkit. (2023). *https://sleuthkit.discourse.group/*. Abgerufen am 12. August 2023 von https://sleuthkit.discourse.group/

Stephan Ludewig, P. (Mai 2019). *Die Sicherstellung und Auswertung des Smartphones – Kriminalpolitischer Anpassungsbedarf?* (K. -K. Zeitschrift, Hrsg.) Abgerufen am 30. Juni 2023 von https://kripoz.de/2019/09/18/die-sicherstellung-und-auswertung-des-smartphones-kriminalpolitischer-anpassungsbedarf/#:~:text=Neben%20auswertbaren%20Computersystemen%2C%20hat%20sich, Aufschluss%20%C3%BCber%20Tat%20und%20T%C3%A4ter.

wikipedia.org. (2023). Abgerufen am 13. August 2023 von https://de.wikipedia.org/wiki/The_Sleuth_Kit

X-Ways Software Technology AG. (2023). *http://www.winhex.net/*. Abgerufen am 20. Juli 2023 von http://www.winhex.net/

X-Ways Software Technology AG. (2023). *http://www.x-ways.net/BYOD-d.html*. Abgerufen am 20. Juli 2023 von http://www.x-ways.net/BYOD-d.html

X-Ways Software Technology AG. (2023). *http://www.x-ways.net/forensics/index-d.html*. Abgerufen am 25. Juli 2023 von http://www.x-ways.net/forensics/index-d.html

X-Ways Software Technology AG. (2023). *https://www.x-ways.net/corporate/contact-d.html*. Abgerufen am 20. Juli 2023 von https://www.x-ways.net/corporate/contact-d.html

X-Ways Software Technology AG. (27. August 2023). *https://www.x-ways.net/Excire_Erkannte_Objekte.txt*. Von https://www.x-ways.net/Excire_Erkannte_Objekte.txt abgerufen

X-Ways Software Technology AG. (2023). *https://www.x-ways.net/winhex/manual-d.pdf.* (S. Fleischmann, Hrsg.) Abgerufen am 21. Juli 2023 von https://www.x-ways.net/winhex/manual-d.pdf

X-Ways Software Technology AG. (2023). *https://www.youtube.com/playlist?list=PLB0pU0wP67A-_DeVFfswVlZuRTH4cWswQ*. Abgerufen am 21. Juli 2023 von https://www.youtube.com/playlist?list=PLB0pU0wP67A-_DeVFfswVlZuRTH4cWswQ

X-Ways Software Technology AG. (2023). *https://www.youtube.com/watch?v=OuT33vh8ZoM*. Abgerufen am 23. Juli 2023 von https://www.youtube.com/watch?v=OuT33vh8ZoM

X-Ways Software Technology AG. (2023). *https://www.youtube.com/watch?v=Vbz9-GLiCOY&list=PLB0pU0wP67A-_DeVFfswVlZuRTH4cWswQ&index=3&t=17s*. Abgerufen am 02. August 2023 von https://www.youtube.com/watch?v=Vbz9-GLiCOY&list=PLB0pU0wP67A-_DeVFfswVlZuRTH4cWswQ&index=3&t=17s

X-Ways Software Technology AG. (2023). *www.x-ways.net*. Abgerufen am 04. Juli 2023 von https://www.x-ways.net/forensics/index-m.html

Abbildungsverzeichnis

Eigenständigkeitserklärung

Hiermit erkläre ich, Michael Krimplstötter, Matrikel-Nr. 360485,

- dass ich die vorliegende Ausarbeitung der alternativen Prüfungsleistung selbstständig und ohne unzulässige fremde Hilfe erbracht habe.
- dass ich keine anderen als die zugelassenen Hilfsmittel benutzt habe.
- dass von meiner Ausarbeitung/ Lösung eine elektronische Kopie gefertigt und gespeichert werden darf, um eine Überprüfung mittels einer Anti-Plagiatssoftware seitens der Hochschule Wismar zu ermöglichen.
- dass mir bekannt ist, dass die Arbeit bei Nichtabgabe oder nicht vollständiger Abgabe der Eigenerklärung als nicht bestanden gilt.

Ort: Bad Feilnbach, Datum: 15.10.2023

Unterschrift*

* Bei einer reinen digitalen Bearbeitung reicht es aus, wenn Sie nur den Namen, Matrikelnummer,
Ort und Datum digital ausfüllen - die Unterschrift können Sie dann auslassen. Sollten Sie die
Alternative Prüfungsleistung handschriftlich lösen, ist die Eigenständigkeitserklärung mit Unterschrift zusammen mit den Lösungen hochzuladen.