HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Frau
Isabelle Mirtschink

Vergleich verschiedener forensischer Anwendungen im Zusammenhang mit dem Encrypting File System

Mittweida, 2023

Fakultät Angewandte Computer- und Biowissenschaften

BACHELORARBEIT

Vergleich verschiedener forensischer Anwendungen im Zusammenhang mit dem Encrypting File System

Autor:
Frau

Isabelle Mirtschink

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO20w5-B

Erstprüfer:
Prof. Dr. rer. pol. Dirk Pawlaszczyk

Zweitprüfer:
Dipl. Inf. Andreas Sommer

Einreichung:
Mittweida, 13.09.2023

Verteidigung/Bewertung:
Mittweida, 2023

Faculty Applied Computer- and Biosciences

BACHELOR THESIS

Comparison of different forensic applications in connection with the Encrypting File System

author:
Ms.

Isabelle Mirtschink

course of studies:
General and digital forensics

seminar group:
Fo20w5-B

first examiner:
Prof. Dr. rer. Pol. Dirk Pawlaszczyk

second examiner:
Dipl. Inf. Andreas Sommer

submission:
Mittweida, 13.09.2023

defence/ evaluation:
Mittweida, 2023

Bibliografische Beschreibung:

Mirtschink, Isabelle:
Vergleich verschiedener forensischer Anwendungen im Zusammenhang mit dem Encrypting File System. - 2023. – 7, 45, 0 S.

Mittweida, Hochschule Mittweida, Fakultät Angewandte Computer- und Biowissenschaften, Bachelor of Science, 2023

Referat:

In der vorliegenden Arbeit wird auf die Analyse des Encrypting File System (EFS) von Windows in Bezug auf verschiedene forensische Anwendungen eingegangen. Dazu werden die unterschiedlichen Vorgehensweisen der forensichen Anwendungen AXIOM, X-Ways Forensics, Autopsy und IPED analysiert. Ziel der Arbeit ist es zu untersuchen, ob diese forensischen Anwendungen verschlüsselte Dateien erkennen und entschlüsseln können.
Dafür wird zu Beginn ein kurzer Überblick über die Entwicklung von Windows und seine Verschlüsselungsmöglichkeiten gegeben. Im Anschluss beschäftigt sich die Arbeit mit den ausgewählten forensischen Programmen und deren Leistung in Bezug auf mit dem Encrypting File System von Windows verschlüsselten Ordnern.

Abstract:

In this paper, the analysis of the Encrypting File System (EFS) of Windows in relation to different forensic applications is addressed. For this purpose, the different procedures of the forensic applications AXIOM, X-Ways Forensics, Autopsy and IPED are analysed. The aim of the work is to examine whether these forensic applications can recognise and decrypt encrypted files.
For this purpose, a short overview of the development of Windows and its encryption possibilities is given at the beginning. Subsequently, the work deals with the selected forensic programmes and their performance in relation to folders encrypted with the Windows Encrypting File System.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AES	Advanced Encryption Standard
CA	Certification Authority
CPU	Central Processing Unit
DDF	Data Decryption Field
DES	Data Encryption Standard
DRA	Data Recovery Agents
EFS	Encrypting File System
FEK	File Encryption Key
FTK	Forensic Toolkit
GPS	Global Positioning System
GUI	grafische Benutzeroberfläche
IDEA	International Data Encryption Algorithm
IPED	Digital Evidence Processor and Indexer
MS-DOS	Microsoft Disk Operating System
NTFS	New Technology File System
PC	Personal Computer
PKI	Public Key Infrastructure
RSA	Rivest-Shamir-Adleman
TPM	Trusted Platform Module
VHD	Virtuelle Festplatte

1 Einleitung und Motivation

In den letzten Jahrzehnten hat die kontinuierliche Entwicklung der Informationstechnologie dazu beigetragen, viele Aspekte des menschlichen Lebens zu verändern. Vor allem das Windows-Betriebssystem hat sich zu einem der am weitesten verbreiteten und einflussreichsten Betriebssysteme der Welt entwickelt. Windows hat die Art und Weise, wie Menschen Computer benutzen, revolutioniert, indem es ihnen den einfachen Zugriff auf Daten und Anwendungen ermöglicht. Es hat zudem die Verbindung mit dem Internet und den Zugang zu einer Fülle von Ressourcen und Wissen erleichtert, was zur Entstehung einer besser vernetzten und informierten globalen Gesellschaft beigetragen hat. Das Windows-Betriebssystem ist zu einem Eckpfeiler der modernen Technologie geworden.

In der vorliegenden Bachelor-These wird auf die Problemstellung der Analyse des Encrypting File System (EFS) von Windows in Bezug auf verschiedene forensische Anwendungen eingegangen. In diesem Bereich besteht eine Lücke in der Forschung, die im Rahmen dieser Bachelorarbeit aufgegriffen werden soll.

Das Thema ist besonders interessant, da verschlüsselte Dateien, wenn sie nicht als solche gekennzeichnet werden, in der Praxis übersehen oder mit beschädigten Dateien verwechselt werden können. Infolgedessen können sie nicht bewertet werden. Dies kann schwerwiegende Folgen haben, da wichtige Informationen im Zusammenhang mit dem Fall fehlen und somit die Genauigkeit der Bewertung beeinträchtigt werden kann.

Das gilt insbesondere für große Datensätze von Dateien, da es unter Umständen schwierig ist, nicht erkannte Dateien manuell zu identifizieren. Dies führt dazu, dass sie übersehen oder falsch gelabelt werden. Infolge dessen können Chancen zur Identifizierung potenzieller Bedrohungen verpasst werden.

Ziel dieser Arbeit ist es, das Potenzial des EFS zur Speicherung sensibler Informationen zu erkunden und die Möglichkeiten zu untersuchen, dieselben Informationen aus dem EFS für forensische Zwecke zu extrahieren. Dabei werden die unterschiedlichen Vorgehensweisen der verschiedenen Anwendungen analysiert. Außerdem wird untersucht, ob sie verschlüsselte Dateien erkennen und entschlüsseln können.

Die folgende Forschungsfrage soll im Rahmen der Bachelorarbeit beantwortet werden: Inwieweit können die ausgewählten forensischen Anwendungen die EFS-verschlüsselten Dateien erkennen und entschlüsseln?

Es werden verschiedene Aspekte beleuchtet, darunter die Geschichte und Entwicklung von Windows sowie seine Sicherheitsfunktionen.

Die Arbeit beginnt mit einem Abriss der Geschichte von Windows. Sie behandelt die Entwicklung von den frühen Versionen bis zur aktuellen Version und untersucht die wichtigsten Meilensteine, die zu seiner Verbesserung beigetragen haben. Danach wird auf die Verschlüsselung und die verfügbaren Verschlüsselungsmethoden unter Windows eingegangen. Der Schwerpunkt liegt auf dem Vergleich verschiedener forensischer Anwendungen zum Anzeigen und Entschlüsseln von EFS-verschlüsselten Dateien.

2 Grundlagen

In verschiedenen Datenverarbeitungsumgebungen sind Verschlüsselungstechniken für die Gewährleistung von Datensicherheit und Vertraulichkeit unerlässlich. Einer Umfrage zufolge haben im Jahr 2022 fast 40 Prozent der Teilnehmer 21 bis 40 Prozent ihrer sensiblen Daten in der Cloud verschlüsselt (Thales Group, 2022). Die Verwendung von Verschlüsselung in Windows-Betriebssystemen bietet einen grundlegenden Schutz vor unbefugtem Zugriff auf sensible Daten.

Der nächste Abschnitt enthält einen chronologischen Überblick über die verschiedenen Versionen des Windows-Betriebssystems sowie eine Beschreibung der verschiedenen Verschlüsselungsmethoden, die zum Schutz von Benutzerdaten eingesetzt werden können. Des Weiteren werden die allgemeineren Konzepte der Verschlüsselung behandelt, welche auch auf eine Vielzahl anderer Technologien anwendbar sind.

2.1 Windows

In den 1980er Jahren wurde das Microsoft Disk Operating System (MS-DOS) von IBM und Microsoft für Personal Computer (PC) erschaffen. Aufgrund der ausschließlichen Verwendung von Befehlen zur Nutzung des Betriebssystems wurde es nicht von der breiten Masse genutzt, da es nicht einfach zu handhaben war. Darum wurde eine Benutzeroberfläche benötigt, welche eine einfache Nutzung ermöglicht. (Faust, 2021)

Um das Erscheinungsbild der Anwendungen zu standardisieren, veröffentlichte Microsoft am 20. November 1985 eine grafische Oberfläche für Windows 1.0 sowie eine standardisierte Art der Darstellung von Anwendungen in Windows (Nadler, 2020). Dies erleichterte den Umgang mit Computern und Software, da die Benutzer nicht mehr lernen mussten, wie man komplizierte Befehlszeilenbefehle verwendet.

Die grafische Benutzeroberfläche (GUI) ermöglichte es den Benutzern auch, visuell mit dem Computer zu interagieren, indem sie auf Symbole und Menüs klicken, anstatt Befehle einzugeben. Ein Hauptaugenmerk des Projekts lag darauf, eine einheitliche Darstellung der Programme zu gewährleisten und die Bedienung der externen Hardware so weit wie möglich zu vereinfachen. (Nadler, 2020)

Nadler (2020) erklärt, dass „[z]um Lieferumfang des Produkts [Microsoft Windows 1.0] […] neben einer Textverarbeitung – Windows Write – und einem Zeichenprogramm – Windows Paint – eine Reihe von Desktopanwendungen wie ein MS-DOS-Dateiverwaltungsprogramm, ein Kalender, ein Karteikasten, ein Notizblock, ein Rechner sowie eine Uhr [gehören]“.

Als Windows 3.0 im Jahr 1990 veröffentlicht wurde, revolutionierte es die Softwareentwicklung und führte zum Aufkommen neuer Hardwarehersteller. In dieser Version von Windows gab es Verbesserungen bei der Grafik, eine verbesserte Benutzeroberfläche, veränderbare Fenster, Zugriff auf mehrere Fenster und eine verbesserte Speicherverwaltung. (heise, o. D.)

Diese Änderungen machten Windows 3.0 im Vergleich zu seinen Vorgängern benutzerfreundlicher und boten eine leistungsfähigere Softwareentwicklung. Dies wiederum ermöglichte leistungsfähigere Computer und öffnete einer Vielzahl von Hardwareherstellern die Tür zum Markt und zur Entwicklung von Computern mit vorinstalliertem Windows (Nadler, 2020). Mit Windows 3.0 hatten Entwickler eine neue Plattform zur Erstellung von Softwareanwendungen, die auf verschiedenen Hardwarekonfigurationen eingesetzt wurden. Dies ermöglichte mehr Herstellern den Markteintritt, da sie ihre eigene Hardware entwickeln konnten, die mit Windows 3.0 kompatibel war. Im Vergleich zu den vorherigen Versionen von Windows wurde durch die verbesserte Grafik, die Benutzeroberfläche und die Speicherverwaltung eine benutzerfreundlichere Erfahrung geschaffen.

Windows 95 war ein großer Durchbruch für Microsoft, da es die erste Version des Betriebssystems war, welche speziell für den PC entwickelt wurde. Es war damit die erste Version von Windows mit einem Startmenü, mit dem Anwendungen und Einstellungen einfach zu öffnen und zu navigieren waren(Nadler, 2020). Durch die Einführung von benutzerfreundlichen Funktionen wie dem Startmenü und der Taskleiste wurde der Umgang mit Computern für normale Benutzer einfacher und zugänglicher, was es beliebter machte. Außerdem ermöglichte es effizienteres Multitasking, da mehrere Anwendungen gleichzeitig genutzt werden konnten, und es war die erste Plattform, die MSN und den Internet Explorer einführte. Dadurch konnten die Benutzer viel einfacher als je zuvor auf das Internet zuzugreifen, auch die Anwendungen konnten leichter miteinander kommunizieren. (Nadler, 2020)

Das Betriebssystem Windows 98 bietet eine einfachere Verbindung zum Internet, Unterstützung für Digital Versatile Discs (DVD) und die Möglichkeit, Universal Serial Bus (USB) -fähige Geräte automatisch zu erkennen. Windows 2000 bot eine verbesserte Stabilität, eine bessere Benutzeroberfläche und Unterstützung für DVD-Player und mobile Computer. (Nadler, 2020)

Windows 2000 Professional kam zu einer Zeit auf den Markt, als das Internet immer beliebter wurde, so dass es mit besserer Internetkompatibilität und Funktionen für die Verbindung mit dem Internet entwickelt wurde. Windows 98 verfügte nicht über die Kompatibilität mit modernerer Hardware und Software, die Windows 2000 bot. Außerdem verfügte Windows 2000 über bessere Sicherheitsfunktionen und eine zuverlässigere Leistung. (Nadler, 2020)

Zu den beliebtesten und am weitesten verbreiteten Betriebssystemen im Jahr 2001 gehörte Windows XP. Die Stabilität des Produkts, die fortschrittlichen Multimedia-

Funktionen, das intuitive Design und die nahtlose Integration mit der neuesten Hardware wurden von Kunden und Unternehmen sehr geschätzt (Nadler, 2020). Diese Version von Windows konnte in den Editionen Home und Professional erworben werden. Windows XP galt als großer Erfolg und wurde bis 2014 offiziell unterstützt (heise, o. D.).

Anfang 2007 ist das Betriebssystem Windows Vista auf den Markt kommen. Dieses ist für sein Aero-Design bekannt. Es umfasst wieder die Start- und Taskleiste und sollte die Bedienung so einfach wie möglich machen. Außerdem wurde das Auffinden und Verwalten von Dateien erleichtert. (Nadler, 2020)

Windows Vista wurde so konzipiert, dass es durch sein intuitives Design, den verbesserten Suchfunktionen und den erweiterten Sicherheitsfunktionen benutzerfreundlicher ist als frühere Windows-Versionen und es den Benutzern erleichtert, zu navigieren und ihre Daten sicher zu speichern.

Die Einführung von Windows 7 im Jahr 2009 brachte eine drastische Verbesserung gegenüber seinem Vorgänger Windows Vista. Diese neue Version bot eine intuitivere Oberfläche für die Benutzer. Zusätzlich zu den Designverbesserungen unterstützte es auch Multitouch-Geräte. (Winhistory, o. D.)

Windows 7 wurde für das Zeitalter des drahtlosen Internets mit Windows Live Services und dem Cloud-Speicher "SkyDrive" entwickelt (Nadler, 2020). So verfügte Windows 7 beispielsweise über eine Funktion zur Freigabe von Dokumenten über das Internet mittels eines Links, mit dem die Benutzer Dokumente einfach an alle Personen mit einer Internetverbindung senden konnten. Windows 7 ermöglichte es den Nutzern, mit Hilfe der Cloud-Speicherfunktion SkyDrive von jedem mit dem Internet verbundenen Computer aus auf ihre Dateien zuzugreifen.

Windows 8 wurde von Microsoft im Oktober 2012 als Nachfolger von Windows 7 eingeführt. Dieses Update enthält eine Touch-Oberfläche anstelle des Startmenüs, einen Startbildschirm mit Kacheln (Winhistory, o. D.). Viele Desktop-Benutzer empfanden den Wechsel vom Standard-Desktop-Format zu diesem neuen Touchscreen-Projekt als verwirrend, und die Änderung löste einige unzufriedene Reaktionen aus, insbesondere bei Geschäftskunden. Darüber hinaus bot der Windows Store den Nutzern eine effizientere Möglichkeit, die benötigten Anwendungen zu finden und herunterzuladen, ohne mehrere Websites durchsuchen zu müssen. (Nadler, 2020)

Im Jahr 2013 brachte Microsoft mit der Veröffentlichung von Windows 8.1 einige traditionelle Desktop-Funktionen und viele Innovationen zurück. Die Rückkehr dieser traditionellen Funktionen wurde von vielen Nutzern begrüßt, die von den ungewohnten Touchscreen-Bedienelementen der ersten Version von Windows 8 frustriert gewesen waren. (Winhistory, o. D.)

Windows 10 brachte das Startmenü hervor, mit dem die Benutzer vertraut waren, behielt aber auch einige der Touch-zentrierten Elemente bei. Außerdem wurden mehrere

Desktops, eine Benachrichtigungszentrale und Cortana, ein von Künstlicher Intelligenz (KI) gestützter Assistent, eingeführt. Mit Windows 10 gab es eine einzige Oberfläche für alle Plattformen - PCs, Tablets und Telefone. Dies ermöglichte den Benutzern einen nahtlosen Wechsel zwischen den Geräten, da das gleiche Betriebssystem verwendet wurde. Sie konnten ein Projekt auf einem Gerät beginnen und auf einem anderen Gerät dort weitermachen, wo sie aufgehört hatten. (Nadler, 2020)

Um einen Anreiz für ein Upgrade von Windows 7 oder 8 zu schaffen, stellte Microsoft das System im ersten Jahr kostenlos zur Verfügung. Dies führte dazu, dass viele Menschen die Software schnell anschafften. Außerdem gab es regelmäßige Updates, die über das Internet bereitgestellt wurden. (Winhistory, o. D.)

Eine der wichtigsten Aktualisierungen von Windows 10 war beispielsweise die Einführung des oben aufgeführten Sprachassistenten Cortana, mit dem die Nutzer über Sprachbefehle auf die Funktionen von Windows 10 zugreifen konnten. Dazu „bietet es höchste Sicherheit, Datenschutz und integriert Technologien wie Mixed Reality, künstliche Intelligenz sowie Funktionen für die kreative Nutzung wie die digitale Stifteingabe", erklärt Nadler (2020). Windows 10 überzeugt zudem mit Funktionen wie Windows Defender, Smartscreen, Windows Firewall und Windows Hello (Nadler, 2020). Laut Microsoft stieg die Zahl der Verbraucher, die Windows Hello zur Anmeldung bei Windows 10 anstelle eines Passworts verwenden, von 69,4 Prozent im Jahr 2019 auf 84,7 Prozent im Jahr 2020 (Microsoft,, 2020).

Windows 10 bietet eine größere Kompatibilität mit Open-Source-Programmen als die Vorgängerversionen, und ermöglicht es Linux, die Graphics Processor Unit (GPU) des Computers für eine leistungsfähigere Verarbeitung zu nutzen. Microsoft Edge nutzt die Chromium-Engine, eine Open-Source-Technologie. Diese Open-Source-Integration macht Windows 10 vielseitiger und ermöglicht Benutzern die Nutzung beliebter Anwendungen wie Google Chrome sowie den Zugriff auf Open-Source-Programme, die eine leistungsfähigere Verarbeitung für Aufgaben wie das maschinelle Lernen ermöglichen. Darüber hinaus bietet die Integration von Windows Defender, Smartscreen und Windows Firewall verbesserte Sicherheit, die in früheren Versionen nicht verfügbar war. (Nadler, 2020)

Das mit Spannung erwartete neue Betriebssystem von Microsoft, Windows 11, wurde im Oktober 2021 veröffentlicht (Nadler, 2020). Diese neue Version stellt einen bedeutenden Schritt nach vorne gegenüber der vorherigen Version, Windows 10, dar.

Zu den wichtigsten neuen Funktionen in Windows 11 gehören nach Panay (2021) eine neu gestaltete visuelle Oberfläche, Unterstützung für Android-Apps über den Amazon Appstore, eine tiefere Integration mit Microsoft Teams und verbesserte Gaming-Funktionen, "[l]ike: DirectX 12 Ultimate, which can enable breathtaking, immersive graphics at high frame rates; DirectStorage for faster load times and more detailed game worlds; and Auto HDR for a wider, more vivid range of colors for a truly captivating visual experience".

DirectX 12 Ultimate unterstützt eine effizientere Grafikverarbeitung und ermöglicht so eine höhere Grafikqualität. DirectStorage kann die Ladezeiten verkürzen, so dass die Spielwelten detaillierter und weitläufiger werden. Auto HDR bietet eine breitere Palette von Farben, die lebendiger und lebensechter aussehen. All dies kann zu einem noch intensiveren Spielerlebnis beitragen.

Als grafische Benutzeroberfläche für MS-DOS hat sich Microsoft Windows seit seiner Einführung im Jahr 1985 dramatisch weiterentwickelt. Das Windows-Betriebssystem dominierte den Desktop-Computermarkt über drei Jahrzehnte, trotz einiger Fehltritte auf dem Weg dorthin. Windows 11, die neueste Version von Microsoft, zeigt das Engagement des Unternehmens, ein einheitliches Computererlebnis zu bieten.

2.2 Verschlüsselungstechniken

Im heutigen digitalen Zeitalter ist die Verschlüsselung wichtiger denn je, um die Sicherheit und den Datenschutz von Informationen zu gewährleisten. Sie wird in verschiedenen Bereichen wie der Kommunikation, dem Finanzwesen, dem Gesundheitswesen und der öffentlichen Sicherheit eingesetzt.

Wie Singh (1999, S. 1) erläutert, mussten die Mächtigen seit Jahrtausenden effizient kommunizieren und gleichzeitig ihre Botschaften vor Feinden geheim halten.

Dies führte zur Entwicklung von Codes und Chiffren, um Nachrichten so zu verschlüsseln, dass nur der vorgesehene Leser sie entziffern konnte. So wurde sichergestellt, dass sensible Informationen vertraulich blieben. Die Regierungen beauftragten Teams mit der Entwicklung komplexer Codes zu Sicherheitszwecken, während der Feind daran arbeitete, sie zu knacken (Singh 1999, S. 4). Es war ein Katz- und Mausspiel zwischen den beiden Seiten, bei dem die Codeentwickler versuchten, die Codeknacker zu überlisten und den Code geheim zu halten.

Die Kryptologie ist die Wissenschaft, die sich mit der sicheren Übertragung und Bewahrung von Informationen beschäftigt. Das Wort *Kryptologie* leitet sich vom griechischen *kryptós*, was "verborgen" bedeutet, und *lógos*, was "Wort" bedeutet, ab. (Lauterschlag, o. D.)

Nach Banoth und Regar (2023, S. 5) ist die Verschlüsselung "[t]he discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modifcation".

Sie umfasst zwei Hauptbereiche. Die Kryptographie, welche sich mit der Verschlüsselung befasst, und die Kryptoanalyse, welche der Entschlüsselung und Dekodierung dient (Lauterschlag, o. D.). Kryptografie ist die Wissenschaft vom Schreiben in Geheimcodes und ein wichtiger Teil der Computersicherheit. Bei der Kryptoanalyse werden mathematische

Techniken eingesetzt, um verschlüsselte Nachrichten zu entschlüsseln, ohne Zugang zum geheimen Schlüssel zu haben.

Banoth und Regar (2023, S. 6) bezeichnen die Kryptoanalyse als „the study of techniques for deciphering encrypted data without having access to the secret data generally needed to do so. Knowing how the system operates and locating a secret key are typically required. Another name for cryptanalysis is codebreaking or cracking the code“.

Die Kryptografie wurde ursprünglich mit der Absicht entwickelt, schriftliche Nachrichten in Zeiten von Konflikten zu schützen. Diese Prinzipien lassen sich jedoch auch auf die Sicherung der Datenübertragungen zwischen Computern sowie den darauf gespeicherten Informationen anwenden. (Lauterschlag, o. D.)

Durch die Verschlüsselung von Daten wird es böswilligen Akteuren schwerer gemacht, auf die Daten zuzugreifen und sie für ihre eigenen Zwecke zu nutzen. Die Kryptografie gewährleistet die Integrität der Daten, so dass im Falle eines Abfangens überprüft werden kann, ob es sich um dieselben Daten handelt, die ursprünglich übertragen wurden.

Wie von Piper (2002, S. 7f) erläutert, beinhaltet die Verschlüsselung die Umwandlung von Klartext (normaler, lesbarer Text) in Chiffretext (verschlüsselter, unlesbarer Text). Dies geschieht unter Verwendung eines bestimmten Algorithmus oder einer Reihe von mathematischen Anweisungen. Die verschlüsselte Nachricht kann nur verstanden werden, wenn ein spezieller Schlüssel an die Personen weitergegeben wird, die zur Einsichtnahme berechtigt sind. Mit Hilfe dieses Schlüssels bleiben die Informationen geheim und sicher vor Manipulationen.

Die Verschlüsselung ist eine wichtige Sicherheitsmaßnahme für die digitale Kommunikation, da sie sicherstellt, dass nur diejenigen, die den richtigen Schlüssel haben, die Daten einsehen und darauf zugreifen können. Ohne Verschlüsselung könnten Daten, die über das Internet gesendet oder auf Computern gespeichert werden, von jedem eingesehen werden, der Zugang zum Computernetzwerk oder Gerät hat. Verschlüsselung hilft, eine Vielzahl von Aktivitäten wie Online-Banking oder und E-Mail-Versand zu sichern und den unbefugten Zugriff auf die persönlichen Daten einer Person zu verhindern.

Es gibt im Bereich der Kryptografie zwei primäre Verschlüsselungsoptionen: symmetrische und asymmetrische Verschlüsselung (Piper und Murphy, 2002, S. 9). Beide Methoden gelten als sicher und werden je nach den Sicherheitsanforderungen an die Daten in unterschiedlichen Situationen eingesetzt.

2.2.1 Symmetrische Verschlüsselung

Die symmetrische Verschlüsselung ist eine Form der Kryptografie, bei der ein Schlüssel sowohl für die Verschlüsselung, als auch für die Entschlüsselung verwendet wird (Piper und Murphy, 2002, S. 10).

Wie von Zhang (2021, S. 618) erklärt und in Abbildung 1 ersichtlich, kombiniert der Benutzer beim symmetrischen Verschlüsselungsalgorithmus den Klartext bzw. die Originaldaten mit einem Schlüssel und einem bestimmten Verschlüsselungsalgorithmus, um ihn in einen unlesbaren Chiffretext zu verwandeln. Um den Chiffretext zu decodieren, muss eine Person nach Erhalt des Chiffriertextes den Verschlüsselungsschlüssel und die Umkehrung desselben Algorithmus verwenden, um ihn zu entschlüsseln und in seine ursprüngliche Form, den Klartext, umzuwandeln. Die Schlüsselübergabe findet über einen geeigneten sicheren Kanal statt. Der Schlüssel stellt sicher, dass nur befugte Personen auf den Inhalt der Nachricht zugreifen können.

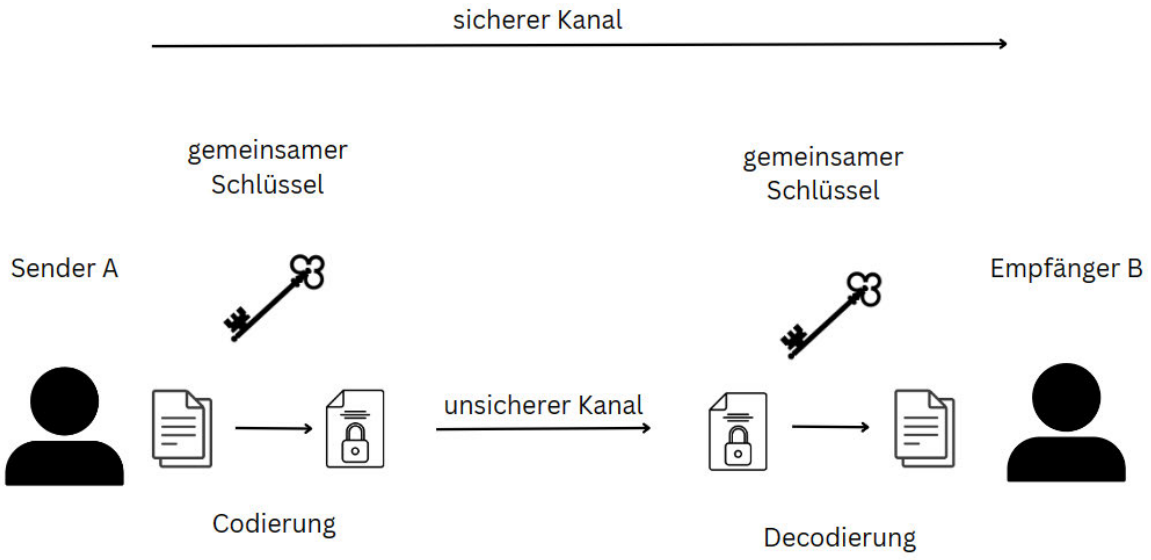


Abbildung 1: Symmetrische Verschlüsselung

Zhang (2021, S. 618) nennt als Vorteile der symmetrischen Verschlüsselung folgende Punkte: Die symmetrische Verschlüsselung ist schneller als andere Verschlüsselungstypen, da ein einziger Schlüssel sowohl für die Verschlüsselung als auch für die Entschlüsselung der Daten verwendet wird. Außerdem ist die symmetrische Verschlüsselung im Vergleich zur asymmetrischen Verschlüsselung ressourceneffizienter, da sie beim Ver- und Entschlüsseln von Daten weniger Rechenleistung benötigt. Aufgrund der Tatsache, dass für die Ver- und Entschlüsselung derselbe Schlüssel verwendet wird, ist die Verwaltung der Schlüssel einfacher. Die Sicherheit der symmetrischen Verschlüsselung beruht darauf, dass der Schlüssel geheim gehalten und nicht unerlaubt an Dritte weitergegeben wird.

Zu den symmetrischen Kryptoverfahren gehören Stromchiffren und Blockchiffren. Stromchiffren sind zum Beispiel der Caesar-Code, der Vernam-Code oder die Vignere-Chiffre. Zu den Blockchiffren gehören der Data Encryption Standard (DES) und der International Data Encryption Algorithm (IDEA).

Stromchiffren erzeugen eine Folge von Bits, die zur Verschlüsselung von Daten verwendet werden, und zwar Bit für Bit, während Blockchiffren einen Bitblock fester Länge zur Verschlüsselung von Daten verwenden (Paar und Pelzl, 2016, S.33f). Somit sind sie schneller und einfacher zu verwenden als Stromchiffren.

2.2.2 Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung, auch bekannt als Public-Key-Verschlüsselung, werden zwei verschiedene Schlüssel für die Ver- und Entschlüsselung von Daten verwendet (Abb. 2). Dieses System arbeitet mit einem öffentlichen und einem privaten Schlüssel. Es ist zwingend erforderlich, dass der geheime Schlüssel nur von seinem ursprünglichen Besitzer aufbewahrt und niemandem sonst offenbart wird; andererseits kann der öffentliche Schlüssel an jeden geschickt werden, der danach fragt. (Zhang, 2021, S. 619)

Die Schritte für die asymmetrische Verschlüsselung sind in Abbildung 2 ersichtlich. Absender A erhält den öffentlichen Schlüssel des Empfängers B aus einer zuverlässigen Quelle. Nachdem er den Schlüssel erhalten hat, verwendete A den öffentlichen Schlüssel von B, um die Nachricht zu verschlüsseln. Nun ist ein Chiffretext, welcher nur mit Hilfe des privaten Schlüssels, den ausschließlich B besitzt, entschlüsselt werden kann.

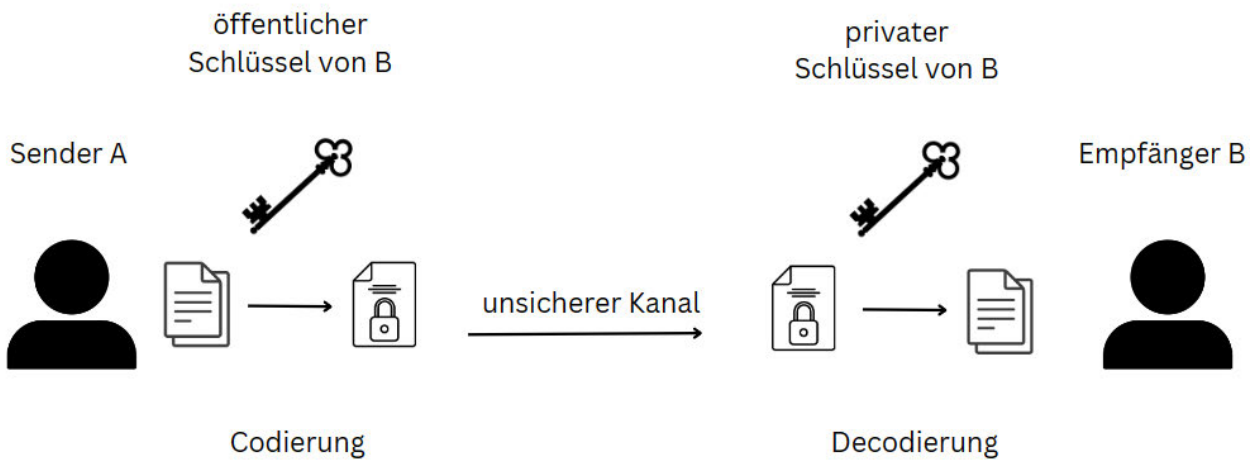


Abbildung 2: Asymmetrische Verschlüsselung

Die asymmetrische Verschlüsselung bietet eine höhere Sicherheit als die symmetrische Verschlüsselung, da der private Schlüssel geheim gehalten wird und für andere Parteien schwer zugänglich ist (Zhang, 2021, S. 619).

Beispiele für asymmetrische Verschlüsselungsmethoden sind Rivest-Shamir-Adleman (RSA) und El Gamal.

2.3 Verschlüsselungsmöglichkeiten unter Windows

Windows bietet zwei integrierte Sicherheitsmaßnahmen, die die Verschlüsselung von Dateien im Betriebssystem ermöglichen und den unbefugten Zugriff auf Daten verhindern.

Die erste Option ist das Encrypting File System (EFS), welches sich am besten für die Verschlüsselung kleiner Dateien eignet. Der BitLocker hingegen wurde entwickelt, um eine ganze Festplatte zu verschlüsseln, was es zur besseren Wahl für größere Dateien oder ganze Laufwerke macht.

EFS ist eine Verschlüsselungsmethode für Dateien oder Ordner auf der Ebene des New Technology File System (NTFS) und wurde erstmals mit Windows 2000 eingeführt. EFS verwendet das Betriebssystem, um Dateien zu verschlüsseln und zu entschlüsseln, während sie auf den physischen Speicher geschrieben oder von ihm gelesen werden. Mit den Versionen ab Windows XP bietet Microsoft zuverlässige digitale Schutzmechanismen, mehr Verschlüsselungsfunktionen und das File Sharing an. (Coles und Landrum, 2009, S. 137)

Das EFS nutzt ein hybrides Verfahren mit einem asymmetrischen RSA-Public-Key-Verfahren und einem symmetrischen DESX bzw. 3DES (Fickert, et al., 2003, S. 224).

Bei dem EFS wird jedem Benutzer ein eindeutiges Paar von öffentlichen und privaten Schlüsseln zugewiesen. Von X.509 ausgestellte Zertifikate werden von EFS unterstützt. Ein Windows-Rechner kann ein selbstsigniertes Zertifikat erstellen, ein digitales Dokument, welches eine Identität an einen öffentlichen Schlüssel bindet. Die Certification Authority (CA) einer Public Key Infrastructure (PKI) ist eine Organisation, die digitale Zertifikate ausstellt, mit denen die Identität einer Person, eines Servers oder einer Website überprüft werden kann. (Pohlmann, et al., 2007, S. 41)

Durch die Speicherung des Zertifikats und des Schlüssels in einem lokalen Benutzerprofil kann der Benutzer von jedem Rechner aus, auf dem er angemeldet ist, auf das Zertifikat und den Schlüssel zugreifen (Pohlmann, et al., 2007, S. 41).

Die Schritte der Verschlüsselung sind in Abbildung 3 ersichtlich. Für jede Datei wird ein eindeutiger symmetrischer Dateiverschlüsselungsschlüssel, der File Encryption Key (FEK), erzeugt. Nach Erhalt des FEK wird die Datei mittels DESX bzw. 3DES-Verschlüsselung verschlüsselt. Der FEK ist der Schlüssel, der zum Verschlüsseln der Datei verwendet wird. Der öffentliche Schlüssel des Benutzers wird zum Verschlüsseln des FEK verwendet, so dass nur der Benutzer mit dem entsprechenden privaten Schlüssel die Datei öffnen kann. (Bucholz und Parkes, 2001, S. 3)

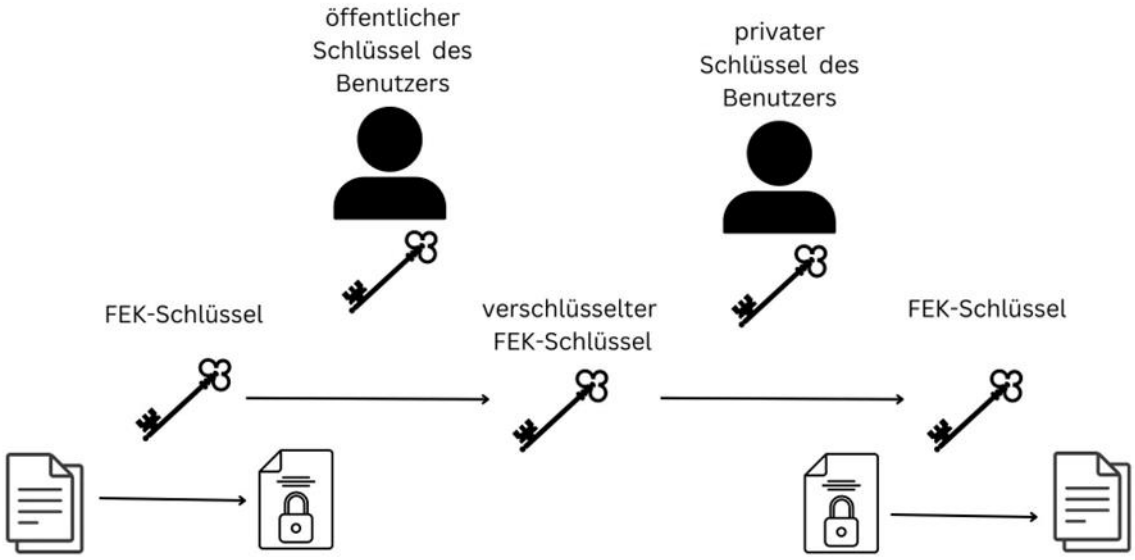


Abbildung 3: Schema der Verschlüsselung mit dem EFS

Ein öffentlicher Schlüssel des Wiederherstellungsagenten, des data recovery agents (DRA), wird ebenfalls zur Verschlüsselung des FEK verwendet (Bucholz und Parkes 2001, S. 3). Der DRA kann seinen öffentlichen Schlüssel verwenden, um den FEK zu entschlüsseln, falls der Benutzer seinen privaten Schlüssel verloren hat. Dies bietet eine zusätzliche Sicherheitsebene für die Datei.

Der Schlüssel wird in den Metadaten der Datei gespeichert, und wenn der Benutzer mit der entsprechenden Sicherheitsfreigabe versucht, die Datei zu öffnen, ruft das NTFS das EFS auf, um den Schlüssel zu extrahieren und die Datei automatisch zu entschlüsseln. (Microsoft, 2021)

Das bedeutet, dass der FEK ohne den privaten Schlüssel des Benutzers nicht entschlüsselt werden kann und die Datei nicht zugänglich ist. Falls der private Schlüssel des Benutzers verloren geht oder gestohlen wird, kann der DRA seinen privaten Schlüssel verwenden, um den FEK zu entschlüsseln.

Kroschel (2010) nennt als einen Nachteil des EFS „die Einsehbarkeit der gesamten Verzeichnisstruktur; die Verschlüsselung tritt erst beim Zugriff auf die Dateiinhalte in Aktion“ und Fickert et al. (2003, S. 227) nennt als größtes Risiko den Verlust des privaten Schlüssels des Benutzers.

Beim hybriden Verschlüsselungssystem wird die symmetrische Verschlüsselung zur schnellen Ver- und Entschlüsselung großer Datenmengen verwendet, während die asymmetrische Verschlüsselung dafür sorgt, dass der bei der symmetrischen Verschlüsselung

verwendete Schlüssel sicher ist und nur den autorisierten Parteien zur Verfügung steht. Dies macht das EFS zu einem sicheren und effizienten Verschlüsselungssystem.

Die andere integrierte Verschlüsselungsmethode ist der BitLocker. Dieser verschlüsselt auf Volume-Ebene, sodass ganze Partitionen bzw. Volumes verschlüsselt werden können. Durch die Verschlüsselung aller Daten auf der Partition oder dem Volume verhindert es den unbefugten Zugriff auf Dateien. BitLocker verwendet den Advanced Encryption Standard (AES) Algorithmus mit einem 256-Bit-Schlüssel. (Tan, et al., 2020, S. 1071)

Der BitLocker baut auf das Trusted Computing auf und nutzt ein Trusted Platform Module (TPM) (Steffan, et al., 2007, S. 3). Das TPM ist ein in die Hardware eingebetteter Sicherheitschip, welcher kritische Daten, wie Passwörter, Kryptographie Schlüssel, Zertifikate, etc. speichert (Intel, o. D.).

Der TPM-Chip speichert die kryptografischen Schlüssel sicher und verhindert, dass sie manipuliert oder gestohlen werden. Er hilft auch bei der Überprüfung der Authentizität von Software- und Hardwarekomponenten und stellt sicher, dass diese nicht manipuliert oder beeinträchtigt werden.

Steffan et al. (2007, S. 10) haben erläutert, dass die Verschlüsselung einzelner Dateien, wie bei EFS, die mit diesen Dateien verbundenen Metadaten nicht schützt. Das bedeutet, selbst wenn die eigentliche Datei verschlüsselt ist, können die zugehörigen Daten wie Dateiname, Erweiterung und Erstellungsdatum immer noch eingesehen und zur Identifizierung der Datei verwendet werden. Die einzige Möglichkeit, die Sicherheit aller Daten zu gewährleisten, besteht demnach in der Verschlüsselung ganzer Datenspeicher-Container oder Festplatten. Durch die Verschlüsselung des gesamten Datenspeichers oder der Festplatte werden alle zugehörigen Daten und die eigentliche Datei verschlüsselt, wodurch sichergestellt wird, dass keine vertraulichen Informationen nach außen dringen, selbst wenn die Datei nicht entschlüsselt wird.

EFS und BitLocker sind beides Verschlüsselungstechnologien für Windows, jedoch mit unterschiedlichen Anwendungsbereichen und Funktionalitäten. Welches der beiden besser geeignet ist, hängt von den spezifischen Anforderungen und dem gewünschten Sicherheitsniveau ab. EFS ist am besten geeignet, wenn eine kleine Anzahl von Dateien oder Ordnern mit sensiblen Daten verschlüsselt werden soll, wie beispielsweise Steuerunterlagen. BitLocker ist besser geeignet, wenn ganze Datenträger verschlüsselt werden sollen, wie zum Beispiel das Systemlaufwerk oder ein externes USB-Laufwerk.

Weitere integrierte Datenschutzmechanismen in Windows sind beispielsweise der Microsoft Windows Defender, Windows Hello oder Windows Device Guard. Microsoft Windows Defender bietet unter anderem ein Schutzprogramm, die Firewall und einen VPN (Voß und Shim, 2022). Windows Hello ermöglicht zusätzliche Authentifizierungsmechanismen, wie Anmeldeoptionen per Iriserkennung, Fingerabdruck oder Stimme, um die Sicherheit

der Daten zu gewährleisten (Gross-Bajohr, 2023). Windows Device Guard bietet Schutz vor Schadsoftware, indem es unbekannte Anwendungen blockiert (Joos, 2017).

Im Rahmen dieser Arbeit wird die Verschlüsselung einzelner Dateien mit Hilfe des Encrypting File System behandelt.

3 Methoden

In diesem Abschnitt wird die Erstellung des verschlüsselten Ordners, die Erstellung des Images und seine Analyse beschrieben. Es werden verschiedene forensische Werkzeuge vorgestellt und zur Untersuchung des Abbilds eingesetzt.

3.1 Vorbereitung

Sowohl das EFS als auch die BitLocker-Laufwerksverschlüsselung werden in den Windows Home-Editionen nicht unterstützt. EFS ist in den Editionen Windows Pro, Education und Enterprise verfügbar, daher wurden die Tests mit der Windows 10 Pro-Edition durchgeführt.

3.1.1.1 Vorbereitung der Festplatte

Um zu testen, ob sich das Wipen von Platten auf ihre Entschlüsselung auswirkt, werden zwei Versuche durchgeführt. Der erste Versuch wird mit einer Partition gemacht, die vorher gewipt wurde. Der zweite Versuch wird mit der eingebauten Partition C:/ gemacht.

Beim Wipen einer Festplatte werden alle Daten, welche sich auf der Festplatte befinden, gelöscht. Um dies zu erreichen, kann auf Windows 10 die Anwendung diskpart.exe genutzt werden. Diese Anwendung dient der Verwaltung aller Laufwerke des Computers (Microsoft, 2023).

Zu Beginn wird mit dem Befehl *list disk* eine Liste von „Datenträgern, Partitionen auf einem Datenträger, Volumes auf einem Datenträger oder von virtuellen Festplatten (VHDs)“ angezeigt (Microsoft, 2023). Wie in Abbildung 4 ersichtlich, wurden hier drei Datenträger angezeigt.

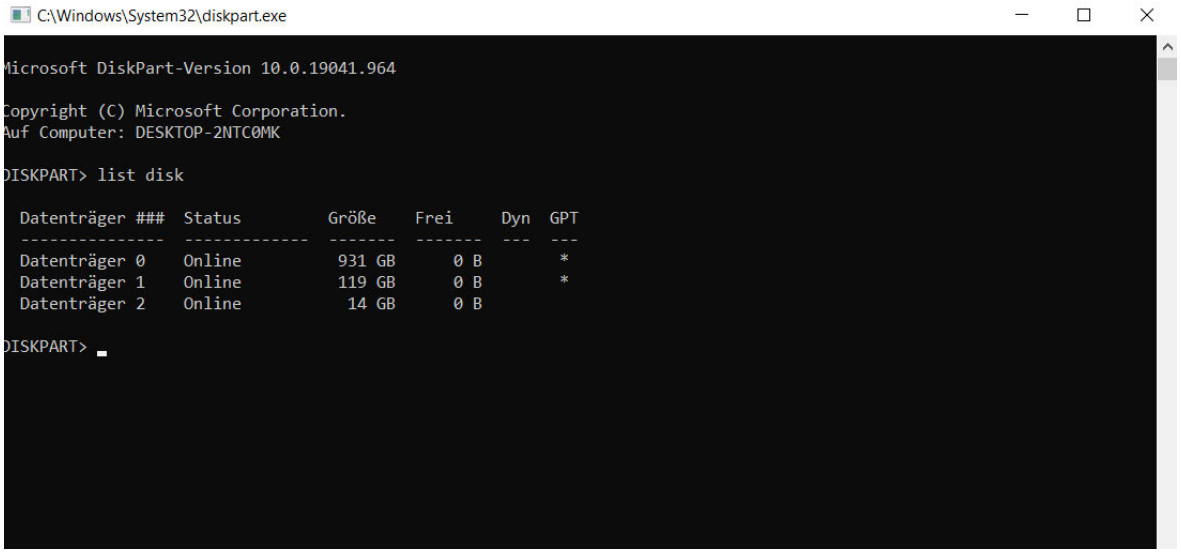


Abbildung 4: Ausführung des Befehls list disk

Mit dem Befehl *select disk 0* wird der Datenträger 0 ausgewählt, um mit diesem zu arbeiten (Microsoft, 2023).

Um zu überprüfen, ob der korrekte Datenträger ausgewählt wurde, wird der Befehl *detail disk* verwendet (Abb. 5). Dieser Befehl zeigt Informationen zum gewählten Datenträger an (Microsoft, 2023).

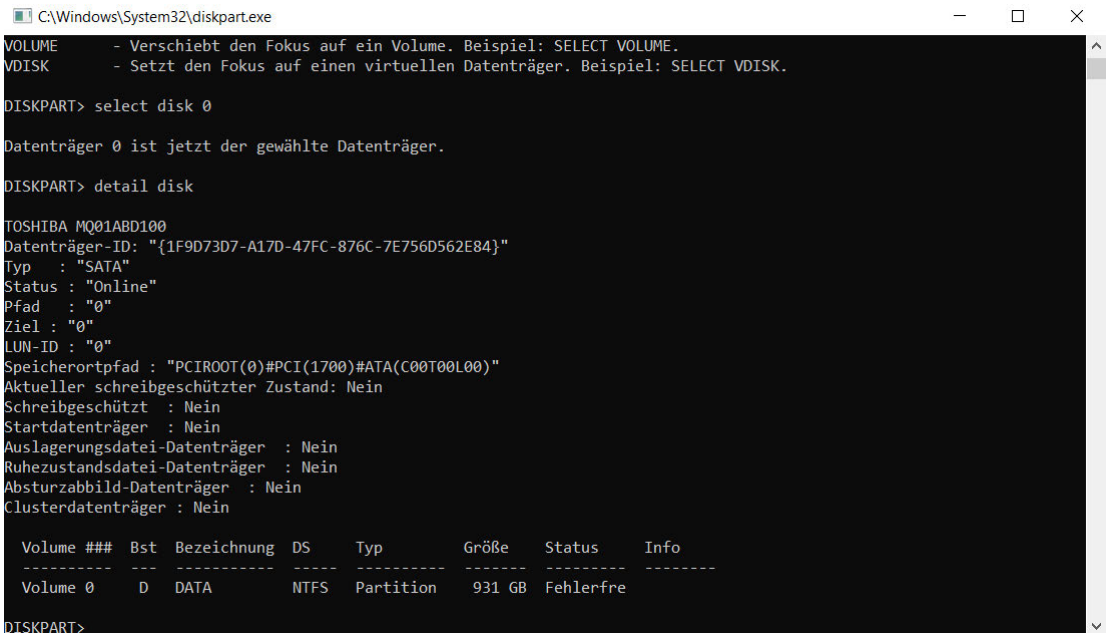


Abbildung 5: Ausführung des Befehls detail disk

Schlussendlich wird mittels des Befehls *clean all* alle Daten des Datenträgers gelöscht, das bedeutet, es werden alle Daten mit Nullen überschrieben (Yang, 2023).

3.1.1.2 Erstellung des versschlüsselten Ordners

Nachdem die Festplatte aufgeräumt wurde, wird der verschlüsselte Ordner mit dem EFS erstellt. Dazu legt man einen neuen Ordner an.

In dieser Arbeit wurden zwei verschiedene Ordner verschlüsselt. Der Ordner Alpha wurde zusammen mit seinem Inhalt verschlüsselt. Durch die Verschlüsselung des Ordners werden die darin gespeicherten Dateien automatisch mitverschlüsselt. In diesem Ordner befinden sich drei Dateien: asymm.png, Book.pdf und HSMW-Graduation-Vorlage_docx.zip.

Der zweite Ordner Beta enthält die Datei Hinweise_Antrag_Abschlussarbeit_digital_Stand_09.03.2021.pdf und wird verschlüsselt, bevor die Datei eingefügt wird. Ziel ist es herauszufinden, ob es einen Unterschied macht, ob die Dateien zuerst verschlüsselt werden oder erst später in einen verschlüsselten Ordner eingefügt werden.

Mit einem Linksklick werden die Eigenschaften des Ordners ausgewählt. Um zu den erweiterten Eigenschaften zu gelangen, wird in der Liste die Option *Erweitert* ausgewählt. Im Anschluss wird die Option "Inhalt verschlüsseln, um Daten zu schützen" (Abb. 6) aktiviert.

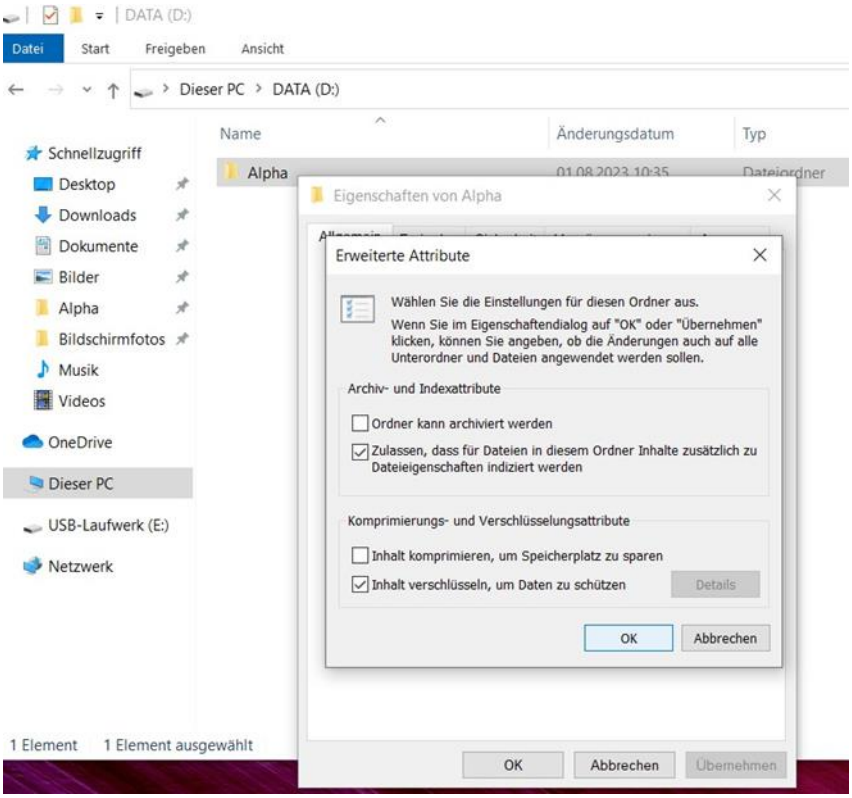


Abbildung 6: Erweiterte Attribute des Ordners

Es wird eine Meldung angezeigt, in welcher der Nutzer aufgefordert wird, seine Präferenzen bezüglich der Verschlüsselung des ausgewählten Ordners und seiner Unterelemente anzugeben. Dabei wird entschieden, ob die Änderungen nur für den Ordner oder auch für

alle untergeordneten Dateien gelten sollen. Nach der Verschlüsselung erscheint ein Vorhängeschloss-Symbol neben dem Ordnersymbol, welches den sicheren Zustand des Ordners anzeigt.

Das bedeutet, dass auch Elemente die nachträglich in den Ordner eingefügt werden, automatisch verschlüsselt werden.

Die Sicherung eines Verzeichnisses kann durch die Speicherung des zugehörigen Dateiverschlüsselungszertifikates und des Schlüssels noch weiter verstärkt werden. Die Sicherung auf einem Wechselmedium ermöglicht den Transport des Schlüssels. Wenn das Benutzerkonto nicht mehr zugänglich ist oder gehackt wurde, kann der Wiederherstellungsschlüssel verwendet werden, um verschlüsselte Informationen zu entsperren.

Im Zertifikatexport-Assistenten wird das gewünschte Format ausgewählt (Abb. 7). In diesem Fall ein privater Informationsaustausch mit Zertifikatsdatenschutz. Anschließend wird die Verschlüsselung und das Password gewählt. Bei der Verschlüsselung entscheidet man zwischen TripleDES-SHA1 und AES256-SHA256. Im gegebenen Fall wurde TripleDES-SHA1 ausgewählt.

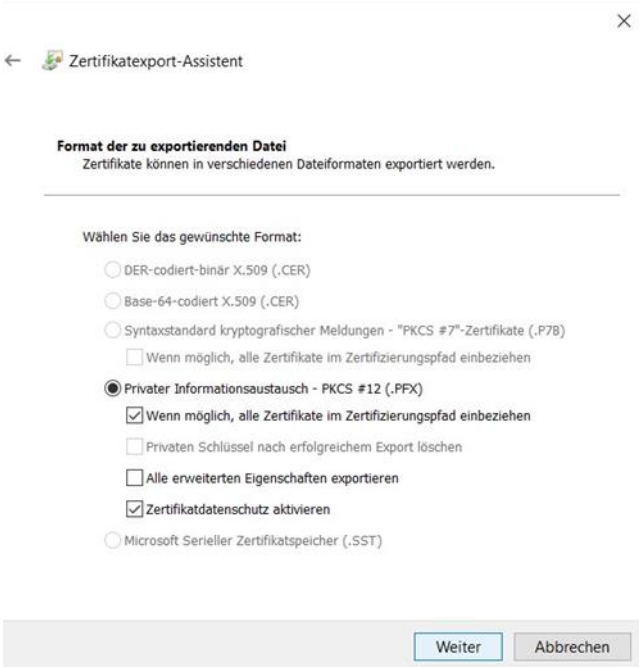


Abbildung 7: Zertifikatexport-Assistent

In dieser Arbeit wurde das Zertifikat unter den Ordner Schlüssel als Schl.pfx gespeichert.

Nachdem alle Änderungen abgeschlossen und bestätigt sind, kann der Prozess des Imaging beginnen.

3.1.1.3 Erstellung des forensische Images

Zur Erstellung des forensischen Images wird der von AccessData bereitgestellte Forensic Toolkit (FTK) Imager genutzt. Der FTK Imager ist ein kostenloses und quelloffenes Softwaretool, das es Benutzern ermöglicht, Images von Speichergeräten zu erstellen und verschiedene andere Aufgaben im Zusammenhang mit der digitalen Forensik durchzuführen. (software.informer, 2013)

Der FTK Imager wird benutzt, um ein forensisch einwandfreies Abbild einer Partition auf einem Speichergerät zu erstellen. Das Image ist eine Block-für-Block-Kopie der Originalpartition, die für forensische Analysen verwendet werden kann. Das von FTK Imager erstellte Abbild wird benutzt, um den Inhalt eines Geräts zu analysieren, ohne es zu verändern. Es kann auch verwendet werden, um gelöschte Dateien wiederherzustellen und digitale Beweise zu analysieren. FTK Imager unterstützt eine Vielzahl von Bildformaten, wie z.B. E01, RAW und DD. Er wird ebenso eingesetzt, um die Integrität eines Bildes zu überprüfen. Zum Beispiel kann FTK Imager bei der Erstellung eines Bildes eine Prüfsumme generieren, um die Integrität des Bildes zu überprüfen, die zu einem späteren Zeitpunkt mit dem Originalbild verglichen werden kann.

Zuerst wird das zu sichernde Speichergerät über eine geeignete Schnittstelle, z. B. ein USB-Kabel, an den Computer angeschlossen. Dabei muss sichergestellt werden, dass das Gerät ordnungsgemäß mit Strom versorgt und von dem Betriebssystem erkannt wird. Es besteht die Möglichkeit den FTK Imager direkt auf einen PC zu installieren und die Sicherung zu starten.

Darauf folgend wird der FTK Imager auf dem eigenen Computer gestartet. Über den Reiter „File“ wird „Create Disk Image“ gewählt. Nun kann der Typ des zu sichernden Speichergerätes ausgewählt werden, wobei zwischen *Physical Drive, Logical Drive, Image File, Contents of a Folder* und *Ferninco Device* unterschieden wird.

Im Anschluss wählt man das Quellgerät, d.h. das zu sichernde Gerät, aus der Liste der verfügbaren Geräte aus. Nach der Eingabe der Informationen zum Fall wird man aufgefordert, den Speicherort für die Imagedatei sowie das Format des Images (z. B. raw, dd oder E01) zu wählen.

Mit dem Klick auf "OK", wird der Imaging-Prozess gestartet. Je nach der Größe des Mediums und der Geschwindigkeit des Computers kann dieser Vorgang einige Zeit in Anspruch nehmen.

Während des Imaging-Prozesses zeigt FTK Imager Fortschrittsbalken an, um darüber zu informieren, wie weit der Imaging-Prozess bereits abgeschlossen ist (Abb. 8).

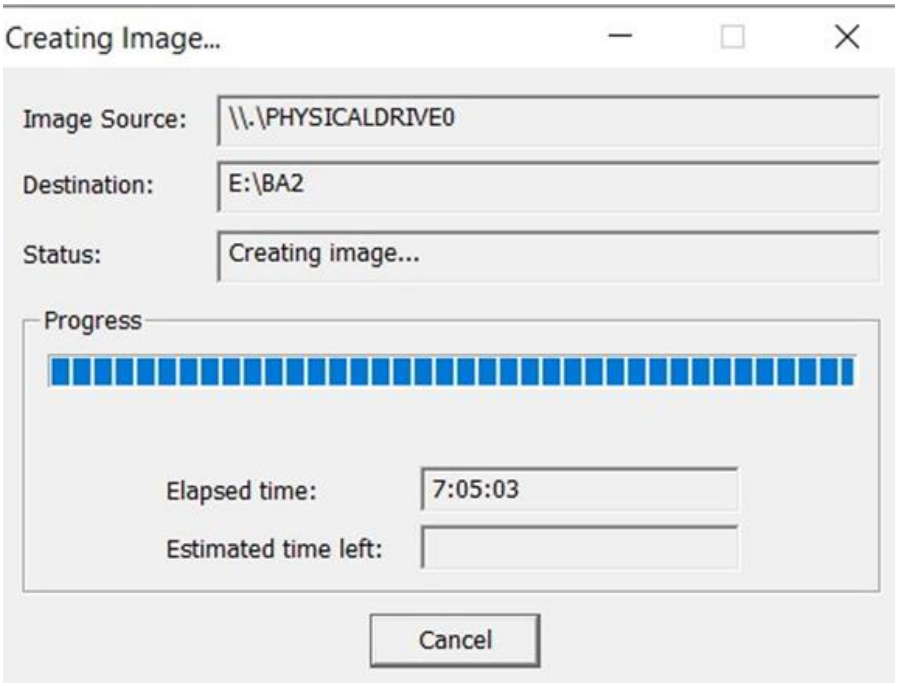


Abbildung 8: Information über den Imaging-Prozess des FTK Imagers

Sobald der Imaging-Vorgang abgeschlossen ist, kann für die Analyse mit forensischen Tools auf die erstellte Datei zugegriffen werden.

3.2 Programme

Forensische Tools spielen eine wichtige Rolle bei Ermittlungen, da sie den Strafverfolgungsbehörden die Informationen liefern, die zur Lösung von Fällen benötigt werden. Durch den Einsatz spezialisierter Tools können gelöschte Dateien wiederhergestellt oder verschlüsselte Dateien entschlüsselt werden. Zu den führenden forensischen Tools gehören X-Ways, Axiom und EnCase.

3.2.1 AXIOM

Magnet AXIOM ist eine forensische Anwendung, welche von Magnet Forensics entwickelt wurde. Sie dient der Analyse von Beweismitteln und der Erstellung von Berichten. AXIOM unterstützt viele verschiedene Datenquellen, wie Smartphone, Computer oder Cloud-Dienste. (Magnet Forensics, 2022)

AXIOM verfügt über unterschiedliche Funktionen, um digitale Beweise intensiv zu untersuchen. Unter anderem können Daten aus digitalen Beweismitteln extrahiert und analysiert werden. Dabei können gelöschte oder versteckte Dateien wiederhergestellt werden. Ein anderer Aspekt ist die Datenvisualisierung. Mithilfe von Diagrammen und Berichten können die analysierten Daten übersichtlicher dargestellt und komplexe Inhalte vereinfacht werden.

Magnet AXIOM besteht aus AXIOM Process und AXIOM Examine. Mittels AXIOM Process können forensische Images von mobilen Geräten, Cloud-Medien oder Computerlaufwerken erstellt werden oder vorhandene Images geladen werden. AXIOM Examine dient der Analyse der Images. Damit können beispielsweise Passwörter entschlüsselt oder Zeitachsen erstellt werden. (Magnet Forensics, 2022)

Für den Test mit dem Programm AXIOM wurde das Image eingelesen und die Beweisanalyse und Artefaktsuche durchgeführt. Nach dem Einlesen des Images suchte das AXIOM-Programm nach Metadaten oder Artefakten, die Beweise liefern könnten. Die Daten werden analysiert, um Muster oder Anomalien zu erkennen, die von Interesse sein können.

Im Anschluss wurde ein Portable Case erstellt, um von zu Hause aus weiterarbeiten zu können. Der Portable Case enthält alle erforderlichen Softwarekomponenten, damit der Benutzer von jedem beliebigen Ort aus auf die Ergebnisse der Beweisanalyse und der Artefaktsuche zugreifen konnte.

Im Programm AXIOM wird die Datei *Book.pdf* im Ordner *Encryption & Credentials* angezeigt (Abb. 9). Die anderen verschlüsselten Dateien bzw. Ordner werden nicht darin angezeigt.

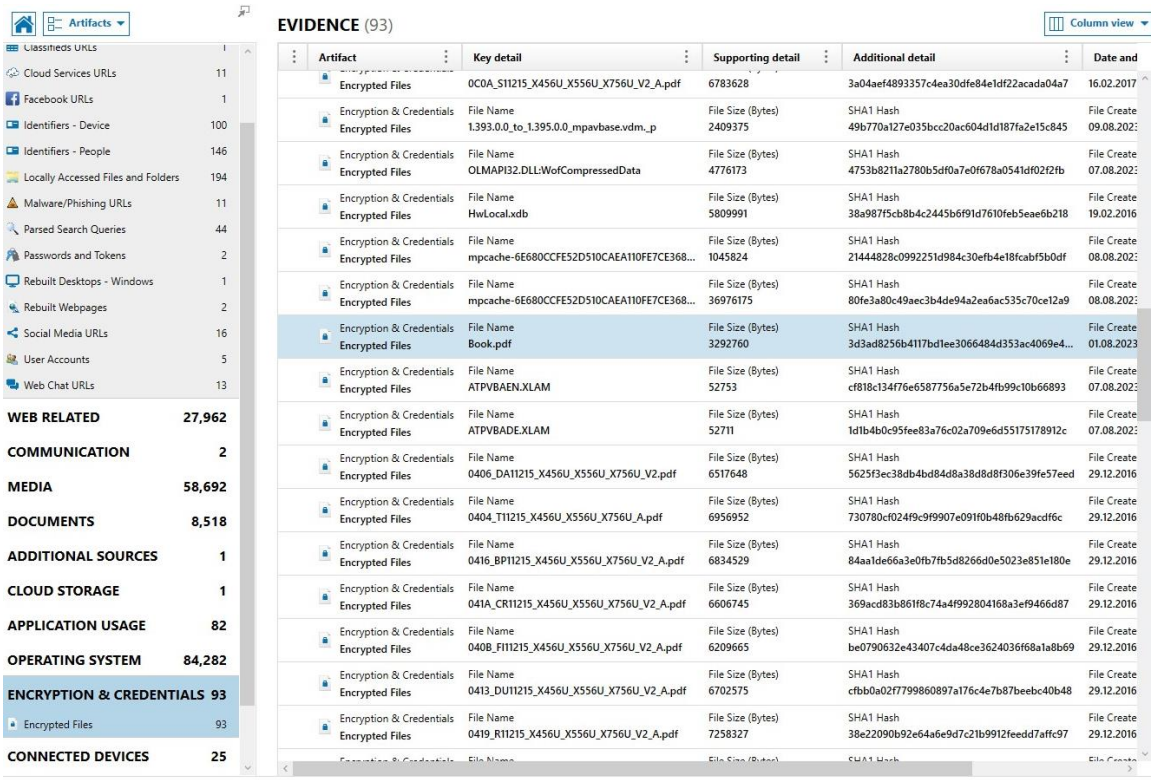


Abbildung 9: Auflistung im Ordner Encryption & Credentials

Bei der Datei *Hinweise_Antrag_Abschlussarbeit_digital_Stand_09.03.2021.pdf* ist in der Vorschau zu sehen, dass die Datei verschlüsselt ist (Abb. 10).

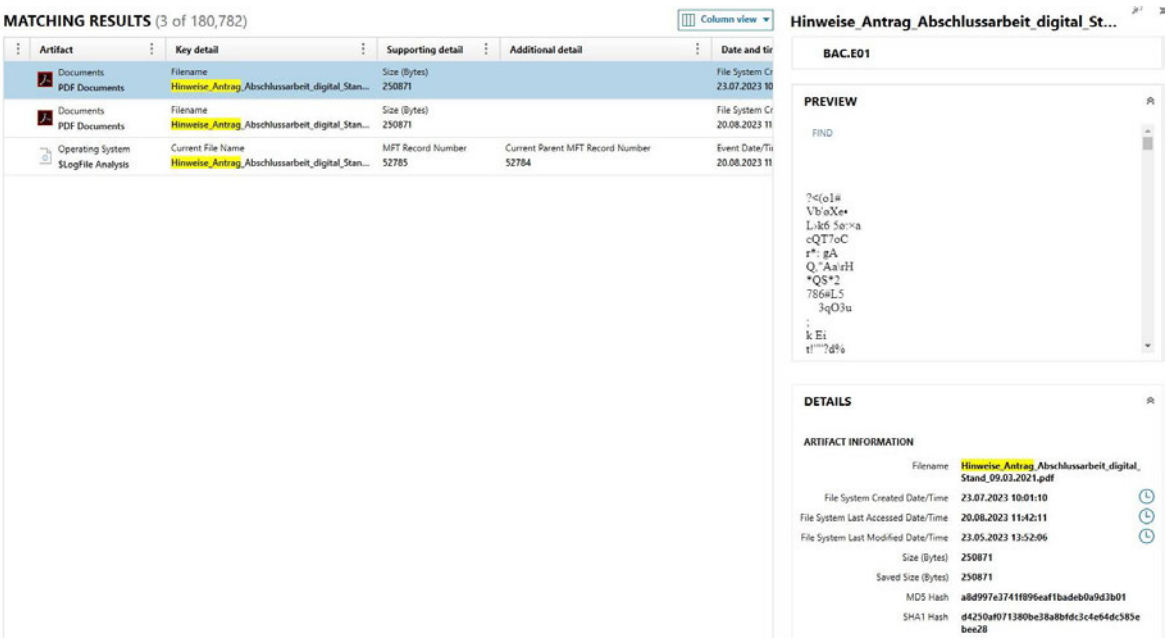


Abbildung 10: Vorschau und Details der Datei Hinweise_Antrag_Abschlussarbeit_digital_Stand_09.03.2021.pdf

Die leeren Vorschaubilder der anderen Dateien zeigen an, dass AXIOM nicht auf die Dateien zugreifen kann. Das bedeutet, dass die Software die Dateien nicht lesen kann, da sie keine Zugriffsrechte auf die Dateien hat und sie daher nicht anzeigen kann.

Die Details der Dateien enthalten die grundlegenden Informationen der Datei, wie Name, Größe, Typ, Artefakttyp, Speicherort, Hashwert und die jeweiligen Zeitstempel (Abb. 11). Diese Daten können verwendet werden, um die verschiedenen Dateitypen in digitalen Beweismitteln zu identifizieren und zu analysieren. Sie können auch verwendet werden, um die Aktivitäten des Benutzers zu bestimmen, der die Dateien erstellt und verändert hat. Diese Informationen sind wichtig, um die digitalen Dateien zu identifizieren, zu authentifizieren und zu verifizieren. Damit können die an der Datei vorgenommenen Änderungen verfolgt und mögliche Manipulationen aufgedeckt, sowie die Aktivität einer bestimmten Datei und ihre Verwendung nachvollzogen werden.

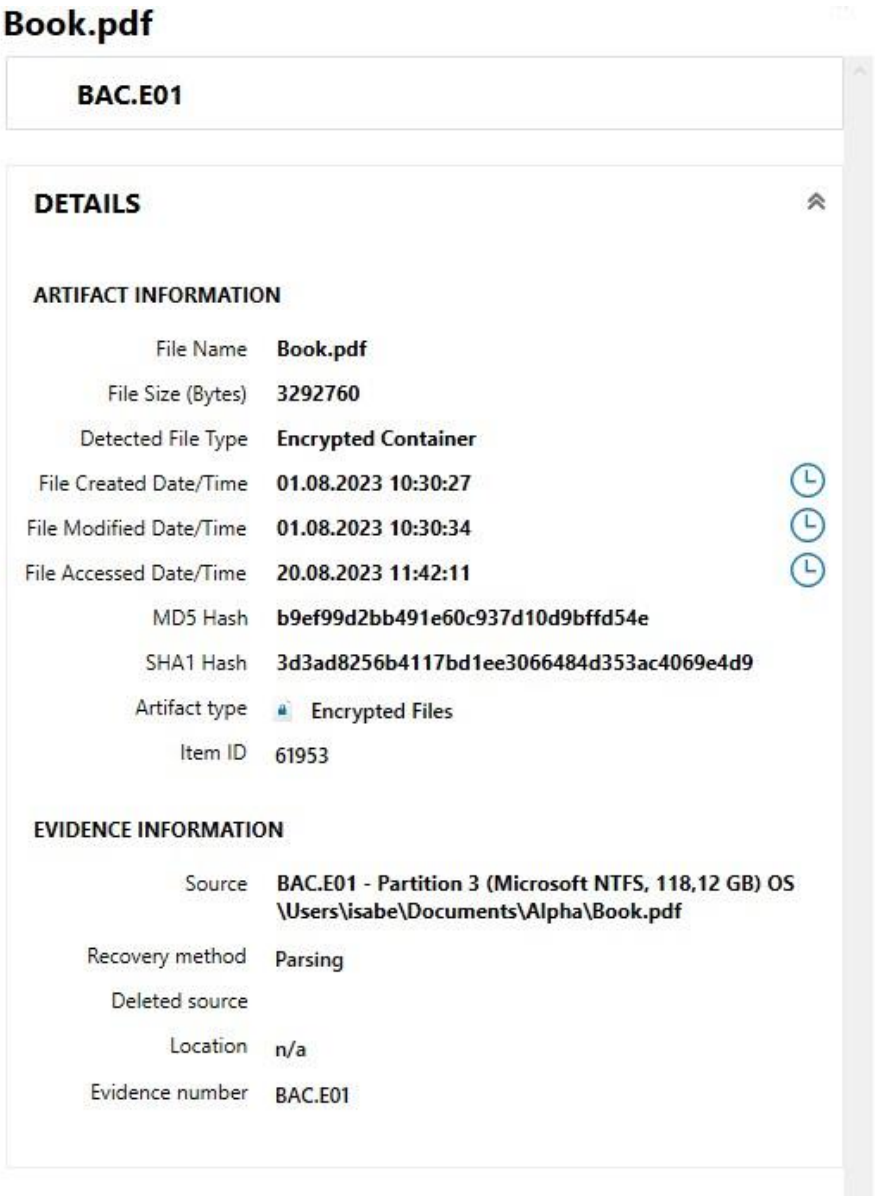


Abbildung 11: Details der Datei Book.pdf

Die AXIOM-Software kennzeichnet eine der vier verschlüsselten Dateien als solche. Die anderen drei waren nicht als verschlüsselt gekennzeichnet. Die Anwendung war nicht in der Lage, die vier Dateien zu entschlüsseln.

3.2.2 X-Ways

X-Ways Forensics von X-Ways Software Technology AG ist eine Anwendung für forensische Analyse (X-Ways, o. D.). Es ist eine leistungsstarke Software, die von Strafverfolgungsbehörden und forensischen Experten weltweit verwendet wird. X-Ways Forensics ist keine Open-Source-Anwendung und kann dementsprechend erst nach Erwerb der Lizenzen eingesetzt werden. Die Anwendung kann von einem USB-Stick ohne Installation auf jedem Windows-System eingesetzt werden und ist insbesondere im Hinblick auf die

deutsche Rechtsprechung zur „rechtssicheren Beweismittelsicherung und -auswertung geeignet“ (X-Ways, o. D.).

X-Ways ermöglicht die effiziente Erfassung von digitalen Beweismitteln aus unterschiedlichen Quellen wie Speicherkarten, Festplatten, USB-Geräten und Netzwerken.

Es können umfassende Analysen durchgeführt werden, um relevante Informationen zu extrahieren. X-Ways besitzt viele leistungsstarke forensische Funktionen, wie Suchfunktionen, Dateisystemanalyse, Datenwiederherstellung, Metadatenextraktion, etc. Des Weiteren können die Daten visualisiert und Berichte erstellt werden.

Die folgenden Versuche werden mit der Version 20.4 durchgeführt.

Bereits in der Vorschau des Ordners Alpha wird darauf hingewiesen, dass dieser verschlüsselt ist (Abb. 12).

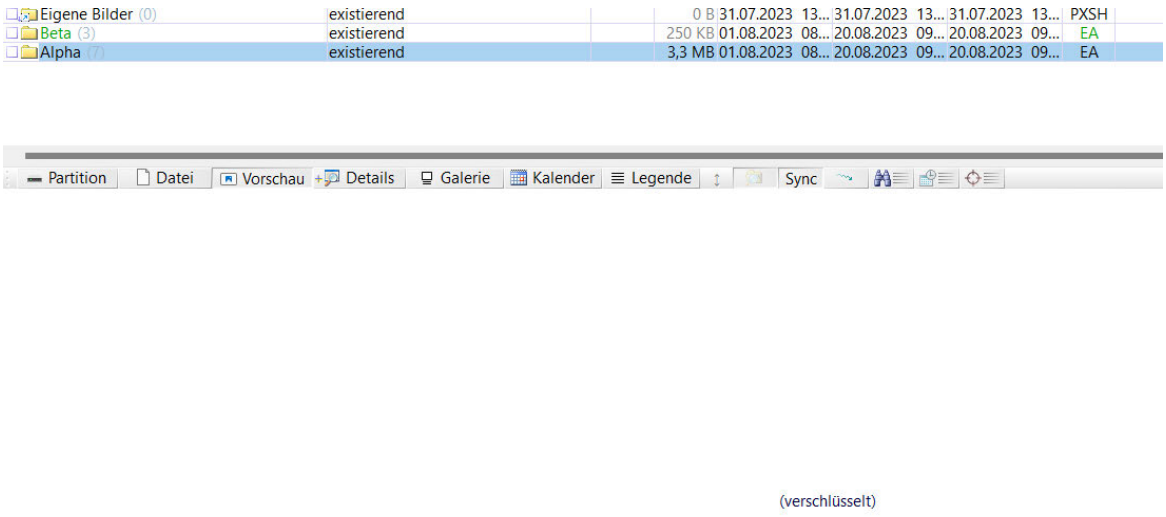


Abbildung 12: Vorschau des Ordners Alpha

Beim Öffnen des verschlüsselten Ordners wird festgestellt, dass es eine neue Datei namens $EFS gibt (Abb. 13).

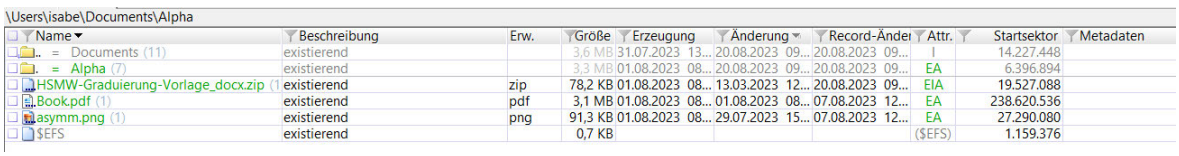


Abbildung 13: Inhalt des Ordners Alpha

Die $EFS-Datei ist eine Datei mit den Verschlüsselungsmetadaten (Abb. 14). Diese beinhalten das Data Decryption Field (DDF). Das DDF des EFS enthält Informationen, welche autorisierten Benutzern die Entschlüsselung der Datei ermöglichen. Es enthält den FEK, der zum Ver- und Entschlüsseln der Datei verwendet wird (Zhou, 2013, S. 2283). Außerdem enthält es den Zertifikats-Thumbprint des Benutzers. Der Thumbprint wird verwendet um zu überprüfen, ob der Benutzer über das richtige Zertifikat für den Zugriff auf die Datei verfügt. Somit wird sichergestellt, dass nur autorisierte Benutzer auf die Datei zugreifen können.

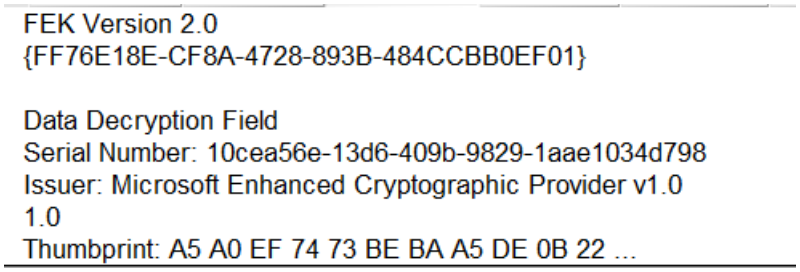


Abbildung 14: Verschlüsselungsmetadaten des Ordners Alpha

Die Seriennummer ist eine eindeutige Kennung für den Verschlüsselungsschlüssel, der zur Verschlüsselung der Dateien verwendet wurde. Durch die Analyse der Seriennummern der beiden Dateien kann festgestellt werden, ob sie mit demselben Schlüssel und somit von derselben Person verschlüsselt wurden. Beim Vergleich der Seriennummer des Ordners Alpha mit der der Ordners Beta, ist festzustellen, dass beide durch denselben Benutzer verschlüsselt wurden (Abb. 15).

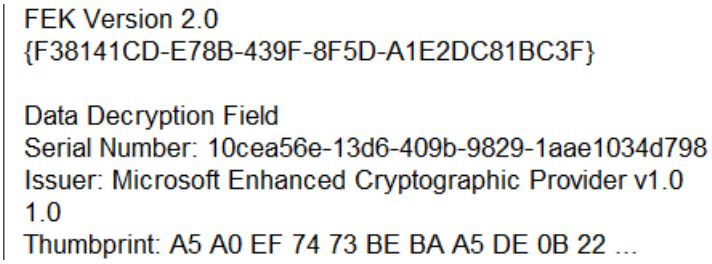


Abbildung 15: Verschlüsselungsmetadaten des Ordners Beta

Die Dateien sind mit dem Attribut E gekennzeichnet. Das E-Attribut wird gesetzt, wenn eine Datei oder ein Verzeichnis auf Dateisystemebene verschlüsselt ist.

Indem man die Partition auswählt und die rekursive Suche aktiviert, werden alle Dateien aus dieser Partition angezeigt. Durch die Verwendung eines Filter ist es möglich alle verschlüsselten Dateien anzuzeigen. Hierfür wird das Filtersymbol neben den Attributen gewählt und ein Häkchen bei "e, e!, E" und bei "e?" gesetzt. Durch die Auswahl dieser Attribute sucht der Filter nach allen Dateien mit Verschlüsselungsattributen und zeigt sie in der Partition an (Abb. 16). So kann der Benutzer alle verschlüsselten Dateien in der Partition leicht identifizieren. Nun können die verschlüsselten Dateien für weitere Analysen ausgewählt werden.

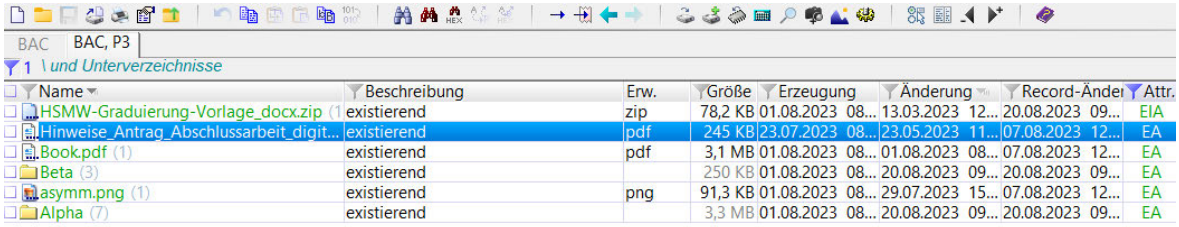


Abbildung 16: Filter der verschlüsselten Dateien

X-Ways hat alle Dateien korrekt als verschlüsselt erkannt. Das Verschlüsselungszertifikat an sich wird nicht als verschlüsselt gekennzeichnet.

Die Dateien können zwar eingesehen werden, sind aber verschlüsselt, so dass nur der verschlüsselte Text zu sehen ist (Abb. 17). Der Chiffretext ist ohne den zum Entschlüsseln erforderlichen Schlüssel nicht entzifferbar. Dadurch wird sichergestellt, dass die Daten sicher sind und nur von denjenigen eingesehen werden können, die über den erforderlichen Zugang verfügen. X-Ways ist nicht in der Lage, die verschlüsselten Dateien zu entschlüsseln.

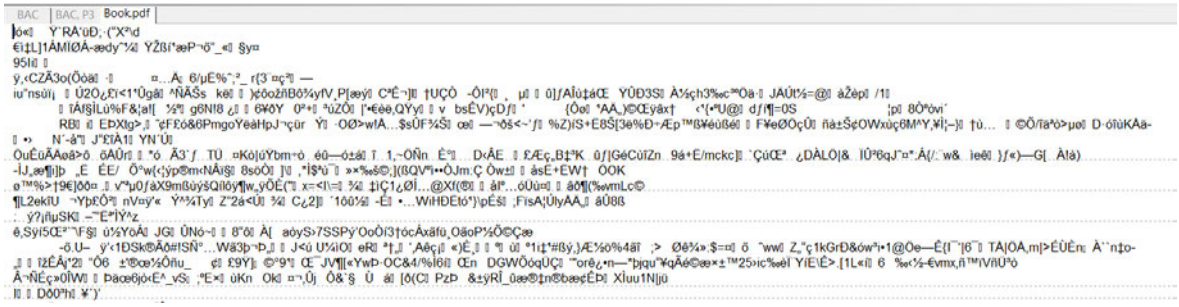


Abbildung 17: Einsicht in die verschlüsselte Datei Book.pdf

3.2.3 Freie Tools

Zusätzlich zu den oben genannten kommerziellen Optionen gibt es viele kostenlose forensische Tools für den Einsatz bei Ermittlungen. Dazu gehören Autopsy, Volatility Framework und The Sleuth Kit, die alle Open-Source-Optionen sind und nützliche Funktionen wie die Suche nach Beweisen oder die Analyse von Disk-Images bieten. Ihnen fehlen zwar einige Funktionen, die kommerzielle Tools bieten, aber sie sind dennoch wertvolle Ressourcen für Ermittler, die nach einer erschwinglichen Option suchen.

3.2.3.1 Autopsy

Autopsy, ein kostenloses und quelloffenes Softwareprogramm, wird von vielen Ermittlern für die Analyse von Images und anderen Beweisquellen verwendet (Adamu, et. al, 2021, S. 104). Es bietet ein großes Set von Werkzeugen, mit denen Ermittler umfassende Untersuchungen durchführen können, von der ersten Beweiserfassung bis zur Erstellung des

Abschlussberichts. Aufgrund seiner Schnelligkeit, Erschwinglichkeit und Benutzerfreundlichkeit ist es sehr beliebt geworden (Raji, et al., 2018, S.2).

Autopsy kann beispielsweise eingesetzt werden, um gelöschte Dateien wiederherzustellen, den Browserverlauf zu analysieren und Netzwerkverbindungen zu identifizieren. Es wird auch zur Analyse von Bildern, E-Mails und anderen Dokumenten verwendet. Darüber hinaus kann Autopsy zur Erstellung detaillierter Berichte benutzt werden, welche in Gerichtsverfahren Anwendung finden.

Nach der Installation ist die Software bereit, für einen Fall verwendet zu werden. Der erste Schritt besteht darin, den Fall einzurichten. Dazu gehört das Anlegen eines neuen Falls, die Angabe von Falldetails und die Auswahl der zu analysierenden Beweismittel. Autopsy unterstützt verschiedene Beweistypen, wie z. B. Festplatten-Images oder einzelne Dateien. Je nachdem wie groß die Datenquelle ist, kann es eine Weile dauern, sie einzulesen und die ausgewählten Module, z.B. Hash Lookup, Picture Analyser, Keyword Search oder Data Source Integrity, zu beenden (Abb. 18).

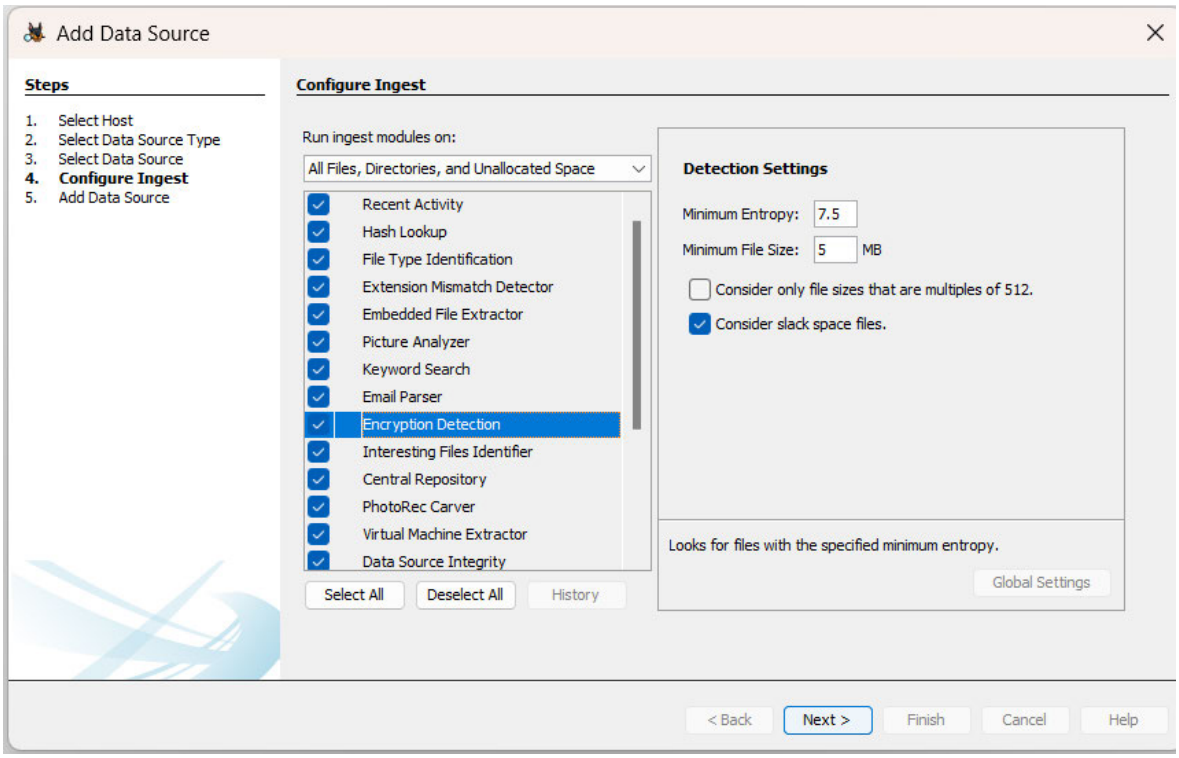


Abbildung 18: Auswahl an Modulen von Autopsy

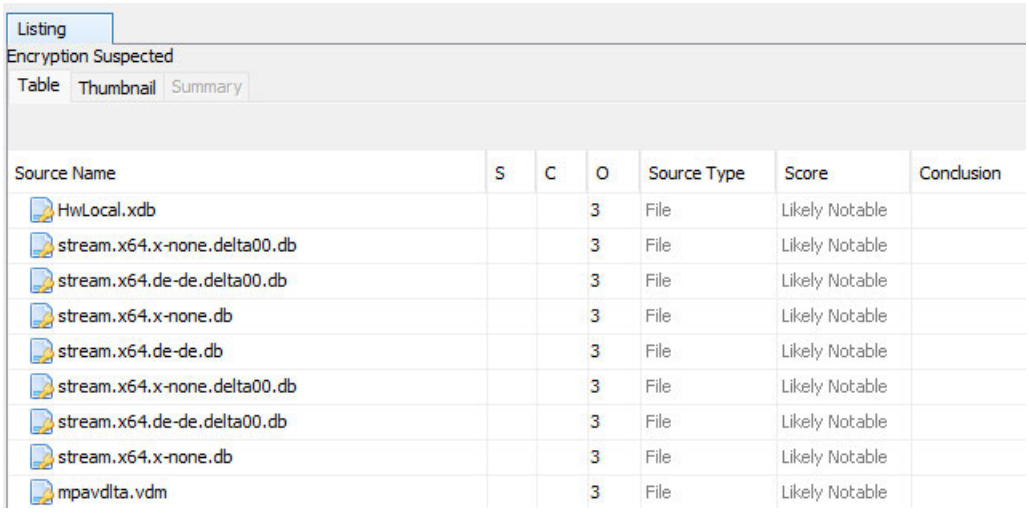
In folgendem Versuch wird mit der Version 4.21.0 gearbeitet.

Die für diese Arbeit wichtigste Analyse ist die *Encryption Detection*. Hierbei kann man in den Einstellungen sowohl die minimale Entropie, als auch die minimale Größe der Datei festlegen. Die Standardeinstellungen sehen eine minimale Entropie von 7,5 und minimale Dateigröße von 5 MB vor (Abb. 18).

Der Algorithmus wurde entwickelt, um nach allen Dateien zu suchen, die einen hohen Grad an Entropie aufweisen, was darauf hindeutet, dass sie verschlüsselt sein könnten. Es sucht auch nach Dateien, die normalerweise für die sichere Speicherung von Daten verwendet werden, z. B. kennwortgeschützte Office-Dateien, PDF-Dateien, Access-Datenbankdateien, BitLocker-Festplatten, SQLCipher und VeraCrypt. (Basis Technologie, 2023)

Im ersten Versuch wurden die Standardeinstellungen übernommen.

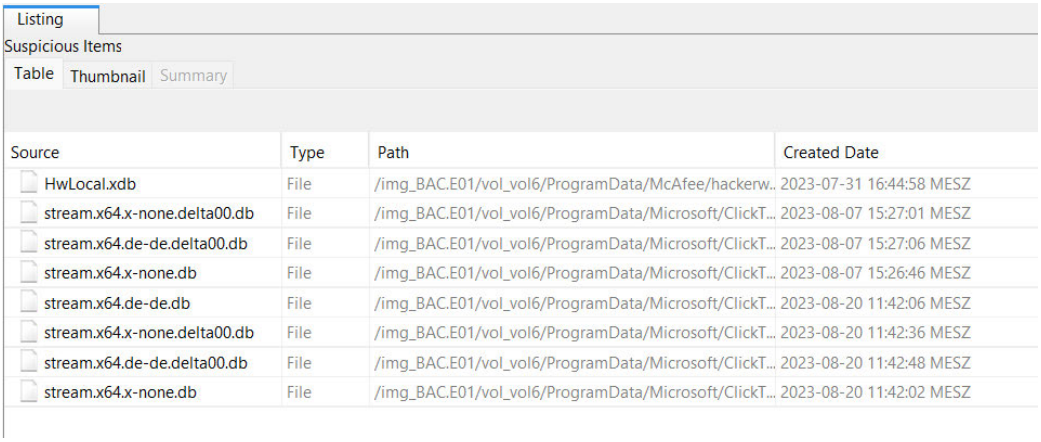
In der Baumübersicht befindet sich dementsprechend der Ordner *Encryption Suspected*. Dieser wurde während der Analysen erstellt. Allerdings erscheint keine der Dateien aus den verschlüsselten Ordnern in dem Ordner (Abb. 19).


Listing
Encryption Suspected
Table Thumbnail Summary

Source Name	S	C	O	Source Type	Score	Conclusion
HwLocal.xdb			3	File	Likely Notable	
stream.x64.x-none.delta00.db			3	File	Likely Notable	
stream.x64.de-de.delta00.db			3	File	Likely Notable	
stream.x64.x-none.db			3	File	Likely Notable	
stream.x64.de-de.db			3	File	Likely Notable	
stream.x64.x-none.delta00.db			3	File	Likely Notable	
stream.x64.de-de.delta00.db			3	File	Likely Notable	
stream.x64.x-none.db			3	File	Likely Notable	
mpavdlta.vdm			3	File	Likely Notable	

Abbildung 19: Liste Encryption Suspected

Dieselben Dateien findet man im Ordner *Suspicious Items* (Abb. 20). Auch hier befinden sich die gesuchten verschlüsselten Dateien nicht.


Listing
Suspicious Items
Table Thumbnail Summary

Source	Type	Path	Created Date
HwLocal.xdb	File	/img_BAC.E01/vol_vol6/ProgramData/McAfee/hackerw..	2023-07-31 16:44:58 MESZ
stream.x64.x-none.delta00.db	File	/img_BAC.E01/vol_vol6/ProgramData/Microsoft/ClickT...	2023-08-07 15:27:01 MESZ
stream.x64.de-de.delta00.db	File	/img_BAC.E01/vol_vol6/ProgramData/Microsoft/ClickT...	2023-08-07 15:27:06 MESZ
stream.x64.x-none.db	File	/img_BAC.E01/vol_vol6/ProgramData/Microsoft/ClickT...	2023-08-07 15:26:46 MESZ
stream.x64.de-de.db	File	/img_BAC.E01/vol_vol6/ProgramData/Microsoft/ClickT...	2023-08-20 11:42:06 MESZ
stream.x64.x-none.delta00.db	File	/img_BAC.E01/vol_vol6/ProgramData/Microsoft/ClickT...	2023-08-20 11:42:36 MESZ
stream.x64.de-de.delta00.db	File	/img_BAC.E01/vol_vol6/ProgramData/Microsoft/ClickT...	2023-08-20 11:42:48 MESZ
stream.x64.x-none.db	File	/img_BAC.E01/vol_vol6/ProgramData/Microsoft/ClickT...	2023-08-20 11:42:02 MESZ

Abbildung 20: Liste der Suspicious Items

Im zweiten Versuch wurde die Größe der Dateien auf ein Megabyte und die Entropie auf 6.0 herabgesetzt. Beide Werte sind für das Programm das jeweilige Minimum.

Beim zweiten Lauf wurde die Datei Book.pdf als verschlüsselt erkannt (Abb. 21). Die anderen verschlüsselten Dateien wurden nicht analysiert.

Dies könnte daran liegen, dass sie nicht die Mindestgröße erreicht haben. Infolgedessen gehen diese Dateien während einer Untersuchung verloren und werden möglicherweise nicht korrekt klassifiziert. Dies kann zu Problemen im Untersuchungsprozess führen, da wichtige Informationen übersehen oder nicht berücksichtigt werden können. Es ist wichtig, dass alle Dateien korrekt identifiziert und analysiert werden.

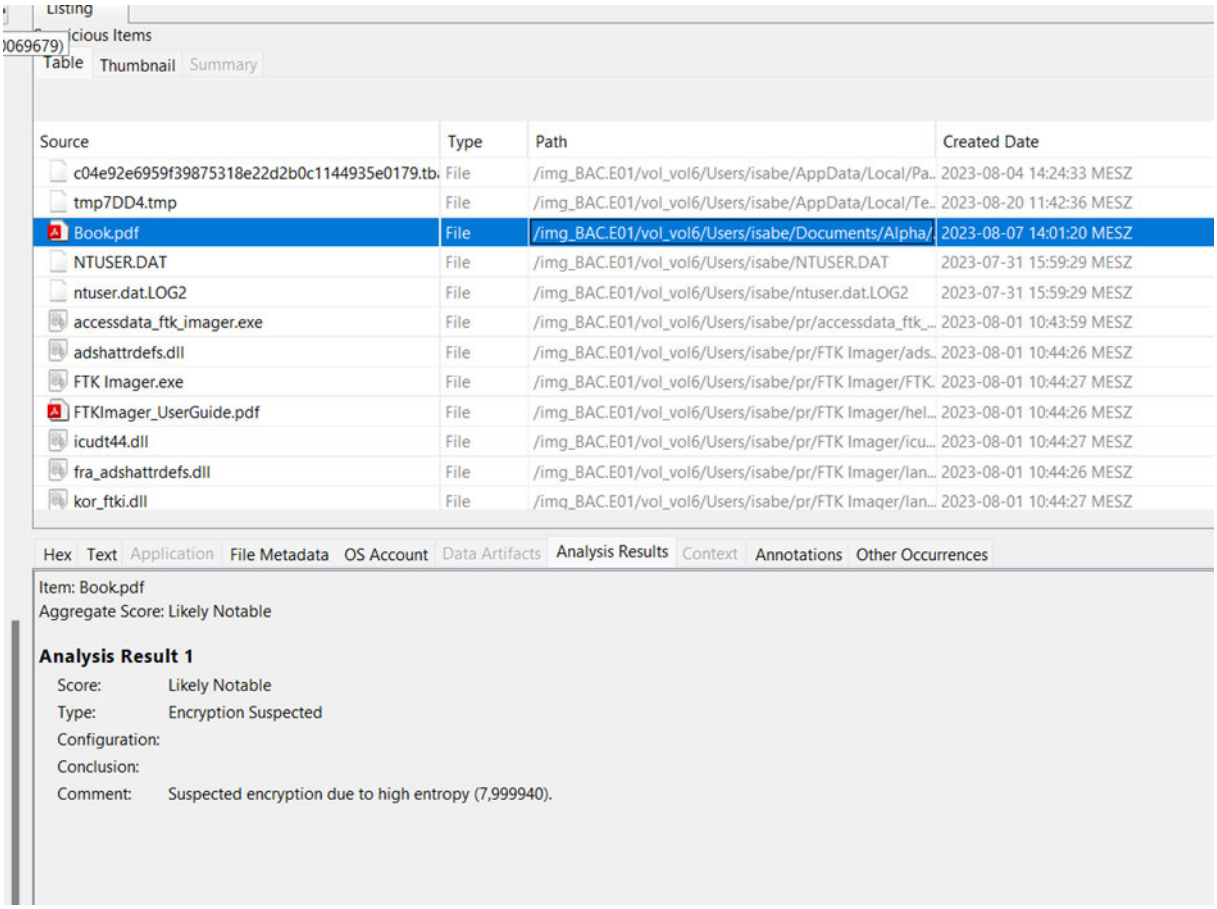


Abbildung 21: Liste der Suspicious Items beim zweiten Versuch

Unter den Metadaten der Ordners Alphas findet man Informationen zum MFT Header (Abb. 22).

From The Sleuth Kit istat Tool:

```
MFT Entry Header Values:
Entry: 52719 Sequence: 47
$LogFile Sequence Number: 178008257143
Allocated Directory
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive, Encrypted
Owner ID: 0
Security ID: 17845 (S-1-5-21-3293361733-2288189047-3987401423-1001)
Last User Journal Update Sequence Number: 33155571264
Created: 2023-08-01 10:28:12.400000000 (MES)
File Modified: 2023-08-20 11:42:11.061738900 (MES)
MFT Modified: 2023-08-20 11:42:11.061738900 (MES)
Accessed: 2023-08-20 11:42:11.061738900 (MES)

$FILE_NAME Attribute Values:
Flags: Directory, Archive
Name: Alpha
Parent MFT Entry: 34179 Sequence: 25
Allocated Size: 0 Actual Size: 0
Created: 2023-08-20 11:42:10.879209900 (MES)
File Modified: 2023-08-20 11:42:10.879209900 (MES)
MFT Modified: 2023-08-20 11:42:10.879209900 (MES)
Accessed: 2023-08-20 11:42:10.879209900 (MES)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-2) Name: N/A Resident size: 76
Type: $INDEX_ROOT (144-1) Name: $I30 Resident size: 520
Type: $LOGGED_UTILITY_STREAM (256-4) Name: $EFS Non-Resident size: 688 init_size: 688
Starting address: 144922, length: 1
```

Abbildung 22: MFT Header Informationen des verschlüsselten Orders Alpha

Das Attribut $STANDARD_INFORMATION speichert Metadaten über die Erstellung, Änderung und Löschung der Datei oder des Verzeichnisses. Dazu gehören die Sicherheitskennung (SID) des Eigentümers, die Uhrzeit und das Datum, an dem jedes dieser Ereignisse stattgefunden hat sowie andere Attribute im Zusammenhang mit der Datei. Das Attribut $FILE_NAME speichert den Namen der Datei oder des Verzeichnisses sowie einen Zeitstempel, wann die Datei erstellt, geändert oder gelöscht wurde. (Naiqi, et al., 2018, S.520)

Wenn Dateien in einem NTFS-Dateisystem gespeichert werden, wird die Master File Table (MFT) verwendet, um Informationen über die Dateien zu speichern. Residente Attribute enthalten alle ihre Informationen im MFT-Eintrag, während nicht-residente Attribute ihre Informationen in Clustern außerhalb der MFT speichern. Die Startadresse des Clusters wird im MFT-Eintrag gespeichert, so dass das System weiß, wo es nach dem vollständigen Inhalt des Attributs suchen muss.

In diesem Fall erfährt man über das Attribut $LOGGED_UTILITY_STREA, dass der Ordner EFS-verschlüsselt und nicht resistent ist (Abb. 23).

From The Sleuth Kit istat Tool:

```
MFT Entry Header Values:
Entry: 52722 Sequence: 163
$LogFile Sequence Number: 177997644749
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive, Encrypted
Owner ID: 0
Security ID: 17844 (S-1-5-21-3293361733-2288189047-3987401423-1001)
Last User Journal Update Sequence Number: 33155572432
Created: 2023-08-01 10:30:27.570000000 (MES)
File Modified: 2023-08-01 10:30:34.000000000 (MES)
MFT Modified: 2023-08-07 14:01:20.439224400 (MES)
Accessed: 2023-08-20 11:42:11.042179700 (MES)

$FILE_NAME Attribute Values:
Flags: Archive
Name: Book.pdf
Parent MFT Entry: 52719 Sequence: 47
Allocated Size: 0 Actual Size: 0
Created: 2023-08-20 11:42:10.971698200 (MES)
File Modified: 2023-08-20 11:42:10.971698200 (MES)
MFT Modified: 2023-08-20 11:42:10.971698200 (MES)
Accessed: 2023-08-20 11:42:10.971698200 (MES)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-2) Name: N/A Resident size: 82
Type: $DATA (128-5) Name: N/A Non-Resident, Encrypted size: 3292760 init_size: 3292760
Starting address: 29827567, length: 804
Type: $LOGGED_UTILITY_STREAM (256-4) Name: $EFS Non-Resident size: 4096 init_size: 4096
Starting address: 203334, length: 1
```

Abbildung 23: MFT Header der Datei Book.pdf

Bei der Datei book.pdf zeigt das Attribut $DATA an, dass der gesamte Inhalt der Datei verschlüsselt und nicht resistent ist. Autopsy hat korrekt erkannt, dass die Datei mit dem EFS von Windows verschlüsselt wurde. Dies wird im Attribut $LOGGED_UTILITY_STREAM gespeichert.

Etwas übersichtlicher steht ebenfalls der Bereich OS Account zur Verfügung (Abb. 24). Dort befinden sich die Informationen über den Besitzer der Datei.

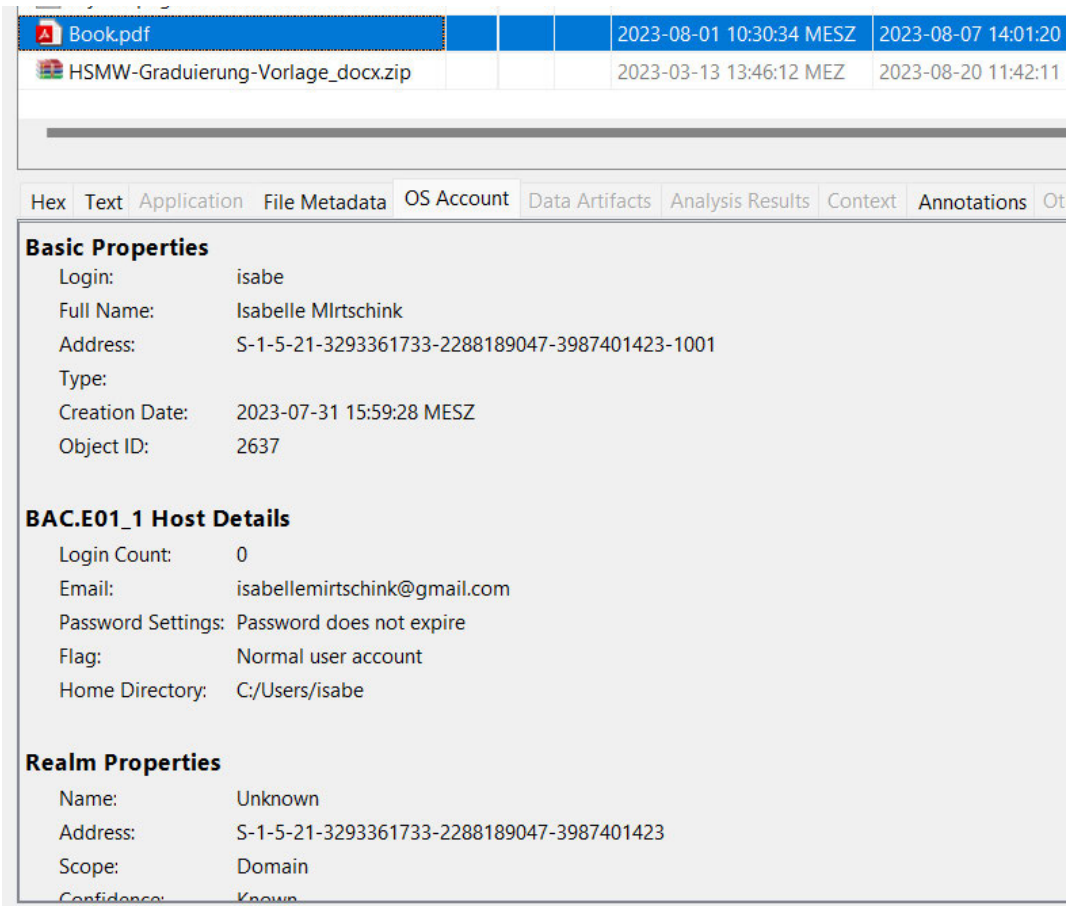


Abbildung 24: Details zu dem Besitzer von Book.pdf

Bei allen Dateien wurde erkannt, dass sie mit dem EFS verschlüsselt wurden. Allerdings wurde keine der Dateien im Ordner *Encryption Suspected* angezeigt.

Weiterhin konnte keine der Dateien entschlüsselt werden (Abb. 25). Die Datei kann nicht geöffnet werden.

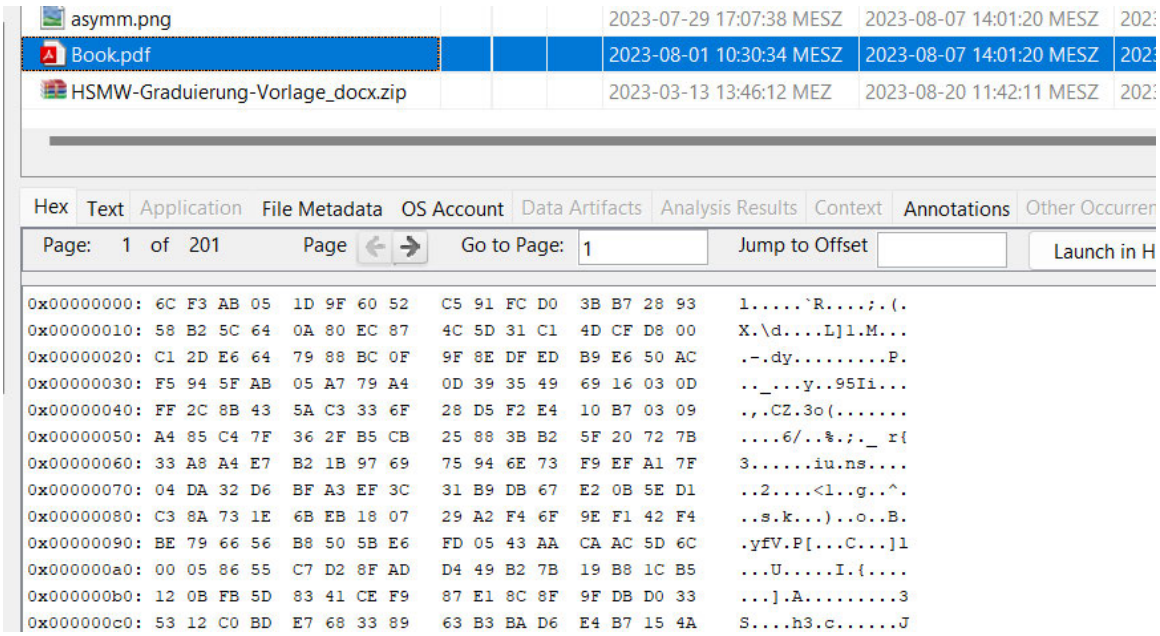


Abbildung 25: Ansicht des Hex der Datei Book.pdf

Die Analyse- und Entschlüsselungsfunktionen von Autopsy beschränken sich auf die Informationen, die in den verschlüsselten Dateien oder Ordnern gespeichert sind, z. B. Datei-Metadaten, Erstellungs- und Änderungsdaten sowie Benutzerkonten, welche Zugriff auf die verschlüsselten Ressourcen haben. Es ist nicht in der Lage, die verschlüsselten Ressourcen selbst zu entschlüsseln.

3.2.3.2 IPED

Der Digital Evidence Processor and Indexer (IPED) ist eine Open-Source-Software, welche zur Analyse und Verarbeitung digitaler Beweismittel verwendet wird. Sie wurde seit 2021 von Experten der Brazilian Federal Police entwickelt. (IPED, o. D.)

Mit dieser Software können digitale Daten, einschließlich E-Mails, Dokumente und Bilder, schnell sortiert, analysiert und dokumentiert werden. Sie kann auch helfen, Muster und andere Hinweise zu erkennen, die zur Untersuchung eines Verbrechens oder eines anderen Fehlverhaltens verwendet werden.

Zu den zahlreichen Funktionen gehören schnelle Hash-Deduplizierung, Signaturanalyse, Georeferenzierung von global positioning system (GPS) Daten, Indizierung und Suche von Dateiinhalten und Metadaten, Erkennung von Verschlüsselung und Erkennung von mehr als 70 Sprachen. (IPED, o. D.)

Unterstützte Imageformate sind unter anderem ad1, dd e01, vhd, und vmdk (nassif, 2023).

Version 3.3 erkennt automatisch verschlüsselte Dateien vieler verschiedener Typen, wie z. B. pdf, zip oder rar (Tolosa, 2022, S.18). Version 3.3 war die erste Version, die eine auf

Entropie basierende Erkennung verwendete und sie ermöglicht eine viel genauere Erkennung von verschlüsselten Dateien als die vorherigen Methoden (Tolosa, 2022, S.18).

Die Dateien werden weder bei dem Filter *Possibly encrypted (entropie)* (Abb. 26), noch bei dem Filter *Encrypted Files* erkannt.

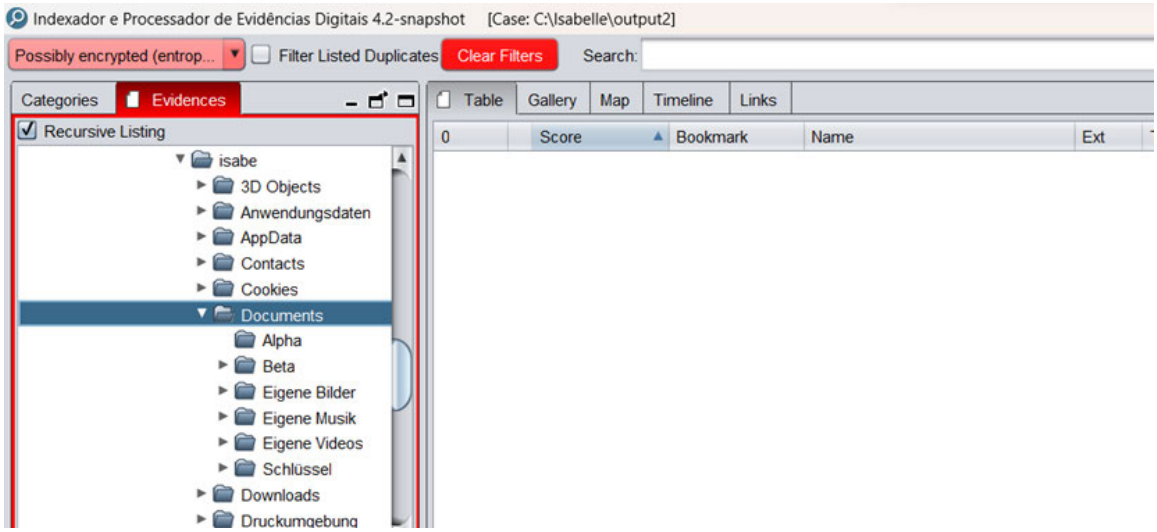


Abbildung 26: Filter Possibly encrypted (entropy)

Die Preview der Dateien kann nicht geöffnet werden, allerdings gibt es eine allgemeine Fehlermeldung (Abb. 27). Anscheinend ist dem Programm nicht bekannt, dass es aufgrund der Verschlüsselung nicht verfügbar ist.

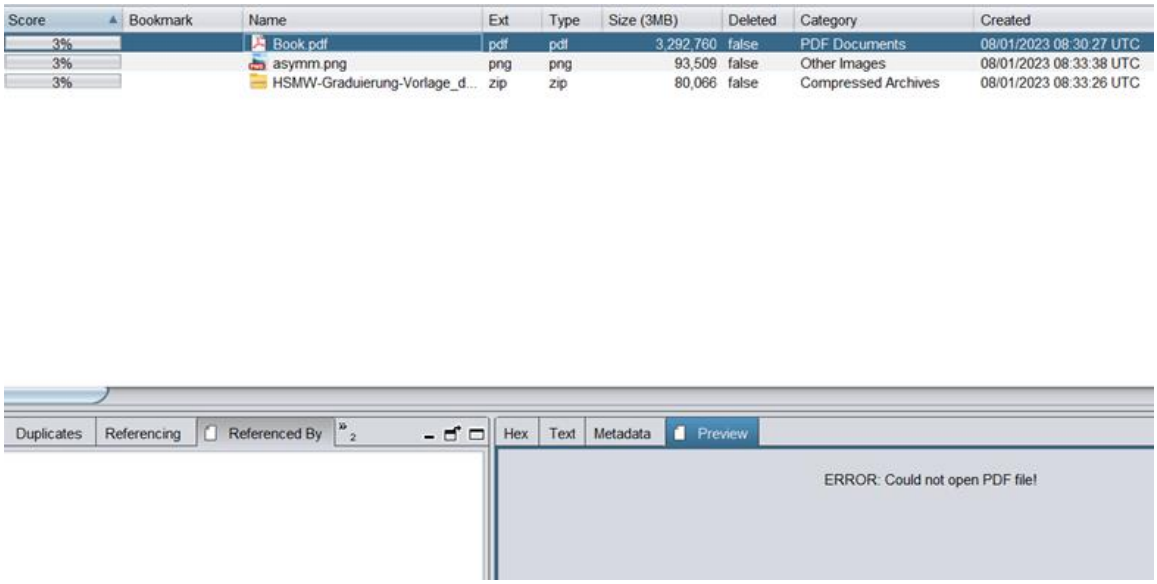
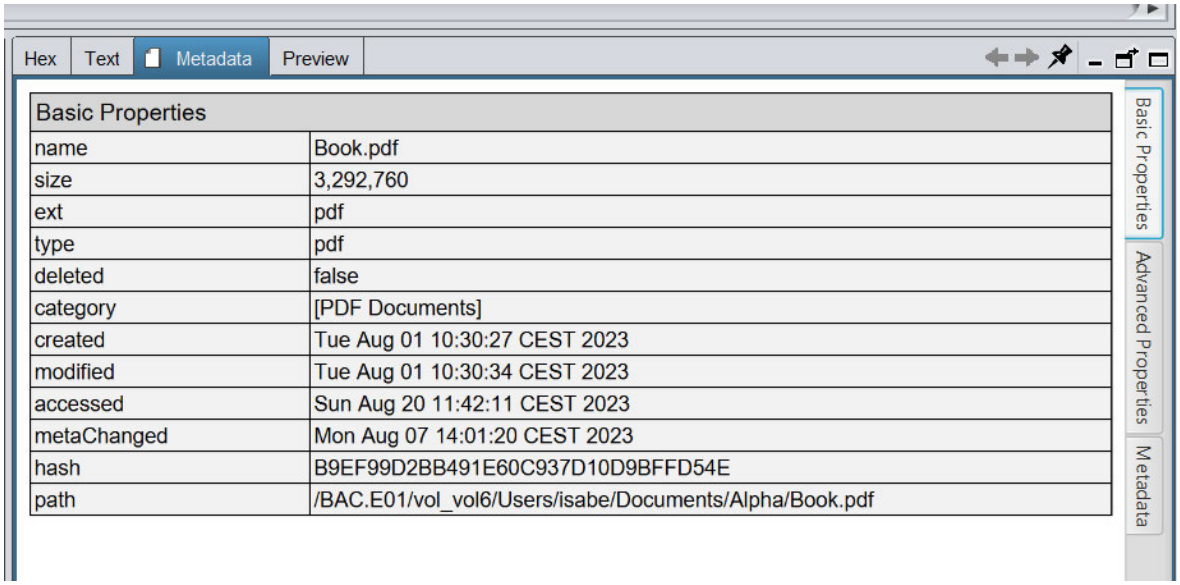


Abbildung 27: Vorschau der Datei Book.pdf

In der IPED-Software sind die Metadaten in drei Bereiche unterteilt. Die allgemeinen Eigenschaften enthalten die grundlegenden Informationen der Datei, wie Name, Größe, Typ, Speicherort, Hash-Wert und die jeweiligen Zeitstempel, die für die Verfolgung der

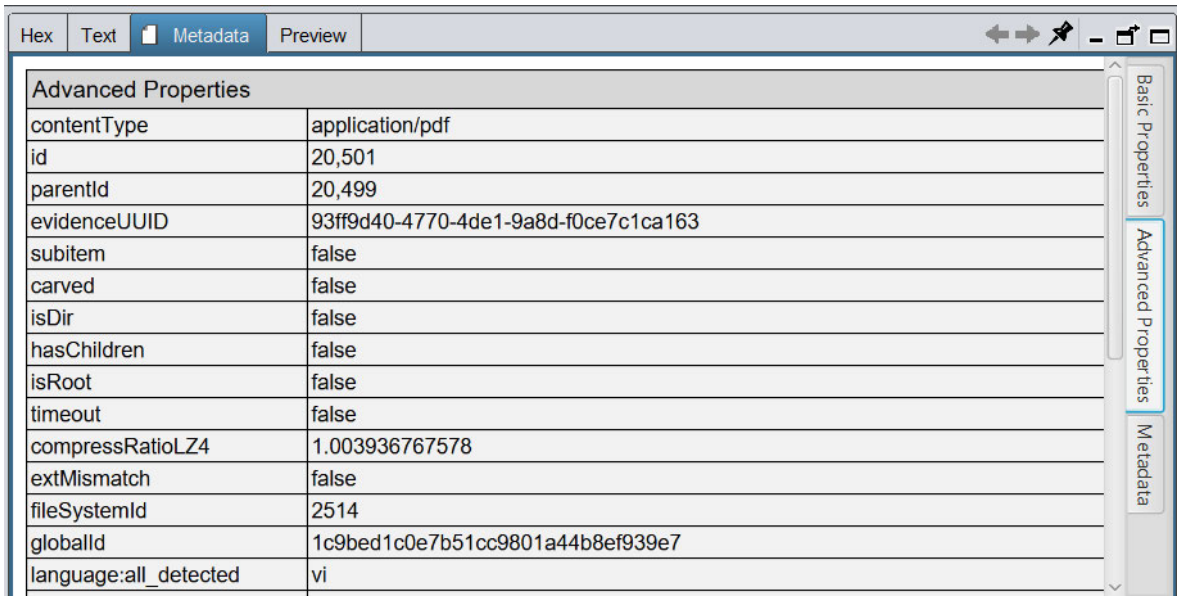
Herkunft vorgenommenen Änderungen wichtig sind (Abb. 28). Diese Informationen können verwendet werden, um die Integrität der Datei zu gewährleisten und mögliche Manipulationen zu erkennen.



Basic Properties	
name	Book.pdf
size	3,292,760
ext	pdf
type	pdf
deleted	false
category	[PDF Documents]
created	Tue Aug 01 10:30:27 CEST 2023
modified	Tue Aug 01 10:30:34 CEST 2023
accessed	Sun Aug 20 11:42:11 CEST 2023
metaChanged	Mon Aug 07 14:01:20 CEST 2023
hash	B9EF99D2BB491E60C937D10D9BFFD54E
path	/BAC.E01/vol_vol6/Users/isabe/Documents/Alpha/Book.pdf

Abbildung 28: Allgemeine Eigenschaften der Datei Book.pdf

In den erweiterten Eigenschaften findet man unter anderem die ID, die ID des übergeordneten Verzeichnisses, mögliche Unterelemente, die Sprache, Die MFT-Sequenznummer, etc. (Abb. 29).



Advanced Properties	
contentType	application/pdf
id	20,501
parentId	20,499
evidenceUUID	93ff9d40-4770-4de1-9a8d-f0ce7c1ca163
subitem	false
carved	false
isDir	false
hasChildren	false
isRoot	false
timeout	false
compressRatioLZ4	1.003936767578
extMismatch	false
fileSystemId	2514
globalId	1c9bed1c0e7b51cc9801a44b8ef939e7
language:all_detected	vi

Abbildung 29: Ausschnitt der erweiterten Eigenschaften der Datei Book.pdf

Die Open-Source-Software IPED war nicht in der Lage, die vier verschlüsselten Ordner als verschlüsselt zu klassifizieren und zu entschlüsseln. Viele Details zu den jeweiligen Dateien wurden erfasst. Dennoch war IPED in der Lage, die Dateinamen, Größen und

Daten für jeden der Ordner zu erfassen. Außerdem wurde für jede der Dateien ein Hash-Wert generiert, der eine detailliertere Prüfung der Daten ermöglicht.

4 Ergebnisse

Ziel dieses Abschnitts ist es, die Ergebnisse der Analyse zu erläutern und eine Interpretation der Ergebnisse zu liefern. Er stützt sich auf die im vorangegangenen Abschnitt gesammelten und analysierten Daten und nutzt sie, um die Auswirkungen der Ergebnisse zu erläutern.

4.1 Vergleich

	AXIOM	**X-Ways**	**Autopsy**	**IPED**
Entschlüsselung	AXIOM war es nicht möglich die verschlüsselten Dateien zu entschlüsseln.	X-Ways war es nicht möglich die verschlüsselten Dateien zu entschlüsseln.	Autopsy war es nicht möglich die verschlüsselten Dateien zu entschlüsseln.	IPED war es nicht möglich die verschlüsselten Dateien zu entschlüsseln.
Verschlüsselung erkannt	Die Datei Book.pdf wird als verschlüsselt erkannt. Die anderen Dateien werden nicht als verschlüsselt erkannt.	Alle Dateien und Ordner werden als verschlüsselt erkannt.	Die Dateien werden nicht im Ordner Encryption suspected oder Suspicious Items gelabelt. Allerdings werden sie in den Metadaten als verschlüsselt gelabelt.	Die Dateien werden nicht als verschlüsselt erkannt. Weder mit dem Filter *Possibly encrypted (entropie)*, noch mit dem Filter *Encrypted Files.* Auch in den Metadaten nicht.
Metadaten	Metadaten bieten die	Die umfangreiche Metadaten eignen sich gut zur Analyse. Die	Die umfangreiche Metadaten eignen	Umfangreiche Metadaten, allerdings durch die

	grundlegenden Informationen.	Datei $EFS ist neu hinzugekommen und bietet die Verschlüsselungsmetadaten.	sich gut zur Analyse.	Verschlüsselung teilweise inkorrekt, wie beispielsweise die erkannte Sprache.
Vorschau	AXIOM bietet entweder leere Vorschaubilder oder den verschlüsselten Text.	An der Vorschau erkennt man die Verschlüsselung.		Bei der Vorschau gibt es eine allgemeine Fehlermeldung.

Tabelle 1: Vergleich der forensischen Anwendungen

4.2 Diskussion

Obwohl keine der vier Anwendungen in der Lage war, die verschlüsselten Dateien zu decodieren, können sie zur Analyse der Metadaten verwendet werden. Anhand dieser Daten lassen sich Muster erkennen und Einblicke in die Art der Dateien gewinnen. In einigen Fällen führt dies zu Hinweisen, die bei der Entschlüsselung der Dateien helfen könnten.

Ein möglicher Grund daafür, dass keine der Dateien entschlüsselt werden konnte, ist der fehlende Zugriff auf den FEK, was bedeutet, dass es keine einfache Möglichkeit zur Entschlüsselung gibt.

Es gab keinen Unterschied zwischen den zwei verwendeten Images. Die Dateien wurden von den Anwendungen nicht in andere Kategorien eingeordnet. Somit konnten auch die anderen vorhandenen Daten der Partition C:\ nicht zur Entschlüsselung der Dateien verwendet werden.

Die forensischen Anwendungen AXIOM und X-Ways wurden ausgewählt, weil sie in der praktischen Polizeiarbeit eingesetzt werden und damit von besonderer Interesse sind. Autopsy und IPED sind Open-Source Anwendungen, welche ebenfalls verwendet werden. Die vier Programme stehen nicht repräsentativ für alle anderen forensischen Anwendungen.

Es besteht die Möglichkeit, dass andere forensischen Tools zur Entschlüsselung der Dateien in der Lage sind. Da sich auch die Open Source Technologien ständig und schnell weiterentwickeln, ist in Zukunft in diesem Bereich verstärkt die Suche nach Lösungen sinnvoll.

4.2.1 AXIOM

Die einzige Datei, die von AXIOM als verschlüsselt markiert wurde, ist Book.pdf. Keine der anderen Dateien wurde als verschlüsselt eingestuft. Die Details der Datei enthalten nur die grundlegenden Informationen. Es besteht die Möglichkeit, dass die anderen Dateien aufgrund ihrer Größe nicht analysiert wurden.

AXIOM ist daher weniger geeignet für die Analyse von Dateien, die mit dem Windows Encrypting File System verschlüsselt wurden. EFS-verschlüsselte Dateien werden von AXIOM nicht unterstützt und können nicht entschlüsselt und analysiert werden. Daher ist es notwendig, andere Methoden zu verwenden, um auf die in diesen Dateien enthaltenen Informationen zuzugreifen.

Im Gegensatz zu den anderen forensischen Anwendungen zeigte es die wenigsten Details an und war nicht in der Lage, weitere der vier EFS-verschlüsselte Dateien als verschlüsselt zu identifizieren.

Damit ist festzustellen, dass AXIOM nicht die beste Wahl für die Untersuchung von EFS-verschlüsselten Dateien ist. Dies deutet darauf hin, dass EFS-verschlüsselte Dateien von AXIOM nicht gut unterstützt werden und dass zusätzliche Maßnahmen ergriffen werden müssen, um auf die darin enthaltenen Informationen zuzugreifen.

4.2.2 X-Ways

X-Ways arbeitet durch Data Carving und durch die Suche nach bekannten Dateisignaturen. Diese Art der Analyse eignet sich hervorragend zum Extrahieren von Metadaten wie Dateiname, Größe und Erstellungsdatum, kann aber die Dateien selbst nicht entschlüsseln.

Der Unterschied zwischen X-Ways und den anderen Programmen ist die neu hinzugefügte $EFS-Datei. Bei der $EFS-Datei handelt es sich um die Zertifikats-Metadaten, die ein Unterobjekt zu den verschlüsselten Dateien sind. Die $EFS-Datei enthält Informationen über die verwendete Verschlüsselung, den Benutzer, der die Datei verschlüsselt hat, und das verwendete Zertifikat. Auf diese Weise können die verschlüsselten Dateien identifiziert werden, und es wird sichergestellt, dass die Dateien nicht ohne die richtigen Anmeldeinformationen entschlüsselt werden können.

Das Vorhandensein der Datei $EFS zeigt an, dass X-Ways korrekt erkannt hat, dass der Ordner mit dem EFS verschlüsselt wurde, da diese Datei in einem unverschlüsselten Ordner nicht vorhanden ist.

Außerdem ist die $EFS-Datei ein spezieller Dateityp, der mit den verschlüsselten Dateien verknüpft ist und zur weiteren Überprüfung der Verschlüsselungsquelle verwendet werden kann. Die $EFS-Datei wird als Unterobjekt der jeweiligen verschlüsselten Datei behandelt.

Es ist auch möglich, das Datum der Verschlüsselung anhand der Seriennummer zu ermitteln. Außerdem kann anhand anderer Metadaten festgestellt werden, ob die Datei von derselben Person verschlüsselt wurde.

Obwohl X-Ways die Dateien nicht entschlüsseln kann, liefert sie den Ermittlern jedoch wertvolle Informationen aus den Verschlüsselungs-Metadaten. Die Verschlüsselungs-Metadaten, die mit $EFS gekennzeichnet sind, können bei jedem verschlüsselten Verzeichnis bzw. jeder verschlüsselten Datei gefunden werden.

Weiterhin kann mit X-Ways das Images nach verschlüsselten Dateien durchsucht werden. Dafür wird nach den Verschlüsselungsattributen "e, e!, E" und "e?" gefiltert. Somit werden keine verschlüsselten Dateien übersehen.

4.2.3 Autopsy

Autopsy hat im Vergleich zu den anderen Programmen die beste Übersicht über die Metadaten. Sie sind weit aufgeschlüsselt und die wichtigsten Informationen sind auf einen Blick zu erkennen. Autopsy bietet den umfassendsten Überblick über die Metadaten, welche ein vollständiges Bild der Beweismittel vermitteln. Außerdem verfügt es über eine übersichtliche Oberfläche, die es dem Benutzer ermöglicht, wichtige Elemente schnell zu erkennen und Schlussfolgerungen aus den Daten zu ziehen.

Bei der Anwendung Autopsy wurde eine der gesuchten Dateien in den Ordner *Encryption Suspected* und *Suspicious Items* gelegt. Dies ließ darauf schließen, dass die anderen Dateien die Mindestgröße nicht erreicht haben. Dadurch können die anderen Dateien bei einer Untersuchung leichter übersehen werden.

Obwohl sich drei der verschlüsselten Dateien nicht in dem Ordner mit den verschlüsselten Dateien befinden, kann man bei der Betrachtung der Metadaten sehen, dass die Dateien korrekt als EFS-verschlüsselt erkannt wurden. Dennoch war Autopsy nicht in der Lage, die Dateien zu entschlüsseln.

Schlussfolgernd kann man sagen, dass die Autopsy-Software für die Analyse der Metadaten besser geeignet ist. Die Autopsy-Software ist so konzipiert, dass sie in der Lage ist, die Metadaten verschlüsselter Dateien zu erkennen und zu analysieren, wie z. B. den Dateinamen, die Größe, das Datum und andere Eigenschaften. Allerdings kann sie den Inhalt der Dateien nicht entschlüsseln und ist daher nicht für die Inhaltsanalyse geeignet.

4.2.4 IPED

IPED konnte keine der vier verschlüsselten Dateien als solche identifizieren. Die Filter *Possibly encrypted (entropie)* und *Encrypted Files* wurden angewandt. Bei der Überprüfung wurden keine passenden Dateien gefunden.

Dies ist unerwartet, da zumindest die Datei Book.pdf von Autopsy mit einer Entropie von 7,999940 als *Suspected Encryption* klassifiziert wurde (Abb. 21). IPED verwendet wie Autopsy die Sleuthkit Library (IPED, o. D.), weshalb vermutet wurde, dass IPED in Bezug auf die verschlüsselten Daten dasselbe Ergebnis erzielt wie Autopsy. Dies ist nicht eingetreten.

Dennoch liefert IPED detaillierte Informationen über die entsprechenden Dateien, weshalb es für die Analyse der Metadaten der verschlüsselten Dateien nützlich ist. Allerdings sind einige Informationen, welche IPED ausliest durch die Verschlüsselung nicht korrekt, wie beispielsweise die erkannte Sprache.

5 Fazit und Ausblick

Diese Arbeit schließt mit einer Schlussfolgerung ab. Des Weiteren werden Möglichkeiten zur weiteren Analyse der Daten vorgeschlagen, um weitere Erkenntnisse zu gewinnen.

5.1 Fazit

Im Rahmen dieser Arbeit wurde das Thema "Vergleich verschiedener forensischer Anwendungen im Zusammenhang mit dem Encrypting File System " untersucht. Die Arbeit konzentriert sich auf die verschiedenen forensischen Anwendungen und deren Fähigkeiten in Bezug auf das Windows Encrypting File System. Analysiert wurden die unterschiedlichen Ansätze der verschiedenen Anwendungen und ob die Anwendungen verschlüsselte Dateien erkennen und entschlüsseln können. Die Analyse sollte auch Aufschluss über die Stärken und Schwächen der verschiedenen Anwendungen geben. Die Arbeit umfasste einen Vergleich der verschiedenen Funktionen, die von den verschiedenen Anwendungen angeboten werden, sowie eine detaillierte Beschreibung des Ver- und Entschlüsselungsprozesses.

Zu diesem Zweck wurden die Programme AXIOM, X-Ways, Autopsy und IPED verwendet. Alle diese Programme sind auf dem Gebiet der digitalen Forensik bekannt und beliebt. Diese Programme werden verwendet, weil sie für die Identifizierung und Analyse digitaler Beweismittel wie Dateien, E-Mails und anderer Daten entwickelt wurden. Sie sind auch in der Lage, gelöschte oder versteckte Daten zu scannen und zu identifizieren, was bei digitalen forensischen Untersuchungen oft wichtig ist. Diese Programme sind leistungsstarke Werkzeuge für die Verarbeitung digitaler Beweise und wurden bereits in zahlreichen erfolgreichen Ermittlungen eingesetzt. Sie sind auch in der digitalen Forensik-Gemeinschaft hoch angesehen und werden regelmäßig mit neuen Funktionen und Möglichkeiten aktualisiert.

In der Einleitung wurde die folgende Forschungsfrage formuliert: Inwieweit können die ausgewählten forensischen Anwendungen die EFS-verschlüsselte Dateien erkennen und entschlüsseln?

Die Untersuchung ergab, dass einige Programme die Verschlüsselung zwar erkennen, aber nicht entschlüsseln konnten. Die Ergebnisse der Analyse zeigten, welche Anwendungen am effektivsten bei der Analyse von Beweisen aus den verschlüsselten Dateien des Windows Encrypting File System waren.

Die Forschungsfrage wird auf Basis der dargestellten Ergebnisse wie folgt beantwortet: Entgegen den Erwartungen wurde festgestellt, dass keine der forensischen Anwendungen AXIOM, X-Ways, Autopsy und IPED die Dateien entschlüsseln kann.

In dieser Arbeit wurde festgestellt, dass X-Ways das Programm ist, welches die verschlüsselten Dateien am besten darstellt. X-Ways bietet eine Möglichkeit alle verschlüsselten Dateien des Images darzustellen, womit gewährleistet ist, dass keine Dateien übersehen werden. Bei Verwendung von X-Ways können alle Dateien mit dem Attribut E für „Verschlüsselt“ markiert werden. Somit ist auf den ersten Blick bekannt, dass es sich um verschlüsselte Dateien handelt.

In Autopsie-Anwendungen muss der Benutzer die Metadaten überprüfen, um festzustellen, ob die Dateien verschlüsselt sind. AXIOM markiert nur eine Datei als verschlüsselt und IPED konnte keine der Dateien als verschlüsselt markieren.

5.2 Ausblick

Weitere Forschung ist notwendig, um das Potenzial des Themas voll auszuschöpfen und das Thema bietet noch viel Material für weiterführende Arbeiten und Forschungen. Die Möglichkeit der Entschlüsselung von EFS-verschlüsselten Dateien zu Zwecken der Strafverfolgung muss gegeben sein.

Bei der Software AXIOM kann genau analysiert werden, weshalb nur eine Datei als verschlüsselt gekennzeichnet wurde und der Rest nicht.

Weiterführend kann man die $EFS Zertifikatsmetadaten von X-Ways analysieren. In einer Fortsetzung dieser Arbeit kann getestet werden, inwieweit man das $EFS-Zertifikat nutzen kann, um die Dateien möglicherweise doch zu entschlüsseln. Durch die Verwendung des $EFS-Zertifikats kann man feststellen, ob eine Datei verschlüsselt ist oder nicht, und dann das Zertifikat verwenden, um die Datei zu entschlüsseln, wenn sie verschlüsselt ist. Dies würde die X-Ways-Software in die Lage versetzen, verschlüsselte Dateien zu erkennen und sie bei Bedarf zu entschlüsseln.

Bei der Autopsy-Software könnte man noch weiter forschen und auch kleinere Dateien auf Verschlüsselung prüfen, sodass die Verschlüsselung nicht erst durch die Suche in den Metadaten erkannt wird.

IPED ist eine gut entwickelte Open-Source-Software, welche viele Analysemöglichkeiten bietet und zur Verarbeitung digitaler Beweise verwendet werden kann. Es ist ein effizientes Werkzeug für Strafverfolgungsbehörden und andere Ermittlungsteams. Leider kann es EFS-verschlüsselte Dateien weder entschlüsseln, noch erkennen. In Zukunft sollte man an einer Möglichkeit arbeiten, diese Lücke zu schließen.

Ebenso sollte nach einer Möglichkeiten gesucht werden, die EFS-verschlüsselten Dateien zu entschlüsseln bzw. Implementierungen für die verwendeten Programmen zu schreiben.

Zukünftige Arbeiten sollten neue Herangehensweisen an das Thema in Betracht ziehen.

Literaturverzeichnis

Adamu, H., Ahmad, A. A., Hassan, A. & Gambasha, S. B., 2021. Web Browser Forensic Tools: Autopsy, BHE and NetAnalysis. *International Journal of Research and Scientific Innovation (IJRSI) |Volume VIII, Issue V, May 2021|ISSN 2321-2705,* Issue https://d1wqtxts1xzle7.cloudfront.net/83671925/103-107-libre.pdf?1649594470=&response-content-disposition=inline%3B+filename%3DWeb_Browser_Forensic_Tools_Autopsy_BHE_a.pdf&Expires=1694336666&Signature=eVW~Pf-kIx10-3fc7OVMw9rIBxVZvJ8veYxEDCoY7vsE36bOqR4XBR, pp. 103-107.

Banoth, R. & Regar, R., 2023. *Classical and Modern Cryptography for Beginners.* s.l.:Springer Nature.

Bucholz, G. & Parkes, H., 2001. *Guide to Securing Microsoft Windows 2000 Encrypting File System.* Version 1.0

Coles, M. & Landrum, R., 2009. *Expert SQL Server 2008 Encryption.* s.l.:Apress, Berkeley, CA.

Faust, D., 2021. WAS IST DOS/MS-DOS?. https://www.biteno.com/was-ist-dos-msdos/(Zugriff: 26.06.2023).

Fickert, T., Nau, M. & Gerling, R. W., 2003. *Encrypting File System unter Windows.* In DuD • Datenschutz und Datensicherheit 27 (2003)

Forensics, M., 2022. GETTING STARTED WITH MAGNET AXIOM. https://support.magnetforensics.com/s/product-documentation?language=en_US(Zugriff: 03.07.2023).

Forensics, X.-W., ohne Datum. X-Ways Forensics: Integrierte Software für Computerforensik. https://x-ways.net/forensics/index-d.html(Zugriff: 05.07.2023).

Gross-Bajohr, I., 2023. Was ist Windows Hello? Wir stellen das Feature vor. https://www.computerbild.de/artikel/cb-Tipps-Windows-Was-ist-Windows-Hello-31436277.html(Zugriff: 29.06.2023).

Group, T., 2022. What percentage of your sensitive data in the cloud is encrypted?. *Statista. Statista Inc. .* https://www.statista.com/statistics/1243960/sensitive-data-encrypted-in-cloud-percentage/(Zugriff: 18.08.2023).

heise, ohne Datum. Windows-History: Die Geschichte des Betriebssystems. https://www.heise.de/download/specials/Windows-History-Die-Geschichte-des-Betriebssystems-3148952(Zugriff: 07.07.2023).

Intel, ohne Datum. Trusted-Platform-Modul (TPM) – Überblick. https://www.intel.de/content/www/de/de/business/enterprise-computers/resources/trusted-platform-module.html(Zugriff: 28.06.2023).

IPED, ohne Datum. IPED. https://github.com/sepinf-inc/IPED(Zugriff: 25.08.2023).

Joos, T., 2017. Windows 10 per Device Guard sicherer machen. https://www.computerweekly.com/de/ratgeber/Windows-10-per-Device-Guard-sicherer-machen(Zugriff: 18.08.2023).

Kroschel, A., 2010. Vergleich: Bitlocker versus Encrypting File System. https://www.windowspro.de/andreas-kroschel/bitlocker-versus-efs(Zugriff: 28.06.2023).

Lauterschlag, E., ohne Datum. Kryptologie: Eine Einführung in die Wissenschaft der Ver- und Entschlüsselung. https://www.was-ist-malware.de/it-sicherheit/kryptologie/(Zugriff: 24.06.2023).

Microsoft, 2020. A breakthrough year for passwordless technology. https://www.microsoft.com/en-us/security/blog/2020/12/17/a-breakthrough-year-for-passwordless-technology/(Zugriff: 06.07.2023).

Microsoft, 2021. 1.3 Overview. https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-gpef/4d4687f9-132c-4501-9996-684b40b14735(Zugriff: 25.06.2023).

Microsoft, et al., 2023. diskpart. https://learn.microsoft.com/de-de/windows-server/administration/windows-commands/diskpart(Zugriff: 02.07.2023).

Nadler, I., 2020. Die Geschichte von Windows. https://news.microsoft.com/de-de/features/windows-geschichte/(Zugriff: 25.06.2023).

Naiqi, L., Zhongshan, W., Yujie, H. & QinKe, 2008. Computer Forensics Research and Implementation Based on NTFS File System. *ISECS International Colloquium on Computing, Communication, Control, and Management.* https://ieeexplore.ieee.org/abstract/document/4609565?casa_token=fUSZjiWduVEAAAAA:iGMl-hecwABzGfWZIzPcxczawfrKz-iaD47gYI8uQd_EON9jMxu9WHyjjoJrTRY88iVhBQm-OmQ, pp. 519-523.

Nassif, L. F., 2023. Beginner's Start Guide. https://github.com/sepinf-inc/IPED/wiki/Beginner's-Start-Guide(Zugriff: 25.08.2023).

Paar, C. & Pelzl, J., 2016. *Kryptografie verständlich.* s.l.:Springer-Verlag Berlin Heidelberg.

Panay, P., 2021. Introducing Windows 11. https://blogs.windows.com/windowsexperience/2021/06/24/introducing-windows-11/(Zugriff: 07.07.2023).

Piper, F. & Murphy, S., 2002. *Cryptography: A Very Short Introduction.* Vol. 68 Hrsg. s.l.:Oxford Paperbacks.

Pohlmann, N., Reimer, H. & Schneider, W., 2007. *ISSE/SECURE 2007 Securing Electronic Business Processes.* 1st Edition Hrsg. Wiesbaden: Friedr. Vieweg & Sohn Verlag | GWV Fachverlage GmbH.

Raji, M., Wimmer, H. & Haddad, R. J., 2018. Analyzing Data from an Android Smartphone while Comparing between Two Forensic Tools. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8478851.

Singh, S., 1999. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. FIRST ANCHOR BOOKS EDITION, SEPTEMBER 2000.

software.informer, 2013. AccessData FTK Imager 3.1. https://accessdata-ftk-imager.software.informer.com/3.1/(Zugriff; 25.08.2023).

Steffan, J. et al., 2007. BitLocker Drive Encryption im mobilen und stationären Unternehmenseinsatz. *Fraunhofer Institut Sichere Informationstechnologie.* https://drhellberg.de/FHDW/Betriebssysteme/4Quartal2009/BitlockerDriveEncryption2009.pdf.

Tan, C., Zhang, L. & Bao, L., 2020. A Deep Exploration of BitLocker Encryption and Security Analysis. *2020 IEEE 20th International Conference on Communication Technology.* https://ieeexplore.ieee.org/abstract/document/9295908?casa_token=jqKZoFL7buMAAAAA:ghgxdRhwHU6rutQA3ocd3I5zmFPy16hO8SkhQqRHG0YQjVDhNTxtGgaUvck4u_MWN6GZk25XYH4.

Technology, B., 2023. Encryption Detection Module. http://sleuthkit.org/autopsy/docs/user-docs/4.19.3/encryption_page.html(Zugriff: 25.08.2023).

Tolosa, C. A. P., 2022. *Indexador e processador de evidências digitais (iped): um poderoso software forense computacional.*

Voß, A. & Shim, D., 2022. Microsoft Windows Defender 2022: Antivirus-Software im Test. https://www.computerbild.de/artikel/cb-Tests-Sicherheit-Windows-Defender-Antivirus-Software-Test-32650953.html(Zugriff: 28.07.2023).

Winhistory, ohne Datum. Microsofts Windows. https://winhistory.de/more/windows.htm(Zugriff: 06.07.2023).

Yang, H., 2023. DiskPart „Clean All“ zum Löschen des SSD-Laufwerks. https://www.diskpart.com/de/articles/diskpart-clean-all.html#:~:text=Was%20macht%20%E2%80%9Eclean%20all%E2%80%9C%20in%20Diskpart%3F%201%20,um%20Daten%20auf%20der%20Festplatte%20zu%20l%C3%B6schen.%20(Zugriff: 02.07.2023).

Zhang, Q., 2021. An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption. *2021 2nd International Conference on Computing and Data Science (CDS).* https://ieeexplore.ieee.org/abstract/document/9463286?casa_token=ZAzi-qdZgVUAAAAA:OTR9iys68Cv3zFUOpD9Z4Ikowd6rQdHQYUwzQDzPXXBIkc6uIrBowU3VDCAsq00bNu_1ky-W36A.

Zhou, J.-J., 2013. Study on Several Confidentiality Protection Technologies for Electronic Document. *International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC).* https://ieeexplore.ieee.org/abstract/document/6885423, pp. S. 2282-2285.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Mittweida, den 13.09.2023

Isabelle Mirtschink