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

Bachelor-Thesis

Rekonstruktion von Daten auf HDDs und SSDs nach unterschiedlichen Lösch-verfahren – Ein Vergleich von vier Datenwiederherstellungsprogrammen

von: Robin Fuchs

Betreuerin: Prof. Dr. Antje Raab-Düsterhöft

Zweitbetreuer: Prof. Dr.-Ing. habil. Andreas Ahrens

Aufgabenstellung

Ziel dieser Bachelorarbeit ist es, die Wirksamkeit forensischer Methoden zur Datenwiederherstellung auf Speichermedien nach Lösch- und Formatierungsvorgängen zu untersuchen. Die Wiederherstellungsmethoden beschränken sich hierbei auf logische Wiederherstellungsmethoden wie die Ausführung von Datenwiederherstellungsprogrammen, sowie einem IT-forensischen Toolkit.

Kurzreferat

Diese Bachelorarbeit befasst sich mit der zunehmenden Bedeutung digitaler Beweismittel und den steigenden Bedrohungen durch Cyberkriminalität, insbesondere durch Angriffe wie Ransomware. Die wachsende Komplexität moderner IT-Systeme eröffnet neue Angriffsflächen, die gezielt ausgenutzt werden können. Vor diesem Hintergrund wird die Entwicklung zuverlässiger Methoden zur sicheren Datenlöschung und Datenwiederherstellung zunehmend essenziell, um den Anforderungen von Unternehmen und Behörden gerecht zu werden.

Ziel der Arbeit ist es, die technischen Möglichkeiten und Herausforderungen der Datenrekonstruktion zu beleuchten und verschiedene Ansätze zur Wiederherstellung gelöschter Daten zu vergleichen. Ein besonderer Fokus liegt auf der Untersuchung der Effektivität forensischer Methoden, insbesondere nach unterschiedlichen Lösch- und Formatierungsvorgängen. Die Arbeit soll ein besseres Verständnis der Verfahren vermitteln und deren Komplexität für eine breite Öffentlichkeit verständlich machen.

Die Ergebnisse der Versuche zeigen, dass gängige Wiederherstellungsmethoden bei unzureichenden Löschmethoden wie Schnellformatierungen, erfolgreich Daten rekonstruieren können.

Abstract

This bachelor thesis addresses the increasing importance of digital evidence and the growing threats posed by cybercrime, particularly attacks such as ransomware. The increasing complexity of modern IT systems creates new vulnerabilities that can be deliberately exploited. Against this backdrop, the development of reliable methods for secure data deletion and data recovery has become increasingly essential to meet the requirements of companies and authorities.

The aim of this thesis is to examine the technical possibilities and challenges of data reconstruction and to compare various approaches to recovering deleted data. A particular focus is placed on investigating the effectiveness of forensic methods, especially following different deletion and formatting processes. The thesis aims to provide a better understanding of these procedures and make their complexity comprehensible to a broader audience.

The experimental results demonstrate that common recovery methods can successfully reconstruct data in cases where deletion techniques, such as quick formatting, are insufficient.

Inhalt

1 Einleitung

Die zunehmende Bedeutung digitaler Beweismittel und die steigende Bedrohung durch Cyberkriminalität wie beispielsweise Angriffe, die durch Ransomware abgebildet wird, sind die Grundlage für die Motivation dieser Arbeit. Mit der wachsenden Komplexität moderner IT-Systeme entstehen neue Angriffsflächen, die von Cyberkriminellen gezielt ausgenutzt werden. Unterstützt durch fortschrittliche Technologien wie Künstliche Intelligenz (KI) und maschinelles Lernen können Schwachstellen teilweise schneller aufgedeckt werden, was ein einfacheres Eindringen in IT-Systeme ermöglichen kann, und die Sicherheit sensibler Daten gefährdet. Vor diesem Hintergrund ist die Entwicklung zuverlässiger Methoden zur sicheren Datenlöschung und Datenwiederherstellung essenziell, um den steigenden Anforderungen von Unternehmen und Behörden gerecht zu werden.

Die Herausforderungen umfassen das Verständnis spezifischer Dateisysteme, das Durchführen von physischen und logischen Rekonstruktionen sowie den Umgang mit Verschlüsselung und fortgeschrittenen Löschtechniken wie dem physikalischen Zerstören von Speichermedien oder Verschlüsselung. Ein spezielles Problem entsteht, wenn Daten physikalisch auf verschiedene Bereiche des Speichermediums verteilt sind. Die daraus resultierende Datenfragmentierung erschwert die Rekonstruktion der Daten. Zu den Techniken der Datenwiederherstellung zählen softwarebasierte Ansätze, welche die Rekonstruktion gelöschter oder beschädigter Dateien über bestimmte Programme wie beispielsweise EaseUS data recovery oder Recuva ermöglichen. Des Weiteren gibt es forensische Methoden, welche tiefgreifende Analysen von Speicherstrukturen erlauben und mit denen man beispielsweise den ungenutzten Speicherplatz manuell untersuchen kann. Hier kommen meistkostenpflichtige Programme wie zum Beispiel X-Ways oder Magnet AXIOM zum Einsatz. Im Bereich der Datenrettung finden sich eine Vielzahl unterschiedlicher Werkzeuge, die sich hinsichtlich ihrer Eignung für die Bewältigung spezifischer Anforderungen unterscheiden. Das Verständnis dieser Prozesse ist für IT-Berater/innen essenziell, um geeignete und gesetzeskonforme Datenlöschmethoden für spezifische Speichertechnologien und Sicherheitsanforderungen empfehlen zu können.

Die Datenwiederherstellung spielt eine zentrale Rolle bei der Unterstützung forensischer Untersuchungen und bei der Verhinderung von Datenverlusten. Zusätzlich dient sie der Einhaltung gesetzlicher Vorschriften und der Sicherstellung der Geschäftskontinuität [12]. Gerade in Zeiten von Cyberangriffen durch Ransomware Gruppen, ist es für Unternehmen essenziell eine Strategie implementiert zu haben, die die Wiederherstellung von Daten ermöglicht. Durch die Verschlüsselung der Daten können Betriebsabläufe behindert, oder sogar komplett zum Stillstand gebracht werden. Neben diesen Schäden, können zusätzlich auch Daten durch Angreifer unbrauchbar gemacht werden, indem sie diese

verschlüsseln und nur gegen ein Lösegeld den dementsprechenden Entschlüsselungsschlüssel preisgeben [13]. Durch eine effektive Wiederherstellungsstrategie lässt sich im besten Fall die Zahlung des Lösegeldes vermeiden und idealerweise die Daten der Präsentation wiederherstellen.

Die Erstellung der Bachelorarbeit zielt darauf ab, die Wirksamkeit der ausgewählten Löschmethoden zu beleuchten und deren Auswirkung auf die Datenwiederherstellung beschreiben zu können. Leser dieser Arbeit profitieren nicht nur von einem Überblick über die eingesetzten Programme und deren Funktionen, sondern erhalten auch wertvolle Einblicke, wie durch die Anwendung sicherer Lösch- und Wiederherstellungsmethoden die IT-Sicherheit nachhaltig erhöht werden kann.

Zunächst werden Grundlagen zum Datenlöschen erläutert, da diese bedeutend für das Verständnis verschiedener Zusammenhänge in der Arbeit sind. Es wird auch einen Fokus auf die Bedeutung der Datenwiederherstellung gelegt, welcher die Effektivität des Datenlöschens mit seinen Ergebnissen unterstreicht. Nachdem eine gründliche Einführung in die genannten Themen erfolgt ist, folgt die Durchführung der Versuche, welche unter anderen auch die Beschreibung der ausgewählten Programme, sowie deren Ausführung beschreibt. Zuletzt werden die Ergebnisse, die aus den Versuchen resultieren, gegenübergestellt und miteinander verglichen. Hierbei wird als größter Bewertungsfaktor die Menge der wiederhergestellten Dateien aus dem Originaldatensatz gewählt. Es wird jedoch auch die Art und Weise betrachtet, wie die Dateien wiederhergestellt worden sind. Die entstandenen Abweichungen innerhalb der ausgewählten Programme werden beobachtet und ebenfalls bewertet.

Abschließend sei darauf hingewiesen, dass in dieser Bachelorarbeit teilweise technische Grundlagen zu spezifischen Themen beschrieben werden, um das Vorgehen in den Experimenten nachvollziehbar zu gestalten. Der Fokus der Arbeit liegt auf der Untersuchung der Effektivität von Datenlösch- und Datenwiederherstellungsverfahren.

2 Planung und Durchführung der Untersuchung

In dieser Bachelorarbeit wird ein praxisorientierter Ansatz verfolgt. Es werden im Laufe der Analyse verschiedene Datenträger wie SSD (Solid State Drive) und HDD (Hard Disk Drive) mit Daten beschrieben. Die genutzten Datenträger unterscheiden sich insofern, dass die Daten unterschiedlich darauf gespeichert werden. HDDs speichern die Daten auf rotierenden magnetischen Platten, die von einem mechanischen Schreib-/Lesekopf ausgelesen werden. SSDs hingegen nutzen sogenannte Flashspeicher, die im Gegensatz zu den Bauteilen in einer HDD nicht beweglich sind, wodurch sie schneller, leiser und robuster sind, da sie nicht durch eine physikalische Abnutzung beschädigt werden. Die Bezeichnung Flash steht hierbei als Synonym für schnell [15].

Auf diesen speziellen Datenträgern wird die Löschung und Wiederherstellung von Daten untersucht. In mehreren Szenarien werden diese Datenträger bzw. ihre Daten gelöscht, formatiert und überschrieben. Die dabei ablaufenden Vorgänge werden detailliert protokolliert, sodass am Ende der Analysen ein Vergleich verschiedener Arten der Datenlöschung und Datenwiederherstellung möglich ist.

Für die Analyse werden unter anderem die Programme Recuva und EaseUS Data Recovery verwendet, die automatisiert Daten auf dem jeweiligen Datenträger erkennen und zusammenfassen. Darüber hinaus kommen spezialisierte Anwendungen zum Einsatz, die erweiterte Kenntnisse erfordern, wie beispielsweise das File-Carving-Programm PhotoRec, bei dem der Zielpfad des Datenträgerimages über die Windows-Kommandozeile festgelegt werden muss, oder das IT-forensische Toolkit X-Ways Forensics, bei dem zunächst ein Fall angelegt und anschließend der Datenträger hinzugefügt wird.

3 Technischer Hintergrund zum Datenlöschen

Die Datenlöschung nimmt eine zentrale Bedeutung im Bereich der IT-Sicherheit ein. Dabei handelt es sich um einen Prozess, bei dem gespeicherte Informationen entfernt oder unzugänglich gemacht werden, dass ein Zugriff entweder vollständig verhindert oder nur mit erheblichem Aufwand realisiert werden kann. Die Datenlöschung auf Speichergeräten wie Festplattenlaufwerken (HDDs) und Solid-State-Drives (SSDs) erfolgt nach technologisch spezifischen Prinzipien, die sich aus der zugrunde liegenden Speichermethode der jeweiligen Technologie ergeben. Im Folgenden werden die technischen Prozesse und Unterschiede der Datenlöschung auf HDDs und SSDs erläutert, einschließlich der Auswirkungen auf Wiederherstellbarkeit, Datensicherheit und die Langlebigkeit der Geräte.

3.1 Festplattenlaufwerke (Hard Disk Drives)

HDDs speichern Daten magnetisch auf rotierenden Platten. Die Daten sind in Sektoren innerhalb von Spuren organisiert, wobei jeder Sektor binäre Informationen durch magnetische Ausrichtungen auf der Plattenoberfläche repräsentiert [15].

Man muss bei der Datenlöschung auf HDDs zwischen logischer und physikalischer Datenlöschung unterscheiden. Beim Löschen einer Datei auf einer Festplatte handelt es sich in der Regel um eine logische Löschung. Das bedeutet, dass der Dateiverweis im Dateisystem entfernt wird, ohne die in den Sektoren gespeicherten Daten direkt zu beeinflussen. Dieser Prozess umfasst die Aktualisierung des Dateisystems, in dem die zuvor von der Datei belegten Sektoren als verfügbar markiert werden. Dies erfolgt durch das Löschen der Verweise auf die Daten innerhalb der Master File Table (MFT) des NT File Systems (NTFS) oder in entsprechenden Strukturen anderer Dateisysteme. Die Daten bleiben in den Sektoren bestehen, jedoch behandelt das Betriebssystem diese Sektoren als freigegebenen Speicherplatz. Solange die gelöschten Sektoren nicht überschrieben wurden, können die Daten häufig mit speziellen Werkzeugen wiederhergestellt werden.

3.2 Solid-State-Drives (SSDs)

Solid State Drives (SSDs) hingegen nutzen NAND-Flash-Speicherzellen, bei denen Daten als Ladungszustände in den Speicherzellen gespeichert werden [21]. Aufgrund der Struktur des Flash-Speichers können Daten in SSD-Zellen nicht direkt überschrieben werden, ohne vorher einen Löschzyklus durchzuführen [15]. Bei SSDs erfolgt bei der logischen Datenlöschung durch den TRIM-Befehl eine komplexere Interaktion zwischen

dem Dateisystem und dem Flash-Speicher. Beim Löschen einer Datei signalisiert das Betriebssystem dem SSD-Controller durch den TRIM-Befehl, dass die Speicherzellen, in denen die Datei gespeichert war, nun ungültig sind. Dadurch wird die SSD-Firmware informiert, dass bestimmte Blöcke künftig überschrieben werden dürfen. Neben dem TRIM-Befehl gibt es auch die Garbage Collection. Diese beginnt anschließend und löscht die ungültig markierten Blöcke der SSD. Der Prozess läuft im Hintergrund ab, häufig während Leerlaufphasen, indem aktive Daten in einer geringeren Anzahl von Blöcken zusammengeführt und ungültige Blöcke freigegeben werden. Bei einer physikalischen Löschung einer SSDs sind Speicherverwaltungsfunktionen wie Wear-Leveling und Over-Provisioning im Einsatz, um die Abnutzung der Speicherzellen gleichmäßig zu verteilen und die Lebensdauer der SSD zu verlängern [17] . Das bloße Überschreiben ist aufgrund des Verschleißausgleichs bei SSDs weniger effektiv, da Daten möglicherweise auf andere physische Zellen umgeleitet werden als die, die die ursprünglichen Daten enthielten. Die meisten SSDs bieten ein vom Hersteller bereitgestelltes sicheres Löschprogramm an, das einen elektrischen Löschzyklus durchführt und alle Zellen auf ihren ursprünglichen Zustand zurücksetzt [10].

3.3 Physikalisches Datenlöschen

Bei der physikalischen Datenlöschung wird das Ziel verfolgt, Daten irreversibel zu entfernen, was insbesondere bei sensiblen Informationen erforderlich ist. Eine gründliche Datenlöschung kann beispielsweise durch das Degaussing, also der Entmagnetisierung erreicht werden. Dabei wird ein starkes Magnetfeld auf die gesamte Festplatte angewendet, wodurch die magnetischen Ausrichtungen der gespeicherten Daten vollständig zerstört werden. Dieser Prozess macht jedoch das Laufwerk unbrauchbar, da auch kritische Formatierungs- und Servospuren gelöscht werden. Als letzte Maßnahme zur Vernichtung von Speichermedien kommt die physische Zerstörung zum Einsatz. Methoden wie Schreddern, Zerkleinern oder Verbrennen beseitigen alle magnetischen und strukturellen Datenreste durch die Zerstörung der physischen Integrität der Festplatte, wodurch eine Wiederherstellung der Daten unmöglich wird. Dieser letzte Schritt wird auch vom BSI als sicherster Weg zum Löschen von Daten beschrieben [3].

3.4 Sicheres Datenlöschen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in ihrem Leitfaden *Daten auf Festplatten, Datenträgern und Smartphones sicher löschen* definiert ab wann Daten sicher gelöscht sind. Dies ist der Fall, wenn diese überschrieben werden. Trotz solcher sicheren Löschmethoden können in seltenen Fällen Restdaten durch magnetische

oder elektronische Rückstände verbleiben. Moderne Standards für sicheres Löschen berücksichtigen jedoch diese technischen Risiken und machen sie durch fortschrittliche Verschlüsselungs- und Löschverfahren in der Praxis vernachlässigbar [3].

3.5 Methoden des Datenlöschens

Ein international anerkanntes und häufig herangezogenes Regelwerk zur sicheren Datenlöschung ist die *NIST Special Publication 800-88 Revision 1 - Guidelines for Media Sanitization* [1]. Diese Publikation des National Institute of Standards and Technology (NIST) enthält detaillierte Empfehlungen zur Auswahl und Implementierung von Methoden für die sichere Entfernung von Daten. Sie berücksichtigt dabei verschiedene Typen von Speichermedien sowie spezifische Nutzungsszenarien. Die in der Publikation beschriebenen Techniken umfassen sowohl logische als auch physikalische Löschmethoden [1]. Während physikalische Löschung durch Überschreiben oder Zerstören des Datenträgers die Wiederherstellung praktisch unmöglich macht, wird in der Praxis häufig auf logische Löschmethoden zurückgegriffen, wie das Entfernen von Verweisen oder die Löschung von Verschlüsselungsschlüsseln. Diese Verfahren sind performanter und schonen Ressourcen, erfüllen jedoch nicht immer die höchsten Sicherheitsstandards [1]. Daher erfordert die Wahl der Löschmethode eine sorgfältige Abwägung zwischen Effizienz und den spezifischen Sicherheitsanforderungen. Eine weitere Richtlinie, die vom BSI erstellt wurde, beschreibt ebenfalls wie Daten sicher gelöscht werden können. Hier wird zusätzlich beschrieben, dass es ein Restrisiko auch bei einer vollständigen Formatierung gibt, dass Daten auf dem Datenträger überbleiben [3].

3.5.1 Logische Löschung auf Dateisystemebene und Metadatenstrukturen

Gängige Dateisysteme wie NTFS verwenden die Master File Table (MFT), während UNIX-basierte Systeme Inodes verwenden, um Dateimetadaten zu speichern. Bei der Löschung werden die Einträge lediglich als frei markiert, während die eigentlichen Daten unverändert bleiben, bis sie überschrieben werden. Da bei einer logischen Löschung nur die Verweise entfernt werden, sind die Daten weiterhin zur Wiederherstellung verfügbar, bis die Sektoren mit neuen Daten überschrieben wurden [9].

3.5.2 Vergleich der Schnellformatierung und Vollständigen Formatierung

Eine Schnellformatierung löscht keine Daten im klassischen Sinn, sondern aktualisiert lediglich das Dateisystem und die Metadatenstrukturen des Datenträgers. Die Informationen über die Dateizuordnungen werden entfernt, und der Datenträger wird so markiert, als wäre dieser leer und bereit für neue Daten. Die tatsächlichen Daten in den Blöcken

bleiben jedoch physisch unverändert auf der Festplatte gespeichert, bis sie durch neue Daten überschrieben werden. Für eine Festplatte im NTFS-Dateisystem beispielsweise bedeutet dies, dass die MFT oder andere Verwaltungsstrukturen zurückgesetzt werden, die Daten jedoch weiterhin im unallocated space (nicht zugewiesener Speicherplatz) vorhanden sein können [19].

Eine vollständige Formatierung hingegen führt in den meisten modernen Betriebssystemen neben dem Zurücksetzen des Dateisystems auch eine Überprüfung der Festplattensektoren durch. Zwar entfernt auch sie primär die Verweise im Dateisystem, jedoch gibt es die Option, alle Blöcke der Festplatte mit Nullen oder Zufallswerten zu überschreiben. Dieser Prozess verhindert, dass Daten in den Blöcken erhalten bleiben, und reduziert die Wahrscheinlichkeit, dass eine spätere Wiederherstellung erfolgreich ist. Jedoch ist es wichtig zu beachten, dass die vollständige Formatierung nicht immer das vollständige Überschreiben sicherstellt. In älteren Betriebssystemen oder bei einfachen Optionen für vollständige Formatierungen kann es vorkommen, dass lediglich eine Oberflächenprüfung ohne vollständiges Überschreiben stattfindet. In solchen Fällen bleiben Datenreste physisch vorhanden und können durch forensische Methoden extrahiert werden, wenn der überschreibende Prozess nicht tief genug erfolgt [20].

3.5.3 Firmware-gesteuerte sichere Löschbefehle auf SSDs

Moderne Dienstprogramme wie Samsung Magician, Intel SSD Toolbox und SanDisk SSD Dashboard ermöglichen den direkten Zugriff auf die SSD-Firmware, um sichere Löschbefehle unabhängig vom Betriebssystem auszuführen. Diese Programme nutzen ATA- (für SATA-SSDs) oder NVMe-Protokollbefehle wie „Secure Erase“ oder „Sanitize“, um eine Datenbereinigung auf physikalischer Ebene durchzuführen und sicherzustellen, dass keine Datenreste in den Speicherzellen verbleiben [11]. Nach dem Löschvorgang führen viele qualitativ hochwertigen Dienstprogramme Integritätsprüfungen durch, indem sie Prüfsummen über die gelöschten Blöcke berechnen und vergleichen, um den Löschvorgang zu verifizieren. Die Dienstprogramme verwenden Protokollbefehle auf Blockebene, die Datenlöschungen physisch auf NAND-Ebene ermöglichen, ohne auf Dateisystemzugriffe angewiesen zu sein. Dazu kommt eine Firmware-unterstützte Sicherheit. Einige SSDs verwenden proprietäre Protokolle, um Verschlüsselungsschlüssel sicher zu löschen, sodass alle Daten effektiv unlesbar werden. Beispielsweise bieten bestimmte Intel SSDs ein kryptografisches Löschprotokoll, das den Verschlüsselungsschlüssel entfernt, um eine sofortige und irreversible Datenlöschung zu erreichen. Moderne SSDs, insbesondere NVMe-Laufwerke, nutzen die parallele Architektur der NAND-Flash-Speicher, um Löschprozesse zu beschleunigen. Die Flash-Speicher sind in parallele Kanäle und Ebenen unterteilt, was eine gleichzeitige Verarbeitung von Lösch-

befehlen ermöglicht. Kanalbasierte Parallelität ermöglicht dem SSD-Controller gleichzeitig Löschbefehle an mehrere Kanäle zu senden, was die Zeit für eine vollständige Löschung erheblich reduziert. Durch eine Ebenenbasierte Blocklöschung kann eine parallele Löschoperationen auf mehreren Ebenen durchgeführt werden was bewirkt, dass Speicherplatz effizienter bereinigt werden kann. Einige SSDs ermöglichen bis zu vier parallele Löschprozesse pro Chip, was die Geschwindigkeit der Datenlöschung weiter erhöht.

3.5.4 Überschreibetechniken für sicheres Löschen von Daten auf Festplatten

HDDs können in der Regel unkomplizierter überschrieben werden, wodurch das Herstellen von Daten erschwert wird. Durch einen Single-Pass-Overwrite wird der Sektorinhalt einmal überschrieben, oft mit einem einfachen Bitmuster. Beim Multi-Pass-Overwrite, wie dem DoD 5220.22-M-Standard [16] werden mehrere Muster verwendet, um Reste von magnetischen Signalen zu minimieren. Eine andere Methode, die nach ihrem Erfinder Gutmann benannt ist, umfasst bis zu 35 Durchgänge mit verschiedenen Bitmustern, um sicherzustellen, dass keine magnetischen Rückstände verbleiben. Sie wurde ursprünglich für ältere Speichertechnologien entwickelt und ist auf modernen Festplatten oft nicht erforderlich.

3.5.5 Grenzen der Datenlöschung durch Formatieren bei HDDs

Oft reicht eine reine Formatierung nicht aus, um alle Daten von einem System zu entfernen. Selbst bei einer vollständigen Formatierung können spezialisierte forensische Programme in seltenen Fällen bestimmte Datenfragmente wiederherstellen, insbesondere wenn die Formatierung nur eine oberflächliche „Säuberung“ ohne mehrfaches Überschreiben durchführt. Solche Programme können verbliebene magnetische Spuren analysieren, was jedoch häufig nur mit hohem technischem Aufwand und bei älteren HDD-Technologien möglich ist. Insgesamt ist das Formatieren einer HDD effektiv für die schnelle Neunutzung oder Bereinigung für den allgemeinen Gebrauch. Für eine vollständige und sichere Datenlöschung, bei der die Wiederherstellung von Daten vollständig ausgeschlossen werden soll, sind jedoch spezielle Methoden wie mehrfaches Überschreiben (z. B. nach DoD-Standard) oder physische Zerstörung der Festplatte notwendig.

3.5.6 Kryptografisches Löschen als zusätzliche Löschmethode

Neben der normalen Datenlöschung stellt die vollständige Festplattenverschlüsselung eine zusätzliche Sicherheitsebene dar, indem die gespeicherten Daten ohne den zugehörigen kryptografischen Schlüssel unlesbar gemacht werden. Beim sogenannten krypto-

grafischen Löschen wird gezielt der Verschlüsselungsschlüssel sicher entfernt oder überschrieben, was dazu führt, dass die verschlüsselten Daten nicht mehr entschlüsselt und somit effektiv als gelöscht betrachtet werden können [3]. Diese Methode ist besonders effizient, da sie unabhängig von der physischen Speichermedienstruktur funktioniert und auch bei großem Datenvolumen eine schnelle Lösung bietet.

3.6 Methoden der Datenwiederherstellung

Die Datenwiederherstellung umfasst spezialisierte Techniken und Werkzeuge zur Rekonstruktion verlorener oder gelöschter Daten von Speichermedien. Diese Methoden sind abhängig von der Art des Speichermediums und dem Umfang der Löschvorgänge, die auf das Medium angewendet wurden. Die Wiederherstellung erfolgt typischerweise auf mehreren Ebenen: logische Wiederherstellung auf Dateisystemebene, physische Wiederherstellung auf Blockebene und die Anwendung fortgeschrittener Techniken zur Analyse von Restdaten.

3.6.1 Logische Datenwiederherstellung

Die logische Datenwiederherstellung basiert auf der Analyse von Dateisystemstrukturen, um verlorene oder gelöschte Dateien wieder zugänglich zu machen, ohne dass ein direkter Zugriff auf die physischen Speicherzellen erforderlich ist. Dabei werden Dateisystem-Metadaten, wie beispielsweise die Haupttabellen des Dateisystems, ausgewertet. Durch die Suche nach nicht verknüpften Einträgen im Dateisystem und die Rekonstruktion von Inhalten anhand intakter Verweisinformationen können verlorene Informationen effizient wiederhergestellt werden. Ein wesentlicher Vorteil der logischen Wiederherstellungsmethode besteht darin, dass sie selbst bei beschädigten oder unvollständigen Dateistrukturen einsetzbar ist, sofern wichtige Metainformationen noch vorhanden sind. Diese Methode ist besonders effektiv, da sie gezielt nach logischen Verweisen sucht, anstatt den gesamten Speicherbereich sektorweises zu analysieren. Dies spart Zeit und minimiert das Risiko, bestehende Daten während des Wiederherstellungsprozesses zu beeinträchtigen [22].

Die logische Datenwiederherstellung zeichnet sich zudem durch ihre Vielseitigkeit aus, da sie mit unterschiedlichen Dateisystemen wie NTFS, FAT oder extended (ext) kompatibel ist. Dies macht sie zu einer universellen Lösung in heterogenen IT-Umgebungen, in denen verschiedene Speichermedien und Betriebssysteme verwendet werden. Darüber hinaus spielt diese Methode eine wichtige Rolle in der IT-Forensik. Sie ermöglicht nicht nur die Wiederherstellung gelöschter Dateien, sondern auch die Analyse von Metadaten

wie Erstellungs- und Zugriffszeitpunkten. Diese Informationen sind in forensischen Untersuchungen von großer Bedeutung, da sie wertvolle Hinweise auf die Nutzung und Manipulation von Daten liefern können.

Insgesamt bietet die logische Datenwiederherstellung eine nicht-invasive, flexible und effektive Möglichkeit, Datenverluste zu beheben, und ist dabei gleichermaßen für private, betriebliche und forensische Anwendungen geeignet. Sie stellt eine risikoarme Lösung dar, die sowohl eine schnelle Wiederherstellung als auch eine umfassende Analyse von Dateisystemstrukturen ermöglicht.

3.6.2 Physische Datenwiederherstellung

Die physische Datenwiederherstellung geht über die logische Ebene hinaus und greift direkt auf die physischen Sektoren oder Blöcke des Speichermediums zu. Diese Methode ist vor allem bei schweren Datenverlusten erforderlich, wenn Metadaten oder Dateisysteme beschädigt wurden oder überschrieben sind. Durch direkten Blockzugriff können Programme wie ddrescue und HDClone sektorweises Überprüfen und blockbasierte Zugriffstechniken durchführen, um physische Sektorinformationen unabhängig vom Dateisystem zu kopieren. In seltenen Fällen kann versucht werden, Daten auch von beschädigten Datenträgern wiederherzustellen, da hierauf Restspuren enthalten sein können, wie in Kapitel 3.4 beschrieben. Diese Programme erstellen oft ein bitweises Abbild des gesamten Speichermediums, das anschließend auf intakte Datenfragmente analysiert wird. Des Weiteren kann auf magnetischen Festplatten die Datenwiederherstellung durch die Nutzung magnetischer Remanenz erfolgen. Diese Techniken sind besonders relevant für die forensische Datenrekonstruktion und erfordern spezialisierte und teilweise kostspielige Hardware. Es gibt auch Szenarien, bei denen eine Rekonstruktion von Daten theoretisch unmöglich ist wie beispielsweise die Entmagnetisierung des Datenträgers [23].

3.6.3 Wiederherstellung bei SSDs

Aufgrund der TRIM-Funktion und des Garbage-Collection-Prozesses kann die Wiederherstellung von Daten auf SSDs besonders herausfordernd sein. Da diese Technologien gelöschte Datenzellen automatisch freigeben, ist der herkömmliche Zugriff auf gelöschte Daten begrenzt. Bei der Wiederherstellung ohne TRIM, wie es beispielsweise in Redundant Array of Independent Disks (RAID) Konfigurationen eingesetzt wird, oder auf älteren SSDs, die TRIM nicht unterstützen, bleibt die Datenstruktur in den Zellen länger erhalten [17]. Programme wie Disk Drill und UFS Explorer nutzen diese Gegebenheiten, um auf intakte Datenzellen zuzugreifen und Dateien zu rekonstruieren, bevor sie durch neue Daten überschrieben werden. Einige Hersteller bieten proprietäre Firmware-Wie-

derherstellungsprogramme an, die Zugriff auf interne Speicherstrukturen gewähren. Beispielsweise ermöglicht das Samsung Magician-Tool bei bestimmten Modellen die Wiederherstellung von Daten in Blöcken, die als frei markiert sind, aber noch keine physische Bereinigung erfahren haben.

3.6.4 Image- und Klontechniken zur Datenextraktion

Eine häufige Methode zur Datenwiederherstellung, insbesondere bei beschädigten oder instabilen Laufwerken, ist das Erstellen eines Abbilds (Image) des Speichermediums. Das Abbild kann dann analysiert werden, um auf intakte Daten zuzugreifen, ohne das Original weiter zu belasten. Programme wie FTK Imager und X-Ways Forensics erstellen eine exakte bitweise Kopie des Speichermediums. Diese Abbilddateien können anschließend untersucht werden, ohne dass weitere physische Zugriffe auf das beschädigte Original erforderlich sind. Eine Alternative ist das Klonen mit ddrescue, welches Laufwerksklone erzeugt und fehlerhafte Sektoren überspringen kann, um möglichst viele Daten zu extrahieren. Es eignet sich besonders für beschädigte Laufwerke und wird oft als erster Schritt in komplexeren Wiederherstellungsprozessen verwendet [24].

4 Bedeutung der Datenwiederherstellung

Obwohl es keine spezifische Richtlinie gibt, die Unternehmen zur Sicherstellung der Datenwiederherstellung verpflichtet, gewinnt dieses Thema angesichts der zunehmenden Bedrohung durch Cyberangriffe, insbesondere durch Ransomware Gruppen und der damit einhergehenden Verschlüsselung der IT-Infrastruktur, immer mehr an Bedeutung. Die Bundesanstalt für Finanzdienstleistungsaufsicht beispielsweise verlangt von Finanzunternehmen Maßnahmen zur Sicherstellung der Verfügbarkeit von IT-Systemen und Daten. Dies ist in speziellen Richtlinien wie den *Bankaufsichtlichen Anforderungen an die IT* (BAIT) festgelegt worden und regelt somit den Umgang mit Anforderungen an die IT von Banken [8].

4.1 Versehentliches Löschen und Betriebskontinuität

Ein großer Anteil der Datenverluste resultiert aus unbeabsichtigtem Löschen durch Benutzer/innen oder Administrator/innen, was zu Betriebsunterbrechungen und erheblichen finanziellen Einbußen führen kann. Die Fähigkeit, gelöschte Daten ohne vollständige Abhängigkeit von Backups wiederherzustellen, ist daher essenziell für die Betriebskontinuität und zur Reduktion von finanziellen Schäden. In diesem Fall kann häufig die Wiederherstellung von Dateisystemen und Metadaten wie in Abschnitt 3.6.1 beschrieben, genutzt werden, da häufig nur ein logischer Löschvorgang genutzt wird.

4.2 Digitale Forensik und Beweissicherung

In forensischen und juristischen Untersuchungen ist die Wiederherstellung gelöschter Daten von zentraler Bedeutung für die Beweissicherung. Forensische Analyst/innen können durch die Wiederherstellung digitaler Spuren wertvolle Erkenntnisse über kriminelle Aktivitäten oder Verstöße gegen Vorschriften gewinnen. Da übliche vom Endnutzer/innen genutzte Löschmethoden, wie das Papierkorb leeren, oft nur die Dateiverweise entfernen, ist häufig eine logischen Datenwiederherstellung, wie in Abschnitt 3.6.1 beschrieben, ausreichend. In seltenen Fällen, in denen Restdaten auf magnetischen Speichermedien wie Festplatten bestehen bleiben, müssen diese mit erhöhtem Aufwand rekonstruiert werden (Abschnitt 3.6.2).

4.3 Disaster Recovery und Business Resilience

In Fällen physischer Katastrophen oder Cyberangriffen, wie Ransomware-Angriffe, kann die Datenwiederherstellung entscheidend sein, um die Geschäftskontinuität zu sichern. Die Fähigkeit, gelöschte oder verschlüsselte Daten zu rekonstruieren, erhöht die Widerstandsfähigkeit von Unternehmen und unterstützt den Notfallwiederherstellungsprozess. Das Unternehmen IBM hat in ihrem Leitfaden *Was ist BCDR?* [12] beschrieben, dass die Prävention von Datenverlusten und Ausfallzeiten stetig teurer werden und somit ein lauffähiges Business Continuity Disaster Recovery Plan unabdingbar ist. Obwohl mehrfache Überschreibmethoden wie der DoD 5220.22-M-Standard [16] eine Wiederherstellung verhindern sollen, können moderne Recovery-Programme zur physikalischen Wiederherstellung (Abschnitt 3.6.2) manchmal dennoch teilweise Daten wiederherstellen, wenn bestimmte Sektoren nicht vollständig überschrieben wurden. Dies kann in Notfällen eine kritische Rettungsoption für wichtige Daten darstellen.

5 Auftretende technische Komplikationen

Das Format und die Struktur eines Dateisystems sind entscheidende Faktoren, die sowohl die Datenlöschung als auch die Datenwiederherstellung maßgeblich beeinflussen. Dateisysteme wie FAT32, NTFS oder ext4 organisieren Daten auf unterschiedliche Weise, wodurch spezifische Herausforderungen entstehen. Eine zentrale Schwierigkeit kann die Fragmentierung sein, bei der Dateien nicht in einem zusammenhängenden Bereich, sondern über verschiedene Sektoren eines Speichermediums verteilt gespeichert werden.

Fragmentierte Daten stellen bei der Löschung ein Risiko dar, da einzelne Fragmente unabsichtlich erhalten bleiben und somit potenziell wiederhergestellt werden können. Umgekehrt erschwert die Fragmentierung auch die Datenwiederherstellung, da eine präzise Analyse der Speicherstruktur erforderlich ist, um alle Fragmente korrekt zu rekonstruieren [25]. Das Verständnis dieser Zusammenhänge ist essenziell, um Schwachstellen in aktuellen Technologien zu identifizieren und effektive Strategien für sichere Datenlösch- und Wiederherstellungsmethoden zu entwickeln.

5.1 Löschmethoden in Abhängigkeit vom Dateisystem

Verschiedene Dateisysteme nutzen verschiedene Ansätze zur Verwaltung von Dateien, insbesondere was die Metadatenverwaltung betrifft. Diese Metadaten beeinflussen, was passiert, wenn eine Datei gelöscht wird, und haben direkte Auswirkungen auf die Wiederherstellbarkeit [27]. Um eine Übersicht über die gängigsten Dateisysteme zu bekommen, sind Unterschiede im Folgenden aufgelistet und detailliert beschrieben.

- NTFS (New Technology File System): NTFS verwendet eine Master File Table (MFT), die jeden Dateieintrag auf dem Datenträger mit einer Reihe von Attributen speichert. Beim Löschen einer Datei wird der Eintrag in der MFT lediglich als „frei“ markiert, während die eigentlichen Daten unverändert bleiben. Das MFT-Attribut „in use“ wird gelöscht, aber die Datenblöcke auf dem Datenträger werden nicht sofort überschrieben. Diese Eigenschaft macht gelöschte Dateien auf NTFS-Laufwerken oft einfach wiederherstellbar, solange sie nicht überschrieben wurden.
- FAT32 (File Allocation Table 32): FAT32, das in älteren Windows-Versionen und kleineren Speichermedien verwendet wird, arbeitet mit einer Zuordnungstabelle (FAT), die die Dateiblöcke auf dem Laufwerk verwaltet. Beim Löschen einer Datei entfernt FAT32 den Verweis auf die Datei aus dem Verzeichnis, mar-

kiert die zugehörigen Cluster als frei und löscht den ersten Buchstaben des Dateinamens. Da der tatsächliche Inhalt auf dem Datenträger unverändert bleibt, können Wiederherstellungsprogramme den ursprünglichen Dateinamen und die Daten wiederherstellen, solange keine neuen Daten die Blöcke überschrieben haben.

- ext4 (Fourth Extended Filesystem): Das ext4-Dateisystem ist ein Journaling-Dateisystem und verbreitet auf Linux-Systemen. Es speichert Dateien über Inodes, die Informationen wie Dateigröße, Erstellungszeit und Blockzuordnung speichern. Bei der Standard-Löschung in ext4 wird der Inodes-Verweis gelöscht, und die Blöcke werden als „frei“ markiert, aber nicht überschrieben. Wiederherstellung ist möglich, jedoch etwas schwieriger als bei NTFS, da ext4 standardmäßig bestimmte Datenblöcke verschlüsselt und Metadaten effektiv löscht.
- APFS (Apple File System): APFS nutzt ebenfalls Journaling und strukturiert Daten in Containern und Volumes. APFS verwendet Klone für Speicherplatzersparnis und schnelle Snapshots für Backups. Beim Löschen wird nur der Verweis auf die Datei entfernt, und die Daten können mit speziellen Programmen, die die Snapshot- und Cloning-Funktionen umgehen, wiederhergestellt werden. Die Wiederherstellung ist jedoch schwerer als bei FAT- oder NTFS-basierten Systemen, da APFS automatisch auf Speicherbereinigung ausgelegt ist.

5.2 Einfluss von Journaling und Metadatenverwaltung

Die Journaling-Funktion einiger Dateisysteme, wie sie bei NTFS, ext4 und APFS existiert, spielt ebenfalls eine bedeutende Rolle. NTFS und ext4 verfügen über Journaling-Mechanismen, die alle Änderungen in einem Protokoll (Journal) aufzeichnen, bevor sie ausgeführt werden. Wenn eine Datei gelöscht wird, kann das Journal Einträge enthalten, die gelöschte Dateien identifizierbar machen, bis der Journaleintrag überschrieben oder gelöscht wird [28]. Hier können forensische Werkzeuge aus dem Journal Hinweise auf den Inhalt und die Existenz der Datei extrahieren. FAT32 hat kein Journaling. Dies bedeutet, dass gelöschte Daten nur im Verzeichnis entfernt werden, ohne dass ein zusätzlicher Speicherort zur Verfolgung der Änderungen existiert. APFS führt ebenfalls ein Journal und kann durch Snapshots ältere Versionen speichern. Der Snapshot-Mechanismus kann ältere Dateiversionen oder gelöschte Dateien enthalten, sofern diese nicht explizit entfernt wurden. Das Wiederherstellen aus einem APFS-Snapshot ist jedoch anspruchsvoller, da Apple spezifische Verschlüsselungsmechanismen einsetzt.

5.3 Auswirkungen der Fragmentierung

Fragmentierung tritt auf, wenn das Dateisystem die Daten einer Datei in nicht zusammenhängenden Blöcken über den Datenträger verteilt. Dieser Effekt kann sowohl bei Festplatten (HDDs) als auch bei Solid-State-Drives (SSDs) auftreten, ist jedoch aufgrund der physischen Zugriffsstruktur bei HDDs besonders relevant [25]. Die Fragmentierung hat tiefgreifende Auswirkungen auf das Löschen und die Wiederherstellung von Daten und beeinflusst den Erfolg und die Methoden, die bei der Datenrekonstruktion eingesetzt werden können.

Die Fragmentierung erschwert den Löschprozess, da sie sicherstellt, dass die Daten einer einzelnen Datei an mehreren nicht zusammenhängenden Orten auf dem Datenträger gespeichert werden. Dies hat je nach Löschmethode und Dateisystem verschiedene Konsequenzen. Bei den meisten Dateisystemen (z. B. NTFS, FAT32, ext4) markiert das Betriebssystem die Datenblöcke einer Datei als „frei“, wenn die Datei gelöscht wird, ohne die tatsächlichen Daten sofort zu überschreiben. Da fragmentierte Dateien auf viele verschiedene Cluster verteilt sind, können diese als frei markierten Cluster im gesamten Dateisystem verstreut sein. Dies erhöht die Wahrscheinlichkeit, dass Fragmente der Datei durch zukünftige Schreibvorgänge nur teilweise überschrieben werden, was das vollständige Löschen ohne gezielte Überschreibmethoden erschwert. Gezielte Löschmethoden und ihre Wirksamkeit wie Multi-Pass-Overwrites können durch Fragmentierung beeinflusst werden. Bei fragmentierten Daten ist es erforderlich, jeden betroffenen Cluster zu überschreiben, was den Aufwand erhöht. Für eine vollständige Datenentfernung muss das Löschprogramm jedes Cluster der fragmentierten Datei identifizieren und löschen, was die Effizienz der Methode vermindern kann. Diese Herausforderung ist besonders bei Festplatten spürbar, da fragmentierte Blöcke zu erhöhtem mechanischem Aufwand führen [29].

Fragmentierte Dateien stellen für Wiederherstellungsprogramme eine besondere Herausforderung dar, da diese Programme die Verknüpfung von Fragmenten rekonstruieren müssen, um die Datei in ihrem ursprünglichen Zustand wiederherzustellen [29]. Dieser Prozess ist komplex und wird durch verschiedene Faktoren beeinflusst. Wenn eine fragmentierte Datei gelöscht wurde, bleibt häufig nur der Verweis auf die einzelnen Datenfragmente erhalten. Bei Dateisystemen wie NTFS können Wiederherstellungsprogramme die Dateieinträge in der Master File Table (MFT) nutzen, um die Verknüpfung der Fragmente zu rekonstruieren. FAT32 und ähnliche Dateisysteme verwenden eine Zuordnungstabelle (File Allocation Table/FAT), um die Cluster einer Datei zu verfolgen. Bei ext4 wird dies durch das extents-Feature erleichtert, das größere, zusammenhängende Datenblöcke anlegt und so die Fragmentierung reduziert. Trotzdem bleibt die Wiederherstellung fragmentierter Dateien komplex, da diese Dateiverweise oft unvollständig oder

beschädigt sind. Der Fragmentierungsgrad beeinflusst direkt die Erfolgschancen der Wiederherstellung. Stark fragmentierte Dateien, deren Fragmente weit über den Datenträger verteilt sind, weisen häufig eine höhere Wiederherstellungsschwierigkeit auf, da einzelne Fragmente möglicherweise bereits von neuen Daten überschrieben wurden. Auch ist es für Wiederherstellungsprogramme schwieriger, die richtige Reihenfolge der Fragmente zu bestimmen, was insbesondere bei textbasierten oder unkomprimierten Datenformaten zur Fehleranfälligkeit führen kann. Bestimmte Wiederherstellungssoftware ist darauf ausgelegt, fragmentierte Dateien gezielt zu rekonstruieren, indem sie tiefergehende Analysen der Dateiverweise und -zuordnungen im Dateisystem vornimmt. Programme wie R-Studio und TestDisk durchsuchen Dateisystemstrukturen, um fragmentierte Einträge aufzuspüren und wiederherzustellen. Diese Programme greifen auf Metadaten und bekannte Datenmuster zu, um zusammengehörige Fragmente zu identifizieren und in ihrer ursprünglichen Anordnung zu rekonstruieren. Der Erfolg hängt jedoch stark davon ab, wie intakt die ursprünglichen Verweise sind.

5.4 Schlussfolgerung

Insgesamt zeigt sich, dass die effiziente Verwaltung von Dateisystemen und die gezielte Reduktion von Fragmentierung entscheidend für die Leistung, Sicherheit und Lebensdauer von Datenträgern sind. Die Wahl eines fragmentierungsresistenten Dateisystems – wie ext4, APFS, ZFS oder Btrfs – ermöglicht es, bereits auf Ebene des Dateisystems eine strukturierte und zusammenhängende Speicherung von Daten sicherzustellen. Besonderheiten bei Dateisystemen wie ZFS oder auch Btrfs sind, dass der gesamte verfügbare Speicherplatz der eingesetzten Speichermedien zu einem Pool zusammengefasst wird. Dieser wird dem Anwendenden vom System zur Verfügung gestellt. Diese Systeme minimieren die Fragmentierung durch innovative Techniken wie Extents, Cloning und Copy-on-Write und gewährleisten damit eine optimierte Datenorganisation, die nicht nur die Leistung verbessert, sondern auch die Wiederherstellbarkeit und Konsistenz der Daten sicherstellt [30]. Mechanische Festplatten profitieren insbesondere von regelmäßigen Defragmentierungen und einer gut gewählten Blockgröße, da die physische Anordnung von Daten direkten Einfluss auf die Zugriffszeiten hat. SSDs hingegen erfordern angepasste Optimierungen wie TRIM und Garbage Collection, um durch gezielte Speicherfreigaben und gleichmäßiges Wear Leveling die Zellenabnutzung zu verringern. Diese SSD-spezifischen Technologien sorgen nicht nur für eine konsistente Schreibgeschwindigkeit, sondern minimieren auch fragmentierte Speicherzugriffe, die die Lebensdauer der Hardware beeinträchtigen könnten.

Erweiterte Dateisysteme wie ZFS und Btrfs bieten durch Snapshots, Journaling und RAID-Unterstützung eine hohe Datensicherheit und Redundanz, was vor allem in unternehmenskritischen Umgebungen von Vorteil ist [28].

Abschließend lässt sich feststellen, dass eine Kombination aus geeigneter Dateisystemwahl, regelmäßiger Defragmentierung, SSD-spezifischen Optimierungen und konsistenter Wartung die Fragmentierungsprobleme nachhaltig reduziert und gleichzeitig die Datenträgerleistung maximiert. Diese strategischen Maßnahmen ermöglichen einen zuverlässigen und schnellen Datenzugriff und verlängern die Lebensdauer der Speichermedien, was insbesondere bei unternehmenskritischen Anwendungen, aber auch im alltäglichen Gebrauch erhebliche Vorteile bietet.

6 Einhaltung von Datenschutz und IT-Sicherheit

Die Einhaltung von Datenschutz und IT-Sicherheit ist entscheidend, um rechtliche Vorgaben wie die Datenschutzgrundverordnung (DSGVO) und das Bundesdatenschutzgesetz (BDSG) zu erfüllen sowie sensible Informationen zu schützen. Die Datenlöschung spielt dabei eine zentrale Rolle, da sie klare Anforderungen an die sichere und vollständige Vernichtung personenbezogener Daten definiert. Unternehmen müssen sicherstellen, dass Daten nur für legitime Zwecke erhoben und nicht länger als nötig gespeichert werden [4]. Dies erfordert regelmäßige Überprüfungen der Aufbewahrungsrichtlinien sowie die Implementierung sicherer Löschmethoden wie ATA Secure Erase oder kryptografisches Löschen, um eine Wiederherstellung zu verhindern.

Artikel 17 der DSGVO gibt betroffenen Personen das Recht, die Löschung ihrer Daten zu verlangen. Dabei sind fortschrittliche Verfahren wie mehrfaches Überschreiben, Degaussing oder spezialisierte Software notwendig, um auch bei modernen Speichermedien wie SSDs die Wiederherstellbarkeit zu verhindern. Zusätzlich fordert Artikel 25 der DSGVO den Einsatz von Datenschutz durch Technik, etwa durch Verschlüsselung oder Firmware-gesteuerte Löschprogramme, um gelöschte Daten dauerhaft unzugänglich zu machen. Besonders bei sensiblen Daten bietet die kryptografische Löschung, bei der die Verschlüsselungsschlüssel entfernt werden, eine effiziente Lösung, die zugleich die Lebensdauer der Hardware schont. Unternehmen sind zudem verpflichtet, alle Löschvorgänge sorgfältig zu dokumentieren, um ihre Rechenschaftspflicht gemäß Artikel 5 der DSGVO zu erfüllen. Die Protokollierung von Löschmethoden, etwa mit Programmen wie ATA Secure Erase oder Prüfsummenvergleichen, ermöglicht eine lückenlose Nachverfolgbarkeit und dient als Nachweis gegenüber Behörden. Sichere Löschtechniken minimieren auch das Risiko von Datenschutzverletzungen. Sollte es dennoch zu Vorfällen kommen, ist eine schnelle Reaktion innerhalb von 72 Stunden erforderlich. Dabei müssen Wiederherstellungsmaßnahmen, wie sie etwa für forensische Analysen genutzt werden, DSGVO-konform durchgeführt werden.

Integrität, Vertraulichkeit und Zugriffskontrolle stehen im Zentrum moderner Sicherheitsanforderungen. Standards wie ISO/IEC 27001 und der EU-Cybersecurity-Act [7] betonen die Bedeutung des Schutzes sensibler Daten durch sichere Löschmethoden wie Multi-Pass-Overwrites, kryptografisches Löschen oder Degaussing. Diese Techniken stellen sicher, dass Daten insbesondere bei der Außerbetriebnahme von Systemen unzugänglich werden. Rollenbasierte Zugriffskontrollen und eine umfassende Protokollierung stellen sicher, dass Löschvorgänge ausschließlich von autorisierten Personen durchgeführt werden. Gleichzeitig gewährleistet geeignete Software die Dokumentation von

Prüfpfaden und die Einhaltung von Sicherheitsrichtlinien. Zusätzlich sind Datenwiederherstellung und forensische Untersuchungen wichtige Bestandteile eines robusten Sicherheitskonzepts. Nach der EU-Richtline für Netz -und Informationssicherheit (NIS2) [6] müssen Unternehmen in der Lage sein, gelöschte Daten für die Beweissicherung und Rekonstruktion von Vorfällen wiederherzustellen. Regelmäßige Tests zur Datenwiederherstellung aus dem Backup gewährleisten die forensische Bereitschaft und erhöhen die Reaktionsfähigkeit bei Sicherheitsvorfällen. Für die Geschäftskontinuität und Bedrohungsabwehr betont der EU-Cybersecurity-Act [7] die Notwendigkeit der Datenverfügbarkeit bei Cybervorfällen. Temporäre Maßnahmen, wie die Deaktivierung der Garbage Collection auf SSDs, ermöglichen die schnelle Wiederherstellung geschäftskritischer Daten. Standards wie NIST SP 800-88 [1] und Empfehlungen des BSI [3] unterstreichen die Bedeutung sicherer Löschverfahren, um Datenverluste zu vermeiden, und empfehlen physische Zerstörung für Datenträger am Ende ihres Lebenszyklus. So wird die Widerstandsfähigkeit gegenüber Bedrohungen und die Kontinuität des Geschäftsbetriebs sichergestellt.

7 Konkrete Problemstellung für die Versuchsreihe

Nach jedem Löschszenario und dessen Untersuchung mit den Werkzeugen, muss der Datenträger sicher gelöscht werden.

Wie in Abschnitt 3.5 beschrieben wird in den Versuchen, die in dieser Bachelorarbeit durchgeführt werden, die Daten nach dem Leitfaden des BSI sicher gelöscht. Die Löschverfahren zwischen den Versuchen werden durch das Tool Parted Magic umgesetzt. Dieses wird durch eine dedizierte Linux Distribution abgebildet und wird über einen Live USB-Stick gestartet. Hierbei muss dieser über das jeweilige Bootmenü eines Rechners gebootet werden. Die Distribution bietet neben dem Überprüfen des Zustandes eines Datenträgers oder dem Partitionieren eines Volumes auch die Möglichkeit über verschiedene Methoden einen Datenträger sicher löschen zu können (*Erase Disk*). Die Möglichkeiten sind in den folgenden Abbildungen 1 und 2 zu sehen.

Für das Überschreiben der HDD wird die Funktion *Disk – Write zeros to the entire drive using dd* genutzt. Dies stellt bestmöglich sicher, dass auf der Festplatte keine Datenreste mehr vorhanden sind.

Für das Überschreiben der SSD wird die Funktion *Secure Erase – ATA Devices* genutzt. Hier wird die Enhanced Methode gewählt, diese soll den Datenträger sicherer löschen als die Standard Methode.

Um sicher zu stellen, dass sich keine Datenreste mehr auf dem jeweiligen Datenträger befinden, wird dieser Vorgang bei jedem sicheren Löschen zweifach durchgeführt.

Abbildung 1: Löschmethoden Parted Magic (1)

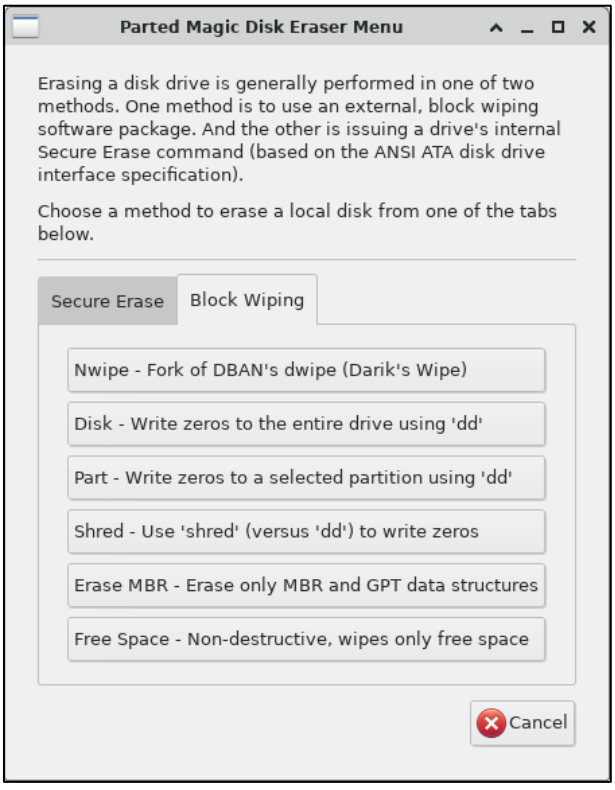


Abbildung 2: Löschmethoden Parted Magic (2)

8 Durchführung

Die Bachelorarbeit widmet sich der Untersuchung der Effektivität verschiedener Löschmethoden und analysiert, wie effektiv die gewählten Datenlöschmethoden auf Festplatten (HDD) und Solid-State-Drives (SSD) wirken. Hierzu werden sowohl gängige Wiederherstellungsprogramme wie Recuva und EaseUS data recovery als auch spezialisierte IT-forensische Werkzeuge wie PhotoRec und X-Ways eingesetzt, um die Genauigkeit und Tiefe der Datenwiederherstellung zu testen. Die in der Bachelorarbeit eingesetzten Programme sind im Anhang näher erläutert.

8.1 Vorstellung des Originaldatensatzes

Der, auf den Abbildungen A1-A5 im Anhang, abgebildete Originaldatensatz beinhaltet insgesamt 209 Dateien auf 3 Ordner verteilt. Dort sind alle Dateien zu sehen, die auch teilweise in der Bachelorarbeit genannt werden.

Die Inhalte der Ordner und ZIP-Archive sind:

1. **1_Der Stein der Weisen** beinhaltet 108 MP3 Dateien.
2. **OneDrive_2024-11-10** mit dem Unterordner **OneDrive Testdaten Download** beinhaltet insgesamt 6 pdf Dateien.
3. **Testdaten.zip** enthält eine identische Kopie des im Stammverzeichnisses befindlichen Dateien, ohne die Datei **OneDrive_2024-11-10.zip.**
4. **Greta Van Fleet.zip** enthält 23 JPG-Bilddateien und 8 MP4 Videodateien.
5. **OneDrive_2024-11-10.zip** ist ein ZIP-Archiv des Ordners OneDrive_2024-11-10.

Die ZIP komprimierten Ordner werden im Dateisystem als Dateien gewertet, jedoch sind die Archive nicht Passwortgesichert, sodass die Dateien problemlos durch ein Tool aus diesem extrahiert und wiederhergestellt werden können.

Die Dateien in den zip komprimierten Ordnern sind teilweise komprimiert worden, sodass beim Wiederherstellen teilweise alle Dateien wiederhergestellt worden sind, jedoch die Größe der Dateien im Ordner der wiederhergestellten Dateien nicht mit der des Originaldatensatzes übereinstimmt. Durch einen Vergleich der Hashwerte konnte jedoch die Gleichheit bestätigt werden.

Für HDD und SSD werden die gleichen Originaldatensätze verwendet.

Nachfolgende Tabelle 1 zeigt eine Übersicht der Dateien, die im Originaldatensatz enthalten sind. In den Szenarien werden diese Tabellen ebenfalls als Übersichten genutzt, um einen schnellen Vergleich der wiederhergestellten Dateien durchführen zu können.

Datei-typ	Vorhandene Dateien
zip	3
xlsx	11
txt	10
png	2
pdf	16
pcap	1
mp3	108
mp4	8
json	10
jpg	27
jfif	1
heic	2
csv	10
Gesamt	209

Tabelle 1: Dateien Original Datensatz HDD und SSD

8.2 Vorbereitung des jeweiligen Datenträgers

Für diesen Zweck wird zu Beginn jedes Versuches der jeweilige Datenträger mit dem Dateisystemformat NTFS formatiert. Anschließend wird dieser mit einem umfangreichen

Datensatz beschrieben, um ein praxisnahes Szenario abzubilden. Im Anschluss wird ein erstellter Datensatz mit diversen Dateien unterschiedlicher Dateiformate auf den Datenträger kopiert. Darunter befinden sich .txt, .pdf, Bild/-Videodateien und andere Dateiformate, siehe Tabelle 1. Hierbei werden teilweise private Daten wie Bilder oder Videos verwendet, um ein realitätsnahes Szenario nachzubilden und Datenschutz und Urheberrechte zu gewährleisten. Zusätzlich wurden auch mit einem Python Skript zufällige Dateien erstellt. Ordner und ZIP-Archive wurden ebenfalls mit in den Datensatz aufgenommen. Um die Integrität der Daten sicherzustellen, wurde vor dem Kopiervorgang ein Secure Hash Algorithm (SHA1) Hashwert der Originaldaten erstellt. Nach Abschluss des Kopiervorgangs wurde dieser Hashwert erneut für die Daten auf dem Ziel-Datenträger erzeugt, um die Übereinstimmung der Daten zu überprüfen.

Nach jedem Versuch muss der jeweilige Datenträger bereinigt werden, damit keine Datenreste für den nächsten Versuch übrigbleiben. Dies wird durch die Software Parted Magic realisiert, dessen genutzte Version im Anhang näher erläutert ist. Diese wurde ausgewählt, da sie über einen Live Linux USB Stick ausgeführt wird und auch auf einer SSD die Speicherzellen so umschreibt, dass diese nicht mehr mit Daten beschrieben sind.

8.3 Löschvorgänge

Die anschließenden Lösch- und Formatierungsvorgänge werden in mehreren Stufen durchgeführt:

Szenario 1: Die auf dem Datenträger befindlichen Dateien werden in den Papierkorb verschoben und anschließend endgültig gelöscht, indem der Papierkorb geleert wird.

S*zenario 2*: Mit der Tastenkombination „Shift + Entf“ unwiderruflich entfernt.

Szenario 3: Der Datenträger wird per Schnellformatierung formatiert.

Szenario 4: Der Datenträger wird über die vollständige Formatierung in der Datenträgerverwaltung formatiert.

Die aufgezeigten Szenarien werden jeweils einmal auf der HDD und auf der SSD ausgeführt.

8.4 Erstellung der Datenträgerimages

Nach jedem Löschvorgang wird mit dem IT-forensischen Imaging Tool FTK Imager ein physisches Image des Datenträgers erzeugt. Dies dient anschließend als Grundlage für die Analyse mit den Wiederherstellungsprogramme. Die Auswahl des richtigen Images ist essenziell für die Datenwiederherstellung, da bei einem physischen Image der gesamte Datenträger an sich abgebildet wird. Bei einem logischen Image würde nur die jeweilige Partition abgebildet werden, was die Datenwiederherstellung aus dem nicht zugewiesenen Speicherplatz nicht möglich macht.

Die folgenden Abbildungen 3 - 6 sind Bildschirmfotos des Programmes FTK Imager und stellen den Prozess der Erstellung eines physischen Datenträgerimages bildlich dar.

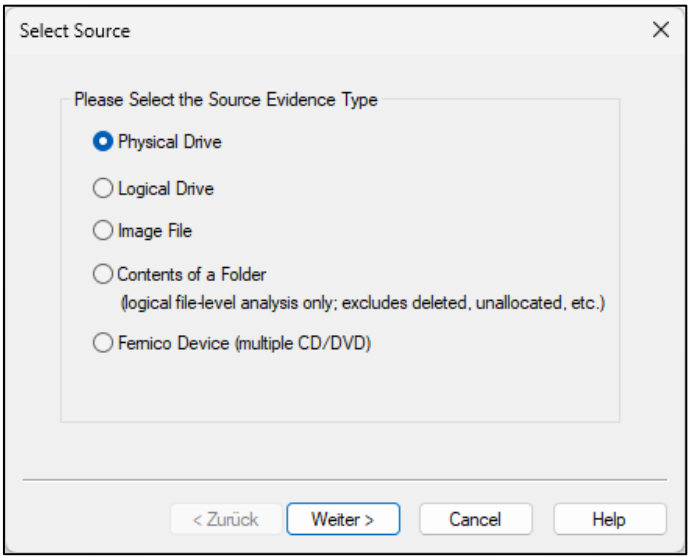


Abbildung 3: Imageerstellung mit FTK (1)

Abbildung 3 zeigt die Auswahl zwischen einem physischen oder logischen Image, einer Image Datei, einem Ordner oder einer CD/DVD. Hier muss gewählt werden, welcher Ziel Image Typ erstellt werden soll.

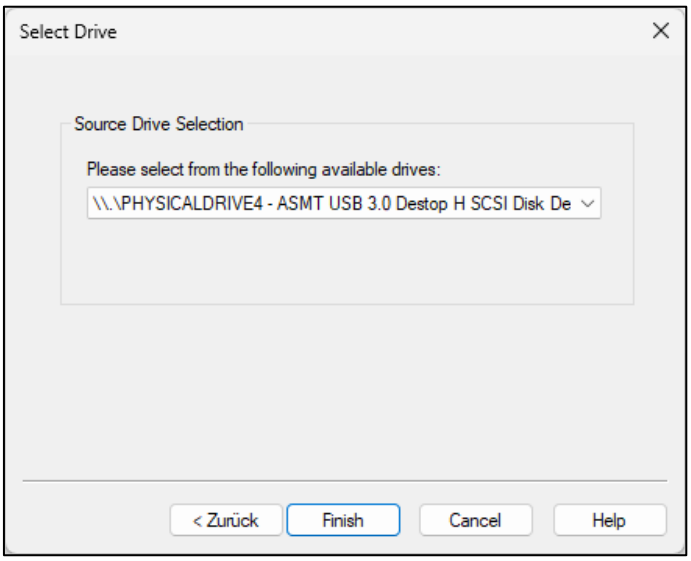


Abbildung 4: Imageerstellung mit FTK (2)

Auf Abbildung 4 ist zu sehen, von welchem Laufwerk das physische Image erstellt werden soll.

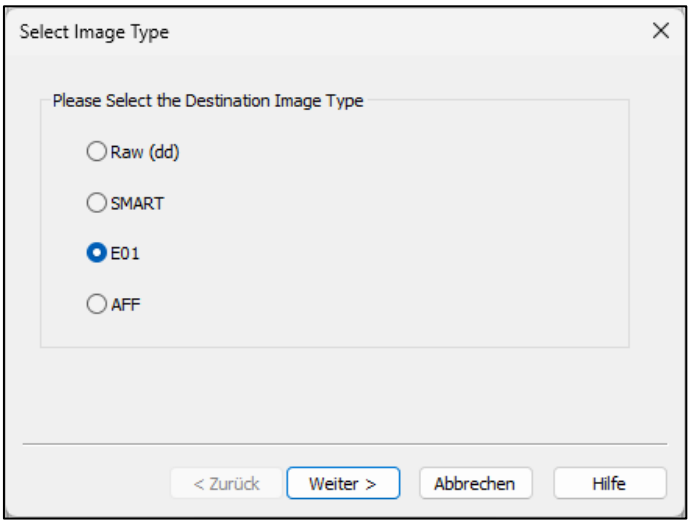


Abbildung 5: Imageerstellung FTK Imager (3)

Nachdem die Quelle und der Zielspeicherort ausgewählt wurde, muss sich noch für ein Imageformat entschieden werden. Das Format E01 ist hierbei ein gängiges Format für Imagedateien und ist sehr kompatibel. Abbildung 5 zeigt die vier möglichen Formate, die zur Auswahl stehen.

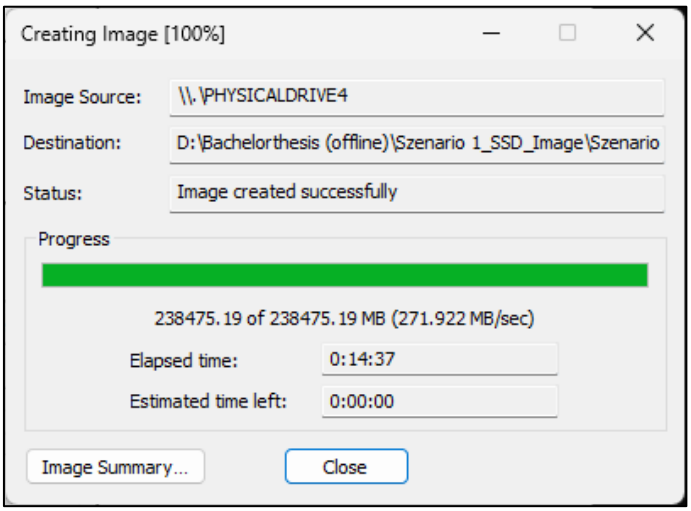


Abbildung 6: Imageerstellung FTK Imager (4)

Nachdem die Imageerstellung beendet ist, kann das Image über diverse Programme wie beispielsweise den Arsenal Image Mounter gemountet werden, um auf dieses zugreifen zu können.

8.5 Datenwiederherstellung

Jeder Löschvorgang wird anschließend eingehend analysiert, um zu ermitteln, inwiefern gelöschte Dateien wiederhergestellt werden können und ob Reste im zugewiesenen oder nicht zugewiesenen Bereich (allocated/unallocated) verbleiben. Für die Untersuchung der Wiederherstellbarkeit kommen zunächst Standard-Wiederherstellungsprogramme wie Recuva und EaseUS data recovery zum Einsatz, die häufig im Internet als wirksame Programme zur Datenwiederherstellung empfohlen werden. Ergänzend dazu werden das File Carving Tool PhotoRec und das spezialisierte IT-forensische Toolkit X-Ways Forensics eingesetzt, die eine tiefere und gezieltere Analyse des Speichermediums ermöglichen sollen. Diese sind zwar grundsätzlich auch benutzerfreundlich, benötigen jedoch eine erweiterte IT-Kenntnis, da hier beispielsweise mit der Kommandozeile von Windows gearbeitet werden muss. Nähere Informationen und Unterschiede zu dem jeweiligen eingesetzten Programm sind dem Anhang zu entnehmen.

Durch die detaillierte Untersuchung dieser Werkzeuge und Methoden soll aufgezeigt werden, wie sicher bzw. effektiv die verschiedenen Löschverfahren für HDDs und SSDs sind und welche Rückschlüsse über verbleibende Daten gezogen werden können. Die Ergebnisse der verschiedenen Programme sollen anschließend verglichen werden. Die Arbeit verfolgt das Ziel, praktische Empfehlungen zur sicheren Datenlöschung zu formulieren und die Grenzen herkömmlicher und forensischer Datenwiederherstellung aufzuzeigen. Diese Erkenntnisse sind besonders relevant für die IT-Forensik, da sie Hinweise geben,

wie zuverlässig Daten auch nach verschiedenen Lösch- und Formatierungsmethoden rekonstruierbar bleiben und welche Maßnahmen zur vollständigen Datenvernichtung erforderlich sind. Die Erfolgsrate der verschiedenen Programme wird anschließend verglichen. Dies wird in Form einer Gegenüberstellung durchgeführt, um einen direkten Vergleich der Ergebnisse vorliegen zu haben.

Im „Szenario 1 der HDD“ werden zusätzlich die einzelnen Schritte durch Bildschirmfotos dokumentiert, die dabei helfen sollen, ein besseres Verständnis für die Programme zu bekommen. Diese detaillierte Dokumentation erfolgt ausschließlich in „Szenario 1“ der HDD, da die Vorgehensweise der Programme in allen Szenarien identisch ist. Eine umfassende Dokumentation aller Schritte würde nicht nur eine äußerst hohe Anzahl an Screenshots generieren, sondern auch keinen zusätzlichen Mehrwert für die jeweilige Analyse bieten.

8.6 Szenario 1 – HDD – Papierkorb

In Szenario 1 wurden Dateien auf die Festplatte kopiert und anschließend über einen Rechtsklick und die Löschfunktion in den Papierkorb verschoben. Dieser wurde dann geleert.

	Wiederhergestellte Dateien aus dem Originaldatensatz			
Dateityp	Recuva	EaseUS	PhotoRec	X-Ways
zip	3	3	2	3
xlsx	11	11	9	11
txt	10	10	5	10
png	2	2	2	2
pdf	16	16	15	16
pcap	1	1	1	1
mp3	108	108	108	105
mp4	8	8	8	8
json	10	10	0	10
jpg	27	27	27	27
jfif	1	1	0	1
heic	2	2	2	2
csv	10	10	0	10
Gesamt	**209**	**209**	**180**	**206**

Tabelle 2: Übersicht Szenario 1 HDD

Ergebnisse Recuva

Die Abbildungen 7 und 8 zeigen den Assistenten, der durch das Programm Recuva zur Verfügung gestellt wird. Zu sehen ist die Auswahl des jeweiligen Datenträgers, der untersucht werden soll. In diesem Fall das gemountete Laufwerk S.

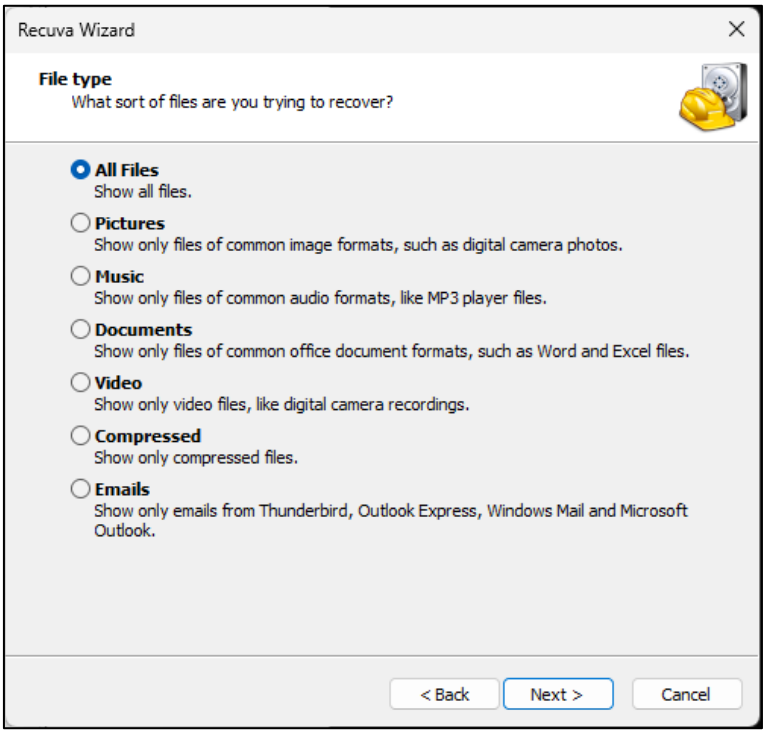


Abbildung 7: Recuva Szenario 1 HDD – Assistent (1)

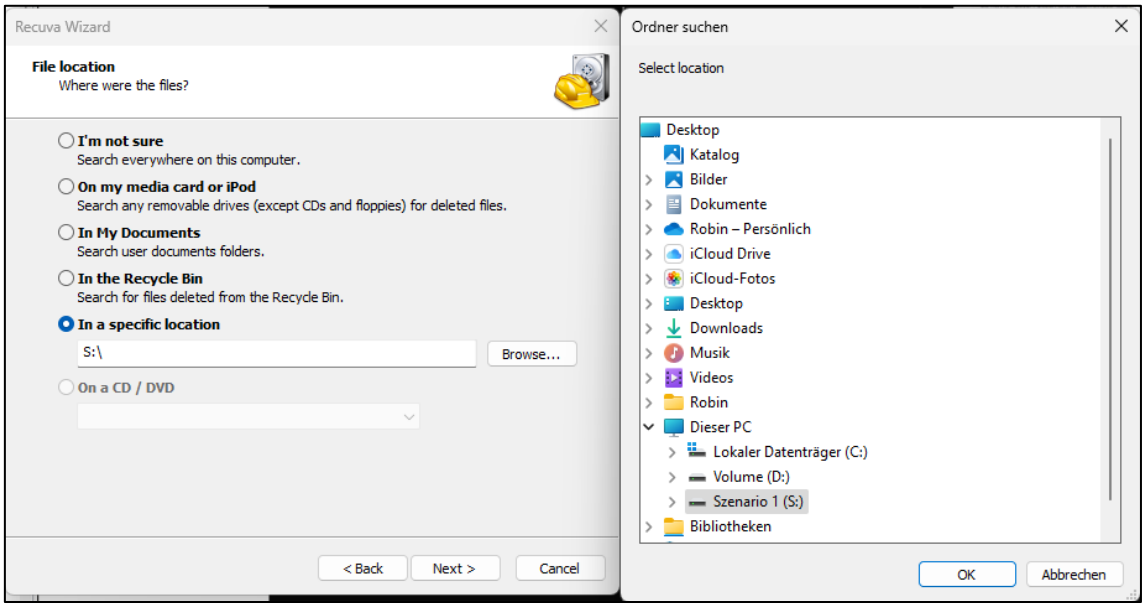
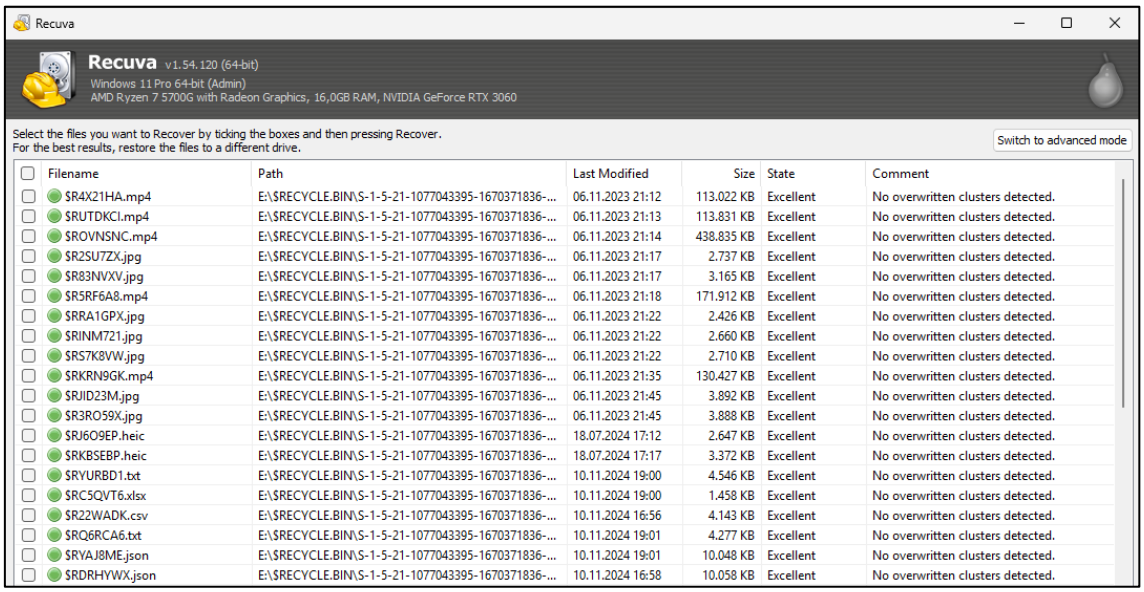


Abbildung 8: Recuva Szenario 1 HDD – Assistent (2)



Filename	Path	Last Modified	Size	State	Comment
$R4X21HA.mp4	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	06.11.2023 21:12	113.022 KB	Excellent	No overwritten clusters detected.
$RUTDKCI.mp4	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	06.11.2023 21:13	113.831 KB	Excellent	No overwritten clusters detected.
$ROVNSNC.mp4	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	06.11.2023 21:14	438.835 KB	Excellent	No overwritten clusters detected.
$R2SU7ZX.jpg	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	06.11.2023 21:17	2.737 KB	Excellent	No overwritten clusters detected.
$R83NVXV.jpg	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	06.11.2023 21:17	3.165 KB	Excellent	No overwritten clusters detected.
$R5RF6A8.mp4	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	06.11.2023 21:18	171.912 KB	Excellent	No overwritten clusters detected.
$RRA1GPX.jpg	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	06.11.2023 21:22	2.426 KB	Excellent	No overwritten clusters detected.
$RINM721.jpg	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	06.11.2023 21:22	2.660 KB	Excellent	No overwritten clusters detected.
$RS7K8VW.jpg	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	06.11.2023 21:22	2.710 KB	Excellent	No overwritten clusters detected.
$RKRN9GK.mp4	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	06.11.2023 21:35	130.427 KB	Excellent	No overwritten clusters detected.
$RJID23M.jpg	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	06.11.2023 21:45	3.892 KB	Excellent	No overwritten clusters detected.
$R3RO59X.jpg	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	06.11.2023 21:45	3.888 KB	Excellent	No overwritten clusters detected.
$RJ6O9EP.heic	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	18.07.2024 17:12	2.647 KB	Excellent	No overwritten clusters detected.
$RKBSEBP.heic	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	18.07.2024 17:17	3.372 KB	Excellent	No overwritten clusters detected.
$RYURBD1.txt	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	10.11.2024 19:00	4.546 KB	Excellent	No overwritten clusters detected.
$RC5QVT6.xlsx	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	10.11.2024 19:00	1.458 KB	Excellent	No overwritten clusters detected.
$R22WADK.csv	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	10.11.2024 16:56	4.143 KB	Excellent	No overwritten clusters detected.
$RQ6RCA6.txt	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	10.11.2024 19:01	4.277 KB	Excellent	No overwritten clusters detected.
$RYAJ8ME.json	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	10.11.2024 19:01	10.048 KB	Excellent	No overwritten clusters detected.
$RDRHYWX.json	E:\$RECYCLE.BIN\S-1-5-21-1077043395-1670371836-...	10.11.2024 16:58	10.058 KB	Excellent	No overwritten clusters detected.

Abbildung 9: Recuva Szenario 1 HDD – Übersicht gefundene Dateien

Abbildung 9 zeigt einen Ausschnitt der gefundenen Dateien durch das Programm Recuva. Zu sehen ist, dass die aus dem Papierkorb wiederhergestellten Dateien umbenannt wurden und das Kürzel $R plus eine Kennziffer bekommen haben.

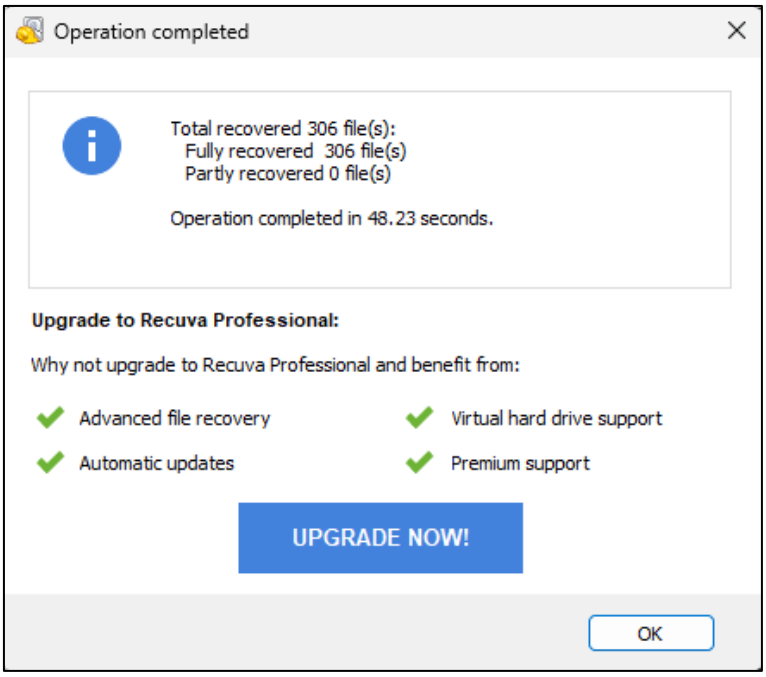


Abbildung 10: Recuva Szenario 1 HDD – Wiederhergestellte Dateien

Die Datenwiederherstellungssoftware Recuva konnte bei der Analyse des Festplatten-Images insgesamt 306 Dateien wiederherstellen, wie auf Abbildung 10 zu sehen ist. Dieser hohe Wert ist darauf zurückzuführen, dass auch die $I-Dateien des Papierkorbs mit

einbezogen und wiederhergestellt wurden. Diese Dateien enthalten die Metadaten der ursprünglich in den Papierkorb verschobenen Dateien und werden automatisch erstellt, sobald eine Datei in den Papierkorb geschoben wird. Nach Abzug der $I-Dateien von der Gesamtanzahl der wiederhergestellten Dateien verbleiben 209 Dateien, die der Anzahl des Originaldatensatzes entsprechen und auf die Festplatte geschrieben wurden.

Wenn man sich die Dateien im Dateiexplorer anzeigen lässt, wird ersichtlich, dass manche der Dateien noch unter ihrem eigentlichen Namen wiederhergestellt worden sind. Zu sehen ist dies auf Abbildung 11. Diese Dateien lagen ursprünglich nicht direkt im Stammverzeichnis der Festplatte, sondern waren in separaten Ordnern gespeichert. Die Dateien lassen sich nach dem Wiederherstellen problemlos öffnen und wiedergeben.

Es wurden durch das Tool alle Dateien aus dem Originaldatensatz wiederhergestellt. Die angesprochenen Dateien, die in Ordnern lagen, wurden lediglich aus diesen entfernt und ohne Ordnerstruktur wiederhergestellt.

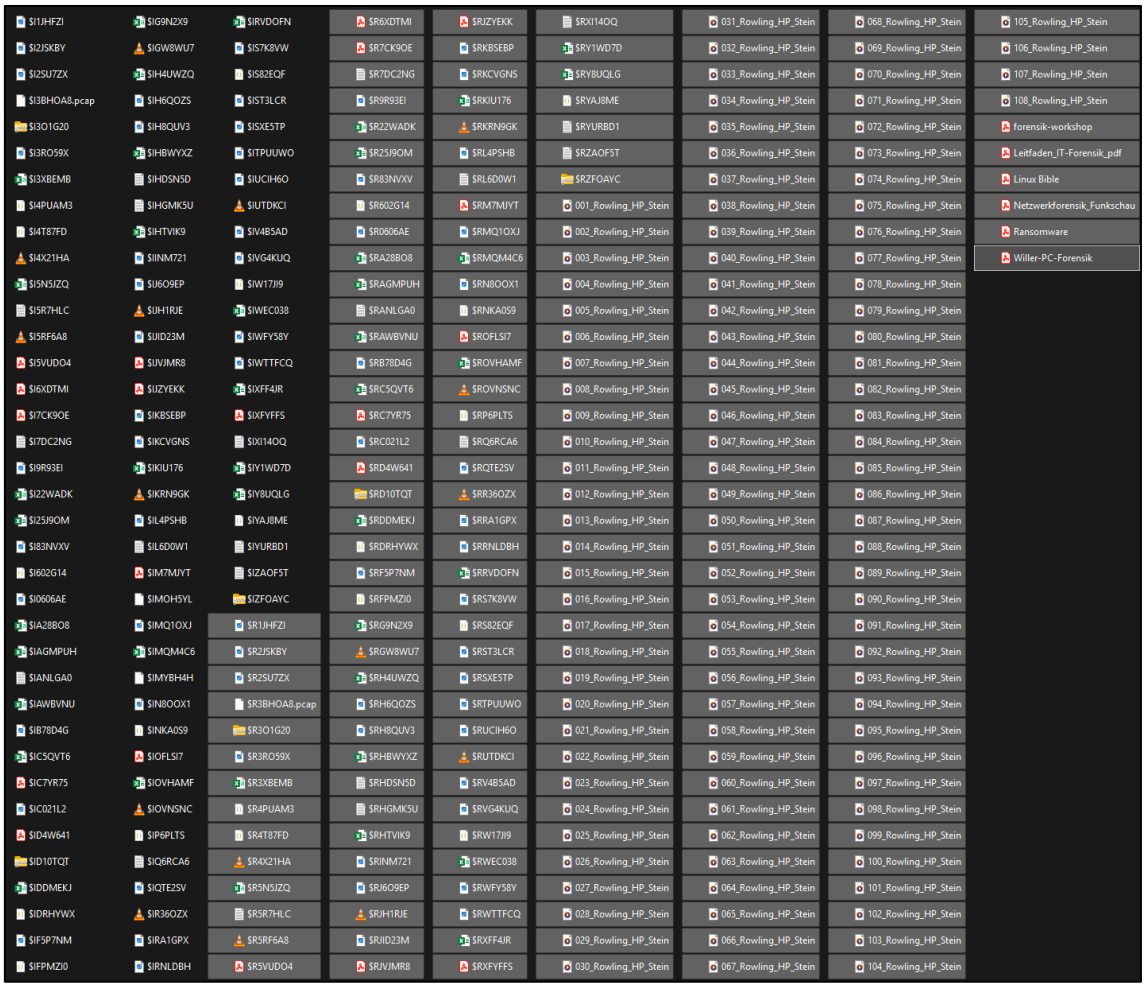


Abbildung 11: Recuva Szenario 1 HDD – Übersicht wiederhergestellte Dateien

Ergebnisse EaseUS data recovery

Die Abbildung 12 zeigt die Übersicht der gefundenen Dateien, die durch das Programm EaseUS data recovery erstellt wird. Diese kann, wie auf der Abbildung oben links zu sehen ist, nach verschiedenen Arten sortiert werden. In diesem Szenario wurde die Partition noch mit wiederhergestellt, weshalb diese auch auf dem Bildschirmfoto zu sehen ist. Darüber hinaus besteht die Möglichkeit, die Ergebnisse nach Dateitypen zu filtern und anzuzeigen. Nach Abschluss des Scanvorgangs können alle gefundenen Dateien durch Betätigen eines Buttons im unteren Bereich der Programmoberfläche wiederhergestellt werden.

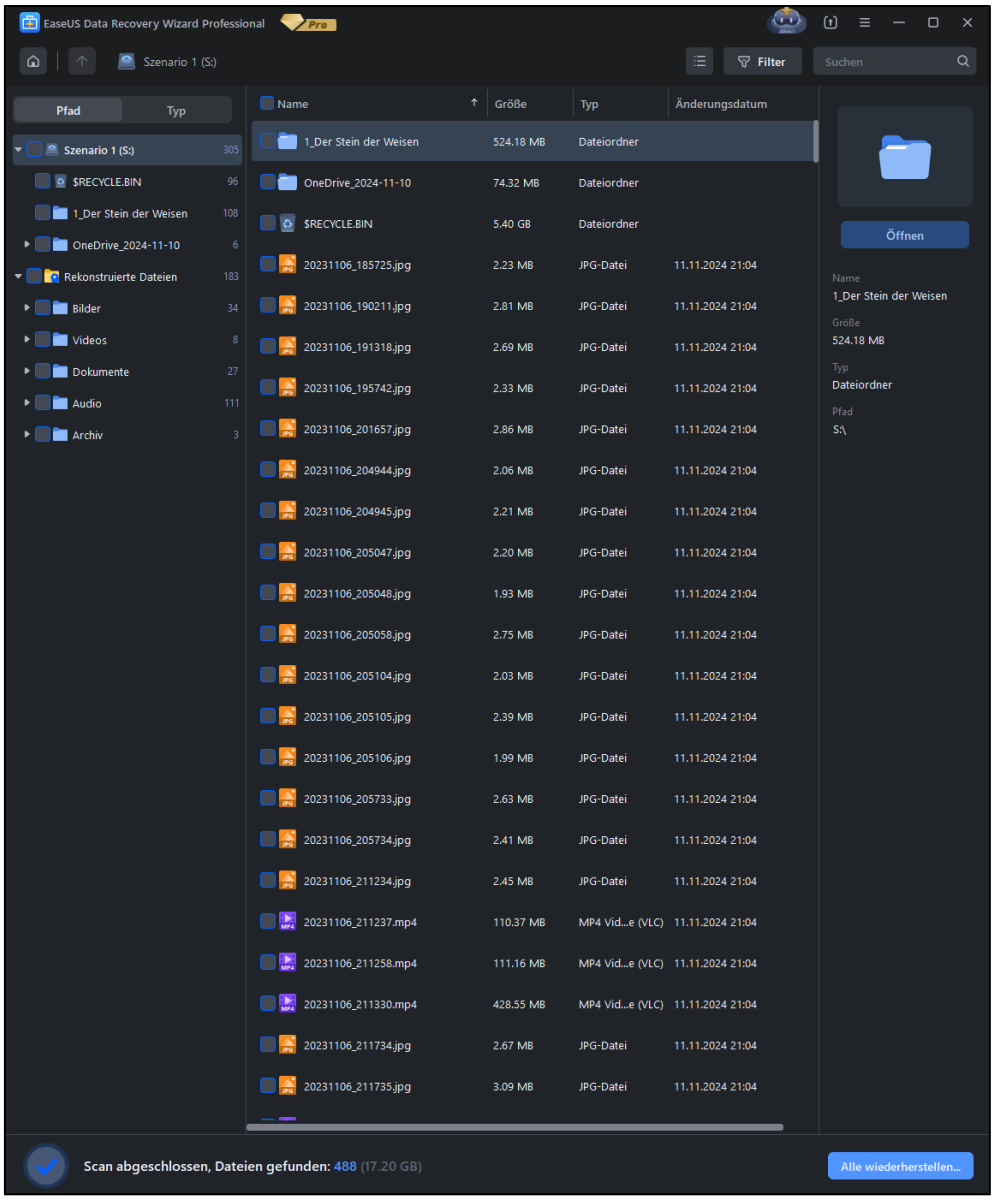


Abbildung 12: EaseUS Szenario 1 HDD - Sortierung Struktur

Abbildung 13: EaseUS Szenario 1 HDD - Gefundene Dateien

Die Datenwiederherstellungssoftware EaseUS Data Recovery konnte, wie in Abbildung 13 dargestellt, im Szenario 1 insgesamt 488 Dateien identifizieren. Das Programm ermöglicht sowohl die Wiederherstellung der Partition mit den darauf gespeicherten Dateien als auch eine zusätzliche Sortierung der wiederhergestellten Dateien nach Dateitypen. Dabei werden zwei separate Ordner erstellt, die mit „Rekonstruierte Dateien“ und „Verlorene Partition 1“ bezeichnet sind.

Im Ordner Rekonstruierte Dateien sind, die wiederhergestellten Dateien in Ordnern gespeichert, die nach Dateitypen sortiert sind. Der Ordner Verlorene Partition 1 beinhaltet die gesamte wiederhergestellte Partition, inklusive des Ordners des Papierkorbes, dem „RECYCLE.BIN“. Dies ist auch der Grund, warum der Ordner 305 Dateien zählt. Wenn dieser abgezogen wird, beinhaltet der Ordner 209 Dateien, was identisch mit dem Originaldatensatz ist.

Die Überprüfung der Dateien ergab, dass das Programm alle Dateien vollständig wiederhergestellt hat. Hierbei hat das Programm auch die Ordnerstruktur wiederhergestellt. Es fehlen keine Dateien und die Dateien haben alle ihren Dateinamen beim Wiederherstellungsprozess behalten.

Ergebnisse PhotoRec

Die Abbildungen 14–17 veranschaulichen den Ablauf, den Nutzende der Software PhotoRec vor der eigentlichen Datenwiederherstellung durchführen. In Abbildung 14 erfolgt die Auswahl des zu untersuchenden Laufwerks. Abbildung 15 zeigt die Wahl der entsprechenden Partition, während in Abbildung 16 das jeweilige Dateisystem festgelegt wird. Im letzten Schritt, dargestellt in Abbildung 17, entscheiden die Nutzenden, ob nur der nicht zugewiesene Speicherplatz (unallocated space) oder die gesamte Partition analysiert wird.

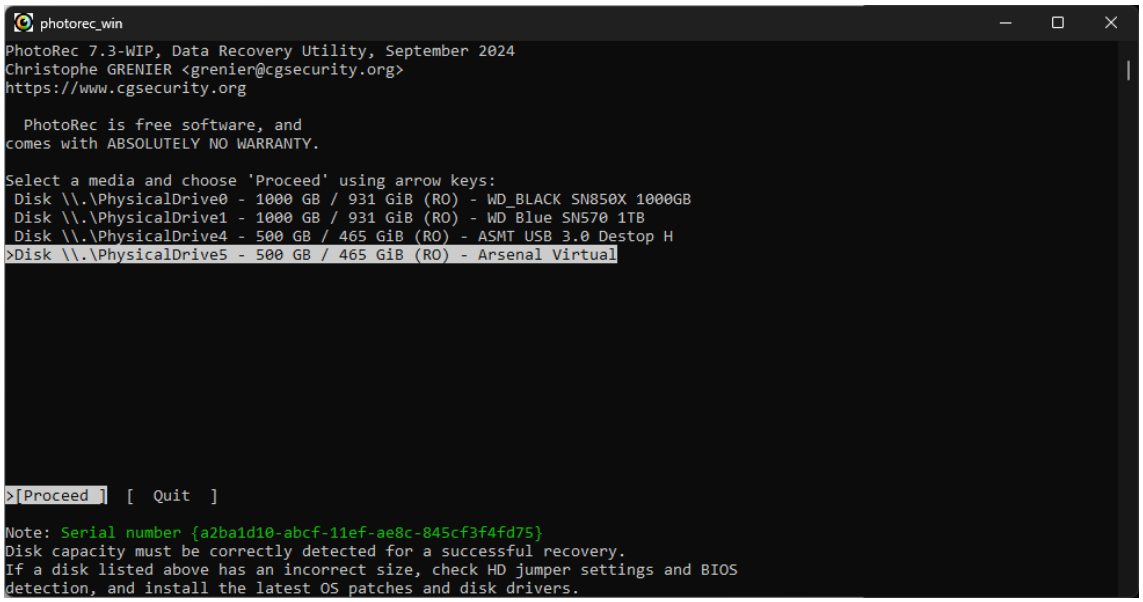


Abbildung 14: PhotoRec Szenario 1 HDD - Auswahl Image (1)

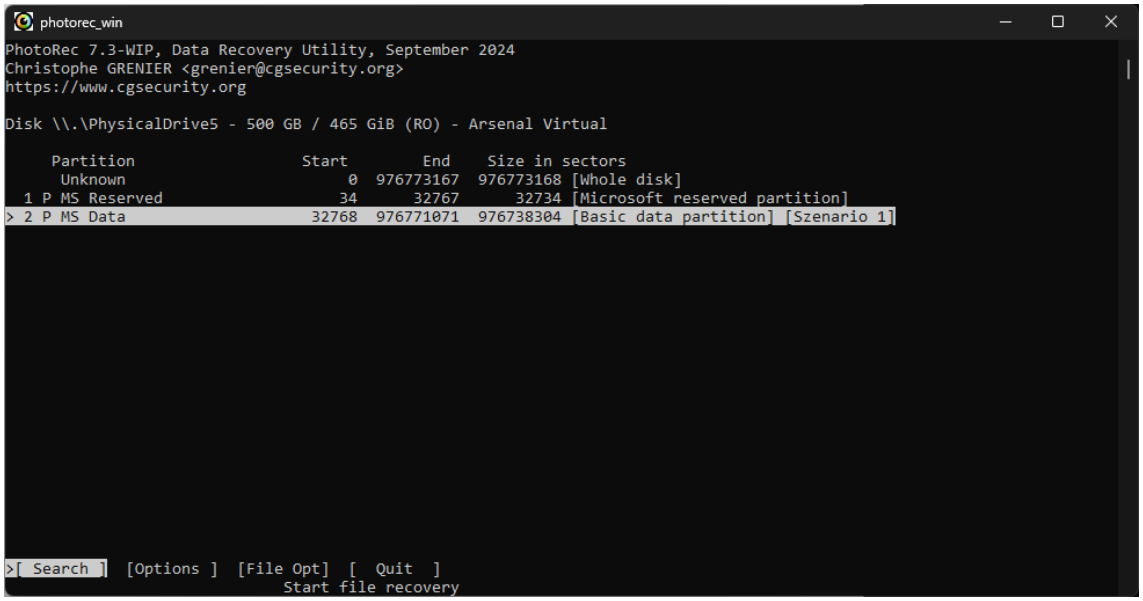


Abbildung 15: PhotoRec Szenario 1 HDD - Auswahl Image (2)

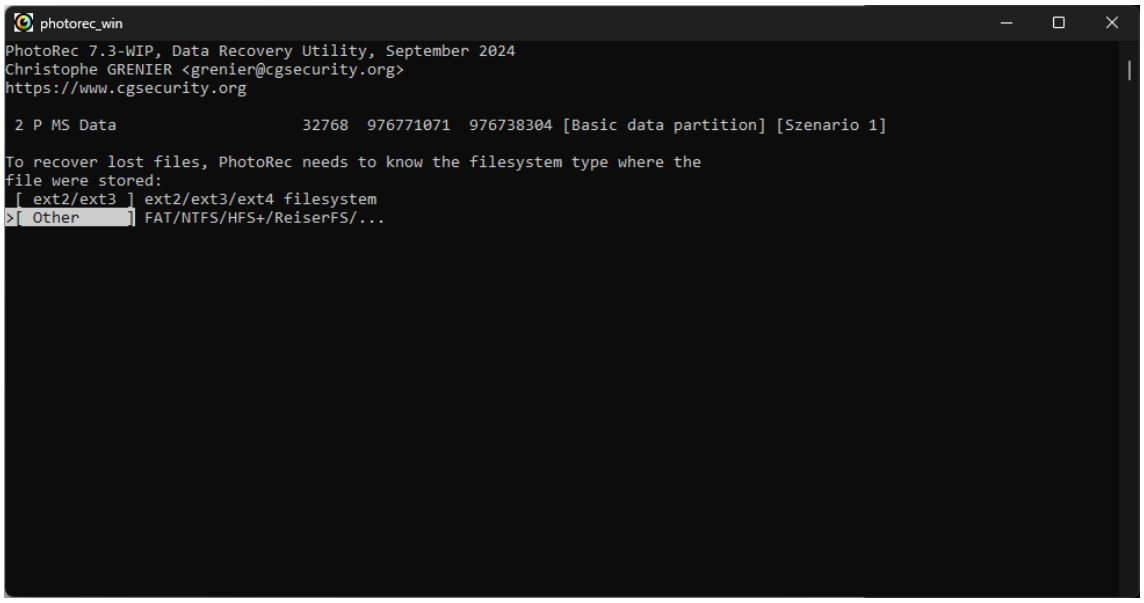


Abbildung 16: PhotoRec Szenario 1 HDD - Auswahl Image (3)

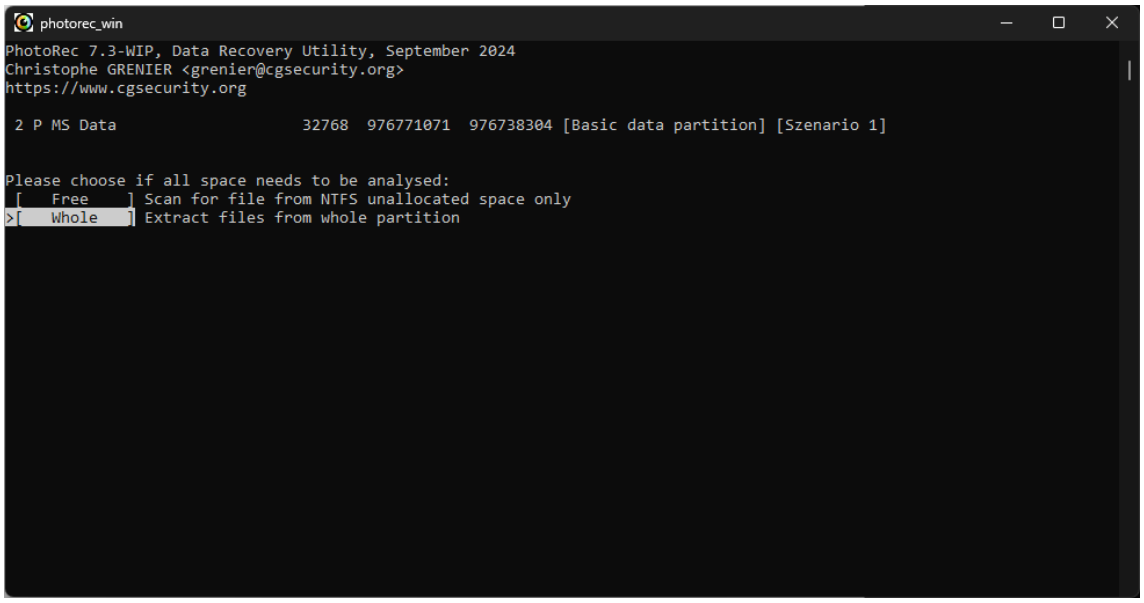


Abbildung 17: PhotoRec Szenario 1 HDD - Auswahl Image (4)

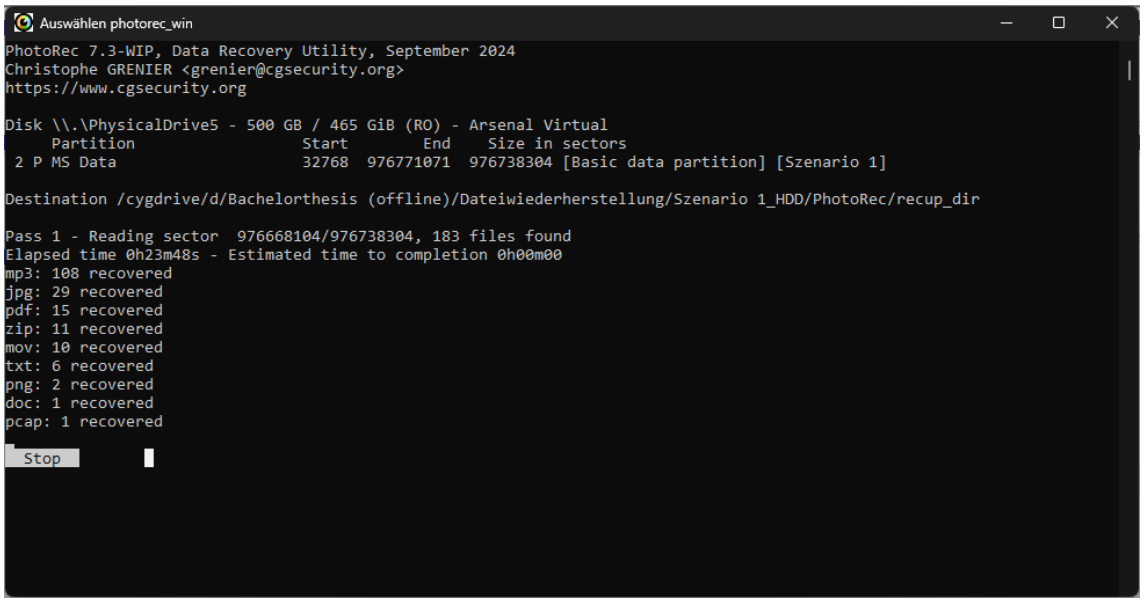


Abbildung 18: PhotoRec Szenario 1 HDD – Fortschritt

Durch das Programm PhotoRec wurden insgesamt 208 Dateien wiederhergestellt. Auf Abbildung 18 ist zu sehen, dass PhotoRec 183 Dateien gefunden hat. Dies liegt daran, dass das Programm generell 3 Dateien zusätzlich erstellt. Hierbei handelt es sich jedoch um Protokolldateien, die nicht zu den wiederhergestellten Dateien aus dem Originaldatensatz gehören. Hinzu kommt, dass PhotoRec 28 Bildern doppelt wiederherstellte. Ein stichprobenartiger Vergleich zweier jpg Bilddateien ergab, dass die Dateinamen identisch sind, die Dateigröße der beiden Dateien, sowie auch die Hashwerte jedoch unterschiedlich sind. Dies könnte daran liegen, dass sich PhotoRec auch die Metadaten Dateien aus dem Papierkorb teilweise wiederhergestellt hat und daraus anschließend kleinere Thumbnailbilder (Vorschaubilder) zustande gekommen sind. Dies könnte in weiteren Arbeiten untersucht werden.

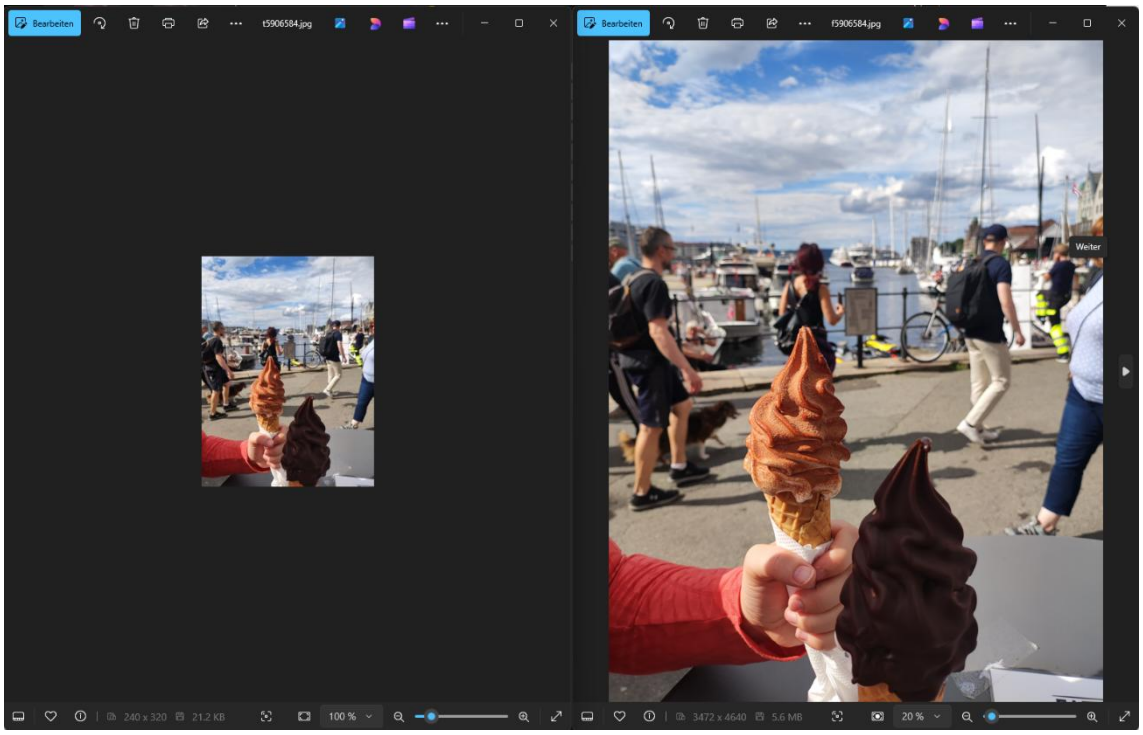


Abbildung 19: PhotoRec Szenario 1 HDD - Vergleich Bilddateien

SHA1 Wert linkes Bild: **2b7ff35c000f86ce8dccf01a53acb83d546d41bd**

SHA1 Wert rechtes Bild: **42c69d286c8b8630ab5c4cb3b2b381f77fd7acf9**

Abbildung 19 zeigt ein Beispielbild für die doppelt erstellten Bilddateien. Auf der Vorschau ist ersichtlich, dass es sich bei dem linken Bild um ein kleineres, anderes Bild handelt. Das rechte Bild ist das originale aus dem Originaldatensatz. Die unten aufgeführten SHA1 Hashwerte bestätigen, dass es sich um zwei unterschiedliche Dateien handelt, obwohl der Dateiname identisch ist.

Beim Wiederherstellungsprozess durch das Programm wurden die meisten Dateien beim Filecarving umgenannt und beginnen alle mit den Buchstaben f. Die Namensvergabe bei dieser Art der Dateiwiederherstellung erfolgt willkürlich, da das Programm die Dateifragmente auf dem Datenträger identifiziert, sammelt und anschließend zusammenführt.

Wie auch beim vorherigen Tool wurden die beiden Ordner aus dem Originaldatensatz aufgelöst und deren Dateien wurden ohne Ordnerstruktur wiederhergestellt. Aus dem Stammverzeichnis des Festplattenimages konnten jedoch nicht alle Dateien wiederhergestellt werden. Es fehlen unter anderem json, jfif, txt, pdf und csv Dateien, sowie das ZIP Archiv „OneDrive_2024-11-10“. Des Weiteren fehlen auch zwei xlsx Dateien, die mit den anderen genannten Dateien im Stammverzeichnis des Datenträgers lagen.

Ergebnisse X-Ways Forensics

Bevor mit dem IT-forensischen Toolkit X-Ways forensics Daten wiederhergestellt werden können, muss ein Fall angelegt werden, in dem anschließend Datenträger hinzugefügt werden können. Diese zwei Schritte sind auf den Abbildungen 20 und 21 zu sehen. Bei der Auswahl des Datenträgers kann zwischen dem logischen Volume bzw. der Partition und dem physischen Datenträger gewählt werden. Für die Datenwiederherstellung macht die Auswahl keinen Unterschied. Dies wurde zur Überprüfung während den Versuchen getestet.

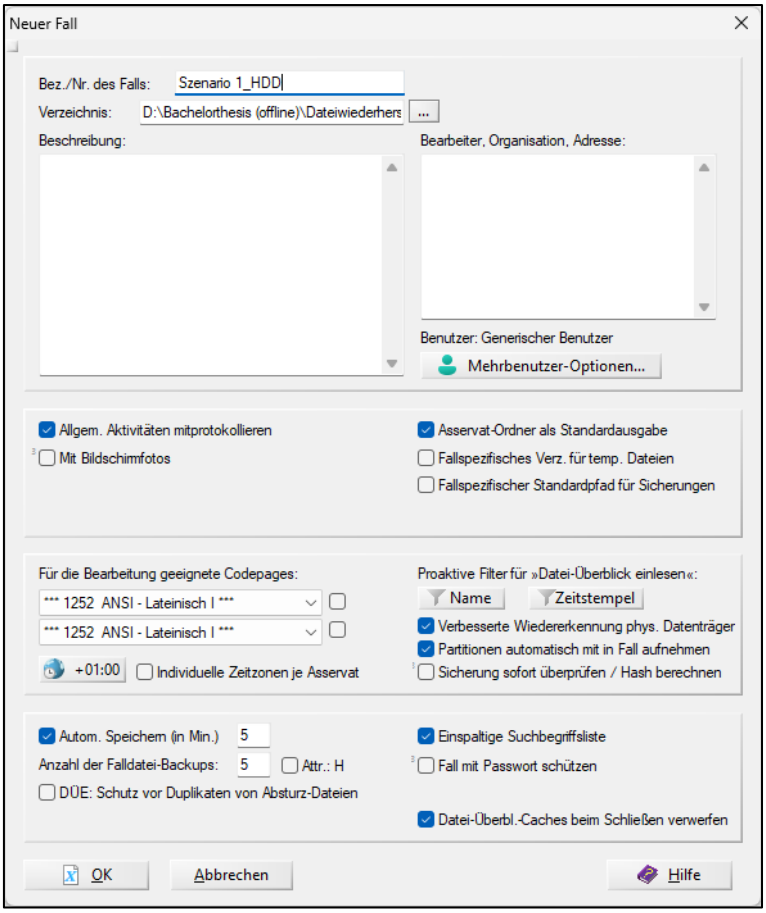


Abbildung 20: X-Ways Szenario 1 HDD - Fall anlegen

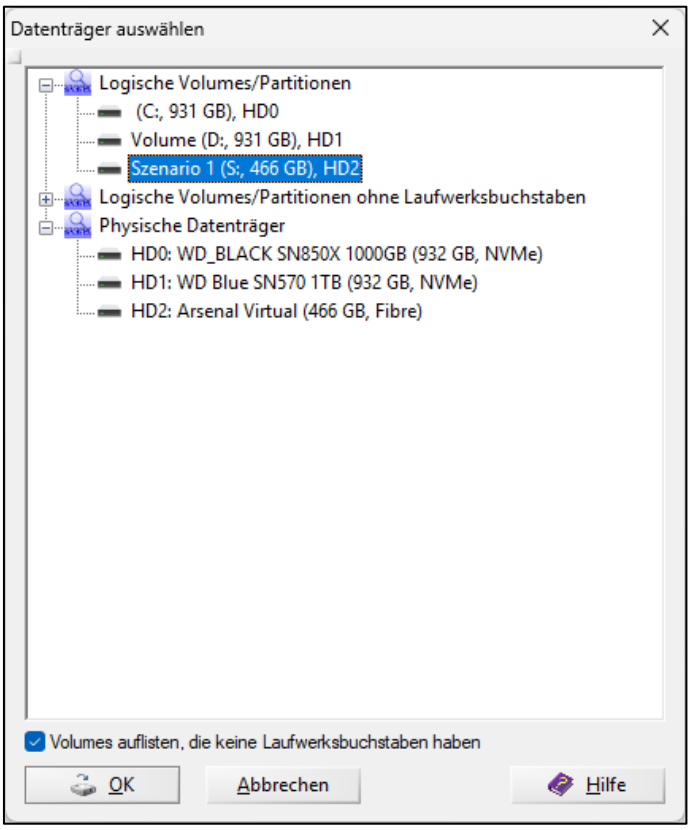


Abbildung 21: X-Ways Szenario 1 HDD - Datenträger hinzufügen

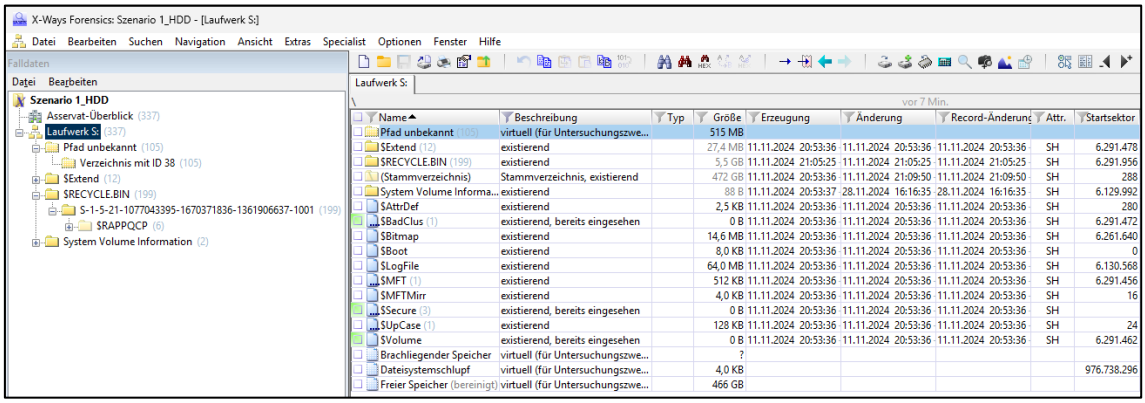


Abbildung 22: X-Ways Szenario 1 HDD - Übersicht Verzeichnis

Das Programm gibt nach dem Hinzufügen des Datenträgers schnell einen Überblick über die gefundenen Dateien. Abbildung 22 zeigt eine Übersicht des gemounteten Laufwerkes S, dass in diesem Fall das Image des ersten Szenarios auf der HDD abbildet.

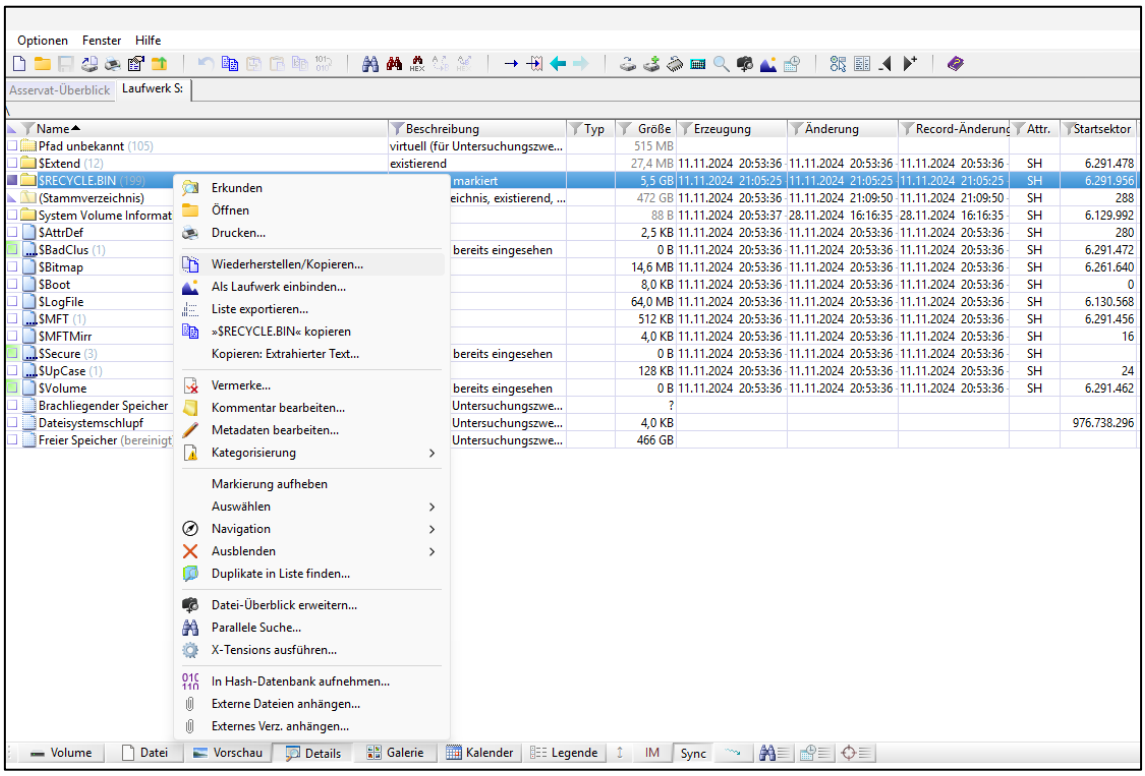


Abbildung 23: X-Ways Szenario 1 HDD - Dateien wiederherstellen

Über einen Rechtsklick auf den jeweiligen Ordner können die gefundenen Dateien wiederhergestellt/kopiert werden, wie auf Abbildung 23 ersichtlich ist.

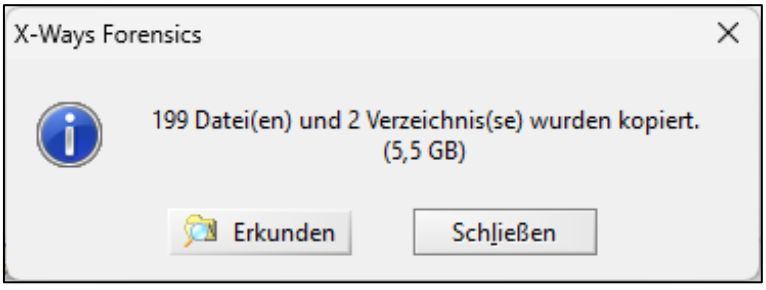


Abbildung 24: X-Ways Szenario 1 HDD - Dateien wiederhergestellt (1)

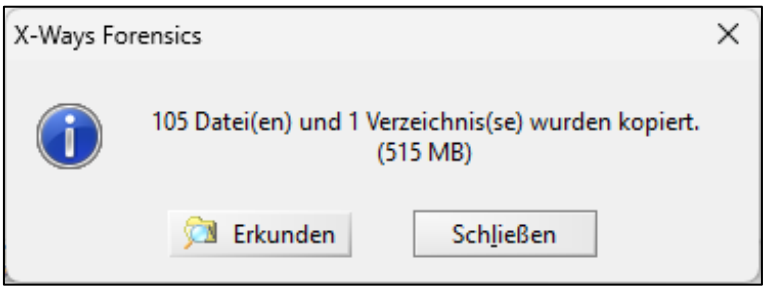


Abbildung 25: X-Ways Szenario 1 HDD - Dateien wiederhergestellt (2)

Das IT-forensische Tool X-Ways Forensics hat auf dem Datenträgerimage insgesamt 304 Dateien wiederherstellen können. Der erfolgreiche Wiederherstellungsprozess dieser Dateien ist auf den Abbildungen 24 und 25 zu sehen. Diese Dateien bestehen aus den Ordnern RECYCLE.BIN und Verzeichnis ID38.

Im RECYCLE.BIN Ordner sind alle Dateien zu finden, die über den Papierkorb gelöscht wurden. Nach Abzug der $I Metadaten Dateien, verbleiben 95 Dateien und ein Ordner. Dieser Ordner ist OneDrive_2024-11-10 mit seinem Unterordner OneDrive Testdaten Download. Der Ordner 1_Der Stein der Weisen ist hierbei nicht wiederhergestellt worden, sondern wurde über den separaten Ordner ID38 abgebildet. Nach einer Kontrolle des Ordners fällt auf, dass 3 der darin befindlichen mp3 Dateien nicht mit wiederhergestellt worden sind. Höchstwahrscheinlich ist beim Carven der Dateien ein Problem aufgetreten. Die drei Dateien konnten auch bei einem erneuten Wiederherstellungsversuch nicht wiederhergestellt werden. Es fehlen insgesamt diese drei Dateien.

Die restlichen wiederhergestellten Dateien, können jedoch problemlos geöffnet werden. Da durch das Tool der Ordner RECYCLE.BIN wiederhergestellt wurde, haben die Dateien ihren Dateinamen nicht behalten.

8.7 Szenario 2 – HDD - Unwiderrufliches Löschen

In Szenario 2 wurden Dateien auf die Festplatte kopiert und anschließend über die Tastenkombination Shift+Entf unwiderruflich gelöscht. Das Verschieben in den Papierkorb wird hiermit übersprungen.

	Wiederhergestellte Dateien aus dem Originaldatensatz			
Dateityp	Recuva	EaseUS	PhotoRec	X-Ways
zip	3	3	2	3
xlsx	10	11	9	9
txt	9	10	5	9
png	2	2	2	2
pdf	16	16	16	15
pcap	1	1	1	1
mp3	108	108	108	108
mp4	8	8	8	8
json	10	10	0	10
jpg	27	27	28	27
jfif	1	1	0	1
heic	2	2	2	2
csv	10	10	0	10
Gesamt	**207**	**209**	**181**	**205**

Tabelle 3: Übersicht Szenario 2 HDD

Ergebnisse Recuva

Bei der Überprüfung der wiederhergestellten Dateien fällt auf, dass zwei Dateien aus dem Originaldatensatz nicht wiederhergestellt wurden. Die Dateinamen lauten ok.txt und movie.xlsx.

Recuva hat in diesem Durchgang keine $I und $R-Dateien aus dem Papierkorb mit wiederhergestellt, da dieser Vorgang mit dem unwiderruflichen Löschen über die Tastenkombination Shift + Entf. übersprungen wurde. Der Grund, warum das Programm genau diese beiden Dateien nicht wiederhergestellt hat, konnte nicht ermittelt werden. Sie lagen wie viele anderen Dateien direkt im Stammverzeichnis des Datenträgers. Genau wie im vorherigen Durchgang hat das Programm auch die Ordner, die auf dem Datenträger lagen, nicht wiederhergestellt, sondern nur die Inhalte. Beispiele hierfür sind die Dateien Will-PC-Forensik.pdf oder auch Ransomware.pdf. Diese lagen im Originaldatensatz im Ordner OneDrive_2024-11-10 und dessen Unterordner OneDrive Testdaten Download. Bei der Wiederherstellung sind diese wie auch andere ohne die Ordnerstruktur wiederhergestellt worden.

Die xlsx Datei news.xlsx und die pdf Datei newspaper.pdf wurden beim Wiederherstellungsprozess in [000001] und [000002] umbenannt. Eine Überprüfung der Hashwerte ergab, dass es sich immer noch um die Originaldateien handelt.

Ergebnisse EaseUS data recovery

Das Programm EaseUS data recovery hat in diesem Szenario insgesamt 209 Dateien identifiziert und wiederhergestellt. Hierbei hat es wie beim Szenario 1 die gesamte Partition wiederhergestellt sowie die Ordner, die auf dem Datenträger geschrieben wurden. Zusätzlich hat das Programm erneut einen separaten Ordner angelegt, in dem die wiederhergestellten Dateien sortiert nach ihrem Dateityp gespeichert sind (Rekonstruierte Dateien). Beim Wiederherstellungsprozess wurden somit alle Dateien aus dem Originaldatensatz wiederhergestellt.

Ergebnisse PhotoRec

Der Wiederherstellungsprozess durch das Programm PhotoRec hat in diesem Durchgang 209 Dateien wiederherstellen können. Davon sind jedoch lediglich 181 Dateien aus dem Originaldatensatz.

Wie im Szenario 1 hat PhotoRec viele Dateien wie JSON, JFIF und CSV nicht rekonstruiert, jedoch einige JPG-Bilddateien doppelt erkannt. Im Gegensatz dazu konnte das Programm in diesem Durchlauf eine zusätzliche PDF-Datei identifizieren, sodass in diesem Prozess alle 16 PDF-Dateien erfolgreich gesichert wurden.

Ergebnisse X-Ways Forensics

Das forensische Toolkit X-Ways rekonstruierte insgesamt 206 Dateien. Dabei wurde die PDF-Datei „Leitfaden_IT_Forensik_pdf“ doppelt gesichert. Ein Vergleich der Datensätze ergab jedoch, dass die folgenden Dateien nicht wiederhergestellt wurden: ok.txt, news.xlsx, movie.xlsx und newspaper.pdf. Diese Dateien befanden sich, ebenso wie andere, im Stammverzeichnis des Datenträgers.

8.8 Szenario 3 – HDD – Schnellformatierung

In Szenario 3 wurden Dateien auf die Festplatte kopiert. Anschließend wurde die Festplatte über den Dateiexplorer mit einem Rechtsklick und der Funktion *Schnellformatierung* formatiert. Hiermit wurde das Dateisystem aktualisiert und die Metadatenstrukturen entfernt, die bestimmen, wo welche Datei liegt.

	Wiederhergestellte Dateien aus dem Originaldatensatz			
Dateityp	Recuva	EaseUS	PhotoRec	X-Ways
zip	2	3	2	0
xlsx	10	10	9	0
txt	0	0	5	0
png	2	2	2	0
pdf	16	16	15	0
pcap	0	0	1	0
mp3	107	107	107	0
mp4	7	8	8	0
json	0	0	0	0
jpg	27	28	28	0
jfif	0	0	0	0
heic	0	2	2	0
csv	0	0	0	0
Gesamt	**171**	**176**	**179**	**0**

Tabelle 4: Übersicht Szenario 3 HDD

Ergebnisse Recuva

Die Datenwiederherstellungssoftware Recuva hat in diesem Durchgang insgesamt 171 Dateien aus dem Originaldatensatz wiederherstellen können. Jedoch ist in der Tabelle 4 zu sehen, dass durch die fortgeschrittene Löschmethode der Schnellformatierung die Wiederherstellung einiger Dateien nicht mehr möglich war.

Eine weitere Auswirkung der Schnellformatierung ist, dass Recuva auch die Dateinamen bei den meisten Dateien nicht wiederherstellen konnte, sodass die erste Datei mit dem Namen [000001**]** beginnt und das Programm hierbei die Dateinamen hochiteriert. Die MP3-Dateien aus dem Ordner „1_Der Stein der Weisen“ konnten größtenteils mitsamt ihren Dateinamen wiederhergestellt werden, jedoch blieb die erste MP3-Datei des Ordners unvollständig. Zudem sind die Dateinamen nicht vollständig korrekt, da das Programm Teile abgeschnitten und den Kapitelnamen in die Dateinamen integriert hat. Dies hat jedoch keine Auswirkung auf die Funktionalität der Audiodateien, alle Dateien lassen sich problemlos öffnen und auch abspielen.

Bei der Wiederherstellung der mp4 Dateien ist die Funktionalität eingeschränkt. Lediglich die mp4 Dateien VID_20231106_210523, VID_20231106_220818 und VID_20231106_220826 lassen sich abspielen. Die restlichen Videodateien sind nicht abspielbar.

Die zip Archive Testdaten.zip und Greta Van Fleet.zip wurden ebenfalls ohne weitere Probleme wiederhergestellt. OneDrive_2024-11-10.zip hingegen wurde nicht wiederhergestellt.

Ergebnisse EaseUS data recovery

Die Datenwiederherstellungssoftware EaseUS data recovery hat in diesem Durchgang insgesamt 182 Dateien wiederherstellen können, wovon jedoch nur 176 auch im Originaldatensatz vorhanden sind.

Des Weiteren ist die Partition dieses Mal nicht mit wiederhergestellt worden, sondern nur die Dateien an sich. Die Differenz von sechs Dateien sind drei defekte mp3 Dateien, eine svg Datei und eine mof Datei, die alle nicht wiedergegeben bzw. geöffnet werden können. Hinzukommt, dass eine jpg Bilddatei aus einem der pdf Dokumente zusätzlich wiederhergestellt wurde. Diese Bilddatei war nicht als jpg Bilddatei auf die Festplatte geschrieben worden. Zu den Dateien, die nicht wiederhergestellt wurden, zählen eine xlsx Datei, die txt, pcap, json, jfif und csv Dateien.

Ergebnisse PhotoRec

Mit dem Programm PhotoRec wurden insgesamt 207 Dateien rekonstruiert, wobei 28 davon doppelt gesichert wurden. Ähnlich wie bei der Datenwiederherstellungssoftware Recuva hat das Programm zusätzliche JPG-Dateien erkannt, die ursprünglich nicht auf den Datenträger geschrieben wurden. Diese Bilder unterscheiden sich von den Dateien des Originaldatensatzes sowohl in ihrer Größe als auch in ihrem Hashwert.

Auf Abbildung A6 im Anhang, ist ersichtlich, dass wenn die Bilder nach Dateityp sortiert sind zu Beginn alle ursprünglichen Bilddateien aufgezeigt werden und dann eine jpg Datei folgt, dessen Bildinhalt nicht zu dem passt, welcher in den anderen Bildern ist. Danach folgen die kleineren zusätzlich erstellen Bilddateien. Woher diese Dateien kommen und warum sie durch verschiedene Programme wie hier PhotoRec, aber auch Recuva erstellt werden, ist offen.

Wie auch bei den ersten beiden Wiederherstellungsprozessen durch PhotoRec wurden die Dateinamen hier nach demselben Namensschema geändert.

Es konnten in diesem Durchlauf insgesamt 30 Dateien nicht wiederhergestellt werden. Hierzu zählen: xlsx, txt, pdf, mp3, json und csv Dateien. Alle erfolgreich wiederhergestellten Dateien können problemlos geöffnet werden.

Ergebnisse X-Ways Forensics

Das forensische Toolkit X-Ways hat bei einer Schnellformatierung der Festplatte keine Dateien finden bzw. wiederherstellen können.

8.9 Szenario 4 – HDD - Vollständige Formatierung

In Szenario 4 wurden Dateien auf die Festplatte kopiert. Anschließend wurde die Festplatte über die Datenträgerverwaltung von Microsoft Windows vollständig formatiert. Hiermit werden alle Daten auf dem jeweiligen Datenträger gelöscht.

	Wiederhergestellte Dateien aus dem Originaldatensatz			
Dateityp	Recuva	EaseUS	PhotoRec	X-Ways
zip	0	0	0	0
xlsx	0	0	0	0
txt	0	0	0	0
png	0	0	0	0
pdf	0	0	0	0
pcap	0	0	0	0
mp3	0	0	0	0
mp4	0	0	0	0
json	0	0	0	0
jpg	0	0	0	0
jfif	0	0	0	0
heic	0	0	0	0
csv	0	0	0	0
Gesamt	**0**	**0**	**0**	**0**

Tabelle 5: Übersicht Szenario 4 HDD

Ergebnisse Recuva

Die Datenwiederherstellungssoftware Recuva hat bei einer vollständigen Formatierung der Festplatte keine Dateien finden bzw. wiederherstellen können. (Festgehalten auf Abbildung A7 im Anhang)

Ergebnisse EaseUS data recovery

Die Datenwiederherstellungssoftware EaseUS data recovery hat bei einer vollständigen Formatierung der Festplatte keine Dateien finden bzw. wiederherstellen können. (Festgehalten auf Abbildung A8 im Anhang)

Ergebnisse PhotoRec

Das File Carving Tool PhotoRec hat bei einer vollständigen Formatierung der Festplatte keine Dateien finden bzw. wiederherstellen können. (Festgehalten auf Abbildung A9 im Anhang)

Ergebnisse X-Ways Forensics

Das forensische Toolkit X-Ways hat bei einer vollständigen Formatierung der Festplatte keine Dateien finden bzw. wiederherstellen können. (Festgehalten auf Abbildung A10 im Anhang)

8.10 Szenario 1 – SSD – Papierkorb

In Szenario 1 wurden Dateien auf die SSD kopiert und anschließend über einen Rechtsklick und die Löschfunktion in den Papierkorb verschoben. Dieser wurde dann geleert.

	Wiederhergestellte Dateien aus dem Originaldatensatz			
Dateityp	Recuva	EaseUS	PhotoRec	X-Ways
zip	3	3	2	3
xlsx	11	11	10	11
txt	10	10	5	10
png	2	2	2	2
pdf	16	16	15	16
pcap	1	1	1	1
mp3	108	108	108	108
mp4	8	8	8	8
json	10	10	0	10
jpg	27	27	28	23
jfif	1	1	0	1
heic	2	2	2	2
csv	10	10	0	10
Gesamt	**209**	**209**	**181**	**205**

Tabelle 6: Übersicht Szenario 1 SSD

Ergebnisse Recuva

Die Datenwiederherstellungssoftware Recuva hat im ersten Szenario mit der SSD alle 209 Dateien aus dem Originaldatensatz erfolgreich rekonstruiert. Wie auch bei der HDD wurden neben den eigentlichen Dateien zusätzlich automatisch erstellte Dateien aus dem Papierkorb-Prozess wiederhergestellt. Die $I-Dateien des RECYCLE.BIN wurden dabei, wie bereits im ersten Szenario, mit 97 Einträgen ebenfalls gesichert. Zieht man diese Anzahl von der Gesamtzahl der rekonstruierten Dateien ab, ergibt sich genau die Anzahl von 209 Dateien aus dem Originaldatensatz. Die Ordnerstruktur wurde, wie im ersten Durchlauf, nicht wiederhergestellt. Insgesamt zeigen sich in diesem Szenario keine Unterschiede im Vergleich zur HDD.

Ergebnisse EaseUS data recovery

Im ersten Szenario der SSD konnte die Datenwiederherstellungssoftware EaseUS data recovery alle 209 Dateien aus dem Originaldatensatz wiederherstellen. Insgesamt hat die Software 483 Dateien in 28 Ordnern wiederhergestellt. Dies sind 5 Dateien weniger als bei dem Versuch der HDD. Hierzu zählt zum einen die gesamte wiederhergestellte Partition, sowie einem separaten Ordner mit den wiederhergestellten Dateien sortiert nach dem jeweiligen Dateityp. Die Software hat ebenfalls wieder die ursprünglichen Ordner wiederhergestellt.

Ergebnisse PhotoRec

Das File Carving Tool PhotoRec hat im ersten Szenario der SSD insgesamt 181 Dateien aus dem Originaldatensatz wiederhergestellt. Bei diesem Durchlauf hat das Tool eine xlsx Datei mehr wiederherstellen können als im ersten Durchlauf auf der HDD. Es handelt sich hierbei um die Datei since.xlsx. Des Weiteren konnten wie auch schon im ersten Durchlauf viele Dateien nicht wiederhergestellt werden. In diesem Durchlauf sind es insgesamt 28 nicht wiederhergestellte Dateien.

Zu diesen Dateien gehören die csv, jfif, sowie json Dateien. Fünf der txt Dateien, sowie eine pdf Datei und das zip Archiv OneDrive_2024-11-10 wurden ebenfalls nicht wiederhergestellt.

Insgesamt wurden durch das Tool zwar 209 Dateien wiederhergestellt. Es sind jedoch 28 jpg Bilddateien die, wie auch im ersten Durchlauf mit dem HDD-Festplattenimage, doppelt wiederhergestellt wurden bzw. neu erzeugte Dateien, die möglicherweise erstellte Thumbnails darstellen.

Ergebnisse X-Ways Forensics

Das IT-forensische Toolkit X-Ways hat beim ersten Durchlauf insgesamt 205 Dateien aus dem Originaldatensatz wiederherstellen können. Hierbei fällt auf, dass vier jpg Dateien nicht wiederhergestellt worden sind. Diese lagen wie auch die anderen jpg Dateien im Stammverzeichnis der SSD. Es handelt sich hierbei um die Dateien: 20231106_185725.jpg, 20231106_190211.jpg, 20231106_191318.jpg und 20231106_195742.jpg. Die restlichen erfolgreich wiederhergestellten Dateien lassen sich problemlos öffnen.

X-Ways hat wie auch auf der HDD die Metadaten Dateien aus dem Papierkorb mit wiederhergestellt. Beim Wiederherstellen der Dateien auf dem Image der SSD hat das Tool jedoch nicht, wie beim ersten Durchlauf, den Ordner 1_Der Stein der Weisen separat wiederhergestellt und umbenannt, sondern hat diesen mit im RECYCLE.BIN wiederhergestellt. Bei diesem Durchlauf fehlen keine mp3 Dateien.

8.11 Szenario 2 – SSD - Unwiderrufliches Löschen

In Szenario 2 wurden Dateien auf die SSD kopiert und anschließend über die Tastenkombination Shift+Entf unwiderruflich gelöscht. Das Verschieben in den Papierkorb wird hiermit übersprungen.

	Wiederhergestellte Dateien aus dem Originaldatensatz			
Dateityp	Recuva	EaseUS	PhotoRec	X-Ways
zip	3	3	2	3
xlsx	11	11	9	11
txt	10	10	5	10
png	2	2	2	2
pdf	16	16	15	16
pcap	1	1	1	1
mp3	108	108	108	108
mp4	8	8	8	8
json	10	10	0	10
jpg	27	27	28	23
jfif	1	1	0	1
heic	2	2	2	2
csv	10	10	0	10
Gesamt	**209**	**209**	**180**	**205**

Tabelle 7: Übersicht Szenario 2 SSD

Ergebnisse Recuva

Die Datenwiederherstellungssoftware Recuva hat in diesem Durchlauf insgesamt alle 209 Dateien des Originaldatensatzes wiederherstellen können. Die einzige Auffälligkeit bei dieser Datenwiederherstellung ist, dass vier der 27 jpg Bilddateien nicht ihren ursprünglichen Dateinamen behalten haben, sondern unbenannt wurden in 000001-000004. Die Bilder lassen sich jedoch problemlos öffnen und anzeigen, aber eine Überprüfung der Hashwerte ergab, dass diese während der Wiederherstellung geändert wurden.

Ergebnisse EaseUS data recovery

Die Datenwiederherstellungssoftware EaseUS Data Recovery hat in diesem Durchlauf ebenfalls alle 209 Dateien aus dem Originaldatensatz erfolgreich rekonstruiert. Zudem wurde die gesamte Partition wiederhergestellt. Zusätzlich erstellte das Programm einen Ordner, in dem die geretteten Dateien nach Dateityp sortiert separat abgelegt sind.

Ergebnisse PhotoRec

Das File-Carving-Tool PhotoRec konnte in diesem Durchlauf, wie auch beim Durchlauf auf dem HDD-Image, nicht alle Dateien aus dem Originaldatensatz rekonstruieren. Insgesamt wurden 180 Dateien extrahiert, jedoch blieben die Dateitypen csv, jfif und json unberücksichtigt. Auch in diesem Fall wurden einige JPG-Dateien doppelt gesichert, während ein zip-Archiv nicht wiederhergestellt wurde. Zudem konnten zwei xlsx-Dateien nicht wiederhergestellt werden.

Ergebnisse X-Ways Forensics

Das IT-forensische Toolkit X-Ways konnte in diesem Durchlauf insgesamt 205 Dateien aus dem Originaldatensatz wiederherstellen. Es fehlen hierbei vier jpg Dateien. Es handelt sich hierbei um die Dateien 20231106_185725, 20231106_190211, 20231106_191318 und 20231106_195742.

8.12 Szenario 3 – SSD – Schnellformatierung

In Szenario 3 wurden Dateien auf die SSD kopiert. Anschließend wurde die Festplatte über den Dateiexplorer mit einem Rechtsklick und der Funktion *Schnellformatierung* formatiert. Hiermit wurde das Dateisystem aktualisiert und die Metadatenstrukturen entfernt, die bestimmen, wo welche Datei liegt.

	Wiederhergestellte Dateien aus dem Originaldatensatz			
Dateityp	Recuva	EaseUS	PhotoRec	X-Ways
zip	2	3	2	0
xlsx	10	10	10	0
txt	0	0	5	0
png	2	2	2	0
pdf	16	16	16	0
pcap	0	0	1	0
mp3	108	108	108	0
mp4	7	8	8	0
json	0	0	0	0
jpg	26	27	26	0
jfif	0	0	0	0
heic	0	2	2	0
csv	0	0	0	0
Gesamt	**171**	**176**	**180**	**0**

Tabelle 8: Übersicht Szenario 3 SSD

Ergebnisse Recuva

Es konnten durch Recuva in diesem Durchgang insgesamt 171 Dateien aus dem Originaldatensatz rekonstruiert werden. Jedoch fehlen auch bei diesem Wiederherstellungsprozess einige Dateien, wie die txt, pcap, json, jfif, heic und csv Dateien. Es konnte hierbei auch eine xlsx Datei nicht wiederhergestellt werden. Hierbei handelt es sich um die Datei Passwörter.xlsx, die kennwortgeschützt auf dem Datenträger gespeichert abgelegt wurde. Diese Dateien lagen alle im Stammverzeichnis der SSD und nicht gesondert in Ordnern.

Des Weiteren fällt auf, dass bei diesem Durchlauf wieder eine der jpg Dateien nicht mit wiederhergestellt worden ist, obwohl dies mit den anderen zusammen am selben Ort gespeichert war. Hierbei handelt es sich um das Bild 20231106_205106.

Beim Wiederherstellungsprozess konnte eine MP4-Datei, 20231106_211237, nicht wiederhergestellt werden. Die anderen MP4-Dateien wurden zwar rekonstruiert, jedoch lassen sich nur die Dateien „VID_20231106_220826“, „VID_20231106_220818“ und „VID_20231106_210523“ erfolgreich öffnen und abspielen. Die übrigen Videos sind nicht abspielbar, da es anscheinend während des Prozesses zu Problemen kam und die Dateien nicht ordnungsgemäß rekonstruiert wurden.

Ergebnisse EaseUS data recovery

Ähnlich wie beim Wiederherstellungsprozess auf der HDD wurde auch im Szenario der Schnellformatierung die Partition nicht rekonstruiert. Die insgesamt 176 Dateien aus dem Originaldatensatz wurden in Ordnern abgelegt, die nach Dateityp sortiert sind. Die Dateiformate txt, pcap, json, jfif und csv konnten nicht gesichert werden, ebenso wie die kennwortgeschützte xlsx-Datei „Passwörter.xlsx“. Alle übrigen Dateien wurden hingegen erfolgreich wiederhergestellt.

Ergebnisse PhotoRec

Beim Wiederherstellungsprozess mit PhotoRec wurden insgesamt 180 Dateien aus dem Originaldatensatz rekonstruiert. Einige Dateien konnten jedoch nicht gesichert werden, darunter json, jfif, csv und fünf der txt-Dateien. Zusätzlich konnte die jpg-Datei „20231106_195742“ in diesem Durchlauf nicht wiederhergestellt werden. Auch die kennwortgeschützte xlsx-Datei „Passwörter.xlsx“ wurde nicht rekonstruiert. Alle betroffenen Dateien befanden sich im Stammverzeichnis der SSD.

Ergebnisse X-Ways Forensics

Das IT-forensische Toolkit X-Ways hat wie auch auf dem Festplattenimage der HDD nach einer Schnellformatierung des Datenträgers keine Daten wiederherstellen bzw. identifizieren können.

8.13 Szenario 4 – SSD - Vollständige Formatierung

In Szenario 4 wurden Dateien auf die SSD kopiert. Anschließend wurde die Festplatte über die Datenträgerverwaltung von Microsoft Windows vollständig formatiert. Hiermit werden alle Daten auf dem jeweiligen Datenträger gelöscht

	Wiederhergestellte Dateien aus dem Originaldatensatz			
Dateityp	Recuva	EaseUS	PhotoRec	X-Ways
zip	0	0	0	0
xlsx	0	0	0	0
txt	0	0	0	0
png	0	0	0	0
pdf	0	0	0	0
pcap	0	0	0	0
mp3	0	0	0	0
mp4	0	0	0	0
json	0	0	0	0
jpg	0	0	0	0
jfif	0	0	0	0
heic	0	0	0	0
csv	0	0	0	0
Gesamt	**0**	**0**	**0**	**0**

Tabelle 9: Übersicht Szenario 4 SSD

Ergebnisse Recuva

Die Datenwiederherstellungssoftware Recuva hat bei einer vollständigen Formatierung der Festplatte keine Dateien finden bzw. wiederherstellen können. (Festgehalten auf Abbildung A11 im Anhang)

Ergebnisse EaseUS data recovery

Die Datenwiederherstellungssoftware EaseUS data recovery hat bei einer vollständigen Formatierung der Festplatte keine Dateien finden bzw. wiederherstellen können. (Festgehalten auf Abbildung A12 im Anhang)

Ergebnisse PhotoRec

Das File Carving Tool PhotoRec hat bei einer vollständigen Formatierung der Festplatte keine Dateien finden bzw. wiederherstellen können. (Festgehalten auf Abbildung A13 im Anhang)

Ergebnisse X-Ways Forensics

Das forensische Toolkit X-Ways hat bei einer vollständigen Formatierung der Festplatte keine Dateien finden bzw. wiederherstellen können. (Festgehalten auf Abbildung A14 im Anhang)

9 Gegenüberstellung der Ergebnisse

HDD				
	Recuva	EaseUS	PhotoRec	X-Ways
Szenario 1	209	209	180	206
Szenario 2	207	209	181	205
Szenario 3	171	176	179	0
Szenario 4	0	0	0	0

Tabelle 10: HDD - Übersicht gesamt

SSD				
	Recuva	EaseUS	PhotoRec	X-Ways
Szenario 1	209	209	181	205
Szenario 2	209	209	180	205
Szenario 3	171	176	180	0
Szenario 4	0	0	0	0

Tabelle 11: SSD - Übersicht gesamt

In den Szenarien 1 und 2 konnten alle getesteten Programme eine große Anzahl an Dateien aus dem Originaldatensatz wiederherstellen. Die herkömmlichen Datenwiederherstellungsprogramme Recuva und EaseUS Data Recovery erzielten hierbei die besten Ergebnisse und konnten in den ersten beiden Szenarien nahezu alle Dateien rekonstruieren. Lediglich zwei Dateien konnten in einem der Szenarien mit Recuva nicht wiederhergestellt werden.

Im Vergleich dazu zeigte das File-Carving-Tool PhotoRec eine geringere Leistung und rekonstruierte durchschnittlich 180 Dateien aus dem Originaldatensatz. Die Schwierigkeiten bei der Wiederherstellung könnten auf die Art der Dateiformate zurückzuführen

sein. Obwohl PhotoRec eine große Bandbreite von 480 unterstützten Dateiformaten abdeckt, scheiterte es offenbar bei spezifischen Formaten wie JSON, CSV und JFIF, die im Originaldatensatz enthalten waren und möglicherweise nicht von PhotoRec unterstützt werden. Spezielle Bildformate wie HEIC konnten von dem Tool jedoch problemlos wiederhergestellt werden.

Das IT-forensische Toolkit X-Ways Forensics zeigte in den Tests nur eine eingeschränkte Leistungsfähigkeit. Während es in den ersten beiden Szenarien noch 205 Dateien erfolgreich wiederherstellen konnte, traten bei der Verarbeitung von Datenträgern mit Schnellformatierung offenbar Schwierigkeiten auf. In diesen Fällen war das Tool nicht mehr in der Lage, Dateien auf dem Datenträgerimage zu identifizieren.

Die vollständige Formatierung des Datenträgers stellte für alle getesteten Programme eine Herausforderung dar. Es war keinem der Programme möglich, Dateien auf dem Datenträger zu identifizieren oder wiederherzustellen. Die in Kapitel 3.5.2 angesprochene vollständige Überschreibung mit Nullen bzw. Zufallswerten hat in im letzten Szenario eine Wiederherstellung von Dateien nicht möglich gemacht.

Um die Konsistenz der Ergebnisse zu überprüfen, wurden einige der verwendeten Programme mehrfach auf dasselbe Datenträgerimage angewendet. Dabei konnte festgestellt werden, dass die Programme bei jedem Durchlauf identische Resultate lieferten, was auf eine hohe Reproduzierbarkeit der Testergebnisse hinweist

10 Fazit

Eine zentrale Erkenntnis der durchgeführten Versuche ist, dass eine Schnellformatierung nicht ausreicht, um Daten sicher von einem Datenträger zu löschen. Selbst gängige Datenwiederherstellungsprogramme wie Recuva konnten nach einer Schnellformatierung noch eine große Anzahl von Dateien wiederherstellen. Dies liegt daran, dass bei der Schnellformatierung lediglich die Dateisystemstruktur gelöscht wird. Obwohl dies die Identifikation von Dateien erschwert, zeigen die Analysen, dass diese Barriere für entsprechende Software nur eine geringfügige Herausforderung darstellt. Im Gegensatz dazu erwies sich die vollständige Formatierung als deutlich effektiver. Die Ergebnisse belegen, dass bei dieser Methode keine der getesteten Anwendungen in der Lage war, Dateien oder Fragmente von Dateien, mit denen noch gearbeitet werden kann, auf dem Datenträgerimage zu identifizieren. Damit kann festgestellt werden, dass diese Löschmethode unter Verwendung der in dieser Arbeit untersuchten Programme als sicher angesehen werden kann. Es ist jedoch zu beachten, dass in der IT-Forensik fortgeschrittene Techniken, wie in Kapitel 3.6.4 beschrieben, existieren, die unter Umständen auch bei einer vollständigen Formatierung Daten wiederherstellen könnten. Ein entscheidender Aspekt, der die Bedeutung einer vollständigen Datenlöschung unterstreicht, ist die potenzielle Gefahr, dass bei unzureichender Löschung sensible Daten, auf Datenträger bestehen bleiben könnten. Bei einer erneuten Nutzung des Speichermediums könnten diese Datenreste von Dritten wiederhergestellt werden. Dies kann nicht nur zu Datenschutzproblemen, sondern auch zu erheblichen rechtlichen Konsequenzen führen, da solche verbliebenen Daten unter Umständen missbraucht oder in juristischen Verfahren fehlerhaft interpretiert werden könnten. Eine zuverlässige Datenlöschung ist daher essenziell, insbesondere im Kontext forensischer Untersuchungen und rechtlicher Sicherheit.

Neben den durchgeführten Versuchen wurde nach jedem Wiederherstellungsprozess der Dateien, eine Liste mit den SHA1 Hashwerten erzeugt, die zeigen sollten, ob die wiederhergestellten Dateien identisch zu denen aus dem Originaldatensatz sind. Es hat sich gezeigt, dass das Programm PhotoRec bei der Wiederherstellung signifikant anders vorgeht als die restlichen Programme. Im ersten Szenario beispielsweise stimmten die Hashwerte der wiederhergestellten Dateien bei den Programm Recuva, EaseUS und auch X-Ways mit denen aus dem Originaldatensatz überein. Beim Programm PhotoRec konnten jedoch nur 45 von 180 aus dem Originaldatensatz wiederhergestellten Dateien identische Hashwerte zugeordnet werden. Die restlichen Dateien konnten zwar problemlos geöffnet werden, unterschieden sich jedoch teilweise in ihrer Dateigröße um wenige Bytes. Diese Auswirkung könnte auf das File Carving durch das Programm zurückzuführen sein, welches auf dem Datenträger nach dem Dateiheader sucht, um den Dateityp einordnen zu können. Hier hat das Programm möglicherweise Bytes nicht mit wiederhergestellt, die an sich zur

Datei gehören, zum Wiederherstellen jedoch nicht notwendig sind. Im Laufe der fortgeschritteneren Löschmethoden, konnten auch bei den anderen Programmen teilweise Änderungen in den Hashwerten der Dateien identifiziert werden. Dies könnte als Nebenwirkung der Dateifragmentierung gewertet werden, da sich die Programme die über den Datenträger verteilten Fragmente zusammensuchen müssen.

Es hat sich auch gezeigt, dass für die praxisnahen Szenarien wie der Papierkorblösung, und dem unwiderruflichen Löschen die Datenwiederherstellungsprogramm wie Recuva oder EaseUS ausreichen, um die Daten ordnungsgemäß wiederherstellen zu können. Es bedarf in diesen Fällen keiner Beauftragung eines Datenrettungsdienstleisters, wenn sich die jeweilige Person mit den Programmen vertraut macht. Alle Programme außer X-Ways haben im Szenario 3 noch über 80% der Originaldateien wiederherstellen können.

Diese Bachelorarbeit zeigt auf, dass unterschiedliche Datenlöschmethoden abweichende Wirksamkeiten aufweisen. Aufgrund der unterschiedlichen technischen Ansätze der eingesetzten Programme lässt sich jedoch nicht abschließend beurteilen, ob andere Programme möglicherweise zu abweichenden Ergebnissen geführt hätten. Die in der Arbeit angesprochenen Unterschiede zwischen HDDs und SSDs konnten in den durchgeführten Versuchen nur eingeschränkt beobachtet werden. Ein deutlicher Unterschied zeigte sich jedoch beim sicheren Löschen der Datenträger. Während das sichere Löschen bzw. Überschreiben der HDD mit einer Kapazität von 500 GB durchschnittlich 1 bis 1,5 Stunden in Anspruch nahm, konnte die SSD mit einer Kapazität von 250 GB mittels Secure Erase innerhalb weniger Minuten vollständig und sicher gelöscht werden. Dies unterstreicht die Effizienz moderner Löschverfahren bei SSDs im Vergleich zu HDDs, auch unter Berücksichtigung der unterschiedlichen Speicherkapazitäten.

Ein weiterer zentraler Befund ist, dass nach dem sicheren Löschen der jeweiligen Datenträger, mit dem Programm Parted Magic, keine Daten mehr auf diesen identifiziert, werden konnten. Dies verdeutlicht die Wirksamkeit der eingesetzten Löschmethoden und ihre Bedeutung für Szenarien, in denen eine vollständige und irreversible Datenlöschung erforderlich ist, beispielsweise im Kontext von Datenschutz oder der Entsorgung sensibler Daten. Die im Rahmen dieser Bachelorarbeit durchgeführten Versuche konzentrierten sich auf die vollständige Datenlöschung eines Speichermediums, einschließlich der Formatierung des gesamten Datenträgers, da dieser Prozess oft in Unternehmen angewendet werden muss, um genutzte Festplatten oder andere Datenträger wieder nutzen zu können. Auf dem Softwaremarkt gibt es zahlreiche Programme, die speziell darauf ausgelegt sind, einzelne Ordner oder Dateien zu löschen. Diese Programme werden häufig unter der Bezeichnung "*Datenshredder*" angeboten. Eine solche Methode der Datenlöschung kann in Szenarien nützlich sein, in denen nicht der gesamte Datenträger gelöscht werden soll.

Zukünftige Untersuchungen könnten sich auf verschiedene Aspekte der Datenlöschung konzentrieren, um die Erkenntnisse dieser Arbeit weiter zu vertiefen. Ein interessanter Ansatz wäre die Analyse von spezialisierten Programmen, sogenannten „Datenshreddern“, die gezielt einzelne Dateien oder Ordner löschen, ohne den gesamten Datenträger zu formatieren. Darüber hinaus könnte ein Vergleich internationaler Standards zur Datenlöschung, wie NIST 800-88 oder DoD 5220.22-M, Aufschluss über die Effektivität dieser Vorgaben in unterschiedlichen Anwendungsszenarien geben. Auch die Untersuchung neuer Speichertechnologien, beispielsweise NVMe-SSDs oder hybride Laufwerke, wäre von Bedeutung, um die Wirksamkeit etablierter Löschmethoden auf moderne Speichermedien zu prüfen. Da Cloud-Speicher zunehmend an Bedeutung gewinnen, könnte zudem die Analyse von Löschmethoden und Sicherheitsmaßnahmen bei externen Dienstleistern eine wichtige Rolle spielen.

Unternehmen und private Nutzer/innen müssen sich der Unterschiede zwischen schnellen und sicheren Löschverfahren bewusst sein, um gezielt Maßnahmen zum Schutz ihrer Daten zu ergreifen. Die in dieser Arbeit aufgezeigte Bedeutung internationaler Standards und spezialisierter Software verdeutlicht, wie wichtig die kontinuierliche Weiterentwicklung und Verbreitung sicherer Löschmethoden ist.

11 Abbildungsverzeichnis

12 Tabellenverzeichnis

13 Literaturverzeichnis

[1] RICHARD KISSEL ANDREW REGENSCHEID MATTHEW SCHOLL KEVIN STINE : NIST Special Publication 800-88 Revision 1 - Guidelines for Media Sanitization

[2] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK : IT-Grundschutz Kompendium – Werkzeug für Informationssicherheit

[3] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK : https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html

[4] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES VOM 27. APRIL 2016 : Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

[5] BUNDESMINISTERIUM DER JUSTIZ : Bundesdatenschutzgesetz (BDSG)

[6] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION : Directive (EU) 2000/2555 of the European Parliament and of the council (NIS-2 Richtlinie)

[7] VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES: über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit)

[8] BUNDESANSTALT FÜR FINANZDIENSTLEISTUNGSAUFSICHT: Rundschreiben 10/2017 (BA) - Bankaufsichtliche Anforderungen an die IT (BAIT)

[9] BUNDESVERBAND GESUNDHEITS-IT E. V. ARBEITSGRUPPE DATENSCHUTZ & IT-SICHERHEIT, DEUTSCHE GESELLSCHAFT FÜR MEDIZINISCHE INFORMATIK, BIOMETRIE UND EPIDEMIOLOGIE E. V. ARBEITSGRUPPE „DATENSCHUTZ UND IT-SICHERHEIT IM GESUNDHEITSWESEN“, GESELLSCHAFT FÜR DATENSCHUTZ UND DATENSICHERHEIT E. V. ARBEITSKREIS „DATENSCHUTZ UND DATENSICHERHEIT IM GESUNDHEITS- UND SOZIALWESEN“: Leitfaden für die Erstellung von Löschkonzepten im Gesundheitswesen (20.06.2020)

[10] LUTZ LABS, MIRIAM ABELS: *Sicher Löschen: Daten von Festplatten, SSDs und Handys entfernen* - https://www.heise.de/hintergrund/Sicher-Loeschen-Daten-von-Festplatten-SSDs-und-Handys-zuverlaessig-entfernen-3891831.html (besucht am: 17.12.2024)

[11] https://www.netzwelt.de/sicherheit/datenloeschung/ssd-formatieren-so-loescht-daten-sicher.html (besucht am: 17.12.2024)

[12] MESH FLINDERS, IAN SMALLEY: *WAS IST BCDR?* - https://www.ibm.com/de-de/topics/business-continuity-disaster-recovery (besucht am: 20.12.2024)

[13] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe_node.html (Managementabstract Fortschrittliche Angriffe PDF) (besucht am: 20.12.2024)

[14] *Festplatte / Harddisk* - https://www.elektronik-kompendium.de/sites/com/0610291.htm (besucht am: 17.12.2024)

[15] IONOS REDAKTION: *SSD vs. HDD Festplatte – was sind die Unterschiede?* - https://www.ionos.de/digitalguide/server/knowhow/ssd-vs-hdd-was-ist-der-unterschied/ (besucht am 18.12.2024)

[16] *DoD 5220.22-M* - https://akec.de/dod/ (besucht am 18.12.2024)

[17] *Was bedeutet Trim?* - https://www.crucial.de/articles/about-ssd/what-is-trim (besucht am 20.12.2024)

[18] *Übersicht über NTFS* - https://learn.microsoft.com/de-de/windows-server/storage/file-server/ntfs-overview (besucht am 21.12.2024)

[19] *Alles über die Formatierung: Was ist der Unterschied zwischen Formatieren und Schnellformatierung?* - https://www.easeus.de/partitionieren-tipps/unterschied-zwischen-formatieren-und-schnellformatierung.html (besucht am 18.12.2024)

[20] *Was sind die Hauptunterschiede zwischen vollständige und schnelle Formatierung?* - https://www.sysdevlabs.com/de/articles/operations-with-storages/full-and-quick-format/ (besucht am 22.12.2024)

[21] *NAND-Flash-Technologie und Solid-State-Laufwerke (SSDs)* - https://www.kingston.com/de/blog/pc-performance/nand-flash-technology-and-ssd (besucht am 21.12.2024)

[22] *Risiken der logischen Datenwiederherstellung* - https://www.stellardatenrettung.de/risiken-der-logischen-datenwiederherstellung.htm (besucht am 02.01.2024)

[23] JAMIE WALLIS*: Physical Data Recovery* - https://www.streetdirectory.com/travel_guide/114073/data_recovery/physical_data_recovery.html (besucht am 18.12.2024)

[24] *Anleitung: Datenrettung mit Linux* - https://www.030-datenrettung.de/datenrettung-linux-ddrescue-anleitung (besucht am: 20.12.2024)

[25] DIRK OLTERSDORF (Online Editor G DATA) *Was ist eigentlich Defragmentieren?* - https://www.gdata.de/ratgeber/was-ist-eigentlich-defragmentieren (besucht am: 21.12.2024)

[26] *Journaling Dateisysteme* - https://www.linux-praxis.de/journaling-dateisysteme (besucht am: 05.01.2024)

[27] EASEUS*: Dateisysteme Vergleich: NTFS, FAT32, exFAT und EXT, welches Dateisystem sollte ich verwenden?* - https://www.easeus.de/festplattenverwaltung/dateisystem.html (besucht am: 20.12.2024)

[28] IT-FORENSIK WIKI HS WISMAR: *Journaling Dateisystem* - https://it-forensik.fiw.hs-wismar.de/index.php/Journaling-Dateisystem (besucht am 04.01.2024)

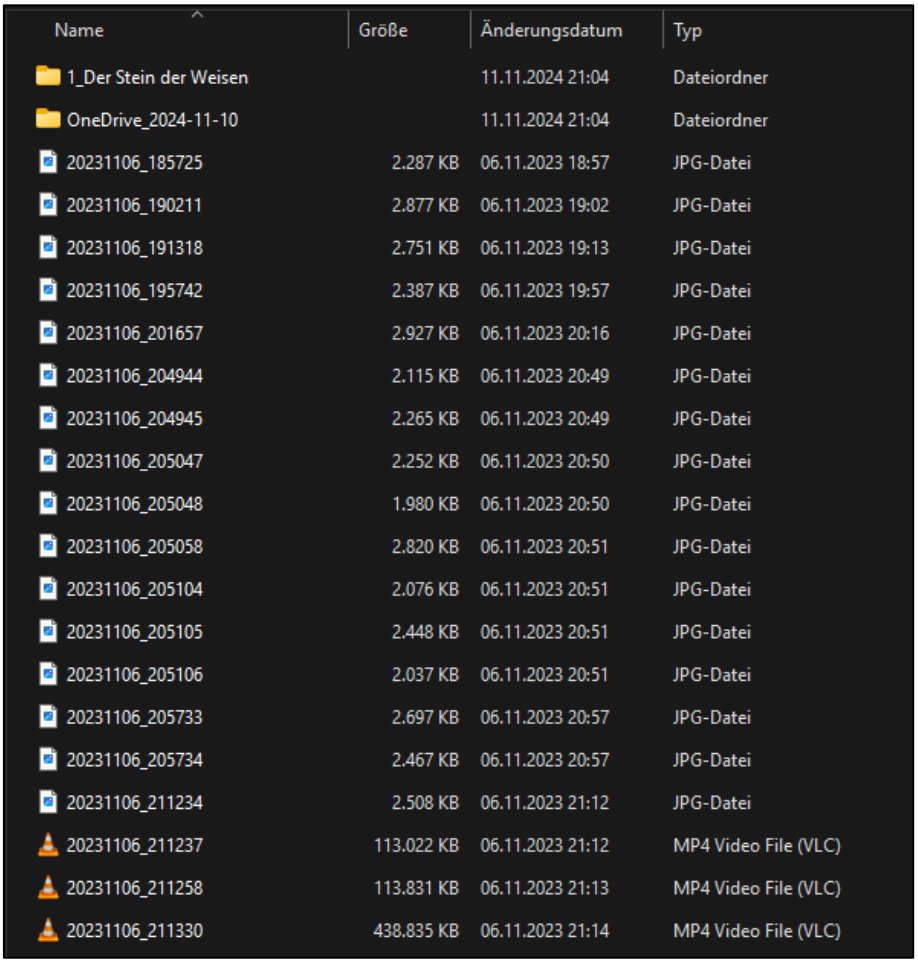
[29] EASEUS*: Wie kann man fragmentierte Dateien wie Bilder und Videos wiederherstellen?* - https://www.easeus.de/dateien-wiederherstellen/fragmentierte-dateien-wiederherstellen.html (besucht am 20.12.2024)

[30] *Das Linux-Dateisystem Ext4* - https://www.heise.de/tests/Das-Linux-Dateisystem-Ext4-221262.html?seite=2 (besucht am 06.01.2024)

14 Anhang

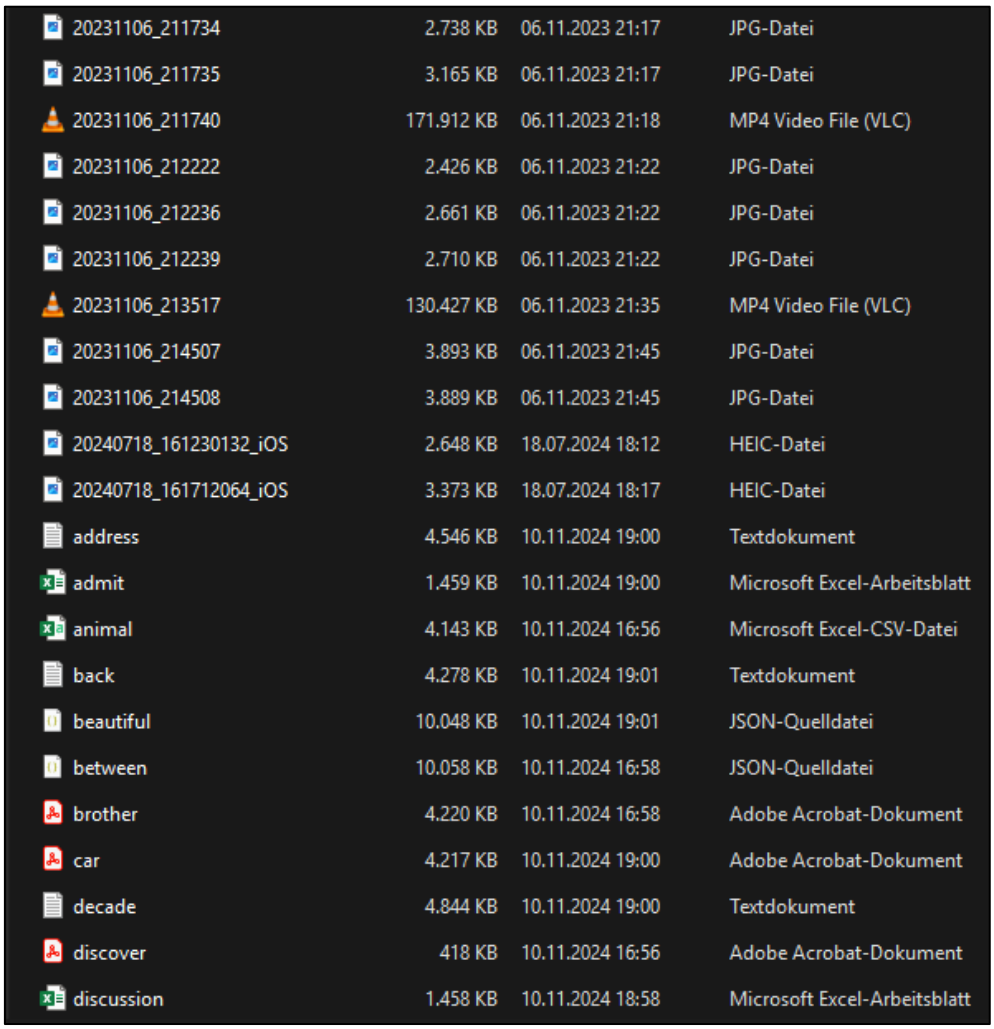
14.1 Abbildungsverzeichnis Anhang

14.2 Abbildungen



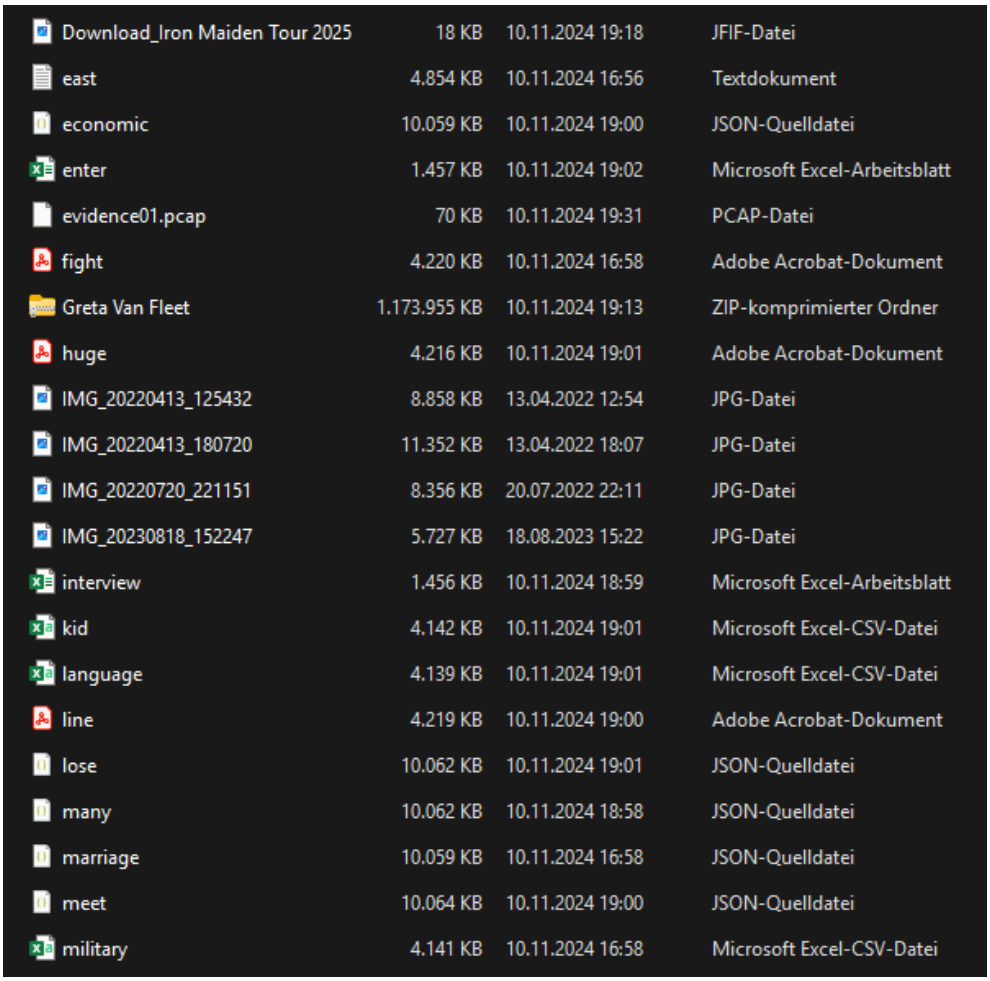
Name	Größe	Änderungsdatum	Typ
1_Der Stein der Weisen		11.11.2024 21:04	Dateiordner
OneDrive_2024-11-10		11.11.2024 21:04	Dateiordner
20231106_185725	2.287 KB	06.11.2023 18:57	JPG-Datei
20231106_190211	2.877 KB	06.11.2023 19:02	JPG-Datei
20231106_191318	2.751 KB	06.11.2023 19:13	JPG-Datei
20231106_195742	2.387 KB	06.11.2023 19:57	JPG-Datei
20231106_201657	2.927 KB	06.11.2023 20:16	JPG-Datei
20231106_204944	2.115 KB	06.11.2023 20:49	JPG-Datei
20231106_204945	2.265 KB	06.11.2023 20:49	JPG-Datei
20231106_205047	2.252 KB	06.11.2023 20:50	JPG-Datei
20231106_205048	1.980 KB	06.11.2023 20:50	JPG-Datei
20231106_205058	2.820 KB	06.11.2023 20:51	JPG-Datei
20231106_205104	2.076 KB	06.11.2023 20:51	JPG-Datei
20231106_205105	2.448 KB	06.11.2023 20:51	JPG-Datei
20231106_205106	2.037 KB	06.11.2023 20:51	JPG-Datei
20231106_205733	2.697 KB	06.11.2023 20:57	JPG-Datei
20231106_205734	2.467 KB	06.11.2023 20:57	JPG-Datei
20231106_211234	2.508 KB	06.11.2023 21:12	JPG-Datei
20231106_211237	113.022 KB	06.11.2023 21:12	MP4 Video File (VLC)
20231106_211258	113.831 KB	06.11.2023 21:13	MP4 Video File (VLC)
20231106_211330	438.835 KB	06.11.2023 21:14	MP4 Video File (VLC)

A 1: Originaldatensatz (1)



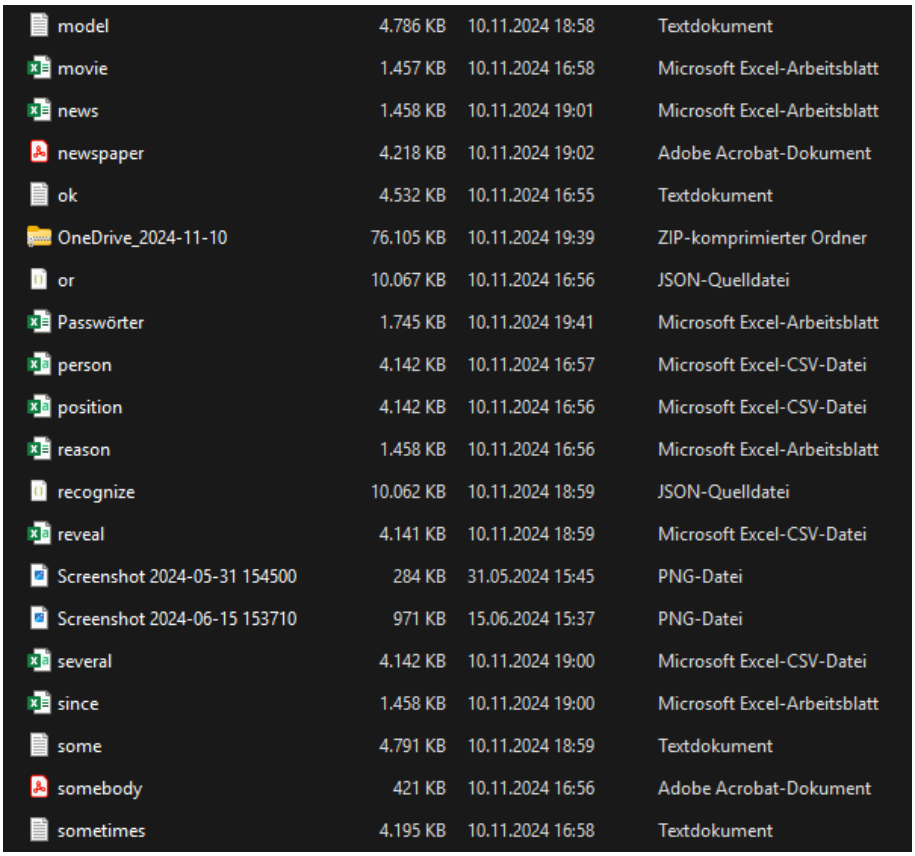
20231106_211734	2.738 KB	06.11.2023 21:17	JPG-Datei
20231106_211735	3.165 KB	06.11.2023 21:17	JPG-Datei
20231106_211740	171.912 KB	06.11.2023 21:18	MP4 Video File (VLC)
20231106_212222	2.426 KB	06.11.2023 21:22	JPG-Datei
20231106_212236	2.661 KB	06.11.2023 21:22	JPG-Datei
20231106_212239	2.710 KB	06.11.2023 21:22	JPG-Datei
20231106_213517	130.427 KB	06.11.2023 21:35	MP4 Video File (VLC)
20231106_214507	3.893 KB	06.11.2023 21:45	JPG-Datei
20231106_214508	3.889 KB	06.11.2023 21:45	JPG-Datei
20240718_161230132_iOS	2.648 KB	18.07.2024 18:12	HEIC-Datei
20240718_161712064_iOS	3.373 KB	18.07.2024 18:17	HEIC-Datei
address	4.546 KB	10.11.2024 19:00	Textdokument
admit	1.459 KB	10.11.2024 19:00	Microsoft Excel-Arbeitsblatt
animal	4.143 KB	10.11.2024 16:56	Microsoft Excel-CSV-Datei
back	4.278 KB	10.11.2024 19:01	Textdokument
beautiful	10.048 KB	10.11.2024 19:01	JSON-Quelldatei
between	10.058 KB	10.11.2024 16:58	JSON-Quelldatei
brother	4.220 KB	10.11.2024 16:58	Adobe Acrobat-Dokument
car	4.217 KB	10.11.2024 19:00	Adobe Acrobat-Dokument
decade	4.844 KB	10.11.2024 19:00	Textdokument
discover	418 KB	10.11.2024 16:56	Adobe Acrobat-Dokument
discussion	1.458 KB	10.11.2024 18:58	Microsoft Excel-Arbeitsblatt

A 2: Originaldatensatz (2)



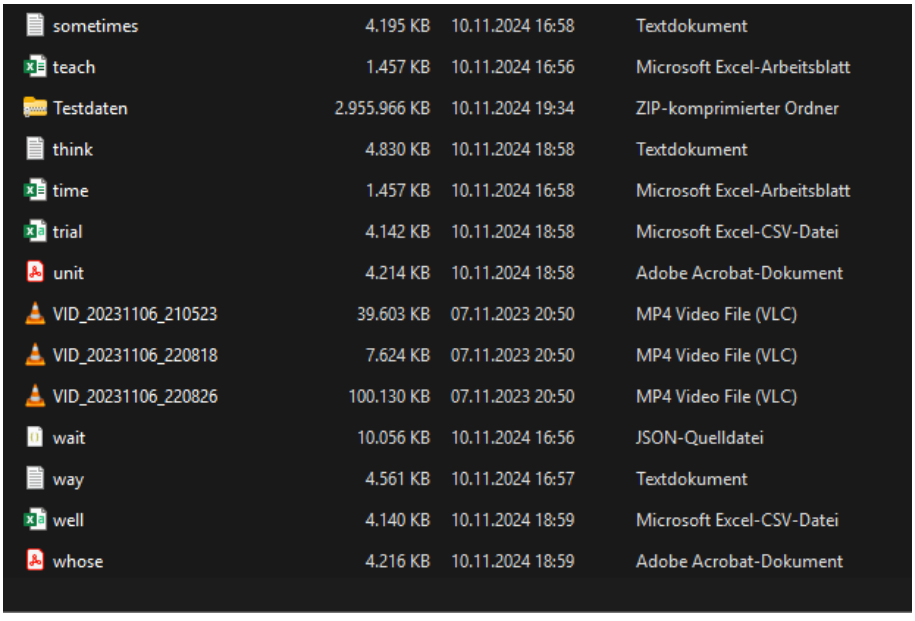
Download_Iron Maiden Tour 2025	18 KB	10.11.2024 19:18	JFIF-Datei
east	4.854 KB	10.11.2024 16:56	Textdokument
economic	10.059 KB	10.11.2024 19:00	JSON-Quelldatei
enter	1.457 KB	10.11.2024 19:02	Microsoft Excel-Arbeitsblatt
evidence01.pcap	70 KB	10.11.2024 19:31	PCAP-Datei
fight	4.220 KB	10.11.2024 16:58	Adobe Acrobat-Dokument
Greta Van Fleet	1.173.955 KB	10.11.2024 19:13	ZIP-komprimierter Ordner
huge	4.216 KB	10.11.2024 19:01	Adobe Acrobat-Dokument
IMG_20220413_125432	8.858 KB	13.04.2022 12:54	JPG-Datei
IMG_20220413_180720	11.352 KB	13.04.2022 18:07	JPG-Datei
IMG_20220720_221151	8.356 KB	20.07.2022 22:11	JPG-Datei
IMG_20230818_152247	5.727 KB	18.08.2023 15:22	JPG-Datei
interview	1.456 KB	10.11.2024 18:59	Microsoft Excel-Arbeitsblatt
kid	4.142 KB	10.11.2024 19:01	Microsoft Excel-CSV-Datei
language	4.139 KB	10.11.2024 19:01	Microsoft Excel-CSV-Datei
line	4.219 KB	10.11.2024 19:00	Adobe Acrobat-Dokument
lose	10.062 KB	10.11.2024 19:01	JSON-Quelldatei
many	10.062 KB	10.11.2024 18:58	JSON-Quelldatei
marriage	10.059 KB	10.11.2024 16:58	JSON-Quelldatei
meet	10.064 KB	10.11.2024 19:00	JSON-Quelldatei
military	4.141 KB	10.11.2024 16:58	Microsoft Excel-CSV-Datei

A 3: Originaldatensatz (3)



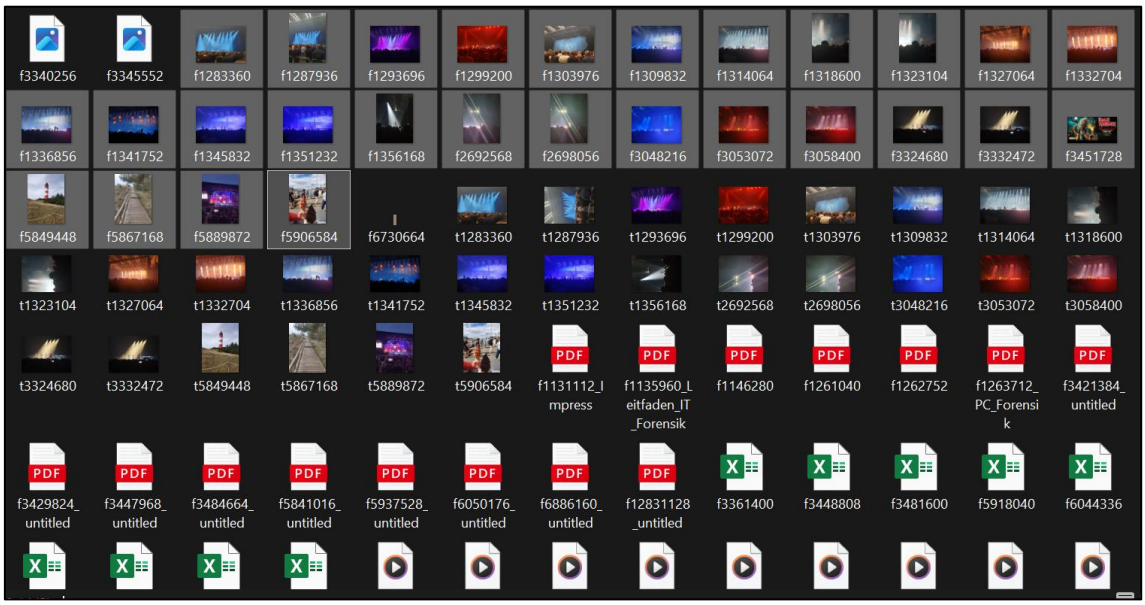
model	4.786 KB	10.11.2024 18:58	Textdokument
movie	1.457 KB	10.11.2024 16:58	Microsoft Excel-Arbeitsblatt
news	1.458 KB	10.11.2024 19:01	Microsoft Excel-Arbeitsblatt
newspaper	4.218 KB	10.11.2024 19:02	Adobe Acrobat-Dokument
ok	4.532 KB	10.11.2024 16:55	Textdokument
OneDrive_2024-11-10	76.105 KB	10.11.2024 19:39	ZIP-komprimierter Ordner
or	10.067 KB	10.11.2024 16:56	JSON-Quelldatei
Passwörter	1.745 KB	10.11.2024 19:41	Microsoft Excel-Arbeitsblatt
person	4.142 KB	10.11.2024 16:57	Microsoft Excel-CSV-Datei
position	4.142 KB	10.11.2024 16:56	Microsoft Excel-CSV-Datei
reason	1.458 KB	10.11.2024 16:56	Microsoft Excel-Arbeitsblatt
recognize	10.062 KB	10.11.2024 18:59	JSON-Quelldatei
reveal	4.141 KB	10.11.2024 18:59	Microsoft Excel-CSV-Datei
Screenshot 2024-05-31 154500	284 KB	31.05.2024 15:45	PNG-Datei
Screenshot 2024-06-15 153710	971 KB	15.06.2024 15:37	PNG-Datei
several	4.142 KB	10.11.2024 19:00	Microsoft Excel-CSV-Datei
since	1.458 KB	10.11.2024 19:00	Microsoft Excel-Arbeitsblatt
some	4.791 KB	10.11.2024 18:59	Textdokument
somebody	421 KB	10.11.2024 16:56	Adobe Acrobat-Dokument
sometimes	4.195 KB	10.11.2024 16:58	Textdokument

A 4: Originaldatensatz (4)

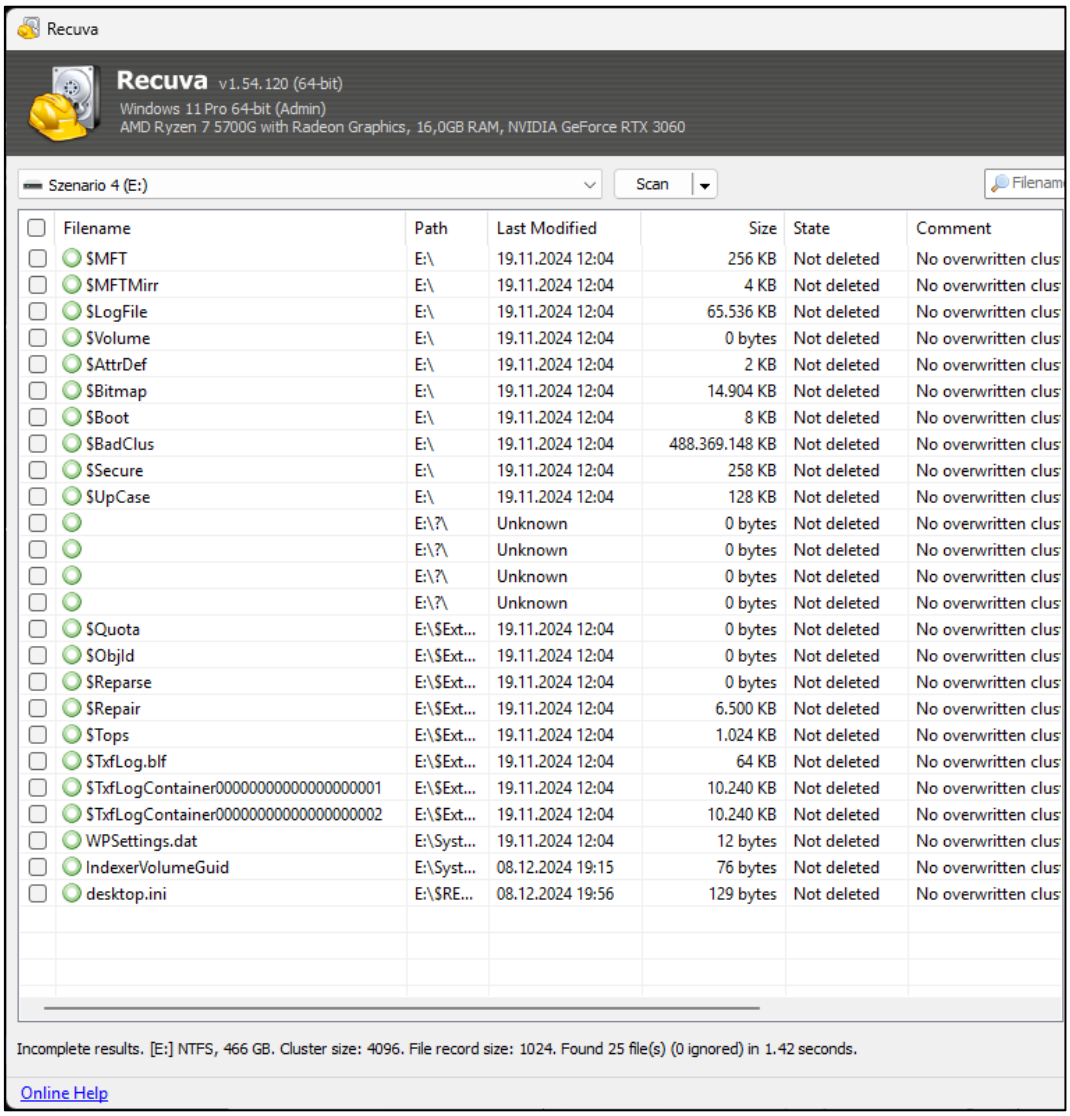


sometimes	4.195 KB	10.11.2024 16:58	Textdokument
teach	1.457 KB	10.11.2024 16:56	Microsoft Excel-Arbeitsblatt
Testdaten	2.955.966 KB	10.11.2024 19:34	ZIP-komprimierter Ordner
think	4.830 KB	10.11.2024 18:58	Textdokument
time	1.457 KB	10.11.2024 16:58	Microsoft Excel-Arbeitsblatt
trial	4.142 KB	10.11.2024 18:58	Microsoft Excel-CSV-Datei
unit	4.214 KB	10.11.2024 18:58	Adobe Acrobat-Dokument
VID_20231106_210523	39.603 KB	07.11.2023 20:50	MP4 Video File (VLC)
VID_20231106_220818	7.624 KB	07.11.2023 20:50	MP4 Video File (VLC)
VID_20231106_220826	100.130 KB	07.11.2023 20:50	MP4 Video File (VLC)
wait	10.056 KB	10.11.2024 16:56	JSON-Quelldatei
way	4.561 KB	10.11.2024 16:57	Textdokument
well	4.140 KB	10.11.2024 18:59	Microsoft Excel-CSV-Datei
whose	4.216 KB	10.11.2024 18:59	Adobe Acrobat-Dokument

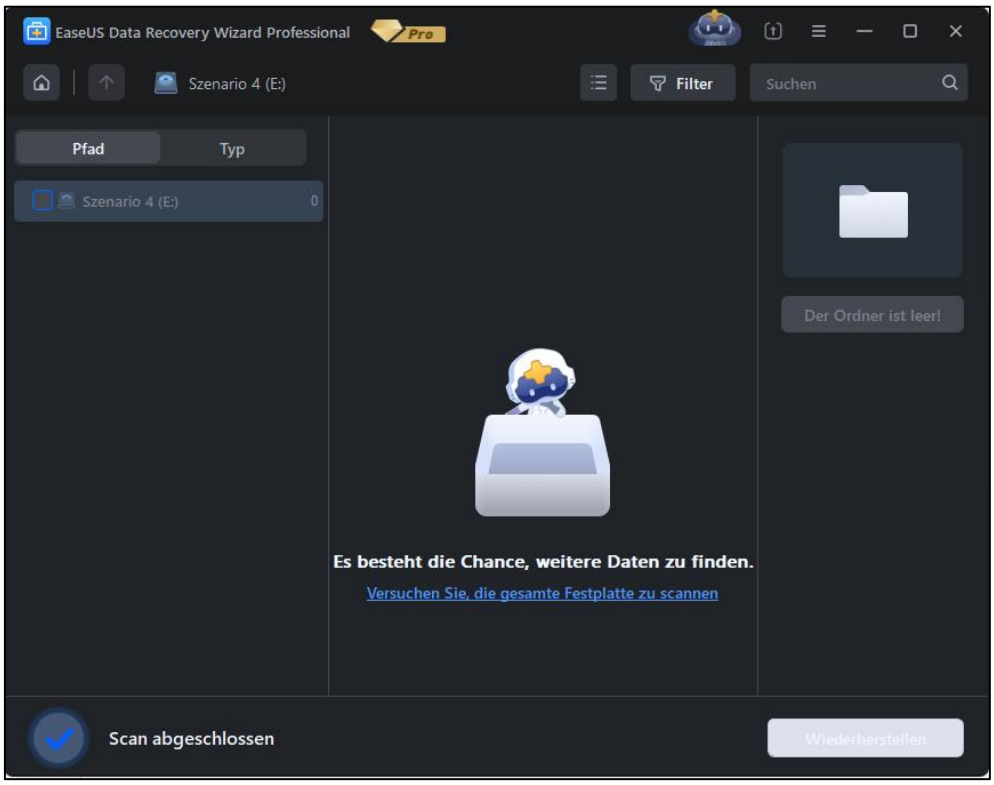
A 5: Originaldatensatz (5)



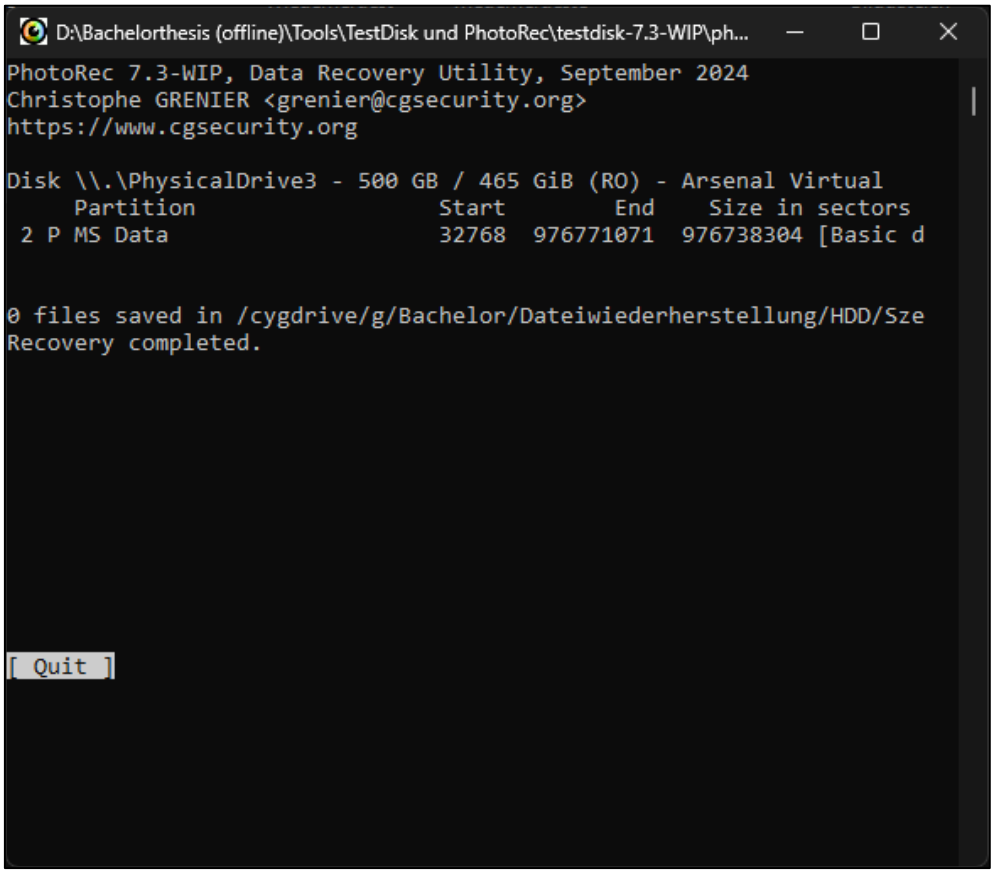
A 6: PhotoRec Szenario 3 HDD - Übersicht Bilddateien



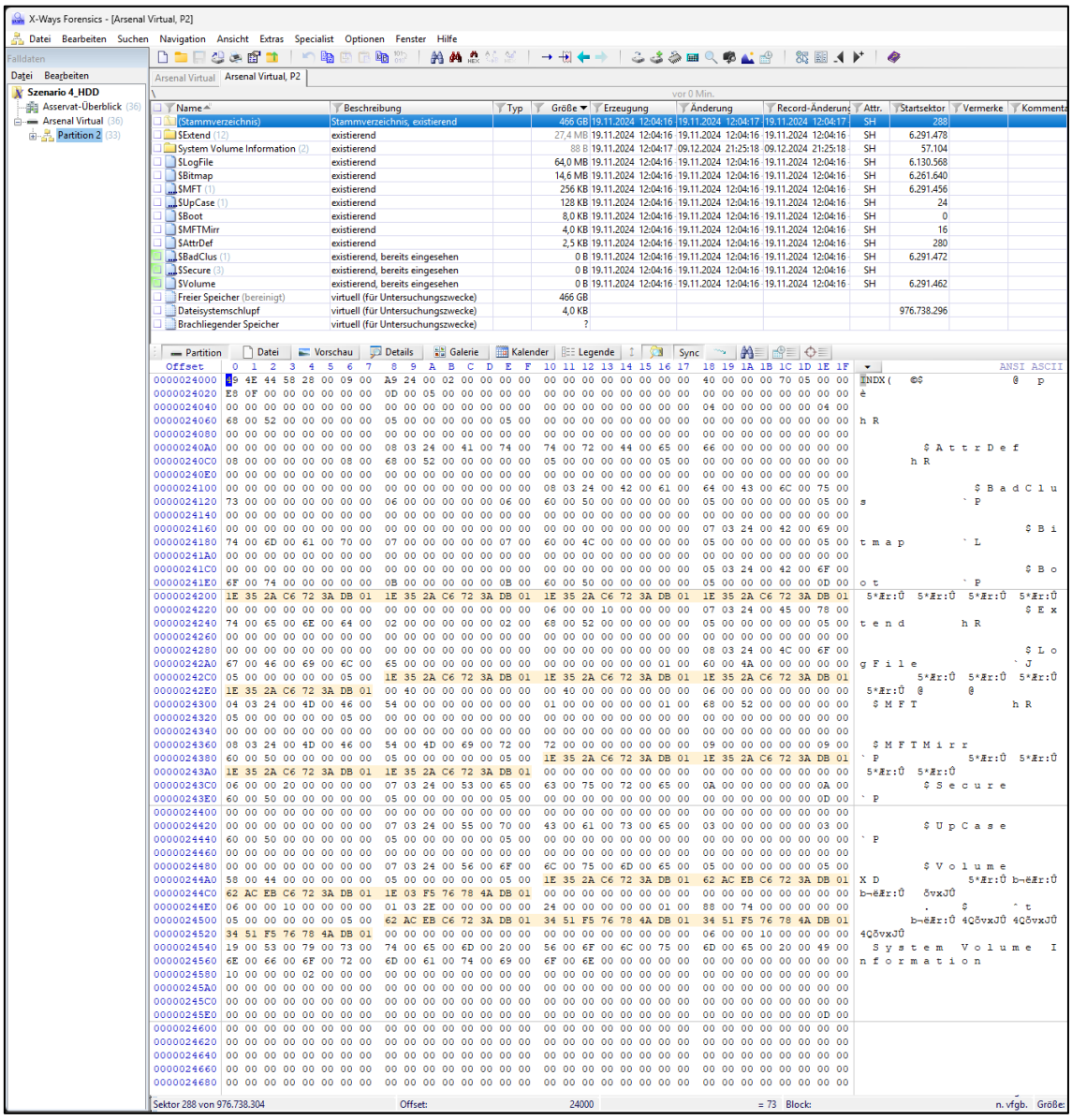
A 7: Recuva Szenario 4 HDD - Übersicht gefundene Dateien



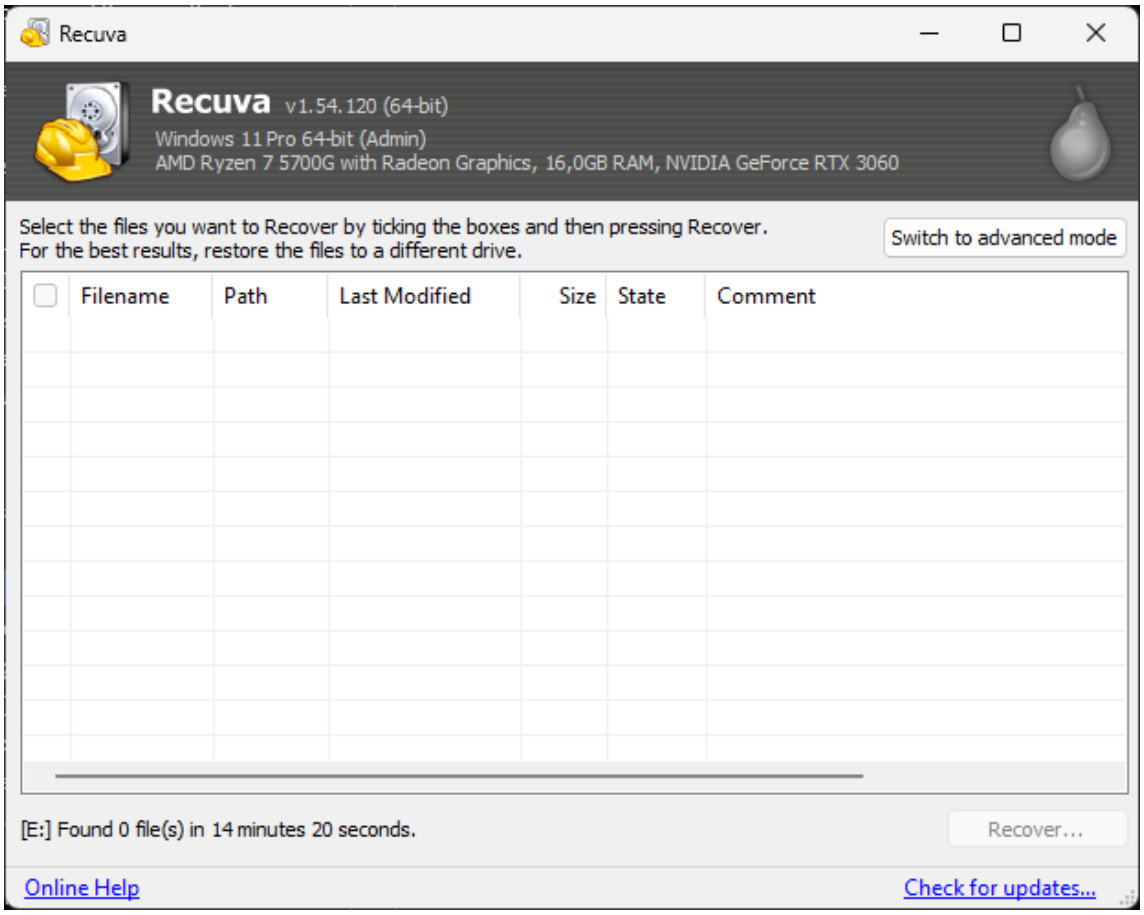
A 8: EaseUS Szenario 4 HDD - Übersicht gefundene Dateien



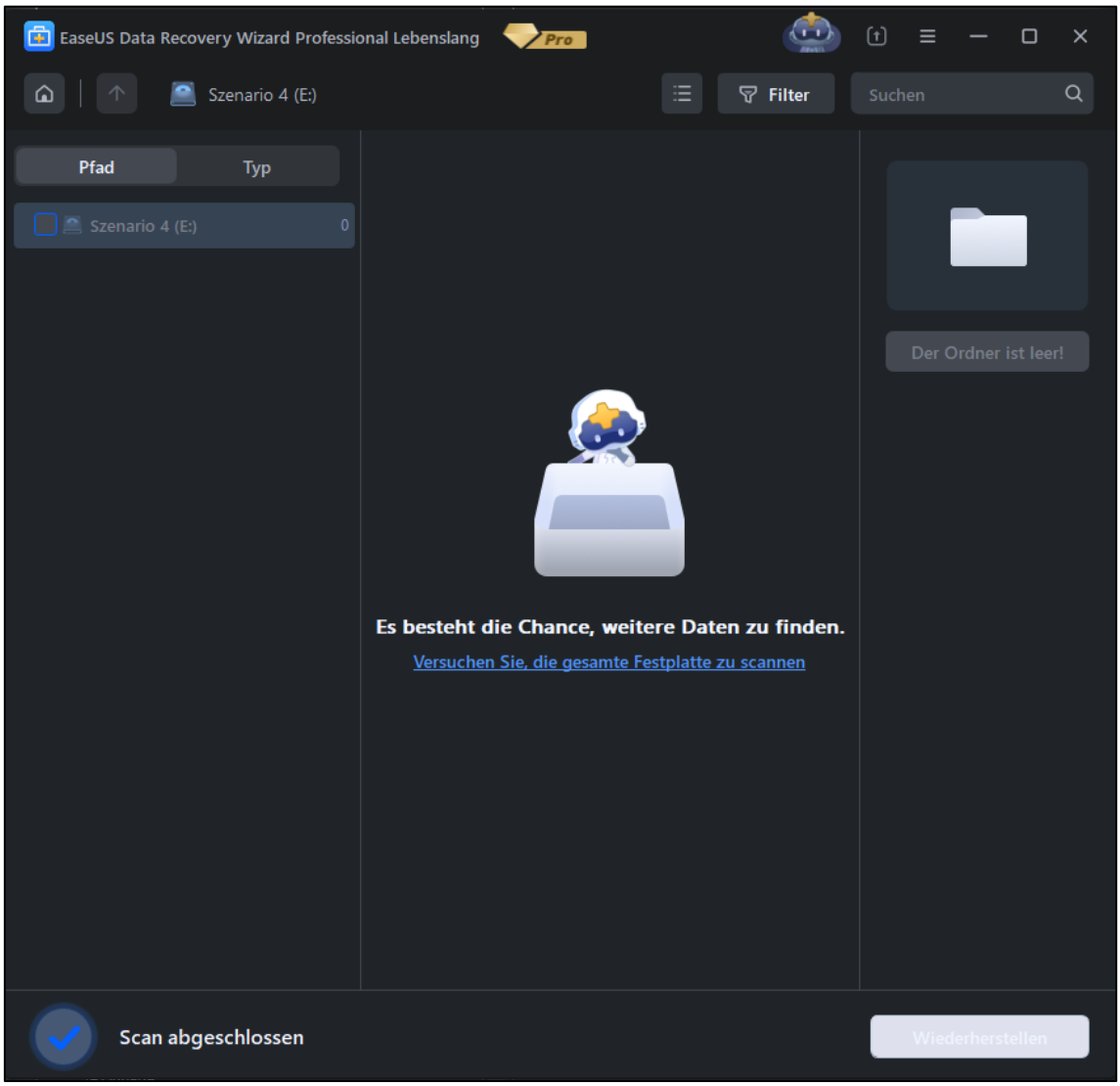
A 9: PhotoRec Szenario 4 HDD - Übersicht gefundene Dateien



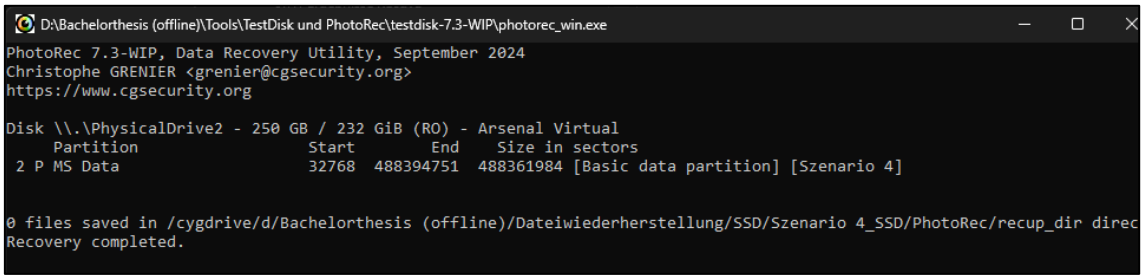
A 10: X-Ways Szenario 4 HDD - Übersicht gefundene Dateien



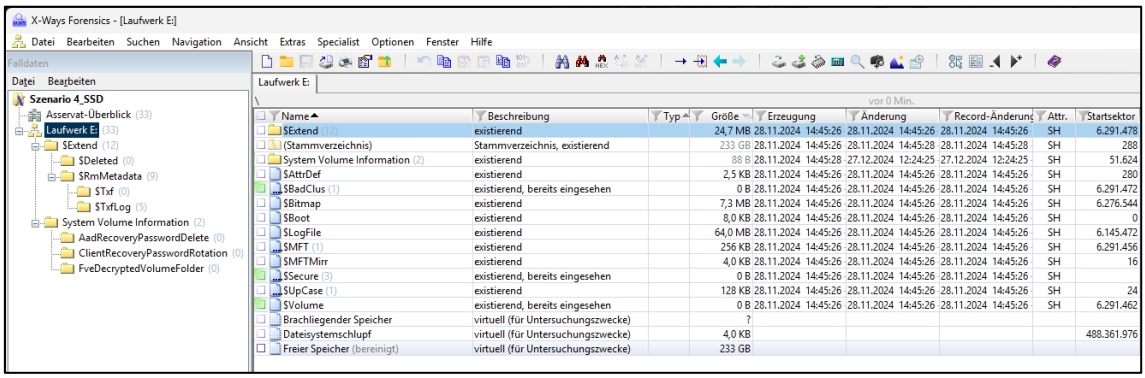
A 11: Recuva Szenario 4 SSD - Übersicht gefundene Dateien



A 12: EaseUS Szenario 4 SSD - Übersicht gefundene Dateien



A 13: PhotoRec Szenario 4 SSD - Übersicht gefundene Dateien



A 14: X-Ways Szenario 4 SSD - Übersicht gefundene Dateien

14.3 Genutzte Hardware und Software

Datenträger Szenarien 1 - 4 HDD:

- Seagate Desktop HDD 500 GB

Datenträger Szenarien 1 - 4 SSD:

- Samsung 870 EVO SSD 250GB

Mounten von Imagedateien:

- Arsenal Image Mounter (Version 3.11.293 – Veröffentlicht: 26.06.2024)

Erstellung von Imagedateien:

- FTK Imager (Version 4.7.1.2 – Veröffentlicht: Januar 2022)

Sicheres Löschen der Datenträger:

- Parted Magic (Version 2024_11_03 – Veröffentlicht: 03.11.2024)

Recuva (Version 1.54.0 – Veröffentlicht: 26.06.2024)

Recuva ist ein kostenloses Programm zur Datenwiederherstellung für Festplattenlaufwerke und Wechseldatenträger. Es ist mit Windows ab Windows XP kompatibel und unterstützt auch 64-Bit-Systeme. Das Programm unterstützt schnelle Scans und auch sogenannte Deep-Scan Modi, ist hierbei jedoch weniger effizient bei stark beschädigten oder fragmentierten Daten. Es wurde hierbei die freie, unbezahlte Version genutzt.

EaseUS Data Recovery (Version 19.2.5 – Veröffentlicht: 18.11.2024)

Das Programm ist eine kostenlose Datenrettungssoftware zur Wiederherstellung gelöschter Dateien aus dem Papierkorb, von Festplatten, SSDs, SD-Karten usw. Es kann ein Upgrade durchgeführt werden, was mehr Funktionen freischaltet. Es bietet ebenfalls schnelle und tiefe Scans, wobei die Suchlogik des Programmes fortschrittlicher und geeigneter für komplexere Wiederherstellungen z.B. nach einem Partitionsverlust, da es die Partition wiederherstellen kann. Zusätzlich ist die Wiederherstellung von Daten aus beschädigten oder nicht zugreifbaren Partitionen möglich. Es wurde die kostenpflichtige Variante der Software genutzt.

PhotoRec (Version 7.3 – Veröffentlicht: September 2024)

PhotoRec ist ein kostenloses, Open-Source-Datenwiederherstellungstool, das auf signaturbasierte Methoden setzt und unabhängig vom Dateisystem arbeitet. Das Programm ist eher an technisch versierte Anwendende gerichtet, da es keine grafische Oberfläche wie bei anderen Datenwiederherstellungsprogrammen gibt, sondern es über die Kommandozeile von Windows gestartet wird und rein textbasiert arbeitet. Die Leistungsfähigkeit ist bei diesem Programm jedoch hoch und es kann Dateien auch von beschädigten oder stark fragmentierten Laufwerken rekonstruieren. Hierbei wurde eine freie, unbezahlte Version genutzt.

X-Ways Forensics (Version 21.3 – Veröffentlicht: 26.10.2024)

Das IT-forensische Toolkit X-Ways Forensics ist ein kostenpflichtiges kommerzielles Programm, welches für die Untersuchung und Analyse von digitalen Beweismitteln programmiert wurde. Neben der Datenwiederherstellung bietet es weitere Funktionen wie Datenträgerabbildung, tiefgehende Dateisystemanalyse und detaillierte Protokollierung von Beweisen. Der Fokus liegt hierbei auf tiefgehenden Dateisystemanalysen und effizienter Datenverarbeitung. Es wurde eine 60-tägige Trail Lizenz seitens des Herstellers zur Verfügung gestellt.