

Methoden und Werkzeuge zur Datenwiederherstellung und Metadaten-Analyse

STUDIENARBEIT

für die Prüfung zum
Bachelor of Science

des Studiengangs Angewandte Informatik

an der Dualen Hochschule Baden-Württemberg Karlsruhe

von

Mael Dossoh

Abgabedatum 19.05.2025

Matrikelnummer: 3167941
Kurs: TINF22B5

Gutachter der Studienakademie Ralf, Brune

Erklärung

(gemäß §5(3) der „Studien- und Prüfungsordnung DHBW Technik“ vom 14.07.21)

Ich versichere hiermit, dass ich meine Projektarbeit mit dem Thema: „**Methoden und Werkzeuge zur Datenwiederherstellung und Metadaten-Analyse**“, selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Karlsruhe, 19.05.2025

Ort, Datum

Unterschrift

Hinweise zur Sprachverwendung und methodischen Unterstützung

In der vorliegenden wissenschaftlichen Arbeit wird bewusst auf gendergerechte Sprache verzichtet. Diese Entscheidung dient der Lesefreundlichkeit sowie der sprachlichen Klarheit und folgt der wissenschaftlichen Konvention, Inhalte möglichst präzise und sachlich darzustellen. Alle Personenbezeichnungen gelten daher geschlechtsneutral.

Zur Unterstützung bei der sprachlichen Ausarbeitung wurde eine KI-basierte Schreibassistenz eingesetzt. Dabei diente sie ausschließlich der sprachlichen Optimierung und Strukturierung. Inhaltliche Ansätze, Argumentationslinien und fachliche Bewertungen stammen vollständig vom Verfasser selbst.

Inhaltsverzeichnis

| | |
|---|----|
| Inhaltsverzeichnis | I |
| Abbildungsverzeichnis | II |
| Abkürzungsverzeichnis | II |
| 1. Einleitung | 1 |
| 1.1. Hintergrund und Relevanz des Themas | 1 |
| 1.2. Zielsetzung | 4 |
| 1.3. Aufbau der Arbeit | 5 |
| 2. Grundlagen | 6 |
| 2.1. Forensik | 6 |
| 2.2. Digitale Forensik | 10 |
| 2.2.1. Datenwiederherstellung | 13 |
| 2.2.2. Metadaten-Analyse | 17 |
| 2.3. Die Ermittlungsumgebung CAINE | 20 |
| 2.3.1. Integrierte Tools | 20 |
| 3. Praktische Umsetzung | 24 |
| 3.1. Einrichtung der virtuellen Analyseumgebung | 25 |
| 3.2. Datenwiederherstellung in der Praxis | 27 |
| 3.2.1. Vorbereitungen | 27 |
| 3.2.2. Durchführung | 28 |
| 3.2.3. Ergebnisse | 29 |
| 3.3. Metadaten Analyse in der Praxis | 29 |
| 3.3.1. Vorbereitungen | 29 |
| 3.3.2. Durchführung | 30 |
| 3.3.3. Ergebnisse | 30 |
| 3.4. Bewertung der Forensischen Umgebung | 30 |
| 4. Fazit | 31 |
| 4.1. Zusammenfassung der Ergebnisse | 31 |
| 4.2. Bewertung der eingesetzten Werkzeuge | 31 |
| 4.3. Ausblick | 31 |
| Literaturverzeichnis | VI |

Abbildungsverzeichnis

| | |
|---|----|
| Abbildung 1: Prognose: Kostenanstieg durch Cyberkriminalität (Statista, 2024) | 2 |
| Abbildung 2: Forensikprozess gemäß ISO (ISO, 2018) | 9 |
| Abbildung 3: Visualisierung der Chain of Custody gemäß ISO 20 (ISO, 2018) | 11 |
| Abbildung 4: Datenwiederherstellungsprozess nach (Spiceworks Inc., 2024) | 15 |
| Abbildung 5: Analyse von Daten mit Autopsy (TSK, 2024) | 21 |
| Abbildung 6: Analyse von Daten mit Autopsy (TSK, 2024) | 22 |
| Abbildung 7: Parameter der CAINE VM | 25 |
| Abbildung 8: Persistente Installation auf der virtuellen Festplatte | 26 |
| Abbildung 9: Anlage von Testdaten | 27 |
| Abbildung 10: Start von Guymager und Übersicht der verfügbaren Laufwerke | 28 |

Abkürzungsverzeichnis

| | |
|--------------|---|
| APFS | Apple File System |
| BA | Bundeskriminalamt |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| CAINE | Computer Aided INvestigative Environment |
| CPU | Central Processing Unit |
| DNA | Desoxyribonucleic Acid |
| DSGVO | Datenschutz-Grundverordnung |
| ENFSI | European Network of Forensic Science Institutes |
| EWf | Expert Witness Format |
| FAT | File Allocation Table |
| GB | Gigabyte |
| IDS | Intrusion Detection System |
| IEC | International Electrotechnical Commission |
| IP | Internet Protocol |
| ISO | International Organization for Standardization |

| | |
|--------------|--|
| IT | Informationstechnologie |
| KI | Künstliche Intelligenz |
| MB | Megabyte |
| MFT | Master File Table |
| NIST | National Institute of Standards and Technology |
| NSU | Nationalsozialistischer Untergrund |
| NTFS | New Technology File System |
| OT | Operational Technology |
| RAM | Random Access Memory |
| RAW | Raw Image |
| SOP | Standard Operating Procedure |
| TSK | The Sleuth Kit |
| VM | Virtuelle Machine |
| inode | index node |

1. Einleitung

Dieses Kapitel führt in Thema, Zielsetzung und Methodik dieser Studienarbeit ein. Im Zentrum steht die Untersuchung forensischer Verfahren zur Datenwiederherstellung und Metadatenanalyse.

In Abschnitt 1.1 wird die gesellschaftliche, wirtschaftliche und sicherheitstechnische Relevanz der digitalen Forensik aufgezeigt. Dabei werden die Bedrohungslage durch Cyberkriminalität sowie die Rolle der Datenwiederherstellung und Metadatenanalyse als Verfahren in der Beweissicherung hervorgehoben.

Abschnitt 1.2 beschreibt die Ziele dieser Arbeit, darunter die Vorstellung und Bewertung ausgewählter Werkzeuge zur digitalen Spurensicherung. Zudem wird erläutert, welche Anwendungsbereiche, Zielgruppen und Bewertungskriterien im Fokus stehen.

In Abschnitt 1.3 wird der strukturelle und methodische Aufbau der Arbeit dargelegt. Dabei wird aufgezeigt, wie theoretische Grundlagen, praktische Werkzeuganwendung und forensische Standards systematisch miteinander verknüpft sind, um nachvollziehbare Ergebnisse und praxisnahe Empfehlungen zu ermöglichen.

1.1. Hintergrund und Relevanz des Themas

Die Informationstechnologie (IT)-Forensik, auch digitale Forensik genannt, hat sich im vergangenen Jahrhundert zu einem essenziellen Instrument in der Kriminalistik und Sicherheitsforschung entwickelt (Casey, 2011). Mit der zunehmenden Digitalisierung nahezu aller Lebensbereiche ist die IT-Forensik zu einem unverzichtbaren Bestandteil moderner Ermittlungsarbeit geworden (Casey, 2011).

Laut dem **National Institute of Standards and Technology (NIST)** haben die Entwicklungen leistungsfähiger Computersysteme und Netzwerkinfrastrukturen seit den 1980er-Jahren neue Möglichkeiten geschaffen, digitale Spuren zu hinterlassen, zu sichern und auszuwerten (NIST, 2006).

In Unternehmenskontexten kann ein Verlust der Datenintegrität weitreichende Folgen haben. Datenintegrität bezeichnet die Korrektheit und Konsistenz von Daten während ihres gesamten Lebenszyklus (Varonis Systems, 2023). Ein Verstoß gegen die Datenintegrität kann zu fehlerhaften Informationen führen und operative Prozesse stören.

Ein typisches Beispiel für die Folgen eines Datenverlusts stellt ein Produktionsausfall dar. In der Produktion sind vernetzte Systeme potenzielle Ziele für Cyberangriffe. Solche Angriffe auf die sogenannte „Operational Technology“ (OT) können nicht nur Daten gefährden, sondern auch Produktionsprozesse lahmlegen und Ausfallzeiten verursachen (Einsnulleins GmbH, 2023).

Zusätzlich können rechtliche Konsequenzen drohen, insbesondere bei Verstößen gegen Aufbewahrungs- und Datenschutzpflichten. Für Privatpersonen bedeutet der Verlust von Daten ein erhöhtes Risiko für Identitätsdiebstahl. Die zunehmende Verlagerung alltäglicher Aktivitäten in digitale Infrastrukturen macht diese sowohl essenziell als auch verwundbar (Varonis Systems, 2023).

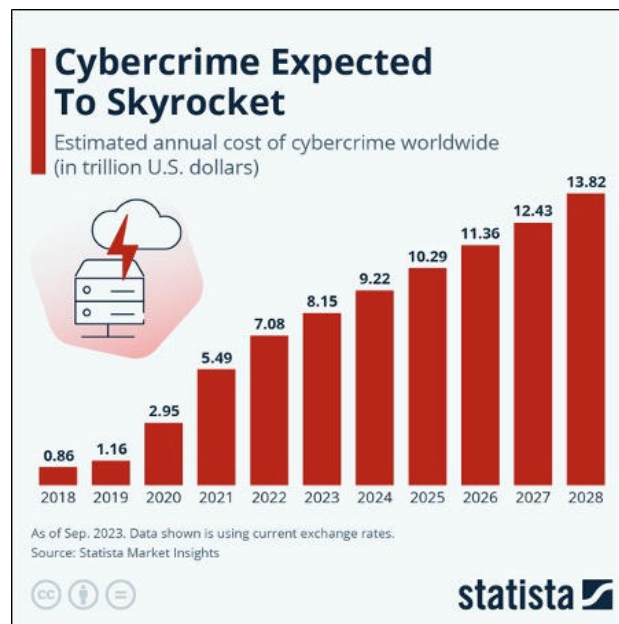


Abbildung 1: Prognose: Kostenanstieg durch Cyberkriminalität (Statista, 2024)

Abbildung 1 visualisiert die prognostizierte Entwicklung der weltweit durch Cyberkriminalität verursachten Kosten. Während diese im Jahr 2018 noch bei rund 0,86 Billionen US-Dollar lagen, sollen sie laut aktuellen Schätzungen bis 2028 auf 13,82 Billionen US-Dollar ansteigen (Statista, 2024).

Die zugrunde liegenden Zahlen berücksichtigen sowohl direkte als auch indirekte Schäden, darunter Datendiebstahl, Erpressung durch Ransomware, Systemausfälle, Betriebsunterbrechungen und regulatorische Sanktionen (Statista, 2024). In ihrer Gesamtheit verdeutlichen die Zahlen das erhebliche ökonomische Ausmaß, das diese Form digitaler Bedrohung mittlerweile angenommen hat. Dadurch gewinnt die Forderung nach wirksamen Schutz- und Reaktionsstrategien zunehmend an Bedeutung.

Eine zentrale Rolle in der Bewältigung solcher Vorfälle spielt die digitale Forensik. Sie ermöglicht nicht nur die nachträgliche Untersuchung von Angriffen, sondern schafft auch eine Grundlage für die rechtssichere Aufbereitung digitaler Spuren. Während die Wiederherstellung verlorener Daten essenziell für forensische Analysen ist, liefert erst die ergänzende Metadatenanalyse die Grundlage einer fundierten Beweissicherung. Durch das Zusammenspiel beider Verfahren kann ein möglichst vollständiges Bild eines digitalen Vorfalls rekonstruiert werden. (Oh, Lee und Hwang, 2022; Forensic Discovery, 2023)

Die Datenwiederherstellung stellt sicher, dass gelöschte, beschädigte oder manipulierte Dateien aus Speichersystemen rekonstruiert werden können, die andernfalls für Ermittlungen verloren wären (Balba, 2024). Dabei handelt es sich nicht ausschließlich um die Reaktion auf böswillige Eingriffe. Häufige Ursachen für Datenverluste sind vielmehr technische Defekte, Anwenderfehler, physische Schäden wie Witterungseinwirkungen, fehlerhafte Softwareaktualisierungen und Stromausfälle (Proact Deutschland GmbH, 2024). Die Wiederherstellung betroffener Dateien ist somit nicht nur für forensische Analysen, sondern auch für die alltägliche IT-Sicherheit von zentraler Bedeutung.

Auch eine vollständige Wiederherstellung reicht nicht aus, um deren Aussagekraft gerichtsfest zu bewerten. Die ergänzende Metadatenanalyse ist notwendig, um Informationen über Dateieigenschaften zu gewinnen. So kann nachvollzogen werden, wann ein Dokument erstellt, bearbeitet oder gelöscht wurde und welchem Benutzerkonto die jeweiligen Aktionen zugeordnet werden können. In der digitalen Forensik liefert diese Kontextualisierung entscheidende Hinweise auf den Ablauf eines sicherheitsrelevanten Vorfalls. (Forensic Discovery, 2023)

Um dieser Aufgabe gerecht zu werden, kommen spezialisierte Werkzeuge zum Einsatz, die eine strukturierte und nachvollziehbare Analyse ermöglichen. Wie Stefan Meier in seiner Dissertation betont, ist die digitale Forensik in vielen Organisationen jedoch noch immer stark technikzentriert ausgerichtet, während prozessorientierte und organisatorische Aspekte häufig unzureichend beachtet werden. In vielen Organisationen fehlt es weiterhin an geeigneten Tools, um digitale Spuren systematisch zu sichern und zugleich gerichtsfest auszuwerten. Die Verbindung technischer Komplexität, rechtlicher Anforderungen und stetig wachsender Datenmengen erhöht die Fehleranfälligkeit forensischer Untersuchungen erheblich (Meier, 2017).

1.2. Zielsetzung

Ziel dieser Arbeit ist es, ausgewählte Werkzeuge zur Datenwiederherstellung und Metadatenanalyse im Kontext der IT-Forensik vorzustellen und hinsichtlich ihrer Praxistauglichkeit zu untersuchen. Die Untersuchung erfolgt auf Grundlage von Fallbeispielen, die typische forensische Szenarien simulieren.

Diese Analysen werden in einer speziell eingerichteten, forensischen Umgebung durchgeführt. Sie basiert auf der Linux-Distribution **Computer Aided INvestigative Environment** (CAINE), die als standardisierte Plattform eine Vielzahl etablierter Open-Source-Tools für die digitale Forensik bereitstellt (Talha *u. a.*, 2024; Hacking Akademie, 2024). Durch ihre vorkonfigurierte Struktur ermöglicht CAINE eine reproduzierbare, forensisch abgesicherte Arbeitsweise. Im Rahmen dieser Umgebung kommen spezifische Werkzeuge zur Anwendung, die auf die beiden zentralen Untersuchungsbereiche dieser Arbeit abgestimmt sind. Der Aufbau und die Funktionsweise der forensischen Umgebung sowie der dort integrierten Werkzeuge werden in Kapitel 2 vorgestellt.

Der Schwerpunkt der Untersuchung liegt auf einer systematischen Bewertung der eingesetzten Werkzeuge anhand praxisrelevanter Kriterien. In diesem Zusammenhang werden insbesondere die Effektivität, die Benutzerfreundlichkeit sowie die Konformität mit forensisch anerkannten Normen und Standards analysiert. Ein besonderer Fokus liegt auf den typischen Herausforderungen der forensischen Praxis.

Auf Grundlage dieser Bewertung sollen praxisnahe Handlungsempfehlungen für den methodisch fundierten Einsatz dieser forensischen Werkzeuge in der digitalen Spu-

rensicherung abgeleitet werden. Adressiert werden sowohl Organisationen als auch technisch versierte Einzelpersonen, die digitale Vorfälle systematisch nachvollziehen möchten.

1.3. Aufbau der Arbeit

Diese Arbeit orientiert sich an etablierten Standards der digitalen Forensik, insbesondere an den Empfehlungen des NIST sowie den Normen der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC).

In Kapitel 2 werden zentrale Begriffe definiert, relevante Teilbereiche systematisch abgegrenzt sowie forensische Verfahren, Standards und rechtliche Rahmenbedingungen dargestellt. Anschließend folgt in Abschnitt 2.3 eine Einführung in die eingesetzte forensische Umgebung und deren Werkzeuge.

Die praktische Umsetzung erfolgt in Kapitel 3 anhand realitätsnaher Fallbeispiele. Dabei wird zunächst der Prozess der Datenwiederherstellung behandelt (Abschnitt 3.2), da Metadaten häufig nur im Zusammenhang mit rekonstruierten Dateien vollständig verfügbar sind (Forensic Discovery, 2023). Im Anschluss folgt die Analyse der Metadaten (Abschnitt 3.3), um die wiederhergestellten Inhalte hinsichtlich ihrer Entstehung, Veränderung und Nutzung zu kontextualisieren.

Beide Teilprozesse werden nach einheitlichen Kriterien bewertet. Bewertet werden sowohl die Effektivität und Benutzerfreundlichkeit der Werkzeuge als auch deren Übereinstimmung mit geltenden forensischen Standards.

Abschließend werden die Ergebnisse in Kapitel 4 zusammengeführt und praxisorientierte Empfehlungen für den Einsatz forensischer Tools formuliert. Die Arbeit richtet sich an Organisationen ebenso wie an Privatpersonen.

2. Grundlagen

Zur Vermittlung eines fundierten Verständnisses der forensischen Analyse von Dateien stellt dieses Kapitel die theoretischen und methodischen Grundlagen dar, die das Verständnis der eingesetzten Verfahren und Werkzeuge ermöglichen.

In Abschnitt 2.1 werden zunächst der Begriff „*Forensik*“ definiert, dessen historische Entwicklung skizziert und die grundlegenden Anwendungsbereiche erläutert.

Abschnitt 2.2 widmet sich der digitalen Forensik im engeren Sinne. Es beschreibt zentrale Einsatzbereiche und differenziert diese in spezifische Themenfelder wie forensische Verfahren und Standards, Datenwiederherstellung sowie Metadatenanalyse.

In Abschnitt 2.3 wird die Ermittlungsumgebung CAINE vorgestellt. Diese forensische Linux-Distribution beinhaltet eine Vielzahl integrierter Werkzeuge, die im Rahmen der Analyse zum Einsatz kommen. Betrachtet werden sowohl die in CAINE enthaltenen Tools als auch alternative Anwendungen, die je nach forensischem Szenario ergänzend genutzt werden können.

2.1. Forensik

Der Begriff „*Forensik*“ geht auf das lateinische „*forum*“ zurück, den zentralen Platz im antiken Rom, an dem unter anderem öffentliche Gerichtsverhandlungen stattfanden. Ursprünglich bezeichnete er somit das Vorgehen, vor Gericht Aussagen zu tätigen oder Beweise vorzulegen (Stiller, 2019).

Bereits in der Antike wurden forensische Verfahren wie Obduktionen genutzt, etwa im römischen Rechtssystem zur Klärung von Todesursachen (Serlo Education e.V., 2023). Im Mittelalter dominierten dagegen Geständnisse und Folter als Mittel der Strafverfolgung.

Erst im 19. Jahrhundert begann mit der Einführung wissenschaftlicher Methoden die moderne Forensik. Mit der Etablierung von Standards und Laborverfahren wurde sie zu einer anerkannten wissenschaftlichen Disziplin (KSV Polizeipraxis, 2022).

Heutzutage wird die Forensik als interdisziplinärer Bereich verstanden, der natur-, sozial-, rechts- und ingenieurwissenschaftliche Methoden einsetzt, um strafrechtlich relevante Sachverhalte aufzuklären (Katz E, 2015). Ziel der forensischen Arbeit ist es, objektive Beweise zu sichern, Hypothesen über Tatabläufe zu überprüfen und zur Wahrheitsfindung im Rahmen juristischer Verfahren beizutragen.


Dabei erfolgt die Untersuchung stets unter der Annahme der Nachvollziehbarkeit, Reproduzierbarkeit und gerichtlichen Verwertbarkeit der Ergebnisse (Katz E, 2015).

Die Informationsplattform Studieren.de bietet einen orientierenden Überblick über ausgewählte forensische Fachbereiche, geordnet nach ihrer wissenschaftlichen Herkunft. Die Zuordnung orientiert sich dabei an einer thematischen Gliederung, wie sie in deren Übersicht zu forensischen Studieninhalten dargestellt ist (studieren.de, 2025).

Zu forensischen Disziplinen aus dem Bereich Medizin und Biowissenschaften zählen unter anderem die Rechtsmedizin, die Pathologie, die Thanatologie sowie anthropologische Verfahren wie die Gesichtsrekonstruktion oder die Altersdiagnostik. Im Bereich Technik und Ingenieurwesen finden sich klassische Spurenanalysen wie die Untersuchung von Schuh- und Reifenspuren, die Analyse technischer Geräte sowie die forensische Waffenuntersuchung inklusive Schusswaffen- und Pyrotechnikbewertung. (studieren.de, 2025)

Die Digitale Forensik und Kommunikationsanalyse umfasst moderne Disziplinen wie die Computer-Forensik, die Analyse von digitalen Spuren und Metadaten, die Sicherung von IT-Geräten sowie die Untersuchung von Cybercrime-Vorfällen wie Phishing und Hacking. Schließlich gehören zur Gruppe der Sozial- und Geisteswissenschaften Disziplinen wie die Kriminalpsychologie, Täterprofilanalysen, Serienanalysen sowie die Handschrift- und Urkundenprüfung. (studieren.de, 2025)

Während einige dieser Disziplinen wie die Rechtsmedizin bereits seit über einem Jahrhundert Bestandteil kriminalistischer Arbeit sind, wurden andere, wie die digitale Forensik, erst in den letzten Jahrzehnten entwickelt. Die Akzeptanz forensischer Methoden nahm im Zuge der fortschreitenden Weiterentwicklung wissenschaftlicher Verfahren und deren zunehmender gerichtlicher Verwertbarkeit zu (Bundeskriminalamt, 2024a).



Ein Beispiel für die Bedeutung forensischer Techniken in der Strafverfolgung ist die Einführung der **Desoxyribonucleic Acid (DNA)**-Analyse durch das Bundeskriminalamt im Jahr 1998. Bis 2018 konnten durch diese über 266.000 Treffer erzielt werden, wovon ein großer Teil zur Aufklärung von Eigentums-, Gewalt- und Sexualdelikten beitrug (Statista, 2018; Bundeskriminalamt, 2024b).

Im bekannten Fall des **Nationalsozialistischen Untergrunds (NSU)** spielten forensische Methoden eine zentrale Rolle bei der Aufklärung der Taten. Durch die systematische Analyse von DNA-Spuren, Waffen und anderen Tatortbefunden konnten Verbindungen zwischen den einzelnen Verbrechen hergestellt und die Hauptverantwortlichen identifiziert werden. So führte unter anderem der Fund der Dienstwaffen der ermordeten Polizistin Michèle Kiesewetter im Wohnmobil der NSU-Mitglieder im November 2011 zu einem entscheidenden Durchbruch in den Ermittlungen (Bayerischer Landtag, 2023). Komplexe Fälle wie der NSU-Prozess verdeutlichen die Bedeutung standardisierter Verfahren in der forensischen Spurensicherung. Ohne strukturierte Abläufe und nachvollziehbare Dokumentation wäre die gerichtliche Verwertbarkeit vieler Beweismittel nicht gewährleistet gewesen.

Zur Sicherstellung der Qualität forensischer Arbeit tragen internationale Institutionen wie das NIST und das **European Network of Forensic Science Institutes (ENFSI)** maßgeblich bei. In Deutschland übernimmt das **Bundeskriminalamt (BKA)** eine vergleichbare Rolle. Diese Einrichtungen orientieren sich an internationalen Normen wie der ISO/IEC 21043, welche die grundlegenden Anforderungen an die Sammlung, Sicherung, Dokumentation und Auswertung von Spuren definieren.

Die ISO/IEC 21043-Reihe gliedert den forensischen Prozess in klar definierte Abschnitte und formuliert für jeden dieser Schritte spezifische Anforderungen. Abbildung 2 zeigt die Beziehungen zwischen den einzelnen Komponenten des forensischen Prozesses und den zugehörigen Abschnitten innerhalb der ISO-Normreihe (ISO, 2018). Sie verdeutlicht, wie strukturierte Abläufe, von der Planung über die Sicherung bis zur Analyse und Berichterstattung, ineinandergreifen und durch normative Vorgaben abgesichert werden.

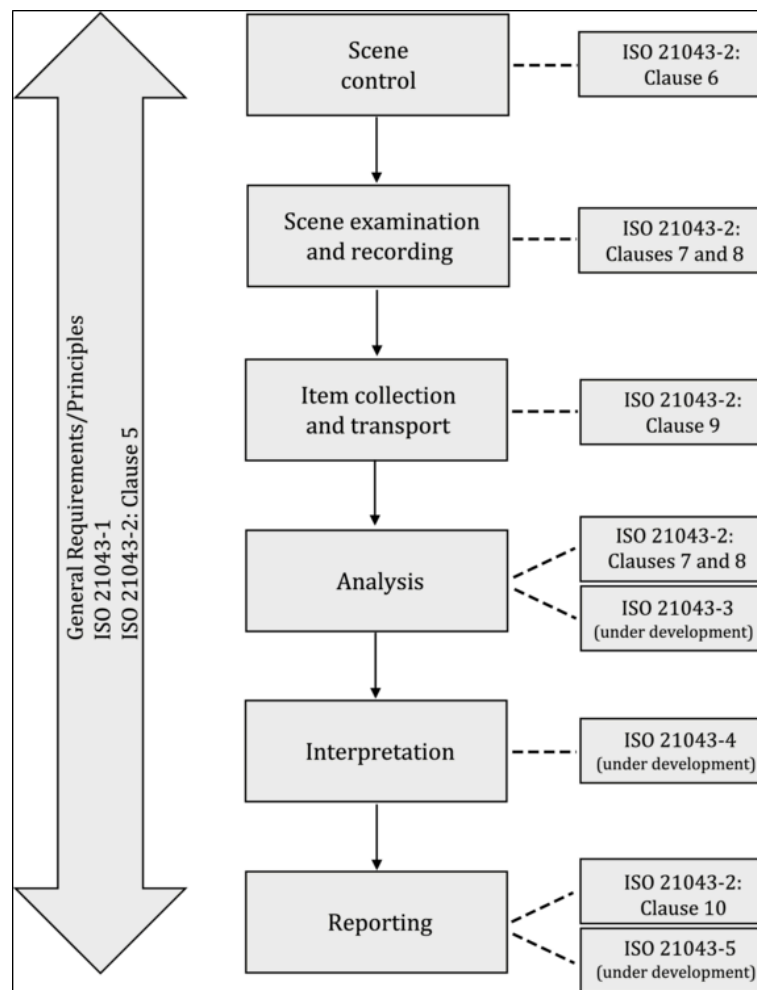


Abbildung 2: Forensikprozess gemäß ISO (ISO, 2018)

Solche Regelwerke schaffen eine einheitliche und überprüfbare Vorgehensweise und sichern die rechtliche Verwertbarkeit forensischer Befunde. In der Praxis helfen sie, Beweismittel reproduzierbar zu sichern und deren Integrität zu gewährleisten. Die Anwendung forensischer Methoden unterliegt zudem rechtlichen und ethischen Vorgaben. So sind genetische Untersuchungen in Deutschland durch §§81e–h StPO geregelt und bedürfen einer richterlichen Anordnung. Dabei gelten die Grundsätze der Verhältnismäßigkeit, des Datenschutzes und der Unschuldsvermutung (Bundeskriminalamt, 2024b).

Während klassische Forensik auf physische Spuren fokussiert, rückt die digitale Forensik zunehmend in den Vordergrund, insbesondere bei der Aufklärung von IT-Sicherheitsvorfällen.

2.2. Digitale Forensik

Der Baustein „DER.2.2 Vorsorge für die IT-Forensik“ aus dem IT-Grundschutz-Kompendium des **Bundesamt für Sicherheit in der Informationstechnik (BSI)** beschreibt, wie Organisationen sich gezielt auf IT-forensische Untersuchungen vorbereiten können (BSI, 2023). Als zentrale Bundesbehörde für Informationssicherheit definiert und standardisiert das BSI sicherheitsrelevante IT-Verfahren in Deutschland (BSI, 2023). In diesem Kontext definiert es digitale Forensik wie folgt:

„IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Datennetzen zur Aufklärung von Sicherheitsvorfällen in IT-Systemen.“ (BSI, 2023)

Diese Definition betont den strukturierten und nachvollziehbaren Umgang mit digitalen Spuren. Im Unterschied zur klassischen Forensik, die physische Beweismittel untersucht, befasst sich die digitale Forensik mit Artefakten wie Logdateien, Dateisystemstrukturen und Netzwerkdaten (BSI, 2023).

Aufgaben und Ziele

Zentrales Anliegen der digitalen Forensik ist die gerichts feste Sicherung digitaler Beweismittel (BSI, 2023). Darüber hinaus unterstützt sie die technische Bewertung von Sicherheitsvorfällen, etwa durch die Analyse von Schadensursachen oder die Identifikation von Angriffsvektoren. Auf dieser Grundlage lassen sich geeignete Maßnahmen zur Wiederherstellung und Prävention ableiten. Ebenso bedeutend ist die vollständige Dokumentation forensischer Prozesse, insbesondere im Hinblick auf regulatorische Anforderungen und die Nachvollziehbarkeit organisatorischer Abläufe (ISO/IEC, 2012). Zu den Kernaufgaben zählen die Erkennung relevanter Datenquellen, deren manipulationssichere Sicherung, die technische Analyse sowie die rechtssichere Dokumentation aller Arbeitsschritte. Dabei müssen Integrität, Authentizität und Beweiskraft der erhobenen Daten jederzeit gewährleistet sein (NIST, 2006).

Rechtliche und normative Rahmenbedingungen

IT-forensische Untersuchungen unterliegen klaren rechtlichen Vorgaben. Damit ihre Ergebnisse vor Gericht Bestand haben, müssen sie standardkonform erhoben, gesichert, dokumentiert und analysiert werden. International sind die Normen ISO/IEC 27037 und NIST SP 800-86 maßgeblich. Sie definieren Anforderungen an die forensische Vorgehensweise, insbesondere im Hinblick auf die Wahrung der Integrität und Authentizität digitaler Beweismittel (NIST, 2006; ISO/IEC, 2012).

Ein zentrales Element ist die sogenannte Chain of Custody. Sie beschreibt die lückenlose und nachvollziehbare Dokumentation aller Stationen, die ein digitales Beweisobjekt im Verlauf einer Untersuchung durchläuft (ISO/IEC, 2012). Abbildung 3 veranschaulicht die typischen Schritte dieses Prozesses.

Der Ablauf beginnt mit der Evidence Identification, also der Feststellung und Abgrenzung relevanter Spuren. Es folgt die Evidence Collection, bei der Daten forensisch gesichert und überführt werden. In der Phase Evidence Transportation wird das Material unter Wahrung der Integrität weitergegeben. Die Evidence Storage umfasst die gesicherte, protokollierte Aufbewahrung.

Die Documentation & Reporting verknüpft alle Schritte durch eine lückenlose Protokollierung. Danach erfolgt die Evidence Analysis, also die technische Auswertung. Abschließend kann in der Phase Evidence Disposal eine dokumentierte Entsorgung erfolgen, sofern rechtlich zulässig.



Abbildung 3: Visualisierung der Chain of Custody gemäß ISO 20 (ISO, 2018)

Eine strukturierte Vorgehensweise ist Voraussetzung für die rechtliche Verwertbarkeit und technische Überprüfbarkeit digitaler Beweismittel. In Deutschland betont das BSI im Baustein „DER.2.2 Vorsorge für die IT-Forensik“ des IT-Grundschutz-Kompendiums die Notwendigkeit frühzeitiger organisatorischer und technischer Maßnahmen für ein gerichtsfestes und nachvollziehbares Vorgehen (BSI, 2023).

Anwendungsbereiche

Die digitale Forensik entwickelte sich ursprünglich als Instrument der Strafverfolgung zur Analyse digitaler Spuren bei Cyberkriminalität, Betrugsdelikten und klassischen Ermittlungen. Behörden nutzen dabei IT-forensische Verfahren zur gerichtsfesten Auswertung von Mail-Kommunikation, Netzwerkverkehr oder manipulierten Dateien (Casey, 2011). Inzwischen findet sie auch in Unternehmen Anwendung, etwa zur Aufklärung interner Sicherheitsvorfälle, Datenschutzverstöße oder Regelverletzungen (Meier, 2017). Darüber hinaus trägt sie zur Einhaltung gesetzlicher Vorgaben und zur Analyse datenschutzrelevanter Abläufe bei. Die IT-forensische Praxis lässt sich in mehrere spezialisierte Bereiche unterteilen:

- **Netzwerkforensik:** Untersuchung von Kommunikations- und Verkehrsdaten zur Erkennung verdächtiger Aktivitäten (Carrier, 2005)
- **Speicherforensik:** Analyse physischer Datenträger auf gelöschte oder versteckte Inhalte (Carrier, 2005)
- **Random Access Memory (RAM)-Analyse:** Auswertung flüchtiger Daten wie aktiver Prozesse oder kryptografischer Schlüssel (Carrier, 2005)
- **Dateisystemanalyse:** Rekonstruktion von Dateiaktionen und Zeitstempeln auf struktureller Ebene (Carrier, 2005)
- **Metadatenanalyse:** Interpretation eingebetteter Informationen zu Erstellung, Bearbeitung oder Herkunft (Carrier, 2005)

Im Fokus dieser Arbeit stehen zwei dieser Disziplinen: die Wiederherstellung gelöschter Daten sowie die Analyse von Metadaten. Beide Bereiche werden in den folgenden Kapiteln systematisch behandelt.

2.2.1. Datenwiederherstellung

In der digitalen Forensik wird Datenwiederherstellung als ein strukturierter Prozess verstanden, der darauf abzielt, gelöschte, beschädigte oder anderweitig unzugängliche Daten aus digitalen Speichermedien zu rekonstruieren (FasterCapital, 2025). Ziel ist es, Informationsobjekte wieder lesbar und analysierbar zu machen, die infolge technischer Defekte, unbeabsichtigter Löschung oder gezielter Manipulation aus dem regulären Zugriff entfernt wurden. Insbesondere im Rahmen forensischer Ermittlungen kommt der Datenwiederherstellung eine bedeutende Rolle zu, da sie potenziell beweisrelevante Inhalte rekonstruieren kann, selbst wenn diese auf herkömmlichem Wege nicht mehr adressierbar sind (FasterCapital, 2025).

Struktur und Verwaltung digitaler Daten

Digitale Daten werden als Abfolge von Bits gespeichert. Dateisysteme verwalten diese mithilfe sogenannter Pointer, auch Verweise genannt, die Beginn und Ende einer Datei auf dem Speichermedium markieren. Solange diese Pointer existieren, lässt sich die Datei eindeutig identifizieren und nutzen (Oh, Lee und Hwang, 2022). Gehen diese Pointer jedoch verloren, beispielsweise infolge eines Stromausfalls oder durch das plötzliche Entfernen des Speichermediums, kann es zu einer Korruption der Datenstruktur kommen. Diese bezeichnet die logische Beschädigung von Metadaten oder Dateiinhalten, wodurch Dateien nur noch unvollständig vorliegen oder nicht mehr lesbar sind (FasterCapital, 2025).

Die Wiederherstellung ist in solchen Fällen zwar noch möglich, jedoch deutlich aufwendiger und mit geringerer Erfolgsaussicht verbunden. Dies gilt insbesondere im Vergleich zur einfachen Dateilöschung, bei der die Verweise entfernt werden, die eigentlichen Daten jedoch meist noch vollständig auf dem Speichermedium vorhanden sind (Oh, Lee und Hwang, 2022).

Löschung digitaler Daten und Wiederherstellbarkeit

Beim digitalen Löschen von Dateien entfernt das Betriebssystem die Daten in der Regel nicht unmittelbar vom Datenträger. Stattdessen werden lediglich die Verweise im Dateisystem, etwa Einträge in der Dateizuordnungstabelle, als frei markiert (FasterCapital, 2025). Die physisch gespeicherten Inhalte bleiben bestehen, bis sie durch neue Daten überschrieben werden. Genau diese scheinbar gelöschten Bereiche bilden die Grundlage vieler forensischer Wiederherstellungsverfahren (FasterCapital, 2025). Solange die betreffenden Speicherblöcke nicht neu beschrieben wurden, ist eine Wiederherstellung technisch möglich.

klarer als vorher

Methodisches Vorgehen bei der Datenwiederherstellung

Der Artikel „Data Recovery Process: Best Practices and Tools“ hebt hervor, dass die Wiederherstellung von Daten einem strukturierten Ablauf folgen sollte von (Spiceworks Inc., 2024). Dieser orientiert sich an anerkannten forensischen Vorgehensmodellen, wie sie beispielsweise in der Norm ISO/IEC 27037 beschrieben sind (ISO/IEC, 2012). Abbildung 4 veranschaulicht den typischen Ablauf einer Datenwiederherstellung:

- 01) Im ersten Schritt wird das betroffene Gerät außer Betrieb genommen, um unbeabsichtigte Veränderungen an potenziell relevanten Daten zu vermeiden.
- 02) Daraufhin erfolgt eine erste Analyse der auftretenden Symptome, wie etwa ungewöhnliche Betriebsgeräusche, fehlerhafte Dateisystemmeldungen oder der Verlust des Zugriffs auf bestimmte Datenbereiche.
- 03) Parallel dazu wird der Vorfall systematisch dokumentiert. Diese Dokumentation dient der späteren Nachvollziehbarkeit des Geschehens sowie der Identifikation möglicher Ursachen.
- 04) Anschließend wird ein geeignetes Verfahren zur Datenwiederherstellung ausgewählt. Dabei spielen der Schadenstyp, das betroffene Speichermedium und die zugrunde liegende Dateistruktur eine zentrale Rolle.
- 05) Abschließend ist sicherzustellen, dass ein geeigneter Speicherort in ausreichender Größe zur Verfügung steht, um die wiederhergestellten Daten verlustfrei abzulegen.

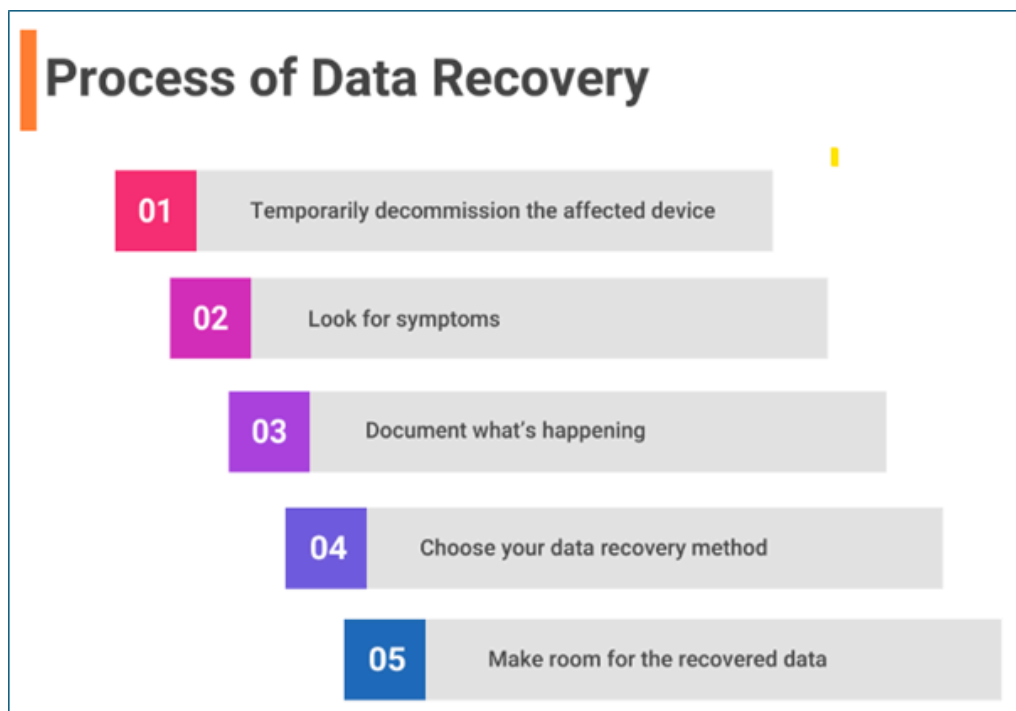


Abbildung 4: Datenwiederherstellungsprozess nach (Spiceworks Inc., 2024)

Arten der Datenwiederherstellung

Je nach Zustand des Datenträgers und der vorliegenden Dateisystemstruktur kommen unterschiedliche Wiederherstellungsverfahren zum Einsatz. Ein zentrales Unterscheidungsmerkmal ist die Trennung zwischen logischer und physischer Wiederherstellung (Spiceworks Inc., 2024):

- **Logische Wiederherstellung:** Erfolgt auf der Ebene des Dateisystems und nutzt dessen Verwaltungsstrukturen zur Rekonstruktion verlorener Dateien. Abhängig vom verwendeten Betriebssystem kommen unterschiedliche Strukturen zum Einsatz. Unter Windows sind dies die **File Allocation Table (FAT)** und die **Master File Table (MFT)**. Die FAT dient in älteren Systemen der Zuordnung von Speicherbereichen, während die MFT im **NTFS-Dateisystem** umfangreiche Metadaten wie Namen und Zeitstempel speichert (Carrier, 2005). Linux-basierte Systeme verwenden **index node-Tabellen (inode)** als zentrales Verzeichnis aller gespeicherten Objekte. Jeder inode identifiziert eine Datei eindeutig und enthält relevante Metadaten (Carrier, 2005).

Schon
enthalten?

gibt es
jetzt
besser

Unter macOS übernimmt das **Apple File System (APFS)** diese Funktion mithilfe von Metadatencontainern, die Informationen wie Speicherort, Zustand und Versionshistorie verwalten. Solange diese Strukturen intakt sind, ist eine zuverlässige Wiederherstellung meist möglich (Carrier, 2005)

- **Physische Wiederherstellung:** Setzt auf Block- bzw. Sektorebene an und wird eingesetzt, wenn die Dateisystemstruktur beschädigt oder vollständig verloren ist (Spiceworks Inc., 2024). In solchen Fällen kommen signaturbasierte Verfahren wie File Carving zum Einsatz, bei denen anhand bekannter Bytefolgen Dateifragmente erkannt und rekonstruiert werden (Spenneberg, 2008). Diese Methode erfordert keine intakten Metadaten und eignet sich besonders bei fragmentierten oder teilüberschriebenen Datenträgern. Wird ein Speichermedium aufgrund defekter Firmware nicht mehr erkannt, kann der physische Datenträger in eine funktionierende Hardware mit kompatibler Firmware überführt werden, um eine bitweise Kopie zu erstellen (Spenneberg, 2008).
- **Hybridmethoden:** Ein dritter Weg besteht in Hybridmethoden, bei denen sowohl Metadatenfragmente als auch signaturbasierte Verfahren kombiniert werden. Sie bieten sich insbesondere bei beschädigten Partitionen oder teilüberschriebenen Datenträgern an (Spiceworks Inc., 2024).

2.2.2. Metadaten-Analyse

Metadaten beschreiben die Rahmenbedingungen digitaler Objekte, etwa wann, durch wen und wie häufig eine Datei erstellt, verändert oder geöffnet wurde (Forensic Discovery, 2023). Sie entstehen meist automatisch im Hintergrund durch das Betriebssystem oder durch Anwendungsprogramme (Oh, Lee und Hwang, 2022; Forensic Discovery, 2023). Diese strukturierten Zusatzinformationen sind für die forensische Analyse von zentraler Bedeutung, da sie Rückschlüsse auf zeitliche Abläufe, Nutzerinteraktionen und potenzielle Manipulationen ermöglichen. Ein Änderungszeitpunkt kann etwa belegen, dass eine Datei nach einem bestimmten Ereignis noch verändert wurde, was im Widerspruch zum angegebenen Kontext stehen kann. Zugriffszeitstempel erlauben darüber hinaus Aussagen darüber, wann und möglicherweise durch wen eine Datei geöffnet wurde (Oh, Lee und Hwang, 2022).

Da sie oft unbemerkt gespeichert werden, gelten Metadaten als besonders verlässliche Informationsquelle. Sie lassen sich in vielen Fällen auch dann noch rekonstruieren, wenn der sichtbare Inhalt gelöscht oder verändert wurde (Spiceworks Inc., 2024). In der forensischen Praxis besitzen sie daher einen hohen Beweiswert, insbesondere zur zeitlichen Einordnung, zur Nutzerzuordnung und zur Überprüfung der Authentizität digitaler Spuren (Forensic Discovery, 2023).

Klassifikation forensisch relevanter Metadaten

Metadaten lassen sich anhand ihrer Herkunft und ihres Zwecks in mehrere Kategorien einteilen. Diese Unterscheidung ist wesentlich, um ihr forensisches Potenzial gezielt auszuschöpfen und ihre Aussagekraft korrekt einzuordnen:

- **Systembezogene Metadaten:** Entstehen unmittelbar durch das Betriebssystem oder das zugrunde liegende Dateisystem. Sie umfassen grundlegende Informationen wie Erstellungs-, Änderungs- und Zugriffszeitpunkte von Dateien oder Ordnern (Carrier, 2005). Im NTFS-Dateisystem von Windows werden diese Daten zentral in der MFT gespeichert. Wie in Unterabschnitt 2.2.1 erläutert, handelt es sich bei der MFT um eine zentrale Verwaltungsstruktur, in der für jede Datei ein eigener Eintrag mit umfassenden Metadaten hinterlegt wird, darunter der Dateiname, der

physische Speicherort, Zeitstempel sowie diverse Dateiattribute (Carrier, 2005). Auch die Windows-Registry zählt zu den Quellen von Systemmetadaten, da sie zahlreiche Interaktionen mit dem System dokumentiert. Dazu gehören unter anderem Informationen über angeschlossene Peripheriegeräte, installierte Software sowie Verweise auf zuletzt geöffnete Dateien (Carrier, 2005).

- **Anwendungsbezogene Metadaten:** Werden von Programmen selbstständig erzeugt und dokumentieren softwareinterne Abläufe sowie technische Bearbeitungsprozesse. Sie entstehen unabhängig vom direkten Benutzerverhalten. In Office-Dokumenten zählen dazu etwa Informationen zum Autor, zu Änderungszeitpunkten oder Versionsverläufen. Auch E-Mail-Header gehören in diese Kategorie, da sie automatisch Angaben zu Absender, Empfänger, Versandzeit und den durchlaufenen Mailservern enthalten (Carrier, 2005).
- **Nutzerbezogene Metadaten:** Entstehen durch direkte Aktionen des Benutzers bei der Nutzung des Systems. Dazu gehören etwa Hinweise auf zuletzt geöffnete Dateien, besuchte Webseiten oder automatisch gespeicherte Verzeichnispfade und Programmverläufe unter Windows. Solche Informationen zeigen, wann und wie Dateien oder Anwendungen verwendet wurden, und ermöglichen eine genaue Nachverfolgung des Nutzerverhaltens (Carrier, 2005).

Methodik und Interpretation forensischer Metadatenanalyse

Die Analyse von Metadaten spielt eine zentrale Rolle in der digitalen Forensik. Sie unterstützt die nachvollziehbare Rekonstruktion von Abläufen, das Erkennen ungewöhnlicher Muster sowie die Aufdeckung potenzieller Manipulationen (Forensic Discovery, 2023). Dabei ist es entscheidend, Metadaten stets im technischen und zeitlichen Entstehungskontext zu bewerten, insbesondere da Zeitstempel durch Betriebssysteme, Dateisysteme oder Kopiervorgänge automatisch beeinflusst werden können.

Die Norm ISO/IEC 27042 bietet grundlegende Empfehlungen für die Analyse digitaler Spuren. Zwar benennt sie keine festen Verfahrensschritte, doch lassen sich daraus vier zentrale Phasen ableiten, die sich in der Praxis bewährt haben (ISO/IEC, 2015):

- **Sicherung:** Die forensisch korrekte Erstellung eines bitweisen Abbilds dient der Integritätssicherung und bildet die Grundlage der Analyse.

- **Extraktion:** Relevante Metadaten werden gezielt aus Dateisystemen, Anwendungen oder Systembereichen wie der Registry ausgelesen.
- **Validierung:** Die Daten werden auf Konsistenz, Integrität und technische Plausibilität überprüft.
- **Interpretation:** Abschließend erfolgt eine kontextbezogene Einordnung der Metadaten im Hinblick auf ihren Aussagewert.

Ein praktisches Beispiel stellt die Untersuchung der Windows-Registry (in Unterabschnitt 2.2.1 vorgestellt) dar, die vielfältige Hinweise auf Nutzeraktivitäten liefert. Diese lassen sich gezielt extrahieren, validieren und im Kontext der jeweiligen Fragestellung interpretieren. Die konsequente Anwendung dieses strukturierten Vorgehens unterstützt eine fundierte, nachvollziehbare und gerichtsfeste Bewertung digitaler Spuren (Carrier, 2005).

2.3. Die Ermittlungsumgebung CAINE

CAINE ist eine auf digitale Forensik spezialisierte Linux-Distribution, die 2008 unter der Leitung des IT-Forensikers Nanni Bassetti entwickelt wurde, um eine praxisnahe Plattform für die Untersuchung digitaler Systeme zu schaffen (caine-live.net, 2024).

Sie unterstützt Strafverfolgungsbehörden, IT-Sicherheitsdienste sowie Privatanutzer und integriert alle Phasen der digitalen Beweissicherung und Analyse (Talha u. a., 2024).

Als technische Basis dient Ubuntu, das aufgrund seiner Stabilität, Benutzerfreundlichkeit und breiten Hardware-Kompatibilität ausgewählt wurde (caine-live.net, 2024). Diese Grundlage erleichtert die Installation, gewährleistet regelmäßige Sicherheitsupdates und ermöglicht die problemlose Integration zusätzlicher Werkzeuge.

Im Unterschied zu allgemeinen Linux-Distributionen bietet CAINE eine gezielte Auswahl forensischer Tools, ergänzt durch Schutzmechanismen wie schreibgeschütztes Mounten, um die Integrität digitaler Beweismittel zu gewährleisten (caine-live.net, 2024).

Die Architektur folgt internationalen Standards wie der ISO/IEC 27037, die Anforderungen an die Identifikation, Sicherung und Auswertung digitaler Spuren definieren (Talha u. a., 2024). Dadurch bietet CAINE eine verlässliche und rechtssichere Umgebung für forensische Analysen.

2.3.1. Integrierte Tools

CAINE beinhaltet Werkzeuge die unterschiedliche Aufgabenbereiche der digitalen Forensik abdecken. Diese Anwendungen unterstützen sämtliche Phasen einer Untersuchung, von der Datenerfassung über die Analyse bis hin zur Auswertung und Berichterstellung (Talha u. a., 2024). Die integrierten Werkzeuge basieren größtenteils auf Open-Source-Software, die gezielt kombiniert wurde, um eine vollständige und praxisorientierte Arbeitsumgebung für forensische Analysen bereitzustellen (Talha u. a., 2024). Im Rahmen dieser Arbeit werden ausgewählte Anwendungen näher vorgestellt, die für die Durchführung der praktischen Untersuchungen von besonderer Bedeutung sind.

Autopsy

Autopsy ist eine grafische Open-Source-Oberfläche für die forensische Analyse von Datenträgern und Dateisystemen. Es unterstützt die Wiederherstellung gelöschter Dateien, die Analyse von Metadaten und die Untersuchung von Benutzeraktivitäten wie Dateizugriffen und Browser-Historien (TSK, 2024). Über spezialisierte Module lassen sich Mail-Daten, Chat-Protokolle und Cloud-Speicher analysieren. Plugins erweitern die Funktionen unter anderem um Mobilfunk- und Netzwerkanalyse (TSK, 2024). Dank breiter Dateisystemunterstützung wie NTFS und FAT sowie der intuitiven Oberfläche eignet sich Autopsy für Einsteiger und professionelle Forensiker (TSK, 2024).

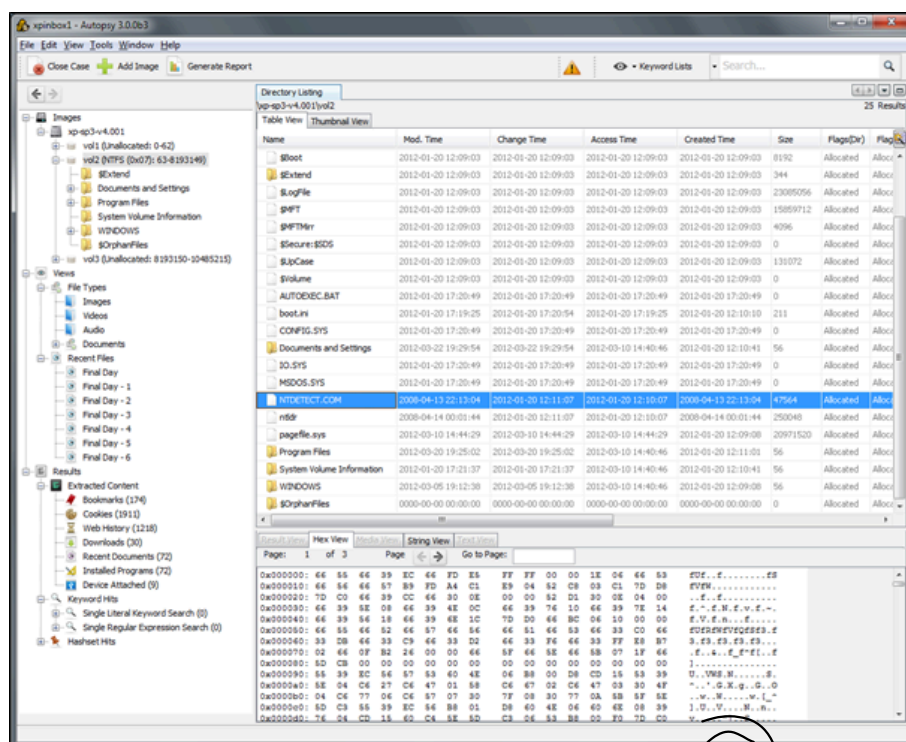
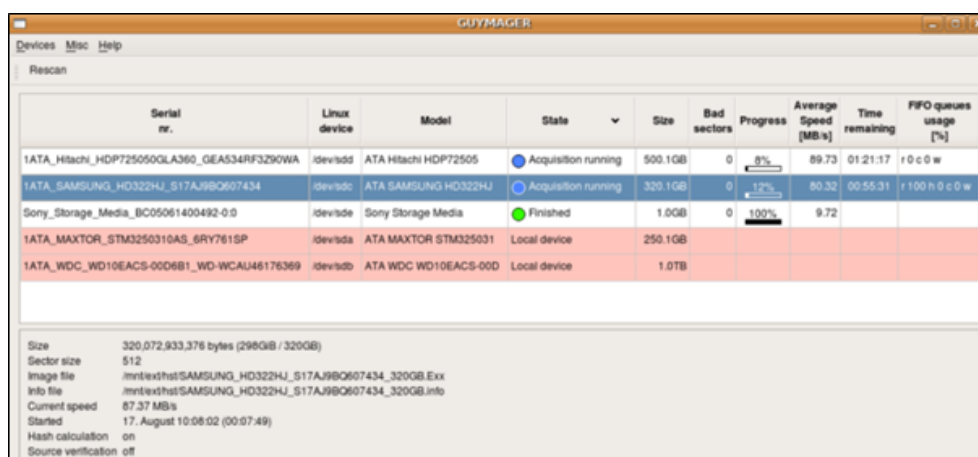


Abbildung 5: Analyse von Daten mit Autopsy (TSK, 2024)

Abbildung 5 zeigt die grafische Benutzeroberfläche von Autopsy. Links befinden sich Datenquellen und Analysebereiche wie Dateitypen oder zuletzt verwendete Dokumente. Zentral werden Dateien samt Metadaten wie Änderungs-, Zugriffs- und Erstellzeiten tabellarisch aufgelistet. Eine Hex- und String-Ansicht am unteren Rand erlaubt die Analyse von Dateiinhalten auf Byte-Ebene. Diese Struktur unterstützt eine systematische Auswertung forensischer Spuren (TSK, 2024).

Guymager

Guymager ist ein Open-Source-Tool zur Erstellung forensischer 1:1-Abbilder von Datenträgern. Es legt besonderen Wert auf eine verlustfreie und beweissichere Datenakquise und unterstützt dabei Formate wie **Expert Witness Format (EWF)** und Roh-Images (Voncken, 2025). Die grafische Benutzeroberfläche ermöglicht eine einfache Auswahl von Quell- und Zielmedium sowie eine detaillierte Konfiguration von Hash-Verfahren. Während der Sicherung zeigt Guymager fortlaufend Informationen über Fortschritt, Lesefehler und Prüfsummen an. Durch seine Effizienz und die gezielte Reduktion auf Kernfunktionen eignet sich das Werkzeug sowohl für den schnellen Einsatz im Feld als auch für umfangreiche forensische Untersuchungen (Voncken, 2025).



| Serial nr. | Linux device | Model | State | Size | Bad sectors | Progress | Average Speed [MB/s] | Time remaining | FIFO queues usage [%] |
|---|--------------|----------------------|---------------------|---------|-------------|----------|----------------------|----------------|-----------------------|
| 1ATA_Hitachi_HDP725050OLA360_GEA534RF3290WA | /dev/sdd | ATA Hitachi HDP72505 | Acquisition running | 500.1GB | 0 | 8% | 89.73 | 01:21:17 | r o c o w |
| 1ATA_SAMSUNG_HD322HJ_S17AJ9BQ607434 | /dev/sdc | ATA SAMSUNG HD322HJ | Acquisition running | 320.1GB | 0 | 12% | 80.32 | 00:55:31 | r 100 h o c o w |
| Sony_Storage_Media_BIC05061400492-0-0 | /dev/sde | Sony Storage Media | Finished | 1.0GB | 0 | 100% | 9.72 | | |
| 1ATA_MAXTOR_STM3250310AS_6RY761SP | /dev/sda | ATA MAXTOR STM325031 | Local device | 250.1GB | | | | | |
| 1ATA_WDC_WD10EACS-00D6B1_WD-WCAU46176369 | /dev/sdb | ATA WDC WD10EACS-00D | Local device | 1.0TB | | | | | |

Size 320,072,933,376 bytes (298GB / 320GB)
Sector size 512
Image file /mnt/ehd/hst/SAMSUNG_HD322HJ_S17AJ9BQ607434_320GB.Exx
Info file /mnt/ehd/hst/SAMSUNG_HD322HJ_S17AJ9BQ607434_320GB.info
Current speed 87.37 MB/s
Started 17. August 10:08:02 (00:07:49)
Hash calculation on
Source verification off

Abbildung 6: Analyse von Daten mit Autopsy (TSK, 2024)

Abbildung 6 veranschaulicht die grafische Oberfläche von Guymager während der Erstellung forensischer Abbilder. Mehrere angeschlossene Datenträger werden angezeigt, wobei der Status der Sicherungsvorgänge, die Fortschrittsanzeige, die durchschnittliche Lesegeschwindigkeit, vorhandene Lesefehler und weitere relevante Informationen angezeigt werden (Voncken, 2025). Die Benutzeroberfläche bietet eine klare Übersicht über alle laufenden Prozesse und erlaubt es, Details wie die Dateigröße des Images, das verwendete Hash-Verfahren sowie den Speicherort der Sicherung einzusehen. Aktive Sicherungsvorgänge sind farblich hervorgehoben, während abgeschlossene und lokale Geräte unterschiedlich markiert werden (Voncken, 2025).

The Sleuth Kit

The Sleuth Kit (TSK) ist eine Sammlung von Kommandozeilenwerkzeugen zur forensischen Analyse von Dateisystemen. Die Suite ermöglicht die Wiederherstellung gelöschter Dateien, die Untersuchung von Dateisystemstrukturen sowie die Extraktion von Metadaten. Besonders effektiv ist TSK bei der Analyse von NTFS-, FAT. Oft wird TSK in Kombination mit grafischen Frontends wie Autopsy verwendet, um die Ergebnisse visuell aufzubereiten. Aufgrund seiner Flexibilität ist TSK ein zentrales Werkzeug in vielen forensischen Untersuchungen (Carrier, 2005).

3. Praktische Umsetzung

In diesem Kapitel werden die praktischen Schritte zur Datenwiederherstellung und Metadatenanalyse in der forensischen Ermittlungsumgebung CAINE beschrieben. Ziel ist es, die zuvor erläuterten theoretischen Grundlagen in die Praxis zu überführen und die Funktionsweise zentraler Werkzeuge nachvollziehbar darzustellen. Die Umsetzung erfolgt anhand realitätsnaher Fallbeispiele, welche typische Szenarien der digitalen Forensik simulieren.

Die Entscheidung für die Open-Source-Distribution CAINE beruht auf mehreren technischen und anwendungsorientierten Kriterien. Sie integriert eine Sammlung etablierter forensischer Werkzeuge, darunter Autopsy, Guymager und TSK, die sich insbesondere für die Analyse von Dateisystemen eignen (Hacking Akademie, 2024). Die grafische Benutzeroberfläche erleichtert nicht nur den Zugang zu forensischen Verfahren, sondern macht die Distribution auch zu einer geeigneten Einstiegslösung für kleine Unternehmen sowie Privatanwender. Ein integrierter Schreibschutz für Blockgeräte stellt sicher, dass die untersuchten Datenträger während der Analyse nicht verändert werden können (Hacking Akademie, 2024). Die fortlaufende Weiterentwicklung der Distribution gewährleistet darüber hinaus die zeitnahe Verfügbarkeit aktueller Werkzeuge und Methoden.

Dem praktischen Vorgehen liegt eine feste Abfolge zugrunde: Zunächst erfolgt die Installation und Einrichtung der virtuellen CAINE-Umgebung, woraufhin die Datenwiederherstellung durchgeführt wird. Erst im Anschluss daran wird die Metadatenanalyse vorgenommen, da diese in der Regel erst im Zusammenhang mit rekonstruiertem Inhalt sinnvoll durchführbar ist (Forensic Discovery, 2023).

Die konkreten Ergebnisse werden in den folgenden Abschnitten zur Datenwiederherstellung (Unterabschnitt 3.2.3) und zur Metadatenanalyse (Unterabschnitt 3.3.3) vorgestellt. Beide Kapitel dienen der praktischen Überprüfung der in den Grundlagenkapiteln vorgestellten Methoden.

3.1. Einrichtung der virtuellen Analyseumgebung

Die forensische Umgebung wird mithilfe von VirtualBox auf einem Windows-System als virtuelle Maschine VM bereitgestellt. Anstelle eines temporären Live-Betriebs wird CAINE vollständig auf einer virtuellen Festplatte installiert, basierend auf dem offiziellen Abbild der Projektwebseite (caine-live.net, 2024). Diese Vorgehensweise ermöglicht es Unternehmen und Privatpersonen, Analyseergebnisse dauerhaft zu speichern und Untersuchungen langfristig nachvollziehbar zu dokumentieren. Die wesentlichen Parameter der eingesetzten VM sind anbei dokumentiert, um die Nachvollziehbarkeit der praktischen Umsetzung im Rahmen dieser Arbeit sicherzustellen. Sie stellen jedoch lediglich eine beispielhafte Konfiguration dar und können je nach Anforderung angepasst werden.

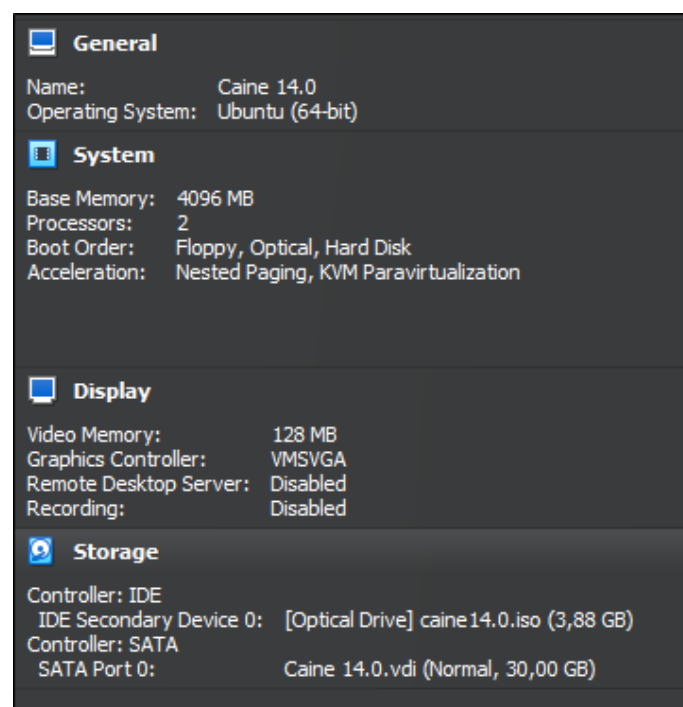


Abbildung 7: Parameter der CAINE VM

- Arbeitsspeicher: 4096 Megabyte
- Prozessor: Zwei virtuelle CPU-Kerne
- Festplattengröße: 30 Gigabyte
- Gastsystem: Linux (Ubuntu 64 Bit)

Die persistente Installation erfolgt über das grafische Installationskript („Install CAINE 24.04“) auf Basis des Ubuntu-Installers. Dabei werden die virtuelle Festplatte partitioniert und ein persistentes Dateisystem eingerichtet, dies hat gegenüber der Live-Umgebung den Vorteil, dass alle Änderungen und Ergebnisse auch nach einem Neustart der VM erhalten bleiben. Die Installation erfolgt in mehreren Schritten, die im Folgenden näher erläutert werden.



Abbildung 8: Persistente Installation auf der virtuellen Festplatte

Nach dem Start der VM wird zunächst die Live-Umgebung geladen. Die Installation erfolgt anschließend auf die virtuelle Festplatte. Nach Abschluss des Installationsprozesses, indem die das System konfiguriert und die Partitionen eingerichtet werden, wird die VM neu gestartet. Dabei wird das System von der virtuellen Festplatte geladen.

3.2. Datenwiederherstellung in der Praxis

Dieser Abschnitt beschreibt die praktische Umsetzung der Datenwiederherstellung in der forensischen Ermittlungsumgebung CAINE. Dabei wird ein forensisches Datenträgerabbild erstellt und anschließend eine gezielte Wiederherstellung gelöschter Dateien durchgeführt. Die Ergebnisse werden im Anschluss analysiert und bewertet.

3.2.1. Vorbereitungen

Im Rahmen der praktischen Analyse erfolgt die Wiederherstellung gelöschter Daten unter Verwendung der Ermittlungsumgebung CAINE. Grundlage der Wiederherstellungsanalyse ist ein forensisches Datenträgerabbild eines NTFS-formatierten Volumes.

Vorbereitung der Testumgebung

Zur Vorbereitung werden auf der bestehenden Festplatte der CAINE-Umgebung exemplarische Testdaten erstellt. Diese Dateien werden im Desktop-Verzeichnis des Benutzerprofils abgelegt.

Die vorbereiteten Dateien umfassen verschiedene Formate, darunter Textdateien (HelloWorld.txt, WorldHELLO.txt) sowie Bilddateien (Lorem Ipsum.png, Ipsum Lorem.jpeg, Lorem.jpeg). Diese Auswahl simuliert typische Nutzerdaten, wie sie im Rahmen forensischer Analysen regelmäßig auftreten (siehe Abbildung 9).



Abbildung 9: Anlage von Testdaten

Durch die gezielte Erstellung und spätere Löschung ausgewählter Dateien wird eine Testumgebung geschaffen, die einem realen Vorfall nachempfunden ist. Hierbei entste-

Mit
Anführungszeichen
wäre gut.
Weiß nicht, ob
du bei "Lorem"
die Bildeinblendung
hast oder ob das
mit "Ipsum.png" zusammen
gehört

Okay ab hier
ist klar. (Ja, ne?!)
Mit. trotzdem im
Fließtext Anführungs-
zeichen verwenden

hen verwaiste Datenblöcke, die im Dateisystem nicht mehr sichtbar, technisch jedoch weiterhin rekonstruierbar sind.

Um die Integrität der Ausgangsdaten zu bewahren, wird zunächst eine vollständige Kopie der Testdateien erstellt. Die Löschvorgänge erfolgen ausschließlich auf der Kopie, nicht auf den Originaldateien. Dieses Vorgehen ermöglicht eine realistische Wiederherstellungssimulation, ohne das ursprüngliche Datenmaterial zu verändern.

Erstellung eines forensischen Abbildes

Im Anschluss wird Guymager gestartet, um ein forensisches Abbild der kopierten Daten zu erstellen. Nach dem Start analysiert Guymager automatisch die vorhandenen Speichermedien und listet diese im Hauptfenster auf (siehe Abbildung 10). Sowohl interne als auch externe Laufwerke werden erkannt. Die Auswahl des zu sichernden Datenträgers erfolgt anhand von Eigenschaften wie Gerätenamen und Größe. Für eine forensisch einwandfreie Sicherung muss das Quelllaufwerk im nicht eingehängten Zustand vorliegen (ISO/IEC, 2015).

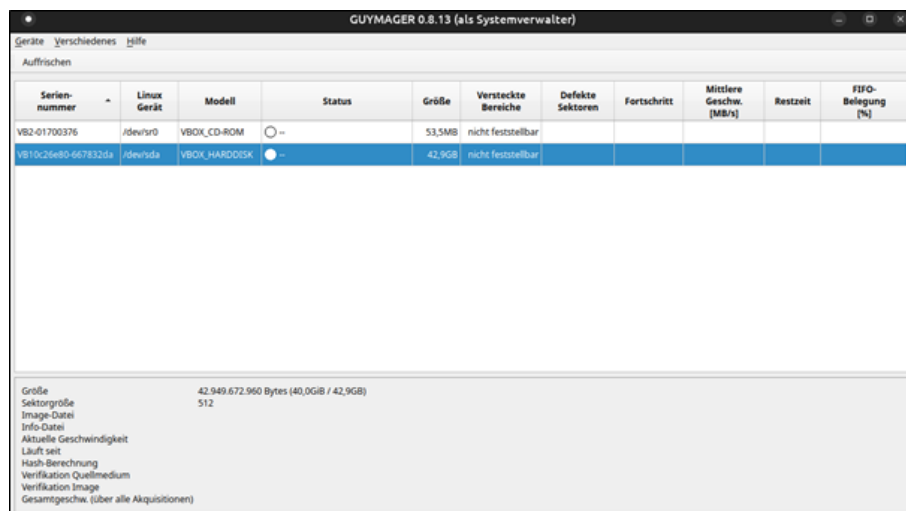


Abbildung 10: Start von Guymager und Übersicht der verfügbaren Laufwerke

3.2.2. Durchführung

- Dateisystemanalyse (NTFS oder FAT), gezielte Wiederherstellung gelöschter Dateien, Suche nach Dateisignaturen

3.2.3. Ergebnisse

- Qualität der Ergebnisse
 - Wurden Daten gut wiederhergestellt?
 - Sind die Daten vollständig (nützlich?)?
 - Wie schwierig war die Nutzung?
 - Hindernisse: kann auf Software oder Hardware beziehen
- Alternativen zu genutzten Programmen?
- Vergleich mit den Standards
- Vergleich mit Normen:
- In Bezug auf Beweismittelsicherung (z. B. Hashes, Protokollierung, Chain of Custody).
- NIST oder ISO/IEC 27037

3.3. Metadaten Analyse in der Praxis

- ExifTool + Autopsy

(Im Bezug zu Grundlagen: Verfahren und Standards)

3.3.1. Vorbereitungen

- Installation von ExifTool, Auswahl repräsentativer Dateien (z. B. JPEG mit EXIF-Daten, DOCX mit Autorfeldern), Sicherung des Ausgangszustands.

Vor dem Einsatz forensischer Werkzeuge sind umfangreiche Vorbereitungen erforderlich, um digitale Beweise zu sichern und gerichtsverwertbar zu dokumentieren. In diesem Abschnitt werden die Schritte zur Vorbereitung der Werkzeuge Autopsy, FTK Imager und The Sleuth Kit beschrieben, darunter: Datensicherung, Systemkonfiguration und Dokumentation der Untersuchungsschritte.

3.3.2. Durchführung

- Analyse mit exiftool, Gegenprüfung mit Autopsy (Metadatenansicht), Extraktion von Erstellungs-/Bearbeitungszeiten, Geräteinformationen, Benutzerinformationen.

3.3.3. Ergebnisse

- Qualität der Ergebnisse
 - Wurden Daten gut wiederhergestellt?
 - Sind die Daten vollständig (nützlich?)?
 - Wie schwierig war die Nutzung?
 - Hindernisse: kann auf Software oder Hardware beziehen
- Vollständigkeit und Aussagekraft der Metadaten, Vergleich beider Werkzeuge, Bewertung der Gerichtsfestigkeit.
- Alternativen zu genutzten Programmen?

3.4. Bewertung der Forensischen Umgebung

- Vor- und Nachteile der Umgebung
- Einordnung der Nutzungsbereiche
- Vergleich mit anderen forensischen Umgebungen (z.B. FTK Imager, EnCase, X1 Social Discovery)

4. Fazit

Dieses Kapitel fasst die Ergebnisse der Untersuchung zusammen und gibt einen Ausblick auf zukünftige Entwicklungen im Bereich der digitalen Forensik. Es werden die wichtigsten Erkenntnisse und Empfehlungen für den Einsatz forensischer Werkzeuge in der Praxis dargelegt.

4.1. Zusammenfassung der Ergebnisse

- Was wurde getan und warum?
- Welche Werkzeuge wurden eingesetzt?
- Wie gut wurden die angestrebten Ergebnisse erreicht?
- Welche Herausforderungen gab es?

4.2. Bewertung der eingesetzten Werkzeuge

- Vor-und Nachteile
- Einordnung der Nutzungsbereiche

4.3. Ausblick

- Aktuelle Entwicklungen im Bereich digitale Forensik
- Künstliche Intelligenz (KI)

Literaturverzeichnis

Formatierung? Sieht bissle unübersichtlich aus

- Balba, M. (2024) *What Is Data Recovery?*. Verfügbar unter: <https://www.ninjaone.com/it-hub/endpoint-management/data-recovery/> (Zugegriffen: 26 Februar 2025).
- Bayerischer Landtag (2023) *Schlussbericht des Untersuchungsausschusses zum NSU-Komplex*. Verfügbar unter: https://www.bayern.landtag.de/fileadmin/Internet_Dokumente/Sonstiges_A/UA_NSU_Schlussbericht_18_29926_fertige_Drs_Plenum.pdf (Zugegriffen: 5 April 2025).
- BSI (2023) *IT-Grundschutz-Kompendium: DER.2.2 Vorsorge für die IT-Forensik*. Bundeskriminalamt (2024b) *DNA-Analytik*. Verfügbar unter: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Kriminaltechnik/Biometrie/DNAAnalytik/dnaAnalytik_node.html (Zugegriffen: 5 April 2025). Bundeskriminalamt (2024a) *IT-Forensik – Methoden und Werkzeuge*. Verfügbar unter: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/IT-Forensik/it_forensik_node.html (Zugegriffen: 3 Januar 2025). caine-live.net (2024) *CAINE – Live Forensic GNU/Linux Environment*. Verfügbar unter: <https://www.caine-live.net/page5/page5.html> (Zugegriffen: 19 April 2025). Carrier, B. (2005) *File System Forensic Analysis*. Casey, E. (2011) *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Einsnulleins GmbH (2023) *IT-Sicherheit: So schützen Sie Ihre IT-Infrastruktur im Unternehmen*. Verfügbar unter: <https://einsnulleins.de/it-dienstleistungen/it-sicherheit> (Zugegriffen: 3 Februar 2025). FasterCapital (2025) *Datenwiederherstellung – Digitale Wahrheiten ans Licht bringen: Die Kunst der Datenwiederherstellung in der Forensik*. Verfügbar unter: <https://fastercapital.com/de/inhalt/Datenwiederherstellung%E2%80%93Digitale-Wahrheiten-ans-Licht-bringen%E2%80%93Die-Kunst-der-Datenwiederherstellung-in-der-Forensik.html> (Zugegriffen: 21 April 2025). Forensic Discovery (2023) *Importance of Metadata in Digital Forensics and eDiscovery*. Verfügbar unter: <https://forensicdiscovery.expert/importance-of-metadata-in-digital-forensics-and-ediscovery/> (Zugegriffen: 26 Februar 2025).

Hacking Akademie (2024) *Hacking-Distros im Vergleich – Kali, Parrot, CAINE & Co.* Verfügbar unter: <https://hacking-akademie.de/hacking-distros-im-vergleich/> (Zugegriffen: 28 Februar 2025).

ISO (2018) *ISO 21043-1-Forensic sciences — Part 1: Terms and definitions*. Verfügbar unter: <https://www.iso.org/standard/70985.html> (Zugegriffen: 5 April 2025).

ISO/IEC (2012) „ISO/IEC 27037: Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence“.

ISO/IEC (2015) „ISO/IEC 27042: Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence“.

Katz E, B.S., Halámek J (2015) „Forensic Science - Multidisciplinary Approach“. Verfügbar unter: <https://www.heraldopenaccess.us/openaccess/forensic-science-multidisciplinary-approach> (Zugegriffen: 5 April 2025).

KSV Polizeipraxis (2022) *Die Kriminalistik im System der Kriminalwissenschaften*. Verfügbar unter: <https://ksv-polizeipraxis.de/die-kriminalistik-im-system-der-kriminalwissenschaften/> (Zugegriffen: 5 April 2025).

Meier, S. (2017) *Digitale Forensik in Unternehmen: Entwicklung eines forensisch orientierten digitalen Reifegradmodells*. Verfügbar unter: https://epub.uni-regensburg.de/35027/1/Dissertation_Veroeffentlichung_Stefan_Meier_A5_digital.pdf (Zugegriffen: 27 Februar 2025).

NIST (2006) *SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response*.

Oh, J., Lee, S. und Hwang, H. (2022) „Forensic Recovery of File System Metadata for Digital Forensic Investigation“.

Proact Deutschland GmbH (2024) *Die 15 häufigsten Gründe für Datenverlust und wie Sie vorbeugen können*. Verfügbar unter: <https://www.proact.de/blog/die-15-haeufigsten-gruende-fuer-datenverlust/> (Zugegriffen: 26 Februar 2025).

Serlo Education e.V. (2023) *Geschichte der Forensik – Einführung in die Forensik*. Verfügbar unter: <https://de.serlo.org/forensik/196353/196356/geschichte-der-forensik> (Zugegriffen: 5 April 2025).

Spenneberg, R. (2008) „Selbst geschnitzt: Carving-Tools spüren Files auf, ohne das Dateisystem zu kennen“. Verfügbar unter: <https://www.linux-magazin.de/ausgaben/2008/06/selbst-geschnitzt/> (Zugegriffen: 21 April 2025).

Spiceworks Inc. (2024) *Data Recovery: Types, Process, and Software*. Verfügbar unter: https://www.spiceworks.com/tech/data-management/articles/what-is-data-recovery-types-process-and-software/?utm_source=chatgpt.com (Zugegriffen: 21 April 2025).

Statista (2018) *Polizeiliche Aufklärung von Straftaten über die DNA-Analyse bis 2018*. Verfügbar unter: <https://de.statista.com/statistik/daten/studie/155755/umfrage/polizeiliche-aufklaerung-von-straftaten-ueber-die-dna-analyse-nach-deliktsbereichen/> (Zugegriffen: 5 April 2025).

Statista (2024) *Number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2024 YTD*. Verfügbar unter: <https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/> (Zugegriffen: 25 November 2024).

Stiller, M. (2019) *Definition von Forensik – Eine begriffliche Annäherung*.

studieren.de (2025) *Forensik: Analytikerinnen für die Verbrechensbekämpfung*. Verfügbar unter: <https://studieren.de/forensik.0.html> (Zugegriffen: 5 April 2025).

Talha, S. u. a. (2024) „A Comparative Study of CAINE Linux: A Digital Forensics Distribution“. Verfügbar unter: <https://www.jcbi.org/index.php/Main/article/download/614/542> (Zugegriffen: 5 April 2025).

TSK (2024) *Autopsy - Digital Forensics*. Verfügbar unter: <https://www.sleuthkit.org/autopsy/desc.php> (Zugegriffen: 21 April 2025).

Varonis Systems (2023) *Datenintegrität: Was ist das und wie ist sie aufrecht zu erhalten?*. Verfügbar unter: <https://www.varonis.com/de/blog/datenintegritat-was-ist-das-und-wie-ist-sie-aufrecht-zu-erhalten> (Zugegriffen: 3 Januar 2025).

Voncken, G. (2025) *Guymager – Forensic Imager for Media Acquisition*. Verfügbar unter: <https://guymager.sourceforge.io/> (Zugegriffen: 17 April 2025).