

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
Tabellenverzeichnis	II
Abkürzungsverzeichnis	II
1. Einleitung	1
1.1. Hintergrund und Relevanz des Themas	1
1.2. Zielsetzung	5
1.3. Aufbau der Arbeit	5
2. Grundlagen	7
2.1. Forensik	7
2.1.1. Begriffsdefinition	10
2.1.2. Abgrenzung	10
2.2. Digitale Forensik	11
2.2.1. Verfahren und Standards	12
2.2.2. Datenwiederherstellung	12
2.2.3. Metadaten-Analyse	12
2.3. Die Ermittlungsumgebung CAINE	12
2.3.1. Integrierte Tools	13
2.3.2. Alternative Tools	13
3. Praktische Umsetzung	14
3.1. Datenwiederherstellung in der Praxis	14
3.1.1. Vorbereitungen	14
3.1.2. Durchführung	15
3.1.3. Ergebnisse und Bewertung	15
3.1.4. Vergleich mit den Standards	15
3.2. Metadaten Analyse in der Praxis	15
3.2.1. Vorbereitungen	15
3.2.2. Durchführung	16
3.2.3. Ergebnisse und Bewertung	16
3.2.4. Vergleich mit den Standards	16
4. Fazit	17
4.1. Zusammenfassung der Untersuchungsergebnisse	17
4.2. Bewertung der eingesetzten Werkzeuge	17
4.3. Ausblick	17
Literaturverzeichnis	VI

Abbildungsverzeichnis

Abbildung 1: Prognose: Kostenanstieg durch Cyberkriminalität (Fleck, 2024) 3

Tabellenverzeichnis

Tabelle 1: Fachbereiche der Forensik und ihre wissenschaftlichen Ursprünge
(Studieren.de, 2025) 8

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
CAINE	Computer Aided INvestigative Environment
DNA	Desoxyribonukleinsäure
DSGVO	Datenschutz-Grundverordnung
FTK	Forensic Toolkit
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Informationstechnologie
KI	Künstliche Intelligenz
NIST	National Institute of Standards and Technology
NSU	Nationalsozialistischer Untergrund
OT	Operational Technology
SOP	Standard Operating Procedure
TSK	The Sleuth Kit

1. Einleitung

Dieses Kapitel führt in die Thematik der forensischen Analyse von Daten ein und bildet damit die Grundlage für das Verständnis der Zielsetzung und der methodischen Ausrichtung dieser Arbeit. Es gliedert sich in folgende drei Abschnitte:

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 und der wachsenden Bedrohung durch Cyberkriminalität hat die IT-Forensik an Bedeutung gewonnen und sich als unverzichtbarer Bestandteil moderner Ermittlungsarbeit etabliert (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 (National Institute of Standards and Technology, 2006).

In Unternehmenskontexten kann ein Verlust der Datenintegrität weitreichende Folgen haben.

Datenintegrität bezeichnet die Korrektheit, Vollständigkeit und Konsistenz von Daten während ihres gesamten Lebenszyklus (Varonis Systems, 2023). Ein Verstoß gegen die Datenintegrität kann zu fehlerhaften Informationen führen, die Geschäftsentscheidungen negativ beeinflussen und operative Prozesse stören (Varonis Systems, 2023). Ein konkretes Beispiel für die Auswirkungen eines Datenverlusts ist der Produktionsausfall. In der Produktion sind vernetzte Maschinen und Systeme potenzielle Ziele für Cyberangriffe. Solche Angriffe auf die sogenannte „Operational Technology“ (OT) können nicht nur Daten gefährden, sondern auch Produktionsprozesse lahmlegen und hohe Ausfallzeiten verursachen (Einsnulleins GmbH, 2023).

Zusätzlich können rechtliche Konsequenzen drohen, insbesondere bei Verstößen gegen Aufbewahrungs- und Datenschutzpflichten (Varonis Systems, 2023). Für Privatpersonen bedeutet der Verlust personenbezogener 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 visualisiert die prognostizierte Entwicklung der weltweit durch Cyberkriminalität verursachten Kosten. Diesen sollen laut aktuellen Schätzungen im Jahr 2027 rund 12,43 Billionen US-Dollar erreichen und bis 2028 auf 13,82 Billionen US-Dollar ansteigen (Fleck, 2024).

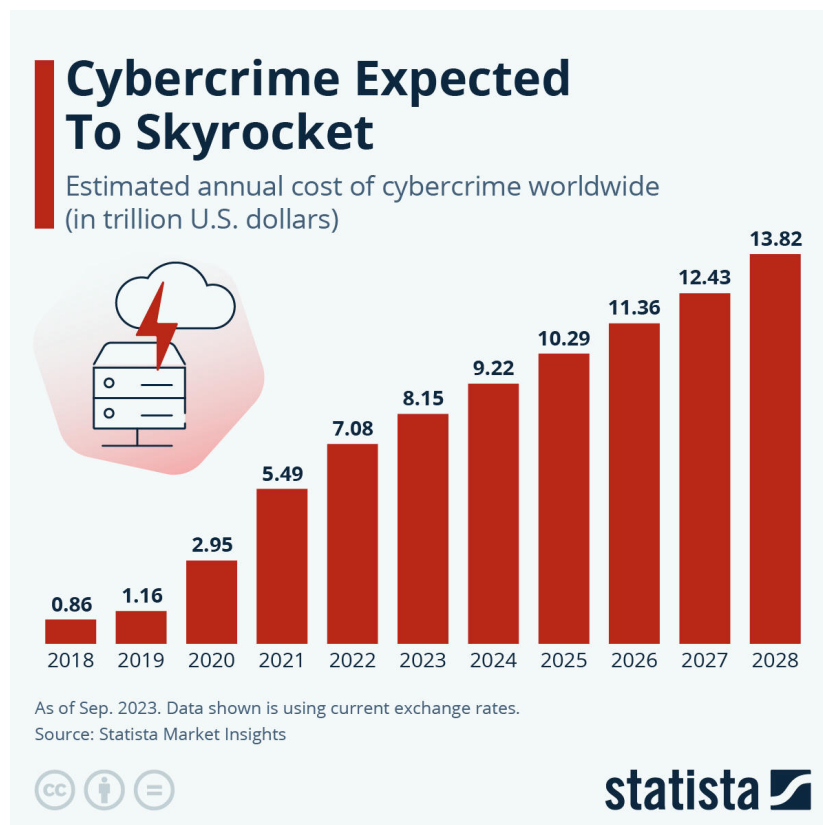


Abbildung 1: Prognose: Kostenanstieg durch Cyberkriminalität (Fleck, 2024)

Die zugrunde liegenden Zahlen berücksichtigen sowohl direkte als auch indirekte Schäden, darunter Datendiebstahl, Erpressung durch Ransomware, Systemausfälle, Betriebsunterbrechungen und regulatorische Sanktionen (Fleck, 2024). In ihrer Gesamtheit verdeutlichen sie das erhebliche ökonomische Ausmaß, das diese Form digitaler Bedrohung mittlerweile angenommen hat.

Die Kombination aus Datenwiederherstellung und Metadatenanalyse bildet die Grundlage einer fundierten Beweissicherung in der digitalen Forensik. Erst 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 ermöglicht es, gelöschte, beschädigte oder manipulierte Dateien aus Speichersystemen zu rekonstruieren, 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 Feuer- oder Wasserein-

wirkung, fehlerhafte Softwareaktualisierungen, Stromausfälle oder das versehentliche Formatieren von Speichermedien (Proact Deutschland GmbH, 2024).

Doch selbst die vollständige Wiederherstellung von Daten reicht nicht aus, um deren Aussagekraft gerichtsfest zu bewerten. Die ergänzende Metadatenanalyse ist erforderlich, um Informationen über Dateieigenschaften, Erstellungs- und Änderungszeitpunkte, Benutzerinteraktionen sowie Zugriffsrechte zu gewinnen. So kann nachvollzogen werden, wann ein Dokument erstellt, bearbeitet, kopiert oder gelöscht wurde und welchem Benutzerkonto die jeweiligen Aktionen zugeordnet werden können. (Forensic Discovery, 2023)

Um dieser komplexen Aufgabe gerecht zu werden, kommen in der digitalen Forensik 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 noch immer technikzentriert ausgerichtet, während prozessorientierte und organisatorische Aspekte häufig unzureichend beachtet werden. In der Praxis fehlt es häufig sowohl an standardisierten Vorgehensweisen als auch 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).

Um diesen Herausforderungen wirksam zu begegnen, ist ein methodisch fundierter und systematischer Einsatz spezialisierter Werkzeuge erforderlich (Lillis u. a., 2016).

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, wie etwa versehentliches Löschen von Daten oder die Analyse manipulierter Dateien.

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 im 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 forensischer Werkzeuge in der digitalen Spurensicherung abgeleitet werden. Diese richten sich sowohl an Unternehmen mit forensischem Bedarf als auch an technisch versierte Privatpersonen, die digitale Vorfälle systematisch nachvollziehen möchten.

1.3. Aufbau der Arbeit

Diese Arbeit orientiert sich methodisch an etablierten Standards der digitalen Forensik, insbesondere an den Empfehlungen des NIST sowie den internationalen

Normen der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC). Diese bilden die Grundlage für eine strukturierte, nachvollziehbare und gerichts feste Vorgehensweise und werden in Kapitel 2 ausführlich erläutert.

Folgende Punkte beschreiben den strukturellen Aufbau dieser Arbeit:

In Kapitel 2 werden zunächst die theoretischen und methodischen Grundlagen der digitalen Forensik dargelegt. Dazu zählen die Definition zentraler Begriffe, eine systematische Abgrenzung relevanter Teilbereiche sowie die Darstellung forensischer Verfahren, Standards und rechtlicher Rahmenbedingungen. Anschließend erfolgt in Abschnitt 2.3 eine Einführung in die eingesetzte forensische Umgebung sowie eine Vorstellung der verwendeten Werkzeuge.

Die praktische Umsetzung erfolgt in Kapitel 3 anhand realitätsnaher Fallbeispiele. Dabei wird zunächst der Prozess der Datenwiederherstellung behandelt (Abschnitt 3.1), da Metadaten häufig nur im Zusammenhang mit rekonstruierten Dateien vollständig verfügbar sind (Forensic Discovery, 2023). Im Anschluss folgt die Analyse der Metadaten (Abschnitt 3.2), um die wiederhergestellten Inhalte hinsichtlich ihrer Entstehung, Veränderung und Nutzung zu kontextualisieren.

Beide Teilprozesse werden unter einheitlichen Bewertungskriterien analysiert. Im Mittelpunkt stehen die Effektivität der eingesetzten Werkzeuge, ihre Benutzerfreundlichkeit sowie die Konformität mit forensisch relevanten Normen und Standards. Die Bewertung berücksichtigt sowohl technische als auch prozedurale Gesichtspunkte.

Auf Grundlage dieser Analyse werden im abschließenden Kapitel Kapitel 4 die Ergebnisse zusammengeführt und praxisnahe Handlungsempfehlungen für den Einsatz forensischer Werkzeuge formuliert. Die Arbeit richtet sich gleichermaßen an Organisationen mit forensischem Bedarf wie an technisch versierte Privatpersonen, die digitale Vorfälle systematisch untersuchen möchten.

2. Grundlagen

Um ein fundiertes Verständnis für die forensische Analyse von Dateien zu ermöglichen, legt dieses Kapitel die theoretischen und methodischen Grundlagen dar, die zum Verständnis der in dieser Arbeit eingesetzten Methoden und Werkzeuge erforderlich sind. In Abschnitt 2.1 werden zunächst die allgemeinen Grundlagen der Forensik eingeführt. Es folgen eine Begriffsdefinition zur Klärung zentraler Terme sowie eine Abgrenzung in der die digitale Forensik von anderen forensischen Disziplinen abhebt.

Daran anschließend befasst sich Abschnitt 2.2 mit der digitalen Forensik im engeren Sinne. Es beschreibt ihre Einsatzbereiche und untergliedert sich in spezifische Themenfelder wie Verfahren und Standards, Datenwiederherstellung und Metadatenanalyse. Abschließend folgt in Abschnitt 2.3 eine Vorstellung der Ermittlungsumgebung CAINE. Diese forensische Linux-Distribution stellt eine Vielzahl integrierter Werkzeuge bereit. Detailliert betrachtet werden sowohl in ihr integrierte Tools als auch alternative Tools, die je nach Anwendungsszenario zum Einsatz kommen können.

2.1. Forensik

Der Begriff „Forensik“ leitet sich vom lateinischen „forum“ ab, dem zentralen Platz im antiken Rom, an dem öffentliche Gerichtsverhandlungen abgehalten wurden. Ursprünglich bezeichnete der Begriff also die Tätigkeit, vor Gericht eine Aussage zu machen oder Beweise zu präsentieren (Stevenson und Brown, 2007).

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 wie der Daktyloskopie und der Bertillonage die moderne Forensik. Mit der Etablierung von Standards und Laborverfahren wurde sie zu einer anerkannten wissenschaftlichen Disziplin (KSV Polizeipraxis, 2022).

Heutzutage wird Forensik als interdisziplinärer Bereich verstanden, der natur-, sozial-, rechts- und ingenieurwissenschaftliche Methoden einsetzt, um strafrechtlich relevante Sachverhalte aufzuklären. 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).

Tabelle 1 bietet einen exemplarischen Überblick über ausgewählte forensische Fachbereiche, geordnet nach ihrer wissenschaftlichen Herkunft. Die Zuordnung orientiert sich dabei an der thematischen Gliederung, wie sie etwa von der Informationsplattform Studieren.de in ihrer Übersicht zu forensischen Studieninhalten dargestellt wird (Studieren.de, 2025).

Wissenschaftsbereich	Forensische Disziplinen
Medizin	Rechtsmedizin, Forensische Toxikologie, Pathologie
Biologie & Genetik	DNA-Analyse, Forensische Anthropologie
Chemie & Physik	Materialanalyse, Sprengstoff- und Drogenanalyse
Psychologie & Psychiatrie	Schuldfähigkeitsbegutachtung, Gefährlichkeitsprognosen
Sprach- & Geisteswissenschaften	Handschriftenanalyse, Linguistische Analyse
Informatik & Technik	Digitale Forensik, Telekommunikationsüberwachung

Tabelle 1: Fachbereiche der Forensik und ihre wissenschaftlichen Ursprünge
(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 mit der Verfeinerung der wissenschaftlichen Verfahren und ihrer gerichtlichen Verwertbarkeit stark zu. (Bundeskriminalamt, 2024a)

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

des Nationalsozialistischen Untergrunds (NSU) spielten forensische Methoden eine entscheidende Rolle bei der Aufklärung der Verbrechen. Durch die Analyse von DNA-Spuren, Waffen und anderen Tatortbefunden konnten Verbindungen zwischen den einzelnen Taten hergestellt und die Täter identifiziert werden. Der Fund der Dienstwaffen der ermordeten Polizistin Michèle Kieseewetter und ihres Kollegen im Wohnmobil der NSU-Mitglieder führten beispielsweise im November 2011 zu einem entscheidenden Durchbruch in den Ermittlungen. Diese Beweise waren maßgeblich für die Anklage und Verurteilung der Hauptangeklagten im NSU-Prozess. (Bayerischer Landtag, 2023)

Die moderne Forensik ist stark durch internationale Organisationen geprägt, die sich mit der Entwicklung und Standardisierung forensischer Verfahren befassen. Zu den wichtigsten zählen:

Das National Institute of Standards and Technology (NIST), das Richtlinien zur Sicherung und Analyse digitaler Beweismittel entwickelt.

Das European Network of Forensic Science Institutes (ENFSI), das sich für eine einheitliche Qualität forensischer Arbeit innerhalb Europas einsetzt.

Die ISO/IEC 27037, welche internationale Standards zur Identifikation, Sicherung und Dokumentation digitaler Beweise definiert (ISO/IEC, 2012).

Diese Standards tragen wesentlich zur gerichtlichen Verwertbarkeit forensischer Befunde bei, da sie nachvollziehbare, reproduzierbare und dokumentierte Verfahren vorschreiben. Zudem fördern sie die internationale Zusammenarbeit zwischen Strafverfolgungsbehörden und forensischen Laboren. Rechtliche und ethische Rahmenbedingungen

Die Anwendung forensischer Methoden unterliegt rechtlichen Beschränkungen und ethischen Anforderungen. In Deutschland sind genetische Untersuchungen durch die Strafprozessordnung (§§ 81e–h StPO) reguliert. Die Entnahme und Verarbeitung personenbezogener Daten – etwa DNA-Proben – ist nur unter bestimmten Voraussetzungen zulässig und bedarf in der Regel einer richterlichen Anordnung. Darüber hinaus müssen bei allen forensischen Maßnahmen die Prinzipien der Verhältnismäßigkeit, des Datenschutzes sowie der Unschuldsvermutung beachtet werden (MT-Portal, 2024).

Dieser Abschnitt behandelt die allgemeinen Grundlagen der Forensik. Er legt die theoretischen und methodischen Grundlagen dar, die zum Verständnis der in dieser Arbeit eingesetzten Methoden und Werkzeuge erforderlich sind. Dabei wird zunächst eine Begriffsdefinition zur Klärung zentraler Terme gegeben. Anschließend erfolgt eine Abgrenzung, die die digitale Forensik von anderen forensischen Disziplinen abhebt.

2.1.1. Begriffsdefinition

Der Begriff Forensik stammt aus dem Lateinischen „*forensis*“ und bedeutet „zum Forum gehörig“, womit ursprünglich öffentliche Gerichtsverhandlungen im antiken Rom gemeint waren (Houck und Siegel, 2010). In der modernen Wissenschaft beschreibt Forensik die methodische Untersuchung von Sachverhalten, um Beweise für juristische oder sicherheitsrelevante Zwecke zu gewinnen. Sie wird in unterschiedlichen Disziplinen angewendet, darunter Kriminalistik, Medizinforensik, Biologie, Chemie und die digitale Forensik (Casey, 2011).

Die forensische Wissenschaft folgt strengen Prinzipien, die sicherstellen sollen, dass gesammelte Beweise belastbar, reproduzierbar und gerichtsfest sind. Dazu gehört die Sicherstellung der Beweisintegrität, die sorgfältige Dokumentation der Untersuchungsschritte sowie die Ketten-of-Custody-Dokumentation, welche sicherstellt, dass digitale und physische Beweismittel während der gesamten Untersuchung unverändert bleiben (National Institute of Standards and Technology, 2006).

2.1.2. Abgrenzung

Überleitung zur digitalen Forensik und abgrenzung, verschiedene Arten Forensische Untersuchungen setzen eine Kombination aus wissenschaftlichen Methoden, technologischen Hilfsmitteln und juristischen Rahmenbedingungen voraus. Sie werden unter anderem in folgenden Bereichen eingesetzt:

- Kriminalistik: Untersuchung von Tatorten, DNA-Analysen, Fingerabdrücke.
- Medizinforensik: Autopsien, toxikologische Analysen.
- Wirtschaftsforensik: Aufdeckung von Betrug, Geldwäsche, Korruption.
- Digitale Forensik: Analyse von IT-Systemen, Netzwerken und digitalen Spuren.

2.2. Digitale Forensik

Der Baustein *DER.2.2 Vorsorge für die IT-Forensik* aus dem IT-Grundschutz-Kompendium des BSI beschreibt, wie Organisationen sich auf IT-forensische Untersuchungen vorbereiten können (Bundesamt für Sicherheit in der Informationstechnik, 2023). Als zentrale Bundesbehörde für Informationssicherheit ist das BSI eine maßgebliche Instanz für die Definition und Standardisierung sicherheitsrelevanter IT-Verfahren in Deutschland (Bundesamt für Sicherheit in der Informationstechnik, 2023). In diesem Zusammenhang liefert das BSI eine präzise Definition der digitalen Forensik:

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

Demnach befasst die digitale Forensik sich somit mit der Identifizierung, Sicherung, Analyse und Dokumentation digitaler Beweismittel. Ziel ist es, Schäden zu bestimmen, Angriffe abzuwehren, zukünftige Gefährdungen zu vermeiden und relevante Beweise gerichtsfest zu sichern und auszuwerten. Das BSI betont dabei insbesondere die Notwendigkeit vorbereitender Maßnahmen zur effektiven Spurensicherung, um den Verlust potenziell kritischer Beweisdaten zu vermeiden. (Bundesamt für Sicherheit in der Informationstechnik, 2023)

- anwendungsbereiche:

Die digitale Forensik wird in unterschiedlichen Bereichen eingesetzt, darunter: Strafverfolgung, Unternehmenssicherheit, Incident Response, Compliance und Datenschutz. Sie umfasst verschiedene Teilbereiche, darunter: Netzwerk-Forensik, Speicher-Forensik, Dateisystem-Forensik, RAM-Forensik, Metadaten-Analyse und Malware-Analyse.

- QUELLE

- relevanz von Dateisystemen - (Ergänzung: Erläuterung typischer Dateisysteme wie NTFS, FAT, ext4 und deren Bedeutung für die forensische Analyse)

2.2.1. Verfahren und Standards

- Normative Rahmenbedingungen und Richtlinien:
 - Welche gesetzliche, ethische und normative Vorgaben, gibt
 - z. B. ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042
- Methoden und Werkzeuge
 - 2.3.2 Beweissicherung und Chain of Custody?
 - 2.3.3 Hashing und Integritätsprüfung?

2.2.2. Datenwiederherstellung

Um ein fundiertes Verständnis für die forensische Analyse von Dateien zu schaffen, werden in diesem Kapitel zentrale Begriffe wie Datenwiederherstellung und Metadatenanalyse definiert und in ihren forensischen Kontext eingeordnet. Abschließend wird die methodische Vorgehensweise skizziert, die in späteren Kapiteln anhand praktischer Werkzeuge wie Autopsy, FTK Imager und The Sleuth Kit vertiefend angewendet wird.

- QUELLEN

2.2.3. Metadaten-Analyse

Metadaten sind strukturierte Daten, die Informationen über andere Daten enthalten. Sie beschreiben Eigenschaften, Struktur und Beziehungen von Datenobjekten. In der digitalen Forensik spielen Metadaten eine wichtige Rolle, da sie Aufschluss über die Herkunft, den Inhalt und die Verwendung von Daten geben. Metadaten-Analyse umfasst die Untersuchung von Metadaten, um digitale Beweise zu identifizieren, zu analysieren und zu interpretieren. Typische Metadaten in der digitalen Forensik sind: Dateiattribute, Zeitstempel, Dateigrößen, Dateipfade und Zugriffsrechte.

- QUELLEN

2.3. Die Ermittlungsumgebung CAINE

CAINE ist eine Linux-Distribution für die digitale Forensik, die eine Vielzahl von Werkzeugen für die forensische Analyse von Dateisystemen und Netzwerken bereitstellt. Zu den wichtigsten Werkzeugen von Caine gehören Autopsy, Forensic Toolkit (FTK) und The Sleuth Kit. Diese Werkzeuge bieten umfangreiche Funktionen zur Datenwiederherstellung, Metadaten-Analyse und forensischen Untersuchung von Dateisystemen.

Im Folgenden werden die wichtigsten Werkzeuge der digitalen Forensik vorgestellt und ihre Funktionsweisen erläutert.

- QUELLEN

2.3.1. Integrierte Tools

Autopsy ist ein Open-Source-Werkzeug für die forensische Analyse von Dateisystemen, das eine Vielzahl von Funktionen zur Datenwiederherstellung und Metadaten-Analyse bietet. Autopsy ermöglicht die Analyse von Dateisystemen, die Wiederherstellung gelöschter Dateien, die Untersuchung von Dateiattributen und die Erstellung forensischer Berichte. Das Werkzeug ist benutzerfreundlich und bietet eine intuitive Benutzeroberfläche, die auch für Einsteiger leicht verständlich ist.

The Sleuth Kit The Sleuth Kit ist ein Open-Source-Werkzeug für die forensische Analyse von Dateisystemen, das eine Vielzahl von Funktionen zur Datenwiederherstellung und Metadaten-Analyse bietet. The Sleuth Kit ist besonders für erfahrene Forensiker geeignet, da es umfangreiche Funktionen und Konfigurationsmöglichkeiten bietet.

- Mehr Beschreiben + QUELLEN

2.3.2. Alternative Tools

- Komplettlösungen
- Einzelne Tools als alternativen zu vorgestellten (Integrierte tools)

3. Praktische Umsetzung

- Einleitung zur praktischen Umsetzung
- Motivation und Zielsetzung
 - Erklären dass es es kriminell, oder ausversehendes löschen eine Wiederherstellung notwendig macht
- Vorgehen und Ziel
- Übergang zu Datenwiederherstellung
 - Datenwiederherstellung zuerst weil -> potenziel Metadaten wiederhergestellt werden und dann analysiert werden

3.1. Datenwiederherstellung in der Praxis

Autopsy + The Sleuth Kit (TSK) Wie in Unterabschnitt 2.3.1 Tool beschreiben, ist Autopsy ein Open-Source-Werkzeug für die forensische Analyse von Daten, das eine Vielzahl von Funktionen zur Datenwiederherstellung bietet. In diesem Unterkapitel werden die Schritte zur Vorbereitung und Durchführung der Datenwiederherstellung mit Autopsy detailliert beschrieben, darunter: Analyse von Dateisystemstrukturen, Wiederherstellung gelöschter Dateien und Erstellung forensischer Berichte...

- (Im bezug zu Grundlagen: Verfahren und standards)

3.1.1. Vorbereitungen

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.

- Möglicherweise Erstellung eines Festplattenimages (z.B. mit FTK Imager), Konfiguration von Autopsy, Auswahl des Moduls „Deleted Files“.

3.1.2. Durchführung

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

3.1.3. Ergebnisse und Bewertung

- 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?

3.1.4. Vergleich mit den Standards

- Vergleich mit Normen:
 - In Bezug auf Beweismittelsicherung (z. B. Hashes, Protokollierung, Chain of Custody).
 - NIST oder ISO/IEC 27037

3.2. Metadaten Analyse in der Praxis

- ExifTool + Autopsy

(Im Bezug zu Grundlagen: Verfahren und Standards)

3.2.1. 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.

3.2.2. Durchführung

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

3.2.3. Ergebnisse und Bewertung

- 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?

3.2.4. Vergleich mit den Standards

- ISO/IEC 27042 (Leitlinie zur Interpretation digitaler Beweise), Anforderungen an Metadaten in Ermittlungsverfahren.

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 Untersuchungsergebnisse

- 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

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).

Bundesamt für Sicherheit in der Informationstechnik (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).

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).

Fleck, A. (2024) *Expected cost of cybercrime worldwide from 2017 to 2027*. Verfügbar unter: <https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/> (Zugegriffen: 27 Februar 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).

Houck, M. und Siegel, J. (2010) *Fundamentals of Forensic Science*. Addison-Wesley.

ISO/IEC (2012) „ISO/IEC 27037: Guidelines for Identification, Collection, Acquisition, and Preservation 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).

Lillis, D. u. a. (2016) „Current challenges and future research areas for digital forensic investigation“.

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).

MT-Portal (2024) *DNA-Untersuchung zur Aufklärung von Straftaten*. Verfügbar unter: <https://mt-portal.de/im-fokus/dna-untersuchung-zur-aufklaerung-von-straftaten/>.

National Institute of Standards and Technology (2006) *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).

Statista Research Department (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).

Stevenson, A. und Brown, L. (2007) *Shorter Oxford English Dictionary on Historical Principles*.

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>.

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).