St. Pölten University of Applied Sciences

/informatik & security

/fh/// st. pölten

SSD Forensics

Forensische Akquise und Analyse im Vergleich zu HDDs

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur

eingereicht von

Cem Öztürk, BSc
is201830

im Rahmen des
Studiengangs Information Security an der Fachhochschule St. Pölten

Betreuung
Betreuer/Betreuerin: Dipl.-Ing. Dr. Robert Luh, BSc
Mitwirkung:

St. Pölten, 06.06.2022

(Unterschrift Autor/Autorin)

(Unterschrift Betreuer/Betreuerin)

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.

- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

St. Pölten, 06.06.2022

(Unterschrift Autor/Autorin)

Zusammenfassung

Die zunehmende Nutzung von Informationstechnologie führte in den letzten Jahren zu einer Digitalisierung der Kriminalität. Angesichts dessen spielt die Identifizierung und gerichtsfeste Beweissicherung von digitalen Spuren für die Aufklärung von Straftaten eine zentrale Rolle. Die fachgerechte Beweisaufnahme durch forensische Ermittler*innen ist dabei ein großer Faktor für die Zulässigkeit und Glaubwürdigkeit von digitalen Beweismitteln vor Gericht. Die Wahrung der Grundsätze der digitalen Forensik wie die Integrität und Authentizität von Beweisdaten werden stets vor neuen Herausforderungen gestellt, wie beispielsweise der Wechsel von herkömmlichen Festplatten („Hard-Disk Drives“, HDD) zu modernen Speichermedien wie „Solid-State-Drives“ (SSD) bzw. Flash-basierte Datenträger. Dieser Wandel der Datenbewahrung hat die Grundsätze der Computerforensik bedeutend verändert. Daher besteht das Ziel dieser Arbeit in der kritischen Analyse der Unterschiede und Eigenschaften der Speichermedien in Bezug auf die Auswirkung auf digital-forensische Untersuchungen. Diese Arbeit gibt einen Einblick in die Grundlagen der digitalen Forensik sowie der Funktionsweise und Eigenschaften von Speichermedien. Hierbei liegt der Fokus auf dem Herzstück der SSD, dem Controller, der die begrenzte Lebensdauer durch implementierte Funktionen erhöhen kann. Mithilfe eines Experimentaufbaus konnte durch verschiedene Testszenarien festgestellt werden, dass nach einer Datenlöschung Funktionen wie TRIM und Garbage-Collection im Vergleich zu anderen Speichermedien eine Datenwiederherstellung auch mit forensischen Mitteln grundsätzlich nicht immer ermöglichen. Daraus lässt sich schließen, dass der Schlüsselfaktor zu den grundlegenden Differenzen und die unvorhersehbaren Auswirkungen auf die Datenwiederherstellung in der Firmware der SSD liegt.

Abstract

The increasing use of information technology has led to a digitalisation of criminality in recent years. In this context, the identification and court-proof preservation of digital evidence plays a central role in the investigation of crimes. The professional collection of evidence by forensic investigators is a major factor for the admissibility and credibility of digital evidence in court. The preservation of the principles of digital forensics, such as the integrity and authenticity of digital evidence. This shift in data storage has significantly changed the principles of computer forensics. Therefore, the aim of this thesis is to critically analyse the differences and characteristics of storage media in terms of their impact on digital forensic investigations. This thesis provides an insight into the basics of digital forensics as well as the functioning and properties of storage media. The focus here is on the centrepiece of the SSD, the controller, which can increase the limited lifetime through implemented functions. With the implementation of an experiment, it was possible to determine through various test cases that after data deletion, functions such as TRIM and garbage collection do not always permit data recovery, even with forensic tools, compared to other storage media. This leads to the conclusion that the key factor to the fundamental differences and the unpredictable impact on data recovery lies in the firmware of the SSD.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

1.1 Ausgangslage/Problemstellung

Die rasante Entwicklung der Informationstechnologie in den letzten Jahren führte zu einer Digitalisierung der Kriminalität. Die Cyberkriminalität hat sich mittlerweile zu einem professionellem sowie lukrativem Geschäft entwickelt. [1] Durch Businessmodelle wie „Cybercrime as a Service“ [1] entstehen schnell wachsende und ernsthafte Bedrohungen für Unternehmen, Organisationen, kritische Infrastrukturen und Staaten. Hierbei werden Dienstleistungen, Werkzeuge und Schadsoftware angeboten, so dass für potenzielle Angriffe keine tiefgehenden Fachkenntnisse mehr notwendig sind. [1] Angesichts dessen steigt der Bedarf an qualifiziertem Fachpersonal, um mittels der digitalen Forensik die Aufklärung solcher Verbrechen, durch die Identifizierung und Sicherstellung von digitalen Spuren, gewährleisten zu können. Durch die zunehmende Nutzung elektronischer Geräte sind oftmals digitale Spuren die einzigen Ermittlungsansätze. [2] Da die Wissenschaft der digitalen Forensik immer in Bewegung ist, sind IT-Forensiker*innen immer wieder vor neuen Herausforderungen gestellt, wie beispielsweise der verbreitete Einsatz von modernen Solid-State-Laufwerken (SSD) bzw. Flash-basierten Speichermedien, die aufgrund ihrer Funktionsweise eine vollständige Rekonstruktion von Daten wesentlich beeinträchtigen können. [3, p. 1] Dabei zeigen sich bei dieser Art von Speichermedien deutliche Unterschiede bei den Themen Datenrekonstruktion, Transparenz und Lebensdauer im Vergleich zu herkömmlichen Festplatten, die sich beträchtlich auf die Erfassung bzw. Akquise von forensischen Daten auswirken können. [4, p. 1]

1.2 Zielsetzung/Fragestellung

Das Ziel dieser Arbeit besteht in der kritischen Analyse der Ergebnisse, die durch die Ausführung von forensischen Werkzeugen in verschiedenen Experimenten bei unterschiedlichen Speichermedien erzielt werden. Zusätzlich sollen auch die Unterschiede zwischen einer SSD und HDD und ihr Verhalten nach dem Löschen von Daten sowie die Auswirkung auf digital-forensische Untersuchungen aufgezeigt werden. Die Zielsetzung der Arbeit führt schlussendlich zu folgenden Forschungsfragen und Hypothesen, die im Rahmen dieser Arbeit beantwortet werden sollen:

1.2.1 Forschungsfragen

- Was sind die Unterschiede der Eigenschaften von SSDs bei der Akquise im laufenden Betrieb sowie im ausgeschaltetem/defekten Zustand im Vergleich zu HDDs?
- Was sind die Unterschiede der Eigenschaften von SSDs bei der Analyse im laufenden Betrieb sowie im ausgeschaltetem/defekten Zustand im Vergleich zu HDDs?
- Wie sind die Unterschiede zwischen SSDs und HDDs in Bezug auf den Wiederherstellungsprozess von residenten und normalen Daten?
- Welchen Unterschied macht die TRIM-Funktion auf Solid-State-Speichermedien bei der Akquise von gelöschten Daten?

1.2.2 Hypothesen

- Daten auf einer SSD mit deaktivierter TRIM-Funktion bleiben nach dem Löschen genauso erhalten wie auf traditionellen Hard-Disk-Laufwerken.
- Die Leerlaufzeit zwischen Löschung und Akquise von Daten hat keinen Einfluss auf den Wiederherstellungsprozess.
- Daten von einer SSD können nicht wiederhergestellt werden, wenn bei dieser Festplatte die TRIM-Funktion aktiviert ist.

- Das Formatieren einer Festplatte hat größere Auswirkungen auf die Akquise als das Löschen der Daten.

1.3 Methodische Vorgehensweise

Der ersten beiden Teile der vorliegenden Arbeit bestehen aus einer strukturierten Literaturanalyse, um die Grundlagen der digitalen Forensik sowie die technischen Unterschiede und Eigenschaften zwischen den Speichertechnologien zu behandeln. Dabei werden literarische Werke, Richtlinien sowie Leitfaden zu den Schlagwörtern Digitale Forensik, Forensische Untersuchungen und Speichermedien herangezogen. Diese Werke werden analysiert, auf Seriosität und Aktualität geprüft und anschließend werden alle für die Arbeit relevante Aussagen ausgewertet und dokumentiert, um eine qualitative Arbeit sicherzustellen. Um die Fragestellungen der vorliegenden Arbeit zu beantworten, werden Experimente durch die Ausführung von forensischen Werkzeugen bei unterschiedlichen Speichermeiden durchgeführt.

1.4 Aufbau der Arbeit

Zu Beginn der Arbeit wird anhand der Grundlagen der digitalen Forensik ein Grundverständnis vermittelt, um einen besseren Einblick in die Thematik zu geben. Hierbei werden für diese Arbeit relevante Teilgebiete oberflächlich erklärt. Danach wird mit den Grundsätzen und Ermittlungsmethoden der digitalen Forensik die Wichtigkeit der Befolgung von klaren Richtlinien dargestellt, um in weiterer Folge forensische Untersuchungen durchführen zu können. In diesem Kontext wird auf ein allgemeines Vorgehensmodell hingewiesen, die in der vorliegenden Arbeit als Grundlage für den praktischen Teil verwendet wurde.

Das Kapitel der technischen Grundlagen soll die Eigenschaften und Besonderheiten der verschiedenen Speichertechnologien aufzeigen. Der Fokus in diesem Abschnitt liegt auf den grundlegenden Funktionen der SDD, deren Implementierung die Aufrechterhaltung der Beweiskette und die Integrität der Daten zusätzlich erschwert. Das Fehlen eines Standards führte zu unterschiedlichen Ansätzen der Hersteller, die im Detail dem Betriebsgeheimnis unterliegen. Aufgrund dessen werden Forensiker/innen vor schwierigen Herausforderungen gestellt und setzen auf Maßnahmen wie das Entlöten und Auslesen einzelner Speicherchips.

Das darauffolgende Kapitel befasst sich mit den Forschungen, die ähnliche Konzepte entwickelt und hinterfragt haben, um potenzielle Herausforderungen für forensische Ermittler/Ermittlerinnen im Rahmen von digital-forensischen Untersuchungen zu identifizieren.

Kapitel 5 beschreibt den Aufbau des Experiments, welche das Setup, die Methodik sowie Vorbereitung beinhaltet. Im weiteren Verlauf werden im Unterkapitel „Durchführung“ die Experimente mit den Ergebnissen aufgelistet und kurz erläutert.

Nachdem die Ergebnisse der Experimente dieser Arbeit dargestellt werden, die durch den Einsatz von forensischen Werkzeugen auf einer HDD und Flash-basierten Speichermedien wie SSDs erzielt wurden, werden diese in einem eigenen Kapitel diskutiert. Zum Abschluss erfolgt eine Conclusio der gesamten Diplomarbeit.

2. Grundlagen der Digitalen Forensik

Dieses Kapitel befasst sich mit den Grundlagen der digitalen Forensik und dient als Grundwissen für das bessere Verständnis des praktischen Teils. Hierbei werden die Unterschiede der SDD und HDD detailliert erläutert.

2.1 Forensik

Schon seit Mitte bis Ende des 19. Jahrhunderts wurde zur Untersuchung von Verbrechen und Identifikation von Kriminellen die Wissenschaft eingesetzt. [5] Dabei wurden Beweise gesammelt, um schließlich Schuld oder Unschuld beweisen zu können und eine Verbindung zwischen Straftat und Verdächtigen herzustellen. [5] Durch die Verwendung von forensischer Wissenschaft können Elemente eines Verbrechens bewiesen, Aussagen von Opfer oder Verdächtigen bestätigt oder in Frage gestellt, Verstorbene oder Verdächtige erkannt oder Verbindungen zu einem Verbrechen oder Tatort hergestellt werden. [5]

2.2 Definition der Digitalen Forensik

"Die digitale Forensik ist die Anwendung von Methoden zur Identifikation, Sammlung, Bewahrung, Validierung, Analyse, Interpretation, Dokumentation und Präsentation von digitalen Beweisen, welche von digitalen Quellen abgeleitet sind. Digitalen Quellen beschränken sich nicht nur auf Laptops, Computer, Tablets und mobilen Geräten, sondern erstrecken sich auch auf Daten, die über öffentliche oder private Netzwerke übertragen werden. Oft beinhaltet die digitale Forensik die Entdeckung sowie Wiederherstellung von Daten mit Hilfe von verschiedenen Methoden und Werkzeugen, die den Ermittlern zur Verfügung stehen."
[6, p. 16]

Forensische Untersuchungen werden durchgeführt, um die Rekonstruktion von unerwünschten Ereignissen, wie beispielsweise kriminelle Cyber-Angriffe, zu erleichtern. Das Ziel ist dabei, zukünftige Vorfälle zu verhindern und künftig diese Taten effizienter und genauer aufklären zu können. [7, p. 22]

2.2.1 Digitale Beweise

„Eoghan Casey" definiert in seinem Buch [8] in Anlehnung an „Chisum" (1999) digitale Beweise als "alle Daten, die mit Hilfe eines Computers gespeichert oder übertragen werden und die eine Theorie über den Tathergang einer Straftat stützen oder widerlegen oder die sich auf kritische Elemente der Straftat beziehen, wie z. B. Internet oder Alibi". [8] Digitale Beweise sind die Erzeugung, Speicherung und Übertragung von allen Informationen in digitaler Form, welche zu einem späteren Zeitpunkt benötigt werden könnten, um eine Tatsache zu beweisen oder zu widerlegen. [9] Digitale Beweise können sich auf Laptops, Desktops, mobilen Geräten, Netzwerken, virtuellen und Cloud-Umgebungen befinden. Sie können auch in Bildern, Videos, Audiodateien, GPS-Systemen, Kameras, Informations- und Unterhaltungssystemen in Autos und sozialen Medien enthalten sein. In der Regel müssen digitale Beweismittel nur als ein Bereich qualifiziert werden, in dem elektronische Daten gespeichert und abgerufen werden können.

Digitale Geräte sind (Smartphone, Tablet, Computer, Laptop, Smartwatch, Überwachungskamera, Navigationsgeräte, Datenträger wie USB-Sticks, SD-Karten usw.) nicht mehr vom Alltag der Menschen wegzudenken, dies führt dazu, dass unbewusst digitale Spuren hinterlassen werden. [4] Durch die technischen Innovationen der letzten Jahre können oft bei vielen, auch nicht digitalen, Straftaten Beweismittel in digitaler Form im Internet oder auf digitalen Geräten von Verdächtigen gefunden werden. [10] Wenn bei einer Untersuchung die Möglichkeit digitaler Beweise besteht, muss eine digital-forensische Untersuchung durchgeführt werden. [4] Dabei werden in der Regel die Geräte von der verdächtigen Person

beschlagnahmt, um sie nach möglichen digitalen Beweismitteln oder Hinweisen zu durchsuchen. [4] Des Weiteren sind digitale Beweise hochveränderlich, während der Verwendung eines Computers können Dateien modifiziert werden, unter anderem ändert sich laufend auch der Inhalt des Arbeitsspeichers [8, p. 26].

2.3 Geschichte der digitalen Forensik

Die Einführung von persönlichen Computern gewann in den 1980er Jahren immer mehr an Popularität, so dass 1984 in FBI-Laboren einige der ersten Werkzeuge, die bei digital-forensischen Untersuchungen eingesetzt worden sind, entwickelt worden sind. [7, p. 21] Die forensischen Untersuchungen wurden vom spezialisierten „Computer Analysis and Response Team“ (CART) des FBI angeführt und war für die Unterstützung bei digitalen Untersuchungen zuständig. [7, p. 21] In den 1990er Jahren arbeiteten zunehmend mehrere Strafverfolgungsbehörden und Abteilungsleiter zusammen und brachten ihr Fachwissen bei regelmäßigen Treffen ein, dies sorgte für ein erhebliches Wachstum der digitalen Forensik als eigenständiger Bereich. [7, p. 21]

1993 veranstaltete das FBI einer der ersten offiziellen Konferenzen im Bereich digitale Forensik. Der Fokus dieser Konferenz, mit dem Namen „International Law Enforcement Conference on Computer Evidence“ lag auf dem Bedarf an formalen Standards sowie Verfahren für die digitale Forensik und Beweiserfassung. [7, p. 21] Durch die vermehrte Veranstaltung solcher Konferenzen kam es zur Gründung von Gremien, die sich mit Standards und „Best Practices“ der digitalen Forensik befassten. So wurde 1998 die „Scientific Working Group on Digital Forensics“ (SWGDE*)* von den Leitern der Bundeskriminalämter gegründet, die für die Ausarbeitung der Erfolgsmethoden für Computerbeweise verantwortlich waren. [7, p. 21]

Zusätzlich kam es auch zur Zusammenarbeit mit anderen Organisationen, wie mit der „American Society of Crime Laboratory“ (ASCLD), die 1973 gegründet wurde und seither an der fortlaufenden Entwicklung von Erfolgsmethoden, Verfahren und Schulungen im Bereich der forensischen Wissenschaft beteiligt ist. [7, p. 21] Das erste offizielle regionale Labor für Computerforensik wurde Anfang der 2000er Jahre vom FBI eingerichtet. Darauffolgend wurde 2002 das „National Program Office“ (NPO) gegründet und fungiert als zentrale Stelle für die Koordination und Unterstützung der Bemühungen der Strafverfolgungsbehörden der „Regional Computer Forensic Laboratory“ (RCFL). [7, p. 21] Aufgrund der rasanten technologischen Entwicklung arbeiten seitdem mehrere Behörden, die jeweils auch über ihre eigenen Abteilungen für Cyberkriminalität, eigene Labors für digitale Forensik und eigene Agenten vor Ort verfügen, wie das FBI, die „Central Intelligence Agency“ (CIA), die „National Security Agency“ (NSA) und das „Government Communications Headquartes“ (GCHQ) an der Bewältigung verschiedener Aufgaben zusammen. [7, p. 21]

2.4 Teildisziplinen der digitalen Forensik

Dieses Kapitel befasst sich mit den relevanten Teildisziplinen der digitalen Forensik, die im praktischen Teil dieser Arbeit wiederzufinden sind. Die Computerforensik und Mobilgeräte-Forensik kann mit den verwendeten Speichermedien der Experimente assoziiert werden und sind in diesem Kapitel näher erläutert.

2.4.1 Computerforensik

Einer der größten Bereiche der digitalen Forensik ist die Computerforensik. In dem Buch von Larry Daniel et. al [11] wird die Computerforensik als Hauptquelle für digitale Beweise beschrieben. Diese Teildisziplin beschäftigt sich grundsätzlich mit der Untersuchung von Beweisen, die auf einer Computerfestplatte gefunden werden, wie beispielsweise Benutzerkonten, Protokolldateien, Zeitstempel, Bilder, E-Mails und auch die Untersuchung von anderen Hardware-Komponenten eines Computers, wie dem Arbeitsspeicher (RAM). [11, p. 18] Jedes digitale Gerät, welches von einem Betriebssystem gesteuert wird und über ein Dateisystem verfügt, wird in die Computerforensik kategorisiert. [12] Grundsätzlich ist die

Datenwiederherstellung die Grundlage der Computerforensik [8, p. 18] und ebenfalls ein großer Schwerpunkt der Experimente in dieser Arbeit, die im weiteren Verlauf in Kapitel 5 behandelt werden.

2.4.2 Mobilgeräte-Forensik

Mobilgeräte-Forensik beinhaltet die Akquise und Analyse von tragbaren Geräten, die Daten speichern und die Kommunikation ermöglichen können. [12] Da der Zugriff auf diese Daten komplexer ist als bei der Computerforensik, kann die Mobilgeräte-Forensik als eigene Disziplin angesehen werden, obwohl es Geräte mit Betriebssystemen und Dateisysteme sind. [12] Dieser Bereich ist aufgrund ihrer hohen Nutzung mittlerweile ebenso gängig wie die Untersuchung von Computern, da heutzutage ein Großteil der Menschen beispielsweise Smartphones besitzen. Diese können Informationen beinhalten, wie beispielsweise Textnachrichten, Bilder, Videos, Audioaufnahmen usw. [11, p. 19]

Insbesondere im Rahmen der Strafverfolgung wird die forensische Untersuchung immer relevanter, da mobile Geräte zunehmend im Privat- als auch im Berufsleben die herkömmlichen Computer ersetzen. [13] Das permanente Wettrennen zwischen Angriff und Verteidigung findet auch in der Mobilgeräte-Forensik statt. Das Ausnutzen von Sicherheitslücken ist oft die einzige Möglichkeit die Schutzmaßnahmen der Hersteller*innen zu überwinden. [13] Dabei werden viele dieser Sicherheitslücken von staatlichen Behörden geheim und offen gehalten und helfen somit indirekt auch den Kriminellen bei deren Straftaten. Durch die Verwendung von verschiedenen Forensik-Tools ist es den Behörden auch möglich, unauffällig aus der Ferne sich Zugang zu den Geräten von Verdächtigen zu schaffen. Dies ist jedoch ein schwerer Eingriff in die Grundrechte eines Menschen, aufgrund dessen ist eine Spionage von mobilen Geräten mit richterlichem Befehl nur bei schweren Straftaten ratsam. [13]

Auch der Bereich der mobilen Geräte schreitet mit immer neuen Veränderungen rasant voran. Das führt bei forensischen Untersuchungen oft zu Schwierigkeiten, da Forensiker sich immer über neue Techniken informieren müssen. Betriebssysteme, Schnittstellen, Hardwarestandards und Speichertechnologien können sich sogar innerhalb kurzer Zeit häufig ändern. [13] Zusätzlich zu den vielen verschiedenen Plattformen der mobilen Geräte kommen infolgedessen bei forensischen Untersuchungen häufig mehrere Tools zum Einsatz. [13]

2.5 Grundsätze der digitalen Forensik

„Identifizierung, Sammlung, Untersuchung und Analyse von Daten unter Wahrung der Integrität der Informationen und unter Beibehaltung einer strengen Beweismittelkette“ [14, pp. ES-1]

Folgende Grundsätze der digitalen Forensik sind wichtige Bestandteile für die Lösung von Vorfällen und Streitigkeiten in Unternehmen, als auch in Straf- und Zivilverfahren:

2.5.1 Integrität

Die Integrität befasst sich mit der Verhinderung aller Art von Veränderung an den Daten die forensisch untersucht werden. [15, p. 103] Durch verschiedene Software-, Hardwarelösungen und technischen Leitlinien beispielweise durch die Verwendung eines Schreibschutzes bzw. Hardware-Write-Blockers, welches ein dezidiertes Gerät ist, können alle Schreibbefehle auf das angeschlossene Speichermedium blockiert und nur lesende Zugriffe erlaubt werden. [11, p. 38] Die Verifizierung, dass keine Veränderungen an Daten während eines bestimmten Prozesses passiert sind, kann zusätzlich durch den Einsatz von kryptographischen Hash-Funktionen erreicht werden. [8, p. 22] Hierbei sollte jede durchgeführte Aktion auf den digitalen Geräten für die Nachvollziehbarkeit entsprechend dokumentiert werden. Im Allgemeinen gilt während der Akquise jeder Art von Änderungen an den Daten zu minimieren, da schon die Ausführung eines Programmes erhebliche Auswirkungen an potenziellen Beweisdaten haben kann. [8, pp. 22-24]

Die Erstellung eines Abbildes bzw. einer Momentaufnahme, dass eine digitale Kopie des aktuellen Zustandes eines digitalen Gerätes ist, ist unabhängig vom Zustand des Gerätes bedeutend, um die Integrität und die ordnungsmäßige Beweismittelkette der Beweismittel nachweisen zu können. [8, p. 22] Durch die Beweismittelkette ist nachweisbar, dass die Daten auf dem Datenträger vom Zeitpunkt der Entnahme bis zur Vorlage vor Gericht weder von Ermittelnden noch von anderen Personen verändert wurden. [16] Die Überprüfung der Integrität der Beweismittel ist ein Prozess, bei dem beispielsweise die „Hash-Werte“, also berechnete Prüfsummen der Daten, des Beweismittels und der ursprünglichen Datei ermittelt und verglichen werden können. [8, p. 22] Eine exakte Kopie oder ein Abbild eines digitalen Gerätes sollte allgemein denselben Hash-Wert wie das Originale haben. Diese Prüfsumme wird mit einem „MD5“-, „SHA1“- oder zunehmend auch „SHA256“-Algorithmus berechnet und schon die kleinste Änderung in der Datei führt in der Regel zu einer Veränderung des Hash-Wertes und würde damit dem Prinzip der Integrität nicht mehr entsprechen. (siehe Tabelle 1 und Tabelle 2) [8, p. 22]

Nachricht	MD5-Hash-Wert
Diese Nachricht könnte ein Beweismittel sein.	CD953EDF37AC5007430970BE61373A91
Diese Nachricht könnte ein Beweismittel sein!	EF696D85B5F64CF9E714964BF2A94141

Tabelle 1: Beispiel für unterschiedliche MD5-Hash-Werte nach einer Änderung [17]

Nachricht	SHA1-Hash-Wert
Diese Nachricht könnte ein Beweismittel sein.	65C6D3211FCFC2F076A437AD1079DD73C4448F62
Diese Nachricht könnte ein Beweismittel sein!	25F35EC92D5A99AB9A99514C2A7C2235B70AD20A

Tabelle 2: Beispiel für unterschiedliche SHA1-Hash-Werte nach einer Änderung [18]

2.5.2 Authentizität

Mit dem Prinzip der Authentizität wird sichergestellt, dass die gesammelten digitalen Beweise oder Spuren mit den ursprünglich beschlagnahmten Daten übereinstimmen. [8, p. 20] Der Vergleich der sichergestellten Daten mit dem Original ist aus technischer Sicht nicht immer möglich, beispielsweise gibt es durch die ständige Veränderung des Inhaltes eines Arbeitsspeichers, nicht die Möglichkeit eine durchgeführte Momentaufnahme des Arbeitsspeichers entsprechend zu vergleichen, da die Originaldaten nicht immer zur Verfügung stehen. [8, p. 20] Vom juristischen Standpunkt aus gesehen ist die Authentizität, die Überzeugung des Gerichtes, dass der Inhalt eines Beweises unverändert geblieben ist und die Informationen tatsächlich von der angeblichen Quelle stammen. [19] Der Nachweis kann dabei eine mündliche Aussage, Indizienbeweise oder technische Merkmale sein. [19] Eine ordnungsgemäße Beweismittelkette ist ein großer Faktor für die Wahrung der Authentizität. Sollte nachgewiesen werden können, dass Beweise oder Spuren nicht verändert oder ausgetauscht wurden, ist es dem Gericht möglich, Beweismittel mit einer Straftat in Verbindung zu bringen. Andernfalls kann dies Zweifel an der Vertrauenswürdigkeit der digitalen Beweise aufkommen lassen. [8, pp. 20-21]

2.5.3 Order of Volatility

Das Prinzip „Order of Volatility” beschreibt die Flüchtigkeit von Daten auf einem System. Damit wird die Dauer der Erhaltung von Daten für eine digital-forensische Untersuchung bestimmt. [20] Zur Verhinderung von Verlusten digitaler Beweise ist ein rasches und effektives Handeln der Ermittler/innen wichtig. Durch das Prinzip kann eine Reihenfolge bei der Akquise von Daten bestimmt werden, desto flüchtiger Daten sind desto eher handelt es sich um eine begrenzte Momentaufnahme. Somit sollten diese Daten so schnell wie möglich

aufgezeichnet bzw. kopiert werden, bevor Änderungen stattfinden und dabei das Prinzip der Integrität verletzt wird. [20]

Um eine Reihenfolge bestimmen zu können, werden digitale Beweise in drei verschiedenen Kategorien unterteilt. [20] Persistente digitale Beweise sind Spuren bzw. Beweise, bei der eine Erhaltung auch ohne Stromversorgung möglich ist und können über einen längeren Zeitraum für eine Analyse verwendet werden. [20] Semi-persistente digitale Beweise bleiben nur bei einer aktiven Stromzufuhr erhalten und können bei einer Unterbrechung vollständig zerstört werden. Daher sollten semi-persistente Spuren für eine spätere Analyse auf einem persistenten Datenträger ordnungsgemäß kopiert bzw. dupliziert werden. [20] Flüchtige Beweise können trotz aktiver Stromversorgung nur kurz verfügbar sein und sollen rasch analysiert oder für eine spätere Analyse dokumentiert und ordnungsgemäß gesichert werden. [20]

Tabelle 3 beschreibt Beispiele unterteilt in Kategorien in Bezug auf die Flüchtigkeit von Daten:

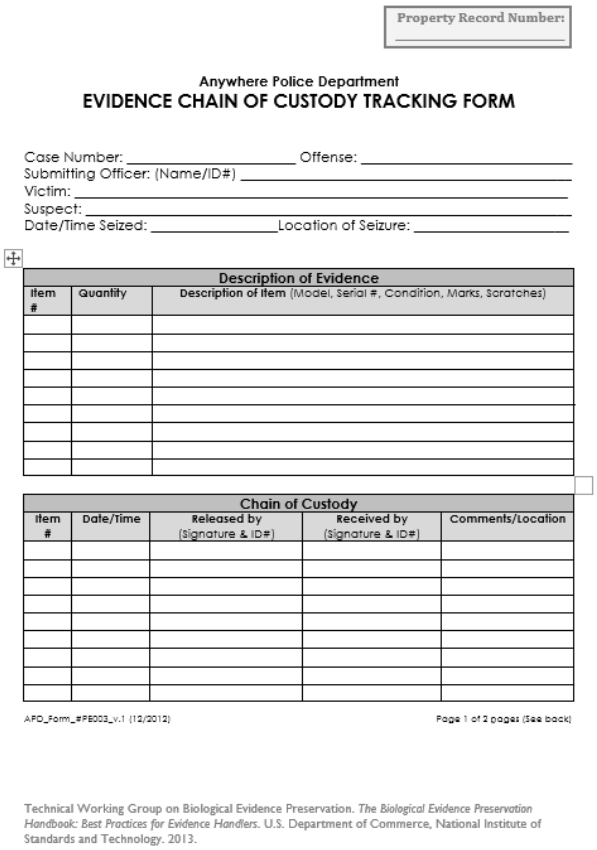
Flüchtig	Semi-persistent	Persistent
CPU-Register, Cache	Arbeitsspeicher (RAM)	Festplatte
Routing-Tabelle	Aktive Prozesse des Systems	CD
Prozesstabelle		DVD
ARP-Cache		USB-Stick
Kernel-Statistiken		Speicherkarten

Tabelle 3: Beispiele der Flüchtigkeit von Daten [20]

2.5.4 Chain of Custody

Bei diesem Prinzip befasst sich mit der Aufrechterhaltung sowie Dokumentation einer ordnungsmäßigen Beweismittelkette beim Umgang mit Beweismitteln und beinhaltet die Tätigkeiten der untersuchenden Person. [8, pp. 21- 22] Jeder Art von Beweismittel muss sorgfältig und ordnungsgemäß dokumentiert und ausgewertet werden, da ein minimaler Fehler bei der Dokumentation ein möglicher Grund für die Unzulässigkeit des Beweismittels vor Gericht sein kann. [8, pp. 21- 22]

Abbildung 1 zeigt ein Beispiel-Formular vom NIST [21], die für die Dokumentation der Beweismittelkette verwendet werden kann. Im oberen Abschnitt des Formulars befinden sich allgemeine Informationen zu einem Fall, wie beispielsweise Nummer des Falls, usw. Relevante Beschreibungen der Beweismittel, wie beispielsweise der Name, die Menge und Seriennummer des Beweismittels, können im mittleren Abschnitt des Formulars erläutert werden. Im unteren Abschnitt des Formulars befindet sich die Beweismittelkette und beschreibt, wann und von wem das Beweismittel in Empfang genommen oder wann es an andere Personen übergeben wurde. Ebenfalls können Personen und Gründe für eine Übergabe dokumentiert werden. Dieses Formular sollte für jedes einzelne Beweismittel angefertigt werden und ist ein wichtiger Teil des forensischen Berichtes.



Property Record Number: _____

Anywhere Police Department
EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____Location of Seizure: _____

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

APD_Form_#P8003_v.1 (12/2012) Page 1 of 2 pages (See back)

Technical Working Group on Biological Evidence Preservation. *The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers.* U.S. Department of Commerce, National Institute of Standards and Technology. 2013.

Abbildung 1: Beispiel-Formular für die Dokumentation einer Beweismittelkette [21]

2.6 Ermittlungsmethoden der digitalen Forensik

In der digitalen Forensik lässt sich der Zeitpunkt einer forensischen Untersuchung in zwei grundlegend verschiedenen Ansätzen einordnen, der sogenannten Live-Response- und der Post-Mortem-Analyse. [15, p. 5011]

2.6.1 Post-Mortem-Analyse

Im Rahmen der Post-Mortem-Analyse bzw. Offline-Forensik werden bereits ausgeschaltete Systeme bzw. persistente Daten sorgfältig sichergestellt und analysiert. Hierbei werden Sicherungskopien bzw. Images der originalen Datenträger erstellt, um eventuell gelöschte, umbenannte, versteckte sowie verschlüsselte Daten wiederherstellen und anschließend analysieren zu können. [20] Bei der Erstellung der Duplikate kann durch die Verwendung eines Write-Blockers die Unversehrtheit der Daten beispielsweise für eine mögliche spätere gerichtliche Verwendung gewährleistet werden. [20] Allerdings können durch diese Methode Informationen, die nur zur Laufzeit eines Systems erhalten bleiben, nicht gesichert und analysiert werden. [20] Einer der wesentlichen Vorzüge einer Post-Mortem-Analyse liegt darin, dass sich durch diesen Ansatz unterschiedliche Analyseverfahren, unter Einhaltung der Grundsätze, zur Verhinderung von Änderungen an den originalen Daten simultan sowie zeitlich unbegrenzt durchgeführt und betroffene Systeme mit neuen Datenträgern durch Sicherungskopien bzw. Backups wiederhergestellt und wieder produktiv betrieben werden können. [22, p. 107]

2.6.2 Live-Response-Analyse

Bei der Live-Response-Analyse oder auch Online-Forensik richtet sich der Fokus auf das Sammeln sowie Sichern relevanter flüchtiger und semi-persistenter Daten von noch eingeschalteten bzw. aktiven Systemen. [20] Dieser Ansatz ist relevant, wenn ein Zugriff auf Datenträger nicht mehr möglich ist und das System aus Verfügbarkeits- oder Abhängigkeitsgründen nicht ausgeschaltet werden kann, da sonst essenzielle Beweisträger verloren gehen würden. [22, p. 241] Somit können potenzielle Beweisdaten, die im ausgeschalteten oder inaktiven Zustand der Systeme irreversibel unauffindbar wären, erfolgreich gesichert werden, wie beispielsweise der Inhalt des Arbeitsspeichers eines Computers, aktive Netzwerkverbindungen sowie offene Dateien und Programme. [20]

> "Eines der Hauptprobleme bei der Live Response Analyse ist allerdings, dass die Reihenfolge der Sicherung der flüchtigen Daten nicht immer zweifelsfrei festgelegt werden kann, da jede Tätigkeit am verdächtigen System auch das verdächtige System selbst verändert. So tauchen beispielsweise bei der Sicherung der Liste der gerade auf dem verdächtigen IT-System laufenden Prozesse auch die für den Sicherungsvorgang verwendeten Befehle auf. Bei unsachgemäßem Tooleinsatz besteht auch die Gefahr, dass weitere Daten zerstört werden bzw. relevante Informationen durch auf dem System installierte Rootkits verschleiert werden können."
> [15, p. 5011]

Jede minimale Handlung kann zu Veränderungen am laufenden System führen, wie z.B. bei Zeitstempeln oder beim Inhalt des Arbeitsspeichers, aufgrund dessen sollten sämtliche durchgeführte Tätigkeiten, für die Nachvollziehbarkeit sowie Glaubwürdigkeit vor Gericht, sorgfältig dokumentiert bzw. protokolliert werden. [22, p. 241] Grundsätzlich ergänzen sich beide Untersuchungsansätze gegenseitig, beispielweise kann die im Rahmen einer Live-Response-Analyse sichergestellten Spuren der flüchtigen und semi-persistenten Daten eine erhebliche Erleichterung für die anschließende Post-Mortem-Analyse sein. [20]

2.7 Vorgehensmodelle und -prozesse der digitalen Forensik

Dieses Kapitel befasst sich mit einem allgemeinen Vorgehensmodell der digitalen Forensik und kann als grundlegender Ausgangspunkt für die Entwicklung einer eigenen Methodik der Vorgehensweise einer digital-forensischen Untersuchung dienen.

2.7.1 SAP-Modell

Das sogenannte „Secure-Analyse-Present"-Modell (Sichern, Analysieren und Präsentieren) ist eines der vereinfachtesten Modelle für digital forensische Analysen und beschreibt die allgemeine Vorgehensweise, unterteilt in drei Phasen (siehe Abbildung 2). [22, pp. 68-69]

Abbildung 2: Das SAP-Modell [23]

Angelehnt an die Darstellung der Prozessphasen des SAP-Modells erfolgt anschließend die Beschreibung der Kernaspekte der einzelnen Phasen. [22, pp. 68-69]

„Secure"/Sichern

Die erste Phase befasst sich mit der Identifizierung von Datenquellen sowie der sorgfältigen Erfassung bzw. Sicherung der Daten. [22, pp. 68-69] Die Sicherung wird nach dem Vier-Augen-Prinzip durchgeführt und muss eine genaue Kopie der Originaldaten sein, um das Prinzip der Integrität zu bewahren. [22, p. 69] Ebenfalls müssen alle durchgeführten Tätigkeiten für die Nachvollziehbarkeit vor Gericht sorgfältig dokumentiert bzw. protokolliert werden. [22, p. 69]

„Analyse"/Analysieren

Im Rahmen der zweiten Phase werden die zuvor gesicherten Daten sorgfältig analysiert und objektiv bewertet. [22, p. 69] In dieser Phase ist eine objektive Bewertung der Ergebnisse sowie die kritische Hinterfragung der gezogenen Schlüsse von großer Bedeutung, um Lücken in der Argumentationskette selbständig und sicher zu identifizieren und darauffolgend eine nachvollziehbare Argumentation bieten zu können. [24, p. 13]

„Present"/Präsentieren

Die letzte Phase des SAP-Modells beschäftigt sich mit der zielgruppengerechten Aufbereitung und Präsentation der Ergebnisse. [22, p. 69] Der Schwerpunkt dieser Phase ist die nachvollziehbare Darlegung auch für technische Laien, beispielsweise zur Verhinderung von Fehlurteilen, weil die Materie nicht verständlich aufbereitet wurde. [22, p. 69]

3. Technische Grundlagen

Dieses Kapitel befasst sich mit den technischen Grundlagen der Speichermedien und dienst als Grundwissen für das bessere Verständnis des praktischen Teils. Hierbei werden die Unterschiede der SDD und HDD detailliert erläutert.

3.1 HDD

Die „Hard Disk Drive" (HDD) ist ein persistenter bzw. nicht-flüchtiger magnetischer Datenträger und einer der wichtigsten Speichermedien der Computertechnik. Die Technologie bzw. Grundkonstruktion hat sich seit der Erfindung nicht grundlegend verändert und wird heute noch verwendet sowie optimiert. Grundsätzlich befinden sich Festplattenlaufwerke in einem Laufwerkschacht und sind über eine Schnittstelle mit der Hauptplatine verbunden. [25]

Die erste HDD wurde 1956 mit der Bezeichnung „IBM 350" im Rahmen der Ankündigung des ersten kommerziellen Computers auf Festplattenbasis durch das Unternehmen „IBM" vorgestellt. Das „IBM 350"-Laufwerk (siehe Abbildung 3) bestand aus fünfzig vertikal gestapelten und mit Eisenoxid beidseitig beschichteten Aluminiumplatten, die sich mit einem Durchmesser von 61 Zentimeter, einer maximalen Kapazität von fünf Megabyte und einer Rotationsgeschwindigkeit von 1200 Umdrehungen pro Minute drehten. [26] Für die Ausführung von Schreibe- oder Lesevorgängen wurde ein Zugriffsarm eingesetzt, der in die Zwischenräume des Plattenstapels mit einer Seilzugmechanik hineingesteuert wurde. [27, p. 15]

Abbildung 3: IBM 350 Disk Storage Unit [28]

Durch den stetigen technologischen Fortschritt kam es in den 70er Jahren zu der Einführung und Verbreitung der Computer für den individuellen persönlichen Gebrauch. [29] Aufgrund der hohen Kosten der Festplattenlaufwerke hatten Nutzer/innen eines PCs nur begrenzte Speichermöglichkeiten wie Diskettenlaufwerke oder Audiokassetten. [29] Durch die Gründung von „Seagate Technology“ wurde 1979 die erste Festplatte im 5,25-Zoll-Format gebaut, die zusätzlich mit den PCs kompatibel waren, und fand den Weg als Massenspeicher in den Massenmarkt. [29] Dies führte in den darauffolgenden Jahren zu einer rasanten Weiterentwicklung der Festplattenlaufwerke sowie der Formfaktoren, wie beispielweise die 0,85-, 1,0-, 1,8-, 2,5- und 3,5-Zoll-Formfaktoren. [26] Die gängigsten Formfaktoren für moderne Festplattenlaufwerke sind 3,5-Zoll in Desktop-Computern und 2,5-Zoll in Laptops und werden über Standardschnittstellen wie beispielsweise „SATA“ („Serial ATA“) oder „SAS“ („Serial attached SCSI“) angeschlossen. [30]

3.1.1 Physikalischer Aufbau

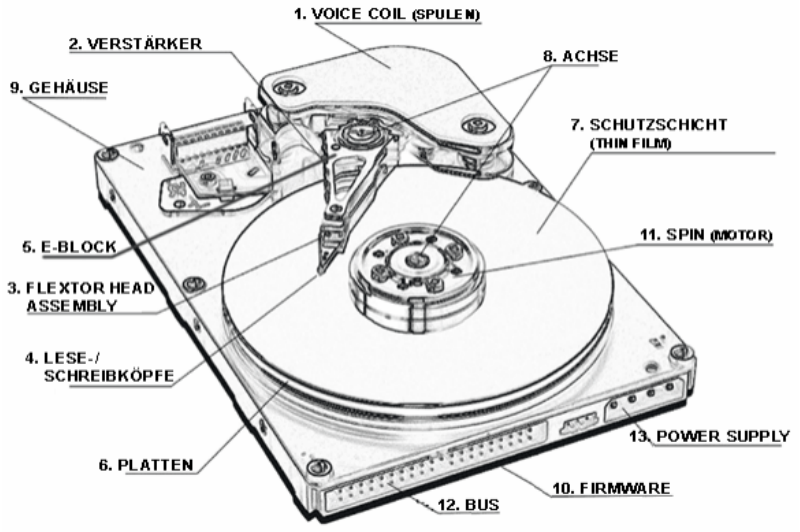


Abbildung 4: Physikalischer Aufbau einer HDD [31]

Eine HDD besteht aus den folgenden Hauptkomponenten (siehe Abbildung 4):

- Mehrere drehbare Scheiben („Platter“)
- Elektromotor für den Antrieb der Scheiben
- Bewegliche Schreib-/Leseköpfe („Heads“)
- Jeweils ein Lager für Scheiben sowie für die Schreib-/Leseköpfe (auch Magnetlager)
- Antrieb für die Schreib-/Leseköpfe
- Steuerelektronik für Motor- und Kopfsteuerung
- Hochleistungs-DSP (Digitaler Signalprozessor) für die Schreib/Leseköpfe
- Cache (2 bis 64 Megabyte)
- Schnittstellen für den Datenaustausch
- Gehäuse. [31]

Das Grundgerüst einer HDD bilden Scheiben bzw. Platten, welche aus flachen, runden und mit magnetischem Material dünn legierten Datenscheiben aus nicht-magnetisierbaren Grundmaterialen wie Glaskeramik oder Aluminium bestehen. [8, p. 447] Diese sind auf einer Achse, die mit einem Elektromotor betrieben wird, befestigt. Zusätzlich werden durch eine abschließende dünne Beschichtung aus diamantähnlichem Kohlenstoff („carbon overcoat“) mechanische Beschädigungen vermieden. [31] Die Schreib- und Leseköpfe befinden sich auf der Ober- und Unterseite der einzelnen Platten und können dabei beidseitig schreiben bzw. lesen. [8, p. 447] Durch die Montierung der Schreib-/Leseköpfe an den Armen („E-Block“), kommt es dabei immer zur gesamten Bewegung der Armkonstruktion, welche durch eine Stromzufuhr einer Spule erfolgt, die am Ende des Armes mit der Steuerelektronik befestigt ist. [31] Durch das dabei entstehende Magnetfeld wird der Arm je nach Stromrichtung des Magnetfeldes in die erforderliche Richtung angetrieben. [31] Zusätzlich kann im Rahmen eines eigenen individuellen Programms der Festplatte die Synchronisation der Köpfe gewährleistet werden. [31] Aufgrund der hohen Drehzahlgeschwindigkeiten lässt die dabei zwischen dem Kopf und der Scheibenoberfläche entstandene Luft, den Kopf einige Nanometer über der Oberfläche schweben. Dieser Effekt tritt nur bei Bewegung der Platten auf, da der Kopf sonst mit der Platte in Kontakt kommen und irreparable Beschädigungen verursachen könnte. [31]

Bei modernen Festplatten besteht aufgrund der geringen Größe der magnetischen Bereiche die Gefahr der Instabilität des magnetischen Zustandes durch thermische Effekte. [30, p. 66] Als geeignete Maßnahme werden die Platten mit zwei parallelen Magnetschichten legiert, welche durch eine Drei-Atom-Schicht aus dem nicht-magnetischen Element Ruthenium getrennt sind. Dabei werden die beiden Schichten in entgegengesetzter Richtung magnetisiert, wodurch sie sich gegenseitig verstärken. [30, p. 66] Eine weitere Maßnahme bzw. Technologie zur Überwindung thermischer Effekte ist die Senkrechtaufzeichnung, die in vielen Festplattenlaufwerken eingesetzt wird und zusätzlich eine potenziell höhere Datendichte ermöglicht. Bei „Perpendicular Magnetic Recording“, der sogenannten Senkrechtaufzeichnung, sind die Platten eines Laufwerks durch Abstandshalter voneinander getrennt und an eine rotierende Spindel geklemmt, die alle Platten gleichzeitig dreht. [30, p. 66]

Wie in Abbildung 4 dargestellt wird, befinden sich die Achsen der Festplatte bei den Scheiben sowie bei den Schreib-/Leseköpfen und bilden dabei zusammen jeweils eine Einheit. [31] Die Spindel der Festplatte, welche mit einem Motor betrieben wird, sorgt dafür, dass die Platten eine konstante Drehzahl zwischen 4.200 und 15.000 Umdrehungen pro Minute erreichen. [32] Je schneller die Spindel die Drehscheiben zum Drehen bringt, desto effizienter ist der Zugriff auf die Daten der Festplatte durch den Lese-/Schreibkopf. Die Rotationsgeschwindigkeiten variieren dabei mit der Auswahl der Festplatten sowie Schnittstellen und können beispielweise bei Hochleistungsrechner und Server durch Festplatten mit SCSI- („Small Computer System Interface“) oder SAS-Schnittstellen zwischen 10.000 und 15.000 Umdrehungen pro Minute erreichen, wobei

die Geschwindigkeiten bei 2,5-Zoll-Festplatten im Bereich von 4.200 bis 7.200 Umdrehungen pro Minute liegen. [31]

In Abbildung 5 wird dargestellt, dass schon kleinste Partikel die Oberfläche der Magnetscheiben und Schreib-/Leseköpfe beschädigen können. [33] Daher werden die Gehäuse von Festplatten mit einem feinen Filter staubdicht abgeschlossen. Zusätzlich wird durch eine kleine Öffnung und dem Einsatz eines Filters der Entstehung möglicher Temperatur- und Luftdruckschwankungen entgegengewirkt, mit dem Ziel keine irreparablen Beschädigungen auf dem Datenträger zu verursachen. [31] Im Falle eines Transportes ergibt sich bei modernen Festplatten die Möglichkeit der Nutzung der „Autopark"-Funktion, dabei werden Schreib-/Leseköpfe nach einer Trennung vom Stromnetz in einen leeren Plattenbereich sicher abgelegt und durch Magnete in dieser Position fixiert. [33]

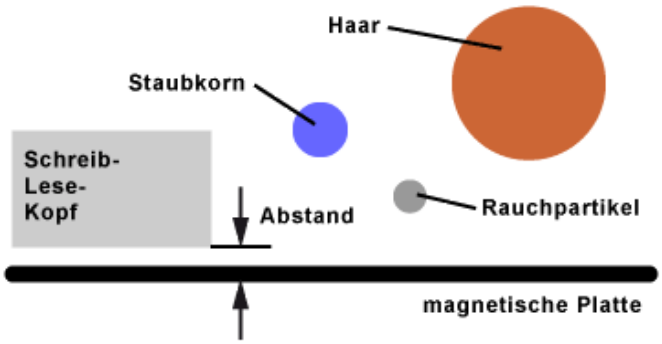


Abbildung 5: Größenvergleich der Partikel und des Abstandes zwischen Kopf und Scheibe [33]

Aufgrund der laufenden neuen Anforderungen in Bezug auf Speicherkapazität und Datentransferrate wurden Schnittstellen für Festplattenlaufwerke im Laufe der Zeit durch neue Standards abgelöst. Folgende Standards zählen zu den gängigsten Schnittstellen von Festplatten:

  - P-ATA (IDE) [34]
- Die Schnittstelle IDE („Intergrated Drive Electronics") basiert auf dem ATA-Standard und definiert die Datenübertragung zwischen verschiedenen Speichermedien über die IDE-Schnittstelle.
  - Durch die Entwicklung des EIDE-Standards („Enhandced Intergrated Drive Electronics") erhielt die neue Schnittstelle zwei Controller sowie vier Datenleitungen. Mit EIDE wurde der Anschluss der Laufwerke, wie Stecker, Kabel und elektrische Signale, definiert.
  - Mit ATA („Advanced Technology Attachment") wurde das Protokoll für den parallelen Datentransfer, bei dem durch Jumper bis zu zwei Adressen angesprochen werden können, definiert. ATA ist nach der Einführung des Nachfolgestandards Serial ATA zur Unterscheidung unter der Bezeichnung P-ATA („Parallel ATA") zusammengeführt worden. [34]
  - SATA [35]
  - „Serial ATA" ist seit 2002 der etablierte Standard für den seriellen Datentransfer von Massenspeichern. Die Vorteile gegenüber P-ATA sind schnellere Datentransfer durch höhere Signalraten, schmälere Kabel und „Hot-Swapping". (Festplattenaustausch im laufenden Betrieb) [35]
  - SCSI [36]
  - Das Protokoll „Small Computer System Interface" wird zur Steuerung der Kommunikation zwischen Massenspeicher und Controller genutzt und bietet eine parallele Datenübertragung. Mit der SCSI-Spezifikation konnte nicht nur mehrere Festplatten, sondern auch externe Geräte an einen Computer angeschlossen werden. [36]
  - SAS [36]

- „Serial Attached SCSI“ basiert auf der SCSI-Technik und ist oft noch bei Servern in Verwendung. Auch SAS bietet wie SATA, dessen Steckverbindungen ebenfalls mit SAS kompatibel sind, eine serielle Datenübertragung. [36]

3.1.2 Logischer Aufbau

Der eigentliche Informationsträger einer HDD wird als die Magnetisierung der Beschichtung der Scheiben definiert, die vom Schreib-/Lesekopf auf kreisförmigen Spuren im Zuge der Rotation der Scheibe aufgebracht wird. [31] Die Magnetscheibe besteht aus vielen einzelnen Spuren, die konzentrisch und meistens auf beiden Seiten angebracht sind. (siehe Abbildung 6) [31] Die Summe aller identischen bzw. übereinander liegenden Spuren der einzelnen Magnetscheiben wird als Zylinder bezeichnet. [37, p. 12] Jede Spur wird dabei in kleine logische Einheiten, der sogenannten „Blöcke“, unterteilt und enthalten 512 Byte an Nutzdaten bzw. Anwenderdaten., [38, p. 12]

Die Sicherstellung des korrekten Schreibens und Lesens von Informationen kann durch die Prüfsummen, die jeder Block verfügt, erreicht werden. Die Summe aller Blöcke mit den identischen Winkelkoordinaten auf den Platten wird als „Sektor“ bezeichnet. [31] Eine bestimmte feste Anzahl an zusammenhängenden bzw. physisch benachbarten Blöcken wird als „Cluster“ zusammengefasst, dabei werden durch das Betriebssystem nicht mehr einzelne Blöcke angesprochen, sondern auf dessen Ebene das Cluster als kleinste Zuordnungseinheit verwendet, wobei dieser Zusammenhang erst auf Hardwaretreiber-Ebene aufgelöst wird. [31] Die Organisation von Blöcken und Clustern kann je nach Dateisystem beispielsweise „New Technology File System“ (NTFS) oder „File Allocation Table“ (FAT) variieren. [31]

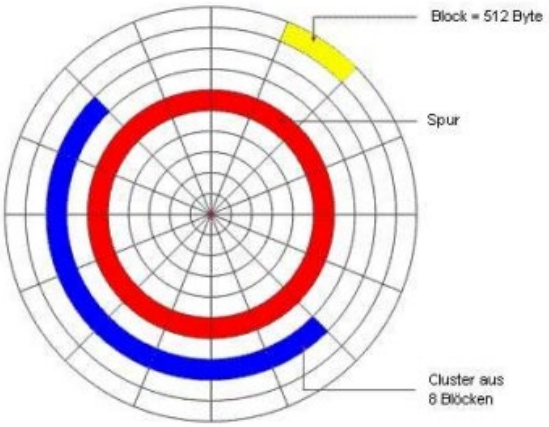


Abbildung 6: Logischer Aufbau einer Scheibe [39]

Damit Daten durch ein Betriebssystem auf einer Festplatte gespeichert werden können, ist eine Formatierung der Festplatte sowie die Erstellung einer Partition notwendig. [30] Eine Partition ist ein logisch isolierter Bereich einer Festplatte, die von Betriebs- und Dateisystemen als separate Einheit behandelt wird. [4] Der erste Sektor einer Festplatte enthält den „Master Boot Record“ (MBR), in der eine Partitionstabelle enthalten ist, welche dem Betriebssystem die Aufteilung der Festplatte mitteilt. [8, p. 450] Gemäß der Auswahl des Betriebssystems können Partitionen mit unterschiedlichen Dateisystemen formatiert werden beispielsweise gibt es unter Windows die Möglichkeit, die Dateisysteme NTFS, FAT32 oder exFAT und unter Linux die Dateisysteme ext2, ext3 oder ext4 für die Formatierung auszuwählen. [4] Ein Dateisystem ist für die Strukturierung sowie Organisierung von Daten zuständig und behält den Überblick der Speicherorte der Daten auf der physischen Festplatte. [4] Unter Windows wird die „Master-File-Table“ (MFT) als Index für die gespeicherten Dateien verwendet. [4]

Das Löschen oder Formatieren einer genutzten Partition hat dabei keinen Einfluss auf die gespeicherten Daten, da in diesem Rahmen nur die Dateizuordnungstabelle gelöscht wird und dadurch eine Wiederherstellung der Daten noch immer möglich ist. In Abbildung 7 wird dargestellt, wie die allgemeine Struktur einer Festplatte mit zwei Partitionen aufgebaut ist. [4]

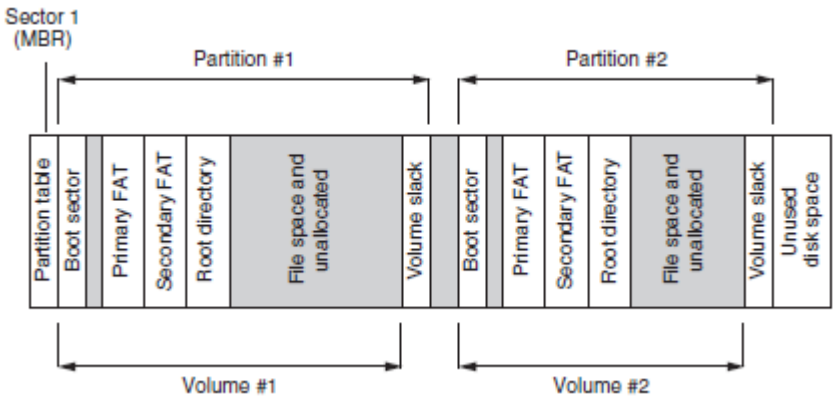


Abbildung 7: allgemeine Struktur einer Festplatte mit zwei Partitionen [8, p. 450]

3.1.3 Schreib-/Leseverfahren

Die Funktionsweise der Speicherung bei einer Festplatte beruht auf die Magnetisierung kleinster Flächen in Platten, hierzu werden die Datenscheiben beim Lesen und Schreiben an dem Schreib-/Lesekopf vorbeigeführt. [33] Die kleinste Einheit für den Lese- oder Schreibvorgang ist, wie in Abbildung 6 dargestellt, der Block, der eine Größe von 512 Bytes aufzeigt. Entsprechend der Polarität der Blöcke wird beim Schreib-/Lesevorgang ein binärer Wert angenommen. [31] Beim Schreibvorgang kommt es anhand einer stromdurchflossenen Spule, die sich am Ende des Schreib-/Lesekopfes bzw. Armes befindet, zur Entstehung eines Magnetfeldes und magnetisiert dabei die Fläche unterhalb des Kopfes auf den Scheiben. Beim Lesevorgang kommt es anhand von den kleinen magnetischen Flächen zur Erzeugung eines Magnetfeldes in der Spule des Kopfes. Dabei wird eine Spannung induziert, welche anschließend verstärkt und als Datenstrom ausgelesen wird. [33]

3.1.4 Wiederherstellung der Hardware

Festplatten haben wie alle anderen digitalen Geräte eine bestimmte Lebensdauer und können daher nicht vor der Gefahr eines Ausfalles ausgeschlossen werden. [36]

Der Ausfall einer Festplatte kann durch folgende Ursachen auftreten:

- Thermische Probleme: Der Betrieb einer Festplatte unter der falschen Temperatur.
- Head-Crash: Durch Erschütterungen im Betrieb kann der Schreib-/Lesekopf die Magnetscheibe direkt berühren und die Speicherschicht beschädigen.
- Längerer Stillstand: Schmierstoffe verlieren dabei an Konsistenz und verdicken, mögliche Blockierung der Magnetscheiben
- Ausfall der Elektronik oder des Motors [36]

Grundsätzlich sind Magnetscheiben bei Ausfällen meistens noch funktionsfähig. [4] Mit dem ordnungsmäßigen Tausch der defekten Komponenten ist somit die Wiederherstellung der Daten in der Regel möglich. [4] Daher sollen zur Vermeidung einer Inkompatibilität immer Ersatzteile vom selben Hersteller und Modell verwendet werden. [4]

3.2 SSD

Bei einer „Solid State Disk“ (SSD) handelt es sich um einen nicht-flüchtigen Datenträger der Computertechnik, welcher gegenwärtig als primäres Datenspeichersystem bzw. als Ergänzung der konventionellen Festplatten betrachtet wird. [40]

In den 1970er Jahren wurden die ersten Speicherformen basierend auf Halbleiterbausteinen entwickelt, die aufgrund ihrer hohen Kosten selten in Verwendung gewesen sind. [41] Die nächsten Implementierungen basierten hauptsächlich auf flüchtigem RAM-Speicher und benötigten daher eine konstante Stromversorgung zur Vermeidung der Verluste von Informationen. [42] Mit der Einführung der nichtflüchtigen Speichertechnologien „NAND“ („Not-And“) und „NOR“ („Not-Or“) gegen Ende der 1990er Jahren, wurde 1988 durch „Digipro“ der erste Prototyp einer Flash-basierten SSD veröffentlicht, die eine Speicherkapazität von 16 Megabyte aufwies und 1990 endgültig ausgeliefert wurden. [42] Im darauffolgenden Jahr wurde ein neuer Prototyp im 3,5-Zoll-Formfaktor von „M-Systems“ vorgestellt und ab 1995 für den kommerziellen Verkauf freigegeben. [42] Durch die stetige Weiterentwicklung der Flash-Speicher wurden schnellere Zugriffszeiten sowie ein geringer Stromverbrauch als bei magnetischen Festplatten erreicht. Dies ermöglichte den Weg in die Servertechnologie sowie im Jahr 2007 die Produktion der ersten Flash-SSDs für den Endverbrauchermarkt, die im weiteren Verlauf zu einem Wandel bzw. Trend in der Datenspeicherung geführt haben. [43]

3.2.1 Physikalischer Aufbau

Eine SSD ist ein Flash-basiertes Speichermedium, bei dem jedes seiner Bauteile auf eine Leiterplatte („PCB“) gelötet ist. Im Gegensatz zu magnetischen Festplatten beinhalten SSDs keine beweglichen Teile und verwenden ausschließlich folgende elektronische Komponenten: [44, p. 2]

- Flash-Speicher (Flash-Bausteine)
- Mikrocontroller
- Host-Interface mit Puffer-Speicher (DRAM-Speicher)
- Passive Bauelemente (beispielweise Filterkondensatoren zur Stabilisierung der Stromversorgung oder Temperatursensoren) [44, p. 3]

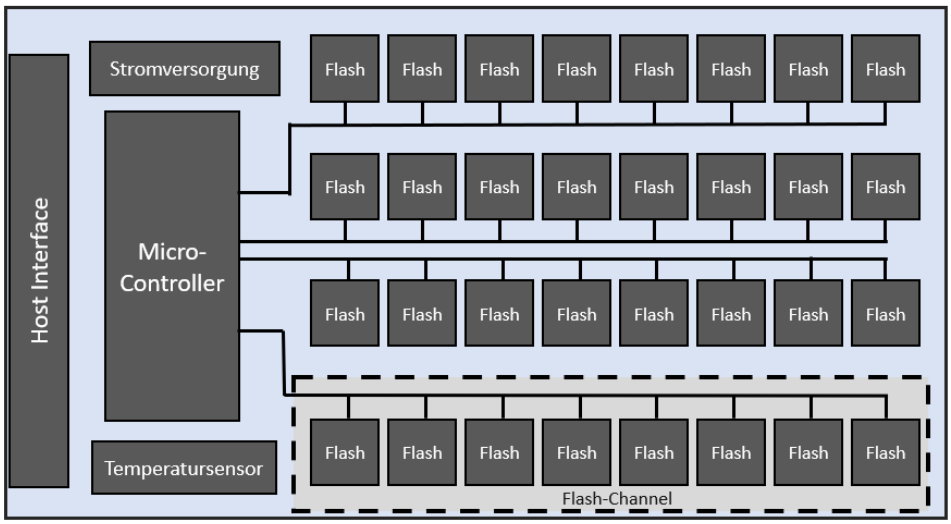


Abbildung 8: Blockschaltbild der SSD [44, p. 2]

Der Flash-Speicher bzw. Halbleiterspeicher kann in Hauptkategorien unterteilt werden, dem „Random Access Memory“ (RAM) und „Read Only Memory“ (ROM). [44, p. 3] RAM ist ein flüchtiger Speicher, der Informationen nur temporär sichert und dabei eine konstante Stromversorgung benötigt, da die Informationen ausschließlich elektrisch auf Transistoren gespeichert sind. [45] ROM ist ein nicht-flüchtiger Speicher und speichert Informationen dauerhaft auf dem Chip. [45] Durch die Verwendung von Binärcode werden Daten, ohne die Abhängigkeit einer konstanten Stromversorgung, in einzelne Zellen geschrieben, die anschließend nicht mehr verändert werden können. [45] „Non-Volatile Memories“ (NVM) liegt zwischen RAM und ROM und ist ein nicht-flüchtiger Speicher, da bei diesem Speicher das Verändern und die Erhaltung, auch bei abgeschalteter Stromversorgung, der gespeicherten Informationen möglich ist. [44, p. 3],

Entsprechend der Anordnung der Speicherzellen innerhalb des Flash-Speichers kann zwischen NAND- und NOR-Flashspeicher unterschieden werden. [44, p. 3] NAND wird aufgrund der höheren Speicherdichte und der höheren Speicherkapazität für die Massenspeicherung von Daten verwendet. [44, p. 61] Flash-basierte Massenspeicherprodukte sind beispielsweise SD-Karten, USB-Laufwerke und SSDs. [44, p. 61] Da bei NOR-Flash-Speicher eine bessere Zugriffsgeschwindigkeit möglich ist, kann es für den Programmspeicher von Mikrocontrollern bzw. als nichtflüchtiger Speicher für beispielsweise das „basic input/output system“ (BIOS) eines PCs verwendet werden. [44, p. 61]

Der „Controller“ ist ein eingebautes Verbindungselement, der die Flash-Speicherbausteine mit der Host-Schnittstelle verbindet und stellt die geeignetste Schnittstelle zwischen den beiden Seiten bereit. [44, p. 9] Eine weitere grundlegende Aufgabe des Controllers ist die effiziente Verarbeitung von Daten sowie die Maximierung der Übertragungsgeschwindigkeit, der Datenintegrität und des Informationserhalts, dabei übersetzt und überwacht der Controller die „Logical Block Addressing“ (LBA) und physikalischen Adressen der Daten im Speicher. [44, p. 8]

Für die Zwischenspeicherung von Daten wird ein schneller „Dynamic Random Access Memory“-Speicher (DRAM) auf der Platine eingesetzt. Dabei werden bei einem Schreibzugriff die Daten, vor der Übertragung zu den Flash-Speichern, im DRAM gespeichert und bringen den Vorteil, dass die Datenaktualisierung beispielsweise in Routing-Tabellen schneller erfolgen kann und der Flash-Speicher nicht abgenutzt wird. [44, p. 3] Für die Verbesserung der Leistung sind die Flash-Speicher in verschiedene Flash-Channels organisiert, welche sich auf die Anzahl der Flash-Chips beziehen, mit denen der Controller gleichzeitig kommunizieren kann. [46] Die Erhöhung der Anzahl von Flash-Kanälen bringt jedoch den Kompromiss zwischen Leistung und Energieverbrauch. [46]

In der Regel beinhalten SSDs aus verschiedenen Gründen weitere mögliche Komponenten, wie beispielsweise externe Gleichspannungswandler bzw. „DC-DC-Wandler“, um die interne Stromversorgung ableiten zu können, Filterkondensatoren zur Stabilisierung der Stromversorgung und aus Gründen der Energieverwaltung der Einsatz von Temperatursensoren. [44, p. 2]

3.2.2 NAND-Flash-Speicher

Flash-Speicher basieren wie SD-Karten, USB-Laufwerke und SSDs auf NAND-Speicher. Die Funktionsweise der Speicherzellen eines NAND-Speichers wiederum beruht auf der „Floating Gate Technology“ (siehe Abbildung 9). [44, p. 3]

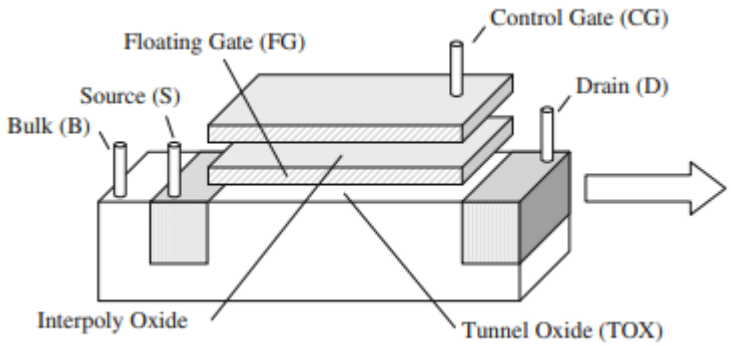


Abbildung 9: Zelle eines Flash-Speichers [44, p. 4]

Das „Floating Gate“ ist mit einer Oxidschicht gegen die Anschlüsse „Source“, „Drain“ und „Control Gate“ isoliert, um das mögliche Abfließen der Elektronen vom Control Gate abzuwenden. [44, p. 3] Durch den quantenmechanischen Tunneleffekt ist es möglich, Elektronen durch die Oxidschicht hindurch in das Floating Gate zu schieben, die sich aufgrund der Isolierung dort niederlassen und auch im spannungslosen Zustand mehrere Jahre erhalten bleiben. [44, p. 3] Dieser Vorgang des Injizierens von Elektronen auf das Floating Gate bewirkt eine Änderung der Schwellenspannung und wird als Schreibvorgang bzw. Programmierung bezeichnet. Für das Löschen der Speicherzelle wird durch das Anlegen einer hohen Spannung am Drain, das Entweihen der Elektronen zur Source sowie die Entleerung des Floating-Gates ermöglicht. [44, p. 3] Beim Lesevorgang wird die Speicherzelle mittels einer niedrigeren Spannung ausgelesen, wenn die Spannung höher ist als die Schwellenspannung der Zelle, ist die Zelle eingeschaltet (logische „0“), andernfalls ist sie ausgeschaltet (logische „1“). (siehe Abbildung 10) [44, p. 3]

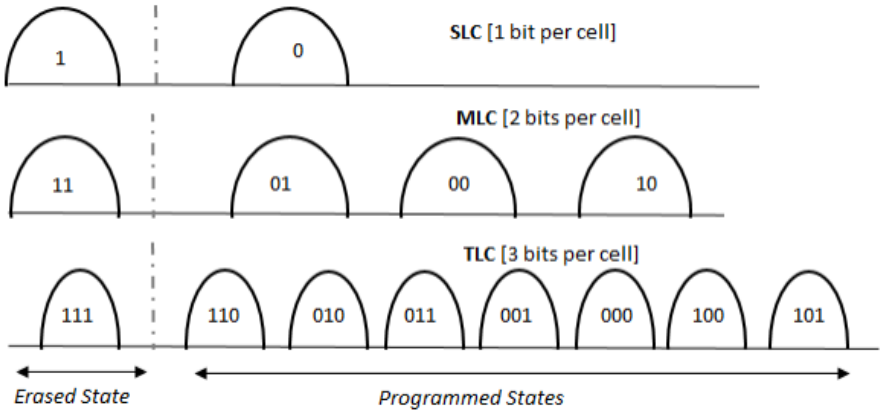


Abbildung 10: Verteilung der Schwellenspannung in SLC-, MLC-, TLC-Zellen [47]

	Zustände	Bit pro Zelle	Schreib-/Löschzyklen
SLC („Single-Level-Cell“)	2	1	bis zu 100.000
MLC („Multi-Level-Cell“)	4	2	3.000 – 10.000
TLC („Triple-Level-Cell“)	8	3	1.000
QLC („Quadruple-Level-Cell“)	16	4	1.000
PLC (“Penta-Level-Cell”) – ab 2026 [48]	32	5	10
HLC (“Hexa-Level-Cell”) – in Forschung [49]	64	6	100 – 1.000

Tabelle 4: Typen der NAND-Speicherzellen [50]

Durch die stetige Weiterentwicklung neuer NAND-Flashspeichertypen (siehe Tabelle 4), ist es möglich mehrere Ladungszustände in Speicherzellen zu nutzen. Dadurch kann eine höhere Speicherkapazität sowie Bitdichte angeboten werden, jedoch mit folgenden Nachteilen:

- Verlust der Perfomance [51]
- Fehleranfälligkeit durch die schwierige Zuordnung der Spannungsniveaus [51]
- Niedrigere Schreib- und Lesezyklen als bei SLC [51]

Bei einer NAND-Speicherzelle wird bei Schreib- und Löschvorgängen die dünne Isolierungsschicht regelmäßig strapaziert. [51] Durch die steigende Anzahl der Schreib-/Löschzyklen kommt es zu einer Verkleinerung und Verschiebung des Spannungsbereiches, dies kann zu Detektionsfehlern während der Lesevorgänge führen und einen größeren Effekt bei Speicherzellen mit mehreren Ladungszuständen haben. [51] Ein Beispiel dazu sind MLC-Speicherzellen, deren vier unterschiedliche Ladungszustände im nahezu selben Spannungsbereich wie bei SLC-NAND angesetzt sind. [51] Da der Spannungsbereich dadurch nur halb so groß ist, können die Effekte der Verkleinerung des Schreib-/Löschbereiches deutlich früher auftreten (siehe Abbildung 11). [51]

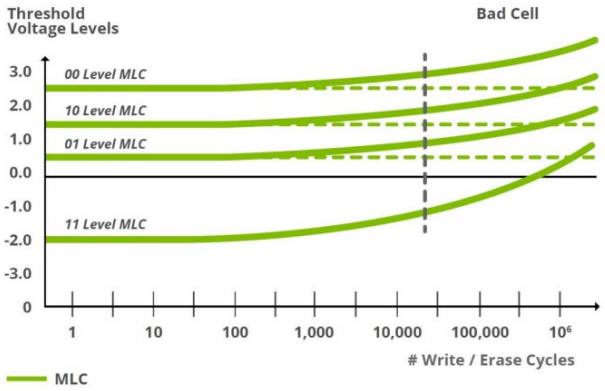


Abbildung 11: Effekt der Verkleinerung des Schreib-/Löschbereichs bei MLC-NAND [51]

Eine Alternative ist der „3D-NAND“ („V-NAND“), ein non-volatiler Flash-Speicher auf Basis der „Charge-Trapping-Technologie“, der durch die vertikale Stapelung mehrerer Schichten von Flash-Speicherzellen zu einer Art Block gestapelt ist und dabei die drei Dimensionen des Raumes nutzt. [44, p. 106] Durch vertikales Stapeln der Zellen ist eine bessere Lagerung bei geringeren Kosten sowie eine größere Zelldichte möglich, wobei hier nur die Zellschichten gestapelt werden. „Charge-Trap-Zellen“ verwenden Siliziumnitrid als Isolator und sind weniger anfällig für Defekte. [52] Schreib-/Löschzyklen benötigen eine geringere Spannung, wodurch die Oxidschicht auf den kleineren Speicherzellen dünner ausfallen kann und zu einer längeren Lebensdauer führt. [52] Eine Herausforderung bei Charge-Traps-Speicherzellen ist jedoch der Datenverlust wegen hoher Temperaturen, die durch das Einschließen und Ansammeln von Elektronen in der „Charge-Trap-Schicht“ entstehen können. [52]

Der erste 3D-NAND-Flashspeicher wurde 2013 mit 24 Schichten von „Samsung“ entwickelt. [53] Im Jahr 2022 stellte „Micron“ den „3D-Nand v6“ mit 232 Schichten vor, die Ende 2022 produziert werden sollen. [54, p. 56]

3.2.3 Architektur des NAND-Flash-Speichers

Das Grundelement eines NAND-Flash-Speichers ist der NAND-String und besteht aus 32, 64 oder 128 in Serie miteinander verbundenen Speicherzellen. [44, p. 4]

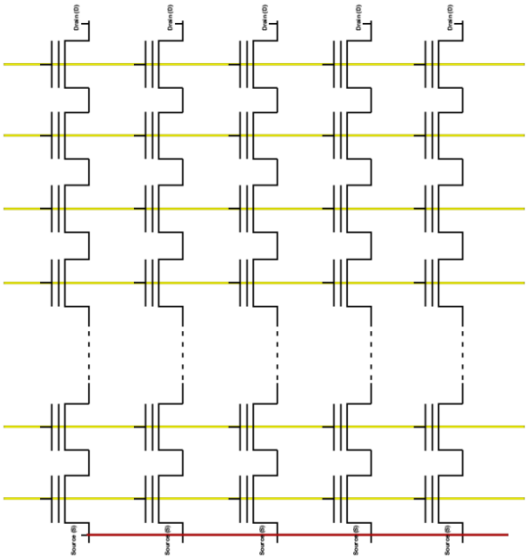


Abbildung 12: NAND-Flash-Array [55]

Um hohe Speichergrößen zu erreichen, werden NAND-String zu größeren Arrays zusammengefasst. [43] Abbildung 12 zeigt das NAND-String-Schema in wiederholter Form in einem Array, wobei mit der roten Linie die „Sources“ (S) und mit der gelben Linie die „Control Gates“ miteinander verbunden werden. [55] Durch eine gemeinsame „Source Line“ (SL) und einer „Bit Line“ (BL) werden alle Strings im Array auf der jeweiligen Seite verbunden. Die „String Select Line“ (SSL) und „Ground Select Line“ (GSL) wird mit String und Ground-Select-Transistoren zusammengeschlossen. [55] Mit dem gelb markierten Bereich auf der linken Seite in der Abbildung 13, wird eine „Page“ dargestellt, die mit einer „Word-Line“ verbunden sind. Eine Page ist die kleinste Einheit die in NAND-Flashspeichern geschrieben und gelesen werden kann. [44, p. 6] Eine zweidimensionale Matrix aus Pages und Strings wird „Block“ genannt (siehe Abbildung 13) und ist die kleinste Einheit, die gelöscht werden kann. [43]

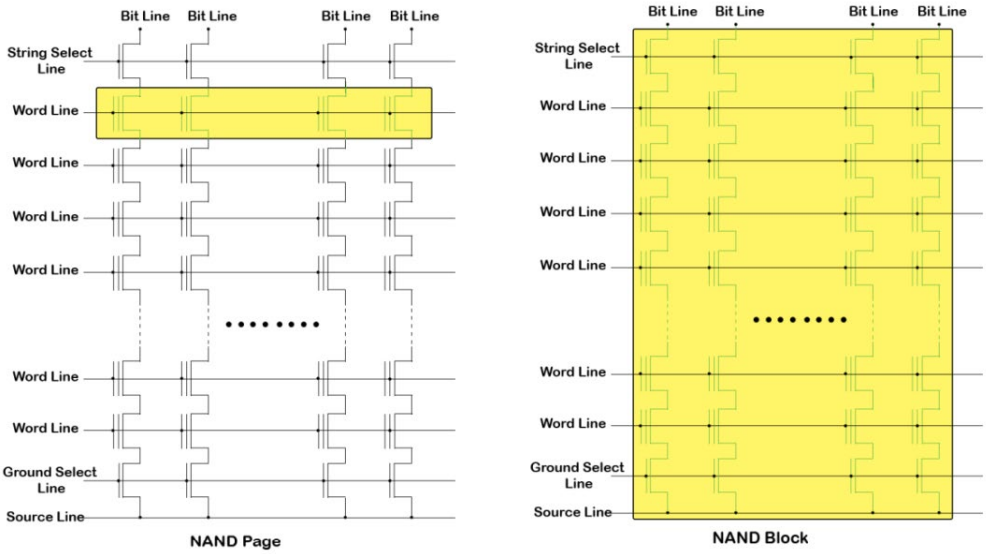


Abbildung 13: NAND-Page und NAND-Block [55]

Der NAND-Block ist ein Baustein für größere Einheiten und wird mit vielen anderen Blöcken in einer „Bank“ gruppiert (siehe Abbildung 14). [55] Diese Gruppierung bildet ein „Plane“ und dessen Anordnung ein „Die“, welches die kleinste Einheit ist, auf der unabhängig voneinander Vorgänge, wie beispielsweise Schreiben/Programmieren, Löschen und Lesen, abgearbeitet werden können. [55] Innerhalb des Dies können zeitgleiche Operationen, beispielsweise „Multi-Plane-read“ ausgeführt werden. [55]

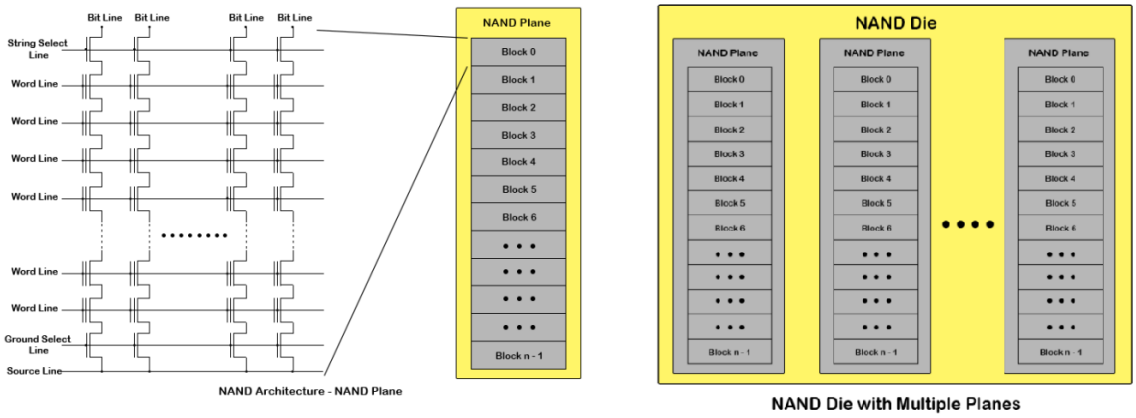


Abbildung 14: NAND-Plane und NAND-Die [55]

Wie in Abbildung 15 zu sehen ist, können NAND-Dies in ein schützendes Gehäuse bzw. Package platziert werden, beispielsweise in Form eines „Thin Small Outline Package“ (TSOP) oder eines „Ball Grid Array“ (BGA). [55] Abschließend werden mehrere TSOPs oder BGAs auf eine Leiterplatte gelötet. [43]

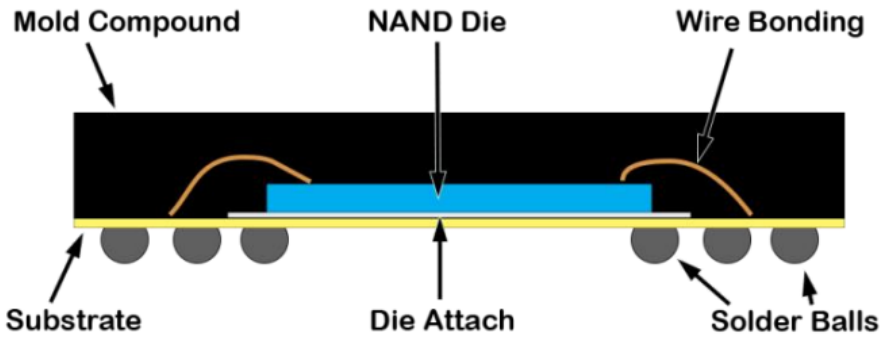


Abbildung 15: BGA-Gehäuse [55]

3.2.4 Flash-Speicher-Controller

Der Controller ist das Herzstück eines Flash-Speichers und hat grundlegende Aufgaben, wie beispielsweise als Schnittstelle zwischen Datenträger und Host dienen und die Datenverwaltung auf dem Datenträger. Der

Controller beinhaltet wichtige Komponenten, implementiert in Hardware und Software, die in folgende Bereiche unterteilt werden können (siehe Abbildung 16): [56, p. 40]

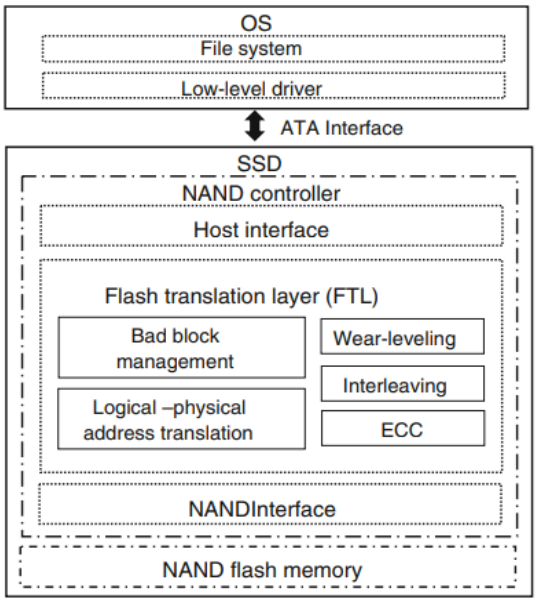


Abbildung 16: Funktionen des Flash-Speicher-Controllers [57, p. 176]

Der erste Bereich des Controllers ist die Host-Schnittstelle, die das erforderliche Standardprotokoll (SSD, SD-Karte, „CompactFlash“, USB-Sticks usw.) implementiert und in diesem Rahmen die Kommunikation zwischen dem Datenträger und dem Host gewährleistet. [56, p. 40] Ein weiterer Bereich beinhaltet das „Flash-File-System“ (FFS) bzw. Dateisystem und ist in Form von Firmware im Controller implementiert. Es befasst sich hauptsächlich mit der Aufgabe Daten transparent in bestimmte logische Blöcke zu schreiben, lesen und zu ändern. [56, p. 40] Trotz des Mangels eines Standards setzten mittlerweile viele Hersteller auf grundlegende Funktionen, wie beispielsweise „Gargabe-Collection“, „Wear-Leveling“. „Bad-Block-Management“ und „Error-Correction-Code“. [56, p. 40]

3.2.5 TRIM

TRIM ist einer der wichtigsten Funktionen für optimiertes Speichermanagement bei Flash-Speichern. Es handelt sich dabei um ein „ATA-Kommando“ und kann in verschiedenen Betriebssystemen eine unterschiedliche Bezeichnung aufweisen. [58] TRIM ist ab „Windows 7“ oder „Windows Server 2008“ standardmäßig aktiviert und kann zusätzlich mit bestimmten Befehlen in der „Windows-Eingabeaufforderung“ (CMD) wieder deaktiviert bzw. aktiviert werden. [59] Für die Verwendung von TRIM muss die Funktion vom Betriebssystem, Controller und der SSD unterstützt werden. [58]
Bei einem Löschvorgang ohne TRIM wird der Bereich, der die Daten enthält, nur als gelöscht markiert und erst bei einem weiteren Schreibvorgang endgültig entfernt. Im Gegensatz dazu wird mit TRIM durch das Betriebssystem dem Flash-Controller mitgeteilt, welche Speicherbereiche Daten enthalten, die keine Verwendung mehr finden bzw. als gelöscht markiert sind und entfernt werden können. [58] Die Garbage-Collection sorgt abschließend als Hintergrundprozess dafür, diese Speicherbereiche dauerhaft zu löschen. Der Vorteil bei TRIM liegt darin, dass bei einem Schreibvorgang auf einer Speicherzelle keine Datenblöcke zuerst gelöscht werden müssen, um neue Daten schreiben zu können. [58], [60]

TRIM kann im Windows-Betriebssystem in der CMD mit folgenden Befehlen aktiviert, deaktiviert und überprüft werden:

Für die Aktivierung von TRIM:

```
fsutil behavior set disabledeletenotify 0
```

Für die Deaktivierung von TRIM:

```
fsutil behavior set disabledeletenotify 1
```

Die Überprüfung des Ergebnisses:

```
fsutil behavior query disabledeletenotify
DisableDeleteNotify = 1 (Windows TRIM ist aktiviert)
DisableDeleteNotify = 0 (Windows TRIM ist deaktiviert)
```

TRIM unterteilt sich in der Implementierung in folgende Arten: [61]

- "Non-deterministic TRIM": Beim Lesevorgang eines „getrimmten" Blocks gibt es in dieser Methode die Möglichkeiten, dass der SSD-Controller die tatsächlichen Daten, Nullen oder einen anderen Wert zurückgibt. Hierbei kann das Ergebnis bei jedem einzelnen Lesevorgang unterschiedlich ausfallen. [61]
- „Deterministic Read After TRIM" (DRAT): In dieser Methode gibt der SSD Controller bei „getrimmten" Blöcken immer einen vordefinierten Wert zurück und kann dabei, wie in diesem Fall, nur aus Nullen bestehen und ist das häufigste Verfahren bei Endverbraucher-SSDs (Client-SSD). [61]
- „Deterministic Zeroes After TRIM" (DZAT): Hierbei werden alle Blöcke, unabhängig vom Inhalt, sofort als Nullen gelesen. Dieser Modus wird vor allem bei SSDs der „Enterprise-Ebene" verwendet, die für die Erstellung eines „SSD-RAID"1 gedacht sind. [61]

3.2.6 Garbage-Collection

Die Garbage-Collection ist eine Hardware-Funktion des Flash-Controllers, die als Hintergrundprozess die automatische Bereinigung und Wiederfreigabe der nicht benötigten Speicherbereiche für die erneute Speicherung von Daten ermöglicht. [43] Bei diesem Prozess werden aus mehreren Blöcken gültige und gelöschte Pages identifiziert und anschließend in einen freien, gelöschten Block zusammengefasst gespeichert. In diesem Zusammenhang werden gelöschte bzw. ungültige Pages als „stale" bezeichnet. Nach der Verlegung werden im Rahmen eines Löschvorganges die Blöcke der übrig gebliebenen stale-Pages bereinigt, die anschließend für neue Schreibvorgänge verwendet werden können. [43]
Ohne TRIM hat die Garbage-Collection keine Informationen über den Inhalt einzelner Pages oder Blöcke und würde somit auch Pages in neue Blöcke kopieren, die eigentlich schon gelöscht worden sind. [43] Dies zeigt auf, dass mit der TRIM-Funktion die Wirksamkeit der Garbage-Collection erheblich erhöht wird und führt zur Reduzierung der Abnutzung und der Erhöhung der Lebensdauer und Geschwindigkeit des Flash-Speichers. [43]

[1] Anordnung mehrerer Festplatten zu einer großen Festplatte.

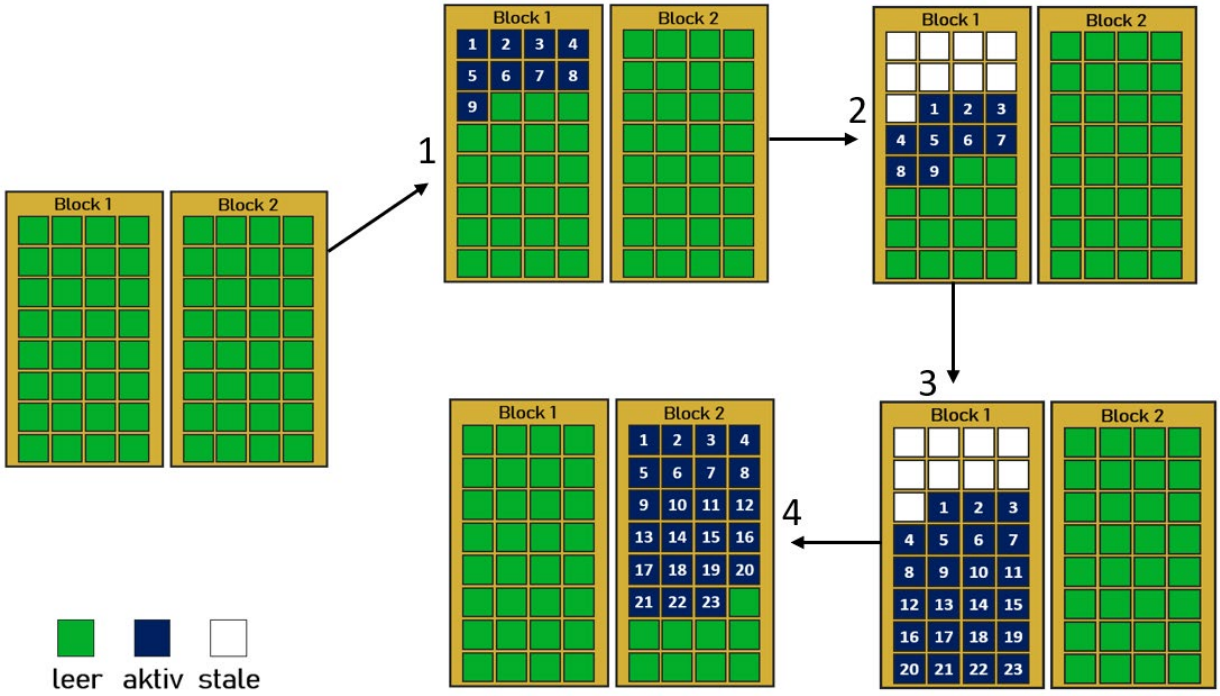


Abbildung 17: Beispiel einer Vorgehensweise der *Garbage-Collection*-Funktion [55]

Abbildung 17 zeigt einen vereinfachten Ablauf des Garbage-Collection-Prozesses mit TRIM anhand von zwei Blöcken mit jeweils 32 Pages. [55] In diesem Beispiel werden primär alle Pages in einen gelöschten bzw. leeren Zustand versetzt. Mit dem ersten Schreibvorgang wird „Block 1“ mit neun Pages an Daten befüllt (1). Sollten diese Daten geändert werden, werden die betroffenen Pages als stale hervorgehoben und die neuen Daten in die nächsten freien Pages kopiert (2). Erst mit dem Löschen des gesamten Blocks können die ungültigen Pages wieder befüllt werden. Mit der Befüllung der restlichen freien Pages des Blocks (3), ist die Durchführung weiterer Schreibvorgänge nicht mehr möglich. Für die Wiederverwendung der neun ungültigen Pages fasst die Garbage-Collection die aktiven Pages ein und kopiert sie in den leeren „Block 2“. Nach dem Kopiervorgang kann „Block 1“ gelöscht werden und anschließend wieder für neue Daten bzw. Speichervorgänge genutzt werden (4). [55]

3.2.7 Wear-Leveling

Die Speicherzellen eines Flash-basierten Datenträgers haben nur eine begrenzte Lebensdauer, die mit Schreib-/Löschzyklen gemessen werden kann. Abhängig von dem Typ der Speicherzellen (SLC, MLC, TLC, QLC, usw.) kann sich die Anzahl der Schreib-/Löschzyklen (siehe Tabelle 4) dabei variieren. [43] Jeder Schreib- und Löschvorgang führt zu einer kontinuierlichen Beschädigung bzw. einem Verschleiß der Oxid-Schicht von Speicherzellen, die die Elektronen mittels dem quantenmechanischen Tunneleffekt überwinden. Aufgrund dessen werden Schreib-/Löschzyklen mit dem Ansatz des Wear-Levelings gleichmäßig auf alle Blöcke verteilt, wobei die Verwaltung dieser Funktion durch den Flash-Controller erfolgt. [43] Dieser nutzt den Algorithmus bei der Speicherung von Daten für die Feststellung und Zuweisung des nächsten beschreibbaren physischen Blocks sowie die nachfolgende Markierung für die Entfernung ungültiger Dateneinheiten. [43] Die Protokollierung aller Schreib-/Löschzyklen wird dabei in einer Tabelle festgehalten. Infolgedessen wird eine gleichmäßige Nutzung aller physischen Blöcke ermöglicht, die zu einer Erhöhung der Lebensdauer des Speichers führt. [43]

Grundsätzlich wird zwischen statischem und dynamischen Wear-Leveling unterschieden. [44, p. 11] Der dynamische Ansatz fasst alle gelöschten Blöcke zusammen und selektiert nach niedrigster Schreib-/Löschrate. [44, p. 11] Der gewählte Block wird anschließend für den nächsten Schreibvorgang verwendet. [44, p. 11] Das Prinzip der Schreib-/Löschrate basiert auf der sorgfältigen Dokumentation des Controllers, in der jegliche Schreibvorgänge protokolliert werden. [62] Beim dynamischen Wear-Leveling ist eine gleichmäßige Auslastung nicht garantiert, da unveränderte Zellen bei diesem Prinzip nicht bewegt werden. [62] Beim statischen Wear-Leveling hingegen werden alle Blöcke nach dem Prinzip der niedrigen Schreib-/Löschrate selektiert. [62] Dabei werden Blöcke mit statischen Daten, die unter einem bestimmten Schwellenwert der Schreib-/Löschrate sind, bei Bedarf auf andere Blöcke verschoben, um den ursprünglichen Block, der eine niedrige Schreib-/Löschrate aufweist, für neue Daten bzw. Schreibvorgänge zu nutzen. [44, p. 11]

3.2.8 Bad-Block-Management

Das Modul Bad-Block-Management behandelt den Prozess der Verschiebung von „Bad-Blocks“, sogenannte fehlerhafte Blöcke, die eine oder mehrere Speicherzellen enthalten, deren Zuverlässigkeit nicht garantiert ist und anschließend mit neuen intakten Blöcken automatisch ersetzt werden. [44, p. 12] Da Flash-Speicher eine gewisse Lebensdauer haben, besteht ein konstantes Risiko eines Ausfalls von Zellen in Speicherblöcken. [63] Durch die Überwachung dieser Zellen auf starke Abnutzung wird vor einem möglichen Ausfall der ganze betroffene physikalische Block als defekt markiert und durch einen fehlerfreien Block aus dem Reservebereich ersetzt bzw. logisch zugeordnet. [63] Dies ermöglicht, ohne der Berücksichtigung physikalischer Defekte, einen transparenten und einschränkungsfreien Zugriff auf die Speicherblöcke. Dabei reduziert sich die Speicherkapazität des Datenträgers, garantiert hingegen die Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der Daten sowie die Beibehaltung der Perfomance. [44, p. 12],

Flash-Speicher beinhalten ab der Werkinitialisierung eine Karte bzw. Zuordnungstabelle (siehe Abbildung 18) mit vorhandenen Bad-Blocks, die unvermeidbar während des Herstellungsprozesses erzeugt werden. [44, p. 12] Die Zuordnungstabelle wird durch die Identifizierung von weiteren defekten Blöcken laufend bis zum Ende der Lebensdauer des Speichers bzw. bis zur Erschöpfung des Reservebereichs aktualisiert. [44, p. 12] Das Risiko der Abnutzung von Zellen wird bei SLC-Speicherzellen nicht so hoch bewertet, aufgrund dessen beträgt das Speichervolumen der Ersatzblöcke durchschnittlich 2 Prozent der Gesamtspeicherkapazität. Bei MLC-Speicherzellen hingegen werden als Reservebereich bis zu 7 Prozent der Gesamtressourcen zur Verfügung gestellt. [63]

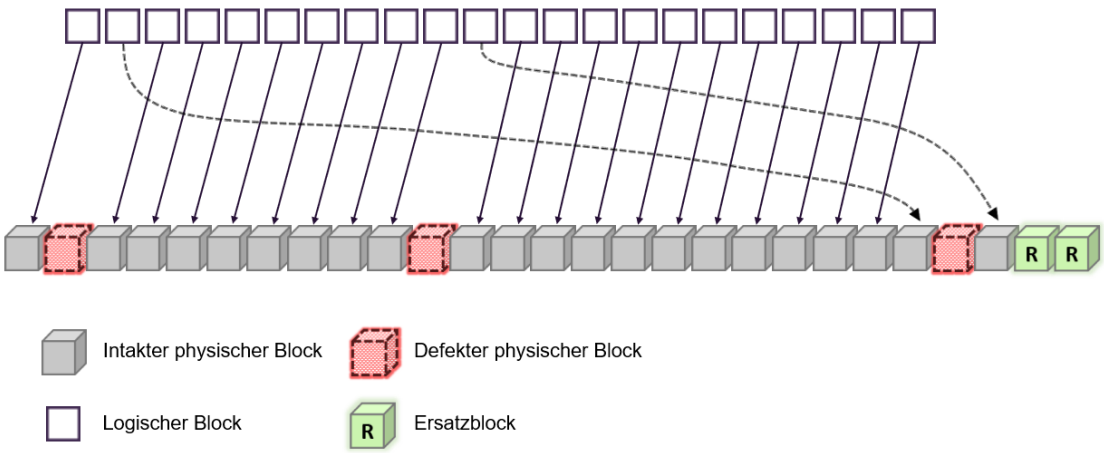


Abbildung 18: Bad-Block-Management [44, p. 12]

3.2.9 Error-Correction-Code (ECC)

Das ECC-Verfahren befasst sich zur Wahrung der Datenintegrität mit der Erkennung und Korrektur von Bitfehlern. [43] Bei Schreibvorgängen werden in jedem Block redundante Informationen bzw. zusätzliche Bits den, sogenannten „Paritätsbits“, erzeugt und mit den Daten gespeichert, um sie beim Lesevorgang mit erneut berechneten Bits vergleichen zu können. [43] Bei einer Übereinstimmung handelt es sich um intakte Daten, sollte es hingegen dabei zu einer Abweichung kommen, wird mit dem eingesetzten Verfahren versucht Fehler zu korrigieren und bei einem Misserfolg scheitert der Lesevorgang. [43] Ungeachtet davon kann ein Fehlschlag auch durch andere Ursachen ausgelöst werden, wie beispielsweise Ungenauigkeit bei der Bestimmung der Schwellspannung. [43] Je nach den verwendeten ECC-Verfahren wird eine unterschiedliche Anzahl von redundanten Bits benötigt. [56, p. 43] Mit der Weiterentwicklung von neuen Speicherzellen steigt auch die Anzahl von Bitfehlerraten, wie beispielsweise durch den Einsatz von MLC- (zwei Bits) und TLC-Speicherzellen (drei Bits). [43] Bei diesen Speicherzellen ist die Behebung von Bitfehlern komplexer, da in jedem Transistor zwei oder drei Bits gespeichert werden und daher komplexere ECC-Algorithmen zur Fehlerkorrektur implementiert werden müssen. [56, p. 43]

Folgende Algorithmen kommen bei NAND-Flash-Speicher zum Einsatz: [64]

- Hamming Codes (für Einzelbitfehler)
- Reed-Solomon-Code (für Mehrbitfehler)
- BCH-Codes (für Mehrbitfehler) [64]

3.2.10 Wiederherstellung der Hardware

Aufgrund der physikalischen Unterschiede zu einer mechanischen Festplatte ist ein erfolgreicher Wiederherstellungsprozess bei einer SSD im Rahmen eines Ausfalles von Bauteilen schwieriger als bei einer HDD. [65] Da alle Bauteile einer SSD auf einer Leiterplatte verlötet werden, ergibt sich die Möglichkeit des Entlötens der defekten Bauteile und das Löten neuer Bauteile vom gleichen Modell. [65] Je nach Typ des Flash-Speichers befinden sich auf der Leiterplatte zwei bis 20 Chips, diese einzeln neu zu verlöten sind und eine schwierige Herausforderung sein kann. [65]

Eine weitere Möglichkeit für die Datenwiederherstellung ist das Entlöten der einzelnen Speicherchips, die anschließend mit speziellen Werkzeugen ausgelesen werden. [66] Dies kann jedoch nicht bei SSDs mit mehreren Speicherchips durchgeführt werden, da bei jedem Hersteller unterschiedliche Strategien zur Adressierung der Chips, zur Durchführung der Funktionen wie beispielsweise Wear-Leveling und Garbage-Collection sowie zur Datenverwaltung, verwendet. [4] Eine Möglichkeit für eine direkten Zugriff auf ausgelötete NAND-Flash-Speicher-Mikrochips ist der „PC-3000 Flash“. [66] Laut Hersteller funktioniert die Datenwiederherstellung mittels eines Lesegeräts, selbst wenn der Controller defekt oder das Speichermedium physisch beschädigt ist. [66]

Abbildung 19: Datenwiederherstellungssystem „PC-3000 Flash“ [66]

Seit der Veröffentlichung des „Macbooks Pro’s“ im Jahre 2016 werden durch „Apple“ die SSD-Speicher direkt am Motherboard verlötet. [67] Für die Datenwiederherstellung wurde bei diesem Modell eine Schnittstelle am Motherboard verwendet, die eine Verbindung zu einem anderen „Macbook Pro“ per USB-Typ-C ermöglicht und anschließend die SSD als externen Datenträger aufzeigt. [67] Im Jahr 2018 wurde diese Schnittstelle wieder entfernt und zusätzlich eine Hardware-Verschlüsselung, unterstützt mit einem „T2-Security-Chip“[2], eingeführt. [68],

4. Related Work

Es wurde bereits eine Vielzahl an wissenschaftlichen Arbeiten zur digitalen Forensik veröffentlicht, welche sich mit den Unterschieden und Eigenschaften von SSD- und HDD-Datenträgern auseinandersetzen. Dieses Kapitel befasst sich dabei mit den Forschungen, die ähnliche Konzepte entwickelt und hinterfragt haben, um potenzielle Herausforderungen für forensische Ermittler/Ermittlerinnen im Rahmen von digital-forensischen Untersuchungen zu identifizieren.

4.1 Vergleich HDD/SSD

Der Hauptfokus in der Arbeit von Kambalapalli [69] ist ein digital-forensischer Vergleich der Datenwiederherstellung einer SSD und HDD, die durch die Verwendung von verschiedenen forensischen Tools bewertet wird. Dabei sind auch die möglichen Herausforderungen für Ermittler/Ermittlerinnen eruiert, die durch die Funktionen einer SSD in Bezug auf digital-forensische Untersuchungen entstehen können. Für das Experiment werden Daten mit unterschiedlichen Dateitypen als „Junk-Dateien“[3] genutzt, die auch mit den gesuchten Beweisdaten, bestehend aus verschiedenen Fotos mit eindeutigen Dateinamen, in verschiedenen Kombinationen mehrfach auf die Datenträger übertragen werden. Darauffolgend werden beide Datenträger formatiert und Abbilder für die anschließende Analyse erstellt. Für die Analyse wurden die forensischen Tools „FTK Toolkit“ und „Autopsy“ verwendet. Basierend auf den Ergebnissen des Experiments wird aufgezeigt, dass SSDs im Gegensatz zu HDDs das Phänomen haben kritische Beweise zerstören zu können und dies für forensische Ermittler/Ermittlerinnen zu Problemen führen kann.

Im Gegensatz dazu diskutiert Geier [4] in seiner Arbeit über die Ursachen dieser Phänomene und befasst sich dabei mit den Funktionen TRIM, Garbage-Collection und Wear-Leveling, die in SSD-Festplatten in Verwendung sind. Hierbei wird die Problematik mit zusätzlichen Speichermedien verglichen, unter anderem

[2] „Sicherheitschip“ der zweiten Generation, der für die Bereitstellung von Sicherheits- und Steuerungsfunktionen zuständig ist.
[3] Dateien, die für die Situation nicht von Nutzen sind.

HDDs, Speicherkarten und USB-Sticks. Die gesamte Speicherkapazität der Geräte wird mit einem Bild im „JPG“-Format befüllt, das durch ein eigenes Skript mehrfach dupliziert wird. Dabei beinhalten die Experimente unterschiedliche Testfälle, die unter anderem die Überprüfung mit und ohne der Funktion TRIM von SSD-Speichern aufweist. Die Resultate zeigen, dass in nahezu allen Fällen die Datenwiederherstellung von HDD-Festplatten mit über 99-Prozent und bei Speicherkarten sowie USB-Sticks mit über 95-Prozent erfolgreich durchgeführt wurden, bei SSDs hingegen mit der TRIM-Funktion die Wiederherstellungsrate bei 0- bis 5-Prozent liegt. Dies zeigt auf, dass Funktionen wie TRIM sich erheblich auf die Datenwiederherstellung bei SSD-Speichermedien auswirken können. Nach der Deaktivierung von TRIM ist eine Wiederherstellungsrate von 85- bis 99-Prozent möglich. Die Erkenntnis, dass unterschiedliche Ergebnisse bei der Datensicherung mit TRIM erzielt wurden, hebt in dieser Arbeit [4] hervor, dass TRIM sich erheblich auf die Datenwiederherstellung auswirkt.

Bei der wissenschaftlichen Arbeit von Kondam [16] wurde der Schwerpunkt auf die möglichen Herausforderungen durch digital-forensischer Untersuchungen von gelöschten Beweisdaten gelegt. Dabei wurden verschiedene forensischer Werkzeuge genutzt, um SSD- und HDD-Festplatten im Vergleich der Forensik zu analysieren. Für die Analyse werden Daten mit unterschiedlichen Formaten erstellt, welche die Beweisdaten eines Mordfalles darstellen sollen. Als Datenträger wird eine SSD und HDD verwendet, die in der ersten Phase mit Beweisdaten befüllt sind und anschließend in der zweiten Phase des Experiments wieder gelöscht werden. Diese Studie kommt zu dem Schluss, dass auf SSDs gelöschte Daten aufgrund der Selbstkorrosion und des deaktivierten TRIM-Befehls ausgelöscht werden, um die Lese-/Schreibgeschwindigkeit zu verbessern, was bei herkömmlichen HDDs nicht der Fall war.

4.2 Vergleich der Ergebnisse mit unterschiedlichen Tools

In der Arbeit von Kondam [16] wird m Rahmen der Analyse die Tools „Autopsy“ sowie „ProDiscover Basic“ verwendet. Das Ergebnis dieser Forschungsarbeit zeigt auf, dass Daten, die auf der HDD gelöscht wurden, vollständig wiederhergestellt werden können und auf SSD-Laufwerken mit dem forensischen Tool „Autopsy“ es nicht möglich ist. Mit „ProDiscover Basic“ hingegen wurden alle gelöschten Daten von der SSD wiederhergestellt. Die Arbeit von Geier [4] zeigt ebenfalls auf, dass durch die Verwendung unterschiedlicher Tools unterschiedliche Ergebnisse bei gleicher Vorgehensweise entstehen können. Bei der Datenwiederherstellung nach einer Formatierung der Speichermedien erwies sich das Programm „Recuva“ als einzige Lösung mit erfolgreicher Wiederherstellungsrate.

5. Experiment & Ergebnisse

Im Rahmen dieses Kapitels wird ein praktisches Experiment durchgeführt, mit dem Ziel der Beantwortung der oben genannten Forschungsfragen sowie der Überprüfung der definierten Hypothesen. Dazu wird zuerst der Aufbau des Experiments mit den Eigenschaften der Test- bzw. Beweisdaten, der verwendeten Hard- und Software näher erläutert. Darauffolgend werden die unterteilten Experimente beschrieben, die auf einer SSD, HDD, SD-Karte und einem USB-Stick durchgeführt werden und abschließend mit ihren Ergebnissen vorgestellt.

5.1 Aufbau des Experiments

5.1.1 Übersicht der Experimente

Das Ziel der folgenden 12 Experimente ist es, die Unterschiede und Eigenschaften der Speichermedien in Bezug auf die forensische Akquise und Analyse von Daten detailliert zu untersuchen:

Nr.	SSD	HDD	USB	SD	Wiederherstellung	Akquise	Leerlaufzeit	TRIM	Resident
1	☑	☑	☑	☑	Löschung	Live	-	☑	-
2	☑	☑	☑	☑	Löschung	Offline	-	☑	-
3	☑	☑	☑	☑	Löschung	Live	1 Minute	☑	-
4	☑	☑	☑	☑	Löschung	Live	1 Stunde	☑	-
5	☑	☑	☑	☑	Löschung	Live	24 Stunden	☑	-
6	☑	☑	☑	☑	Formatierung	Live	-	☑	-
7	☑	☑	☑	☑	Löschung	Live	-	☑	☑
8	☑	☑	☑	☑	Formatierung	Live	-	☑	☑
9	☑	-	-	-	Löschung	Live	-	-	-
10	☑	-	-	-	Formatierung	Live	-	-	-
11	☑	-	-	-	Löschung	Live	-	-	☑
12	☑	-	-	-	Formatierung	Live	-	-	☑

Tabelle 5: Übersicht der Testszenarien (Häkchen = Ja bzw. in Verwendung)

5.1.2 Verwendete Hardware

Für das Experiment wurde als Testsystem ein PC mit den folgenden Spezifikationen in Betracht gezogen:

Beschreibung des Systems	
Modell	HP-Omen 30L Desktop-PC
Prozessor	Ryzen 9 3900
Arbeitsspeicher	32 GB / DDR4-3200
Betriebssystem	Windows 11 Pro 64-Bit

Tabelle 6: Testsystem für das Experiment

Folgende Speichermedien wurden für die Experimente ausgewählt:

Art	Beschreibung	Speicherkapazität	Dateisystem
SSD	Intenso 2,5" SSD SATA III TOP	128 GB	NTFS
HDD	Western Digital WD3200LPVX	320 GB	NTFS
USB	SanDisk Ultra Fit	32 GB	NTFS
SD-Karte	Samsung EVO Plus	128 GB	NTFS

Tabelle 7: Speichermedien des Experiments

Die SSD wird per SATA-Kabel angeschlossen, da bei Verbindungen über USB-Adapter nicht die Funktionalität von TRIM gewährleistet werden kann. Als Dateisystem wird bei allen Datenträgern NTFS verwendet.

5.1.3 Testdaten des Experiments

Für die einzelnen Testfälle werden die Laufwerke mit Beweisdaten ausgelegt, dabei werden bei alle Testszenarien die zu prüfenden Speichermedien mit 50 Prozent und anschließend mit 100 Prozent der Speicherkapazität ausgelastet. Als Beweisdaten werden bestimmte Dateitypen verwendet, um eine einfache Erkennung durch forensische Programme die Überprüfung von intakten Daten zu gewährleisten. Folgende Dateitypen werden für die Experimente verwendet:

- Word-Dokument
- Bild im JPG-Format (siehe Abbildung 20)
- Text-Datei
- Residente Text-Datei

Eine Datei ist resident, wenn alle ihre Informationen und die vollständigen Daten der Datei nur in der MFT- untergebracht sind. Hierbei wird kein Speicherplatz auf dem Datenträger belegt (siehe Abbildung 21). [70] MFT ist die Zuordnungstabelle des Dateisystems NTFS und ist zuständig für die Verknüpfung von logischen Speicheradressen von Dateien mit deren physikalischen Speicherort auf dem Datenträger. [70] Das MFT-Attribut „$80“ beinhaltet die Informationen zum Inhalt einer Datei, sollte diese kleiner als 512 Bytes sein befindet sich die residente Datei gänzlich in diesem Attribut und verbraucht keinen weiteren Speicher als dieser Eintrag selbst. [70]

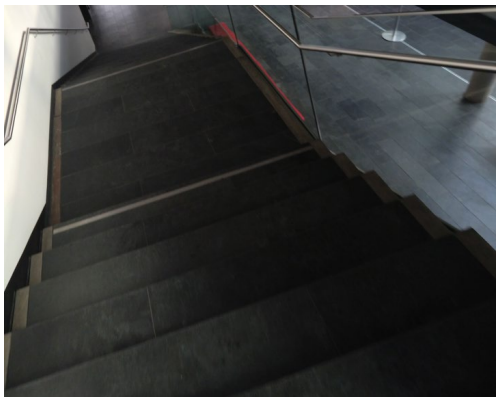


Abbildung 20: Bild-Datei des Experiments

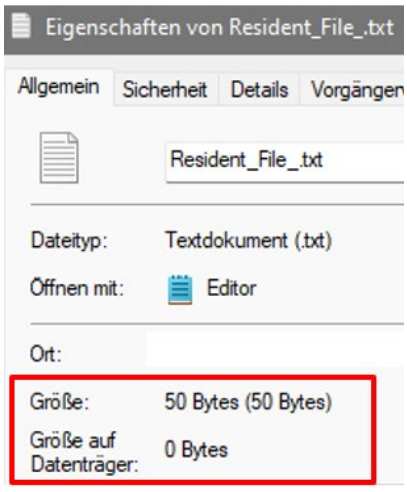


Abbildung 21: Beispiel – residente Datei

Datenablegung

Die zu testenden Datenträger werden jeweils mit 50 Prozent und 100 Prozent befüllt. Hierbei wird im Rahmen der Experimente in folgende Kategorien unterteilt:

- Beweisdaten (Word-Dokumente, Bild- und Text-Dateien)
- Residente Beweisdaten (Text-Dateien)

Bei diesen Daten handelt es sich um einzelne Dateien, die mehrfach dupliziert werden, bis die Speicherkapazität zu 50- (siehe Abbildung 22) oder zu 100-Prozent (siehe Abbildung 23) befüllt ist. Die gleiche Methodik wird im Rahmen der Datenablegung bei der HDD, SD-Karte und beim USB-Stick, entsprechend der Speicherkapazität angepasst, ebenfalls angewendet.

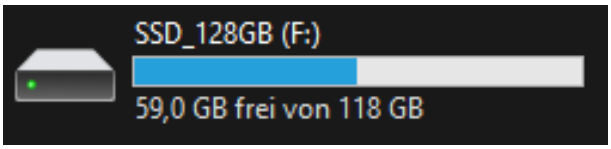


Abbildung 22: 50-Prozent Speicherauslastung SSD

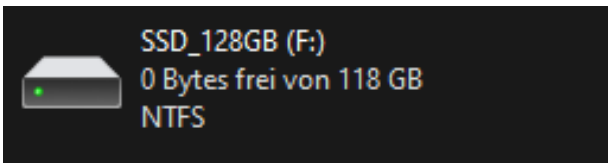


Abbildung 23: 100-Prozent Speicherauslastung SSD

5.1.4 Verwendete Software

Für die Durchführung des Experiments werden Programme ausgewählt, die Open-Source als auch kostenpflichtig sind.

FTK Imager (Version 4.7.1.2)

Für das Erstellen von Sicherungskopien der Speichermedien für die Experimente wird das Tool „FTK Imager“ [71] verwendet, welches ein Teil der „Forensic Toolkit“ Software-Suite von „AccessData“ ist und als eigenständiges Programm für das Erstellen von Sicherungskopien der Datenträger genutzt wird. Diese werden im weiteren Verlauf für die spätere Rekonstruktion verwendet und können die Übereinstimmung der Integrität der gesicherten Daten mit dem Abbild, durch die Erstellung von Prüfsummen überprüfen.

Erstellung einer Sicherungskopie mit FTK Imager

Gemäß dem Experiment wird nach einer Datenlöschung oder einer Formatierung eine Sicherungskopie des Datenträgers erstellt. Wie in Abbildung 24 aufgezeigt wird, startet der Prozess der Erstellung einer Sicherungskopie mit der Option „Create Disk Image…“ unter dem Menüpunkt „Datei“ (siehe Abbildung 25).

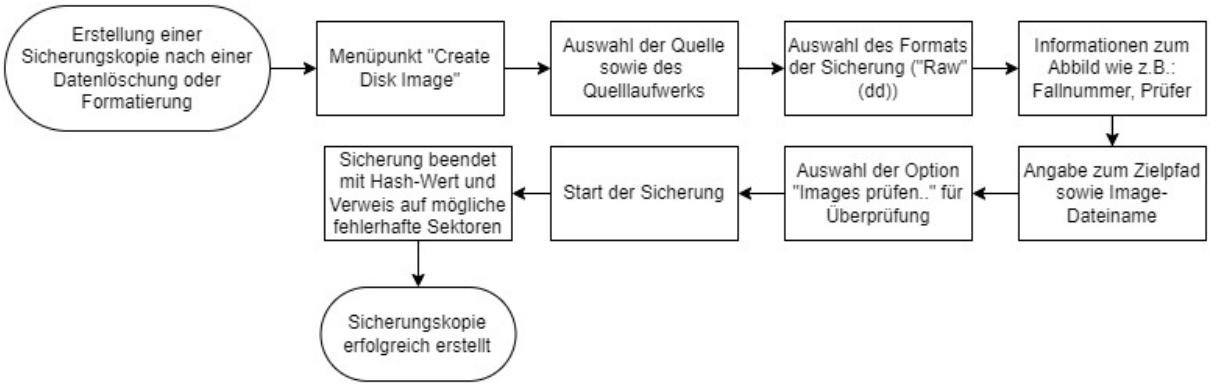


Abbildung 24: Prozess der Erstellung einer Sicherungskopie in „FTK Imager“

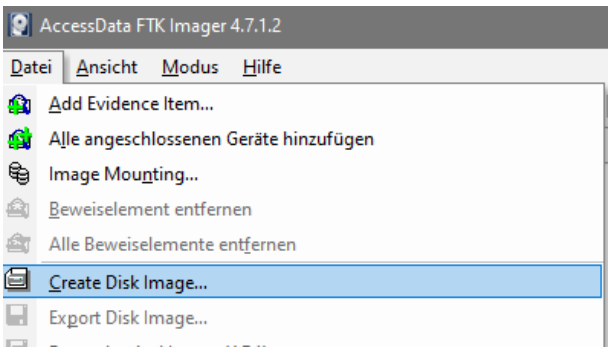


Abbildung 25: „FTK-Imager“ – Option „Create Disk Image“

Darauffolgend wird im weiteren Verlauf des Prozesses die Quelle sowie das Quelllaufwerk ausgewählt, für die eine Sicherungskopie erstellt werden soll. Das Format des zu erstellenden Abbildes wird mit dem Format „Raw (dd)“ festgelegt und anschließend weitere Details bzw. Informationen der Sicherungskopie hinzugefügt (siehe Abbildung 26).

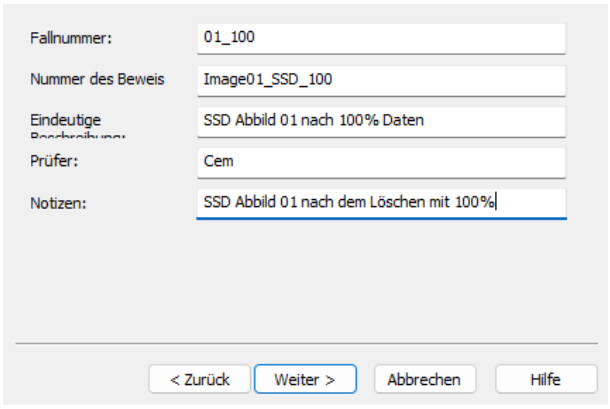


Abbildung 26: „FTK Imager“ – Eingabe von zusätzlichen Informationen für das Abbild der SSD

Wie in Abbildung 27 dargestellt wird, ist darauffolgend der Zielpfad für den Speicherort der Sicherungskopie hinzuzufügen und für die Erzeugung eines Hash-Wertes die Option „Images prüfen, …“ auszuwählen.

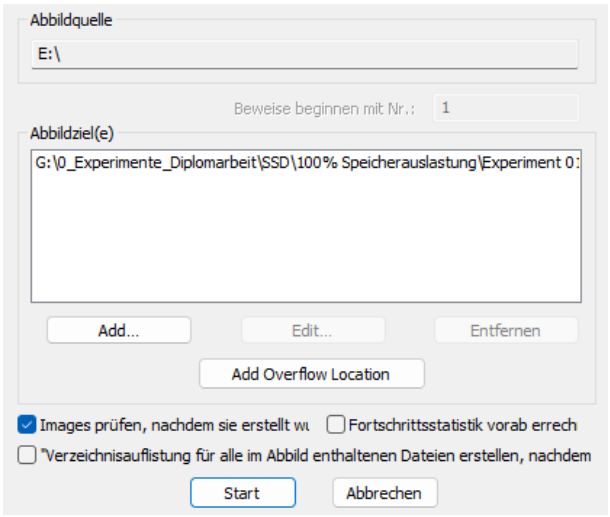


Abbildung 27: „FTK-Imager“ – Überprüfung und Start des Prozesses zur Erstellung eines Abbildes

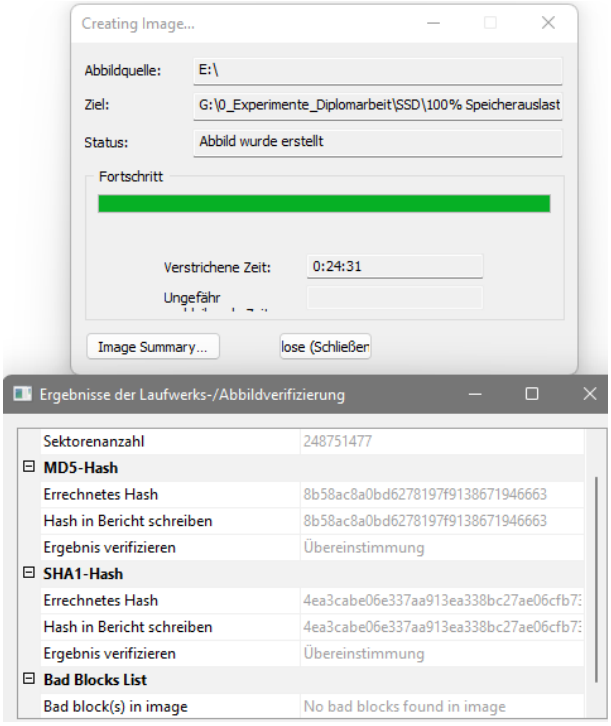


Abbildung 28: „FTK-Imager“ – Verifizierung des Abbildes der SSD

Die Dauer der Erstellung der Sicherungskopie hängt unter anderem mit der Speicherkapazität und der Art des Datenträgers zusammen. Abbildung 28 zeigt auf, dass die Sicherungskopie für den SSD-Speicher ungefähr 25 Minuten lang gedauert hat, hierbei wurde zusätzlich ein Hash-Wert generiert und auf mögliche fehlerhafte Sektoren hingewiesen. Der Prozess für die Erstellung einer Sicherungskopie endet mit diesem Schritt und wird im weiteren Verlauf von den unterschiedlichen Forensik-Programmen für die Analyse verwendet.

Für die Analyse der erstellten Sicherungskopien werden folgende Programme verwendet:

Recuva (Version 1.53.2078)

„Recuva“ [72] ist ein kostenloses Datenwiederherstellungsprogramm von „Pirisoft“. Laut Recuva werden bei einer Löschung von Daten, diese nur in der MFT von Windows als gelöscht markiert, um dem System signalisieren zu können, dass dieser Bereich wieder beschrieben werden kann. Die markierten Daten bleiben dennoch auf dem Laufwerk erhalten, bis sie mit neuen Daten überschrieben werden. [73] Zusätzlich bietet Pirisoft eine kostenpflichtige „Professional“-Version an, die unter anderem die Erstellung und Analyse von virtuellen Laufwerkabbildern mit der Dateierweiterung „.vhd“ unterstützt. Der reguläre Wiederherstellungsprozess beginnt mit der Durchsuchung des MFTs nach gelöscht markierten Daten. Desto schneller ein Laufwerk gescannt wird, desto größer sind die Chancen einer erfolgreichen Wiederherstellung, da laut Recuva MFT-Einträge für gelöschte Dateien bis zur Überschreibung mit neuen Dateneinträgen immer vollständig sein sollten. [73] Des Weiteren bietet Recuva einen Tiefenscan an, hierbei wird in diesem Prozess die MFT, nach Dateien und dem Inhalt eines Laufwerks durchsucht. Durch die Analyse jedes einzelnen Clusters (Block) des Laufwerks nach Dateikopfzeilen („file headers“), die den Beginn einer Datei anzeigen, können Dateinamen und Dateitypen erkannt werden. [73] Aufgrund dessen kann ein Tiefenscan eine lange Zeit beanspruchen, da in diesem Prozess nach einer großen Menge von möglichen Dateitypen gesucht wird. [73] Laut Recuva werden unabhängig der Auswahl der Überprüfung (Regulär oder Tiefenscan) zwei Scans durchgeführt. Der erste Scan analysiert die ausgewählte Ressource und sucht nach Dateien, die versucht werden wiederherzustellen. Der zweite Scan hingegen analysiert dann diese Dateien, um die Chancen für eine erfolgreiche Wiederherstellung bewerten zu können. [73]

Da in dem Experiment die kostenlose Version des Programms verwendet wird und hierbei keine Sicherungskopien erstellt und überprüft werden können, wird das getestete Laufwerk ohne ein Abbild direkt analysiert. Der Wiederherstellungsprozess läuft hierbei folgendermaßen ab:

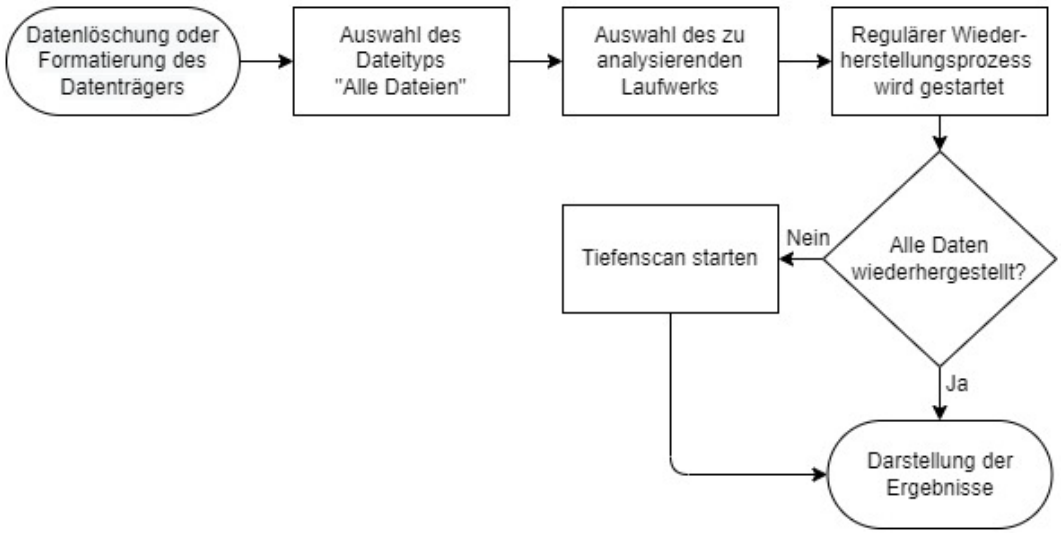


Abbildung 29: Wiederherstellungsprozess mit Recuva

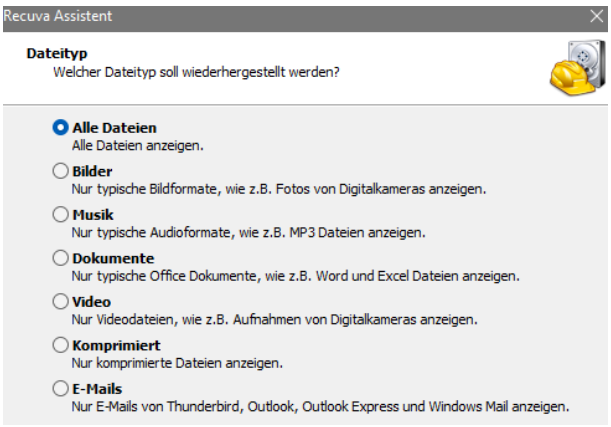


Abbildung 30: Auswahl des Dateityps in Recuva

Wie in Abbildung 29 dargestellt wird, beginnt der Wiederherstellungsprozess je nach Experiment (siehe Tabelle 5) mit einer Datenlöschung oder einer Formatierung des Datenträgers. Darauffolgend wird das Programm gestartet und der Dateityp festgelegt, hierbei wird, wie in Abbildung 30 dargestellt, die Option „Alle Dateien“ ausgewählt.

Abbildung 31: Unmarkierte Option „Tiefensuche aktivieren“ in Recuva

Nach der Auswahl des Laufwerkes für die Überprüfung wird im nächsten Schritt die Option „Tiefensuche aktivieren“ nicht ausgewählt, da primär ein regulärer Scan gestartet werden soll (siehe Abbildung 31).

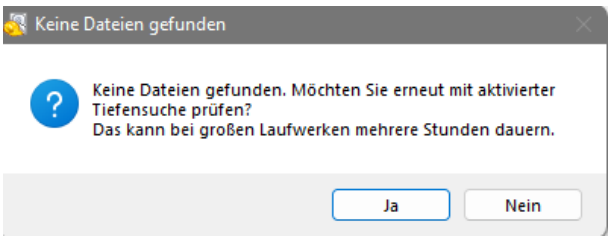


Abbildung 32: Tiefenscan wird gestartet

Sollten durch diesen Vorgang nicht alle Daten erfolgreich wiederhergestellt werden können, wird darauffolgend ein Tiefenscan gestartet, um eine erfolgreichere mögliche Rekonstruktion von Daten

gewährleisten zu können (siehe Abbildung 32). Abbildung 33 zeigt auf, dass die Ergebnisse der Daten, die laut Recuva wiederhergestellt werden können, nach einem Scan aufgelistet werden. Hierbei wird abschließend nach der Wiederherstellung der Daten der jeweiligen Experimente überprüft, ob es sich dabei um intakte Daten handelt.

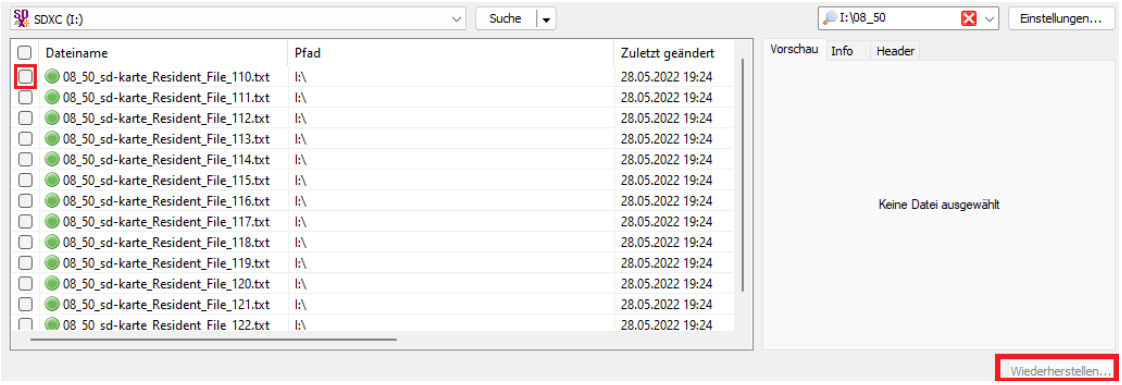


Abbildung 33: Recuva – Auflistung der Ergebnisse nach einem Scan

Autopsy (Version 4.19.3)

„Autopsy“ [74] ist eine Plattform für digital forensische Untersuchungen und grundsätzlich eine grafische Schnittstelle bzw. Benutzeroberfläche zu „The Sleuth Kit“. Die Software wird hauptsächlich für die Datenwiederherstellung verwendet und beinhaltet eine vorinstallierte Liste mit „Ingest“-Modulen, die durch Module von Drittanbietern erweitert werden können. [74] Dadurch ist eine Analyse der Daten in einer Datenquelle möglich und parsen[4] deren Inhalte im Hintergrund wie beispielsweise die Hash-Berechnung, Schlüsselwortsuche und Extraktion von Web-Artefakten. [75]

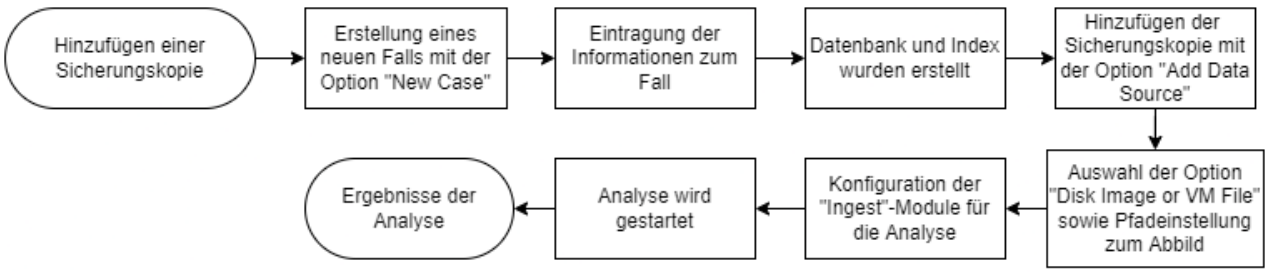


Abbildung 34: Wiederherstellungsprozess mit Autopsy

Abbildung 34 zeigt auf, wie der Wiederherstellungsprozess in den Experimenten mittels Autopsy durchgeführt wird. Im Gegensatz zu Recuva kommen hierbei die erstellten Sicherungskopien zum Einsatz und werden nach der Erstellung eines neuen Falls, der Eintragung von Informationen zum Fall (siehe Abbildung 35) und der Erstellung der Datenbank und des Indexes, mit den Optionen „Add Data Source“ und darauffolgend „Disk Image or VM File“ (siehe Abbildung 36) zum Fall hinzugefügt.

4 „Beim Parsen werden die Informationen des Dokumentes in die Elemente gefiltert, in die die Informationen strukturiert sind.“ [78]

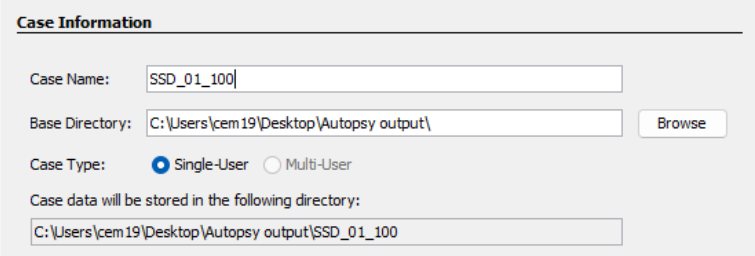


Abbildung 35: „Autopsy“ – Hinzufügen von Informationen zum neuen Fall

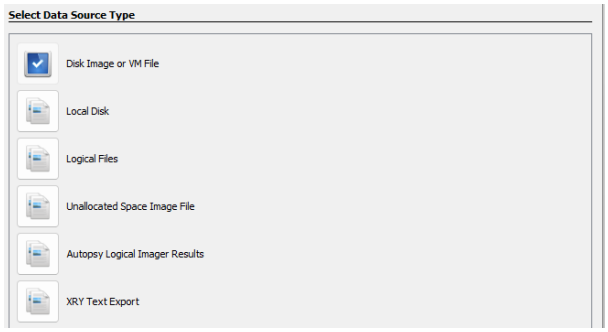


Abbildung 36: „Autopsy“ – Auswahl des Typs der Datenquelle

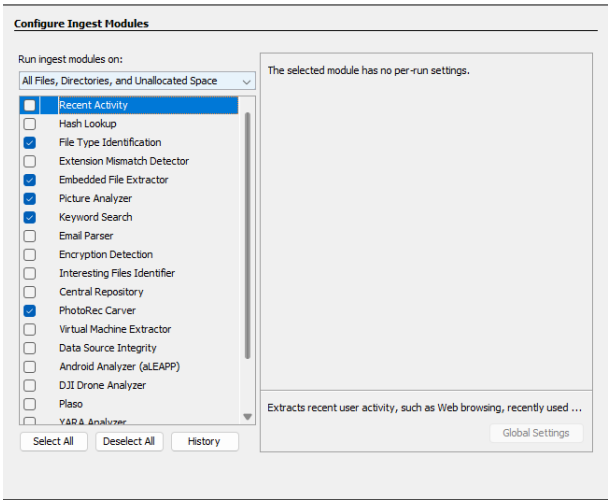


Abbildung 37: „Autopsy“ – Auswahl der Module für die Analyse

Abschließend werden überflüssige Ingest-Module herausgefiltert, die für die Analyse nicht benötigt werden. Wie in Abbildung 37 dargestellt wird wurden folgende Module für die Analyse ausgewählt:

- “File Type Identification”-Modul [76]: Das Modul identifiziert Dateien auf der Grundlage ihrer internen Signaturen und ist nicht auf Dateierweiterungen angewiesen. Dafür wird die „Tika-Bibliothek [77]“ verwendet, die über tausend verschiedene Dateitypen enthält und für die Testdaten des Experiments geeignet sind.
- „Embedded File Extractor“-Modul [78]: Hierbei werden Archivformate wie „ZIP“, „RAR“, „Docx“ usw. geöffnet, um alle Daten auf einem System analysieren zu können und ermöglicht dabei die Schlüsselwort- und Hash-Suche.

- „Picture Analyzer“-Modul [79]: Dieses Modul extrahiert EXIF-Informationen („Exchangeable Image File Format“) aus aufgenommen Bildern, welche Geolokalisierungsdaten, Zeit, Datum sowie das verwendete Kameramodell usw. enthalten können.
- „PhotoRec Carver“ [80]: Hierbei werden Dateien aus nicht zugewiesenem Speicherplatz („unallocated space“) in der Datenquelle gesammelt.
- „Keyword Search“ [81]: Das Modul erleichtert die manuelle Textsuche und extrahiert den Text aus den aufgenommenen Dateien und fügt ihn in einen „Solr-Index“ (Leistungsstarker Index Server [82]) ein, der anschließend durchsucht werden kann.

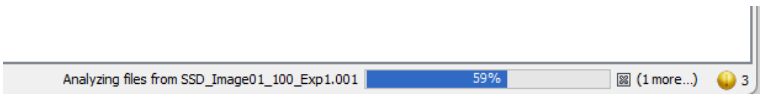


Abbildung 38: „Autopsy“ – Laufende Analyse

Darauffolgend wird die Analyse gestartet (siehe Abbildung 38) und kann je nach Größe und den Spezifikationen des Systems unterschiedlich Zeit in Anspruch nehmen, bis die Analyse abgeschlossen ist. Die Ergebnisse der Analyse (siehe Abbildung 39) werden abschließend nach der Wiederherstellung der Daten der jeweiligen Experimente überprüft und dokumentiert.

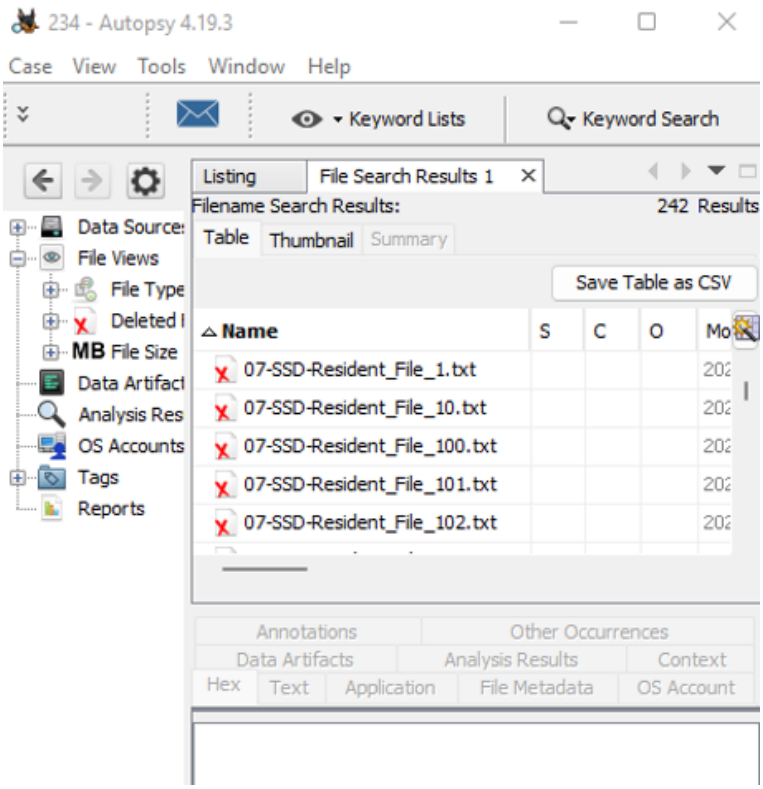


Abbildung 39: Autopsy – mögliche Ergebnisse nach einer Analyse

WinHex (Version 20.5.)

„WinHex“ ist laut dem Hersteller, die deutsche Firma „X-Ways Software Technology AG“, [83] ein universeller Hexadezimal-Editor und für die Nutzung im Bereich der Computerforensik, Datenwiederherstellung,

Datenverarbeitung und IT-Sicherheit besonders geeignet. Der Fokus liegt dabei bei der Datenwiederherstellung, die für die Experimente genutzt werden. Je nach Lizenzmodell beinhaltet das Programm unterschiedliche Funktionen und hat hierbei eigene Lizenzmodelle für polizeiliche, geheimdienstliche und privatwirtschaftliche Ermittlungen [84] sowie für forensische bzw. kriminaltechnischen Untersuchungen. [85]

Da die Software kostenpflichtig ist, wurde für das Experiment eine Testversion [83] verwendet und für die Datenwiederherstellung durch die Analyse der erstellten Sicherungskopien genutzt. Wie in Abbildung 40 dargestellt wird, beginnt der Prozess der Datenwiederherstellung nach der Erstellung bzw. mit dem Hinzufügen der Sicherungskopien.

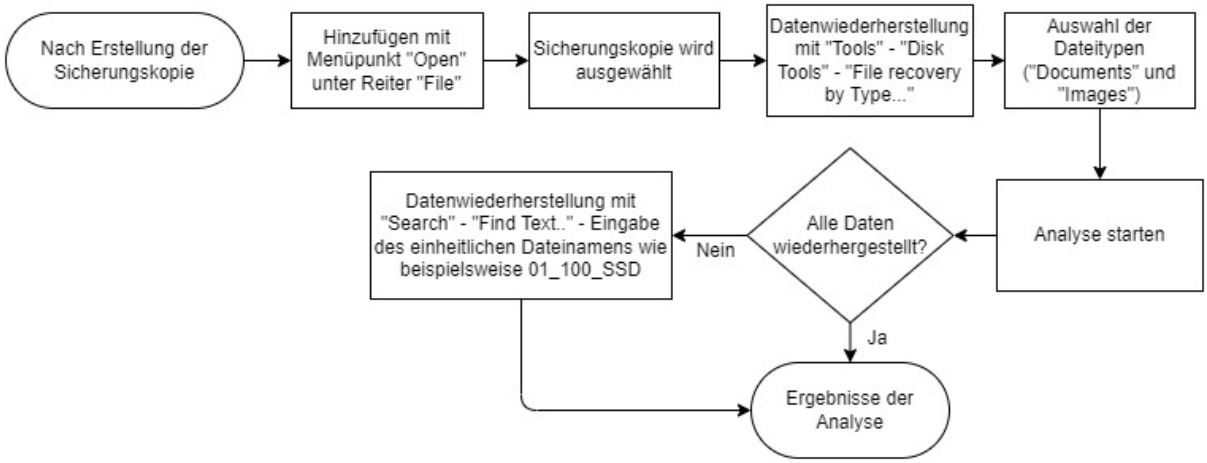


Abbildung 40: Wiederherstellungsprozess mit WinHex

Darauffolgend wird für die Datenwiederherstellung die Funktion „File recovery by Type...“ verwendet, welche sich unter dem Reiter Tools und dem weiteren Menüpunkt „Disk Tools“ befindet. Mit dieser Methode werden Dateitypen ausgewählt, die potenzielle Beweisdaten haben könnten. Zusätzlich wird ein Ausgabepfad angegeben, um alle Funde sichern zu können. Für das Experiment dieser Arbeit werden die Optionen „Pictures“ und „Documents“ ausgewählt, da die Beweisdaten aus diesen Datentypen bestehen. (siehe Abbildung 41)

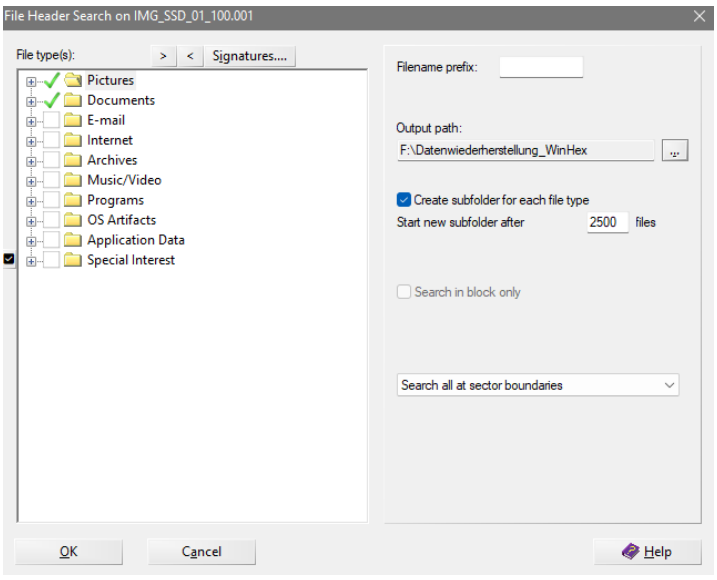


Abbildung 41: WinHex – Auswahl der Dateitypen für die Datenwiederherstellung

Anschließend wird die Analyse, wie in Abbildung 42, gestartet. Je nach Ergebnis der ersten Analyse kann eine weitere Methode für die Datenwiederherstellung verwendet werden.

Abbildung 42: WinHex – laufende Analyse

Die zweite Methode wird über den Reiter „Search“ und dem Unterpunkt „Find Text“ aufgerufen. Hierbei ist zu beachten, dass die Beweisdaten einen bestimmten Namen aufweisen müssen, um diese Methode nutzen zu können. Wie in Abbildung 43 aufgezeigt, können die Namen der Beweisdaten beispielsweise folgendes Schema haben: Die erste Zahl ist die Nummer des Experiments („01“), die mit der Speicherauslastung weitergeführt („100“) und mit der Abkürzung des Speichermediums abgeschlossen wird.

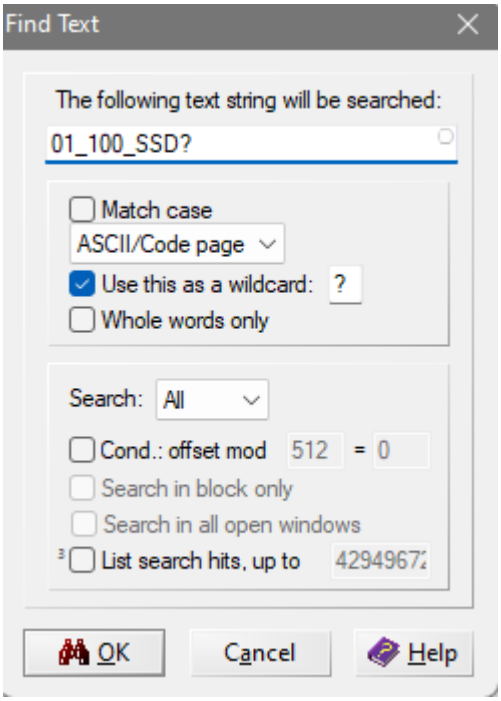


Abbildung 43: WinHex – Datenwiederherstellung über Textsuche

Abschließend werden die Ergebnisse (siehe Abbildung 44Abbildung 39) der Datenwiederherstellung der jeweiligen Experimente überprüft und sorgfältig dokumentiert.

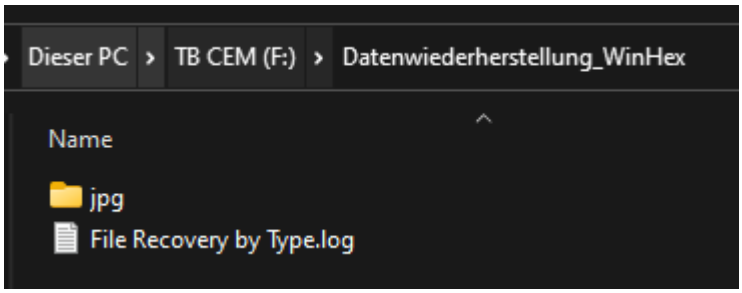


Abbildung 44: WinHex – Ergebnisse im definierten Ausgabeordner

5.2 Durchführung des Experiments

5.2.1 Experiment 1 – Wiederherstellung nach Löschung und Akquise „Live“

Das erste Beispiel des Experiments befasst sich mit der Analyse von Daten, die während eines laufenden Betriebes akquiriert werden. Diese Art der Akquise bzw. die „Live-Response-Analyse“ kann bei einer forensischen Untersuchung die einzige Möglichkeit der Entdeckung und der anschließenden Sicherung von potenziellen Beweisdaten sein. Das Ziel dieses Experiments ist es, die Unterschiede der Speichermedien zu analysieren sowie die Definition der Menge durch die Wiederherstellung von gelöschten Beweisdaten. Hierbei liegt der Fokus auf Flash-Speicher, um eventuelle Differenzen zur HDD in Bezug auf die Datenwiederherstellung erkennen zu können.

Vorgehensweise

Die Vorgehensweise in diesem Fallbeispiel (siehe Abbildung 45) beginnt mit der Formatierung und Partitionierung der Datenträger mit dem Dateisystem NTFS. Darauffolgend werden die Speichermedien mit 50- und 100-Prozent ihrer Speicherkapazität ausgelastet. Unmittelbar nach dem Löschen der Dateien, startet der Wiederherstellungsprozess, hierbei werden die Datenträger nicht vom System getrennt. Wie erläutert, wird bei diesem Experiment der TRIM-Befehl auf der SSD aktiviert.

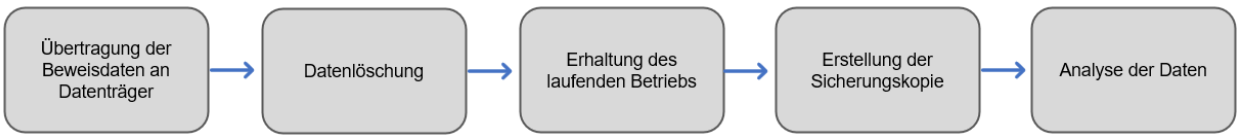


Abbildung 45: Experiment 1 – Vorgehensweise

Ergebnisse

Das Ergebnis des ersten Experiments zeigt auf, dass auf der HDD alle gelöschten Beweisdaten bei beiden Kapazitätsauslastungen erfolgreich wiederhergestellt werden konnten. Dieses Ergebnis spiegelt sich bei der SD-Karte und dem USB-Stick wider. Bei der SSD hingegen konnten keine intakten Daten wiederhergestellt werden, da diese in einem leeren Zustand waren. Dies wird durch die aktivierte TRIM-Funktion verursacht, hierbei gibt der SSD Controller bei „getrimmten“ Blöcken immer einen vordefinierten Wert zurück und kann dabei, wie in diesem Fall, nur aus Nullen (siehe Abbildung 46) bestehen. Ein wichtiger Hinweis ist die Tatsache, dass Namen bzw. Titel der Daten trotzdem sichtbar sind und im Rahmen einer forensischen Untersuchung ein potenzieller Hinweis auf Beweisdaten sein können. Aufgrund der Auslegung der Experimente auf eine erfolgreiche Datenwiederherstellung werden die „leeren“ Daten in eine eigene Spalte („Anzahl Wiederherstellung Metadaten“) in den Ergebnistabellen aufgenommen.

Datenträger	50% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten (z.B.: „leere“ Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
HDD	894	894	894	894	0	0	0
SSD	348	0	0	0	348	348	348
SD-Karte	360	360	360	360	0	0	0
USB-Stick	84	84	84	84	0	0	0

Tabelle 8: Ergebnis Experiment 1 – 50-Prozent Speicherauslastung

Datenträger	100% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten (z.B.: „leere“ Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
HDD	1797	1797	1797	1797	0	0	0
SSD	714	0	0	0	714	714	714
SD-Karte	717	717	717	717	0	0	0
USB-Stick	168	168	168	168	0	0	0

Tabelle 9: Ergebnis Experiment 1 – 100-Prozent Speicherauslastung

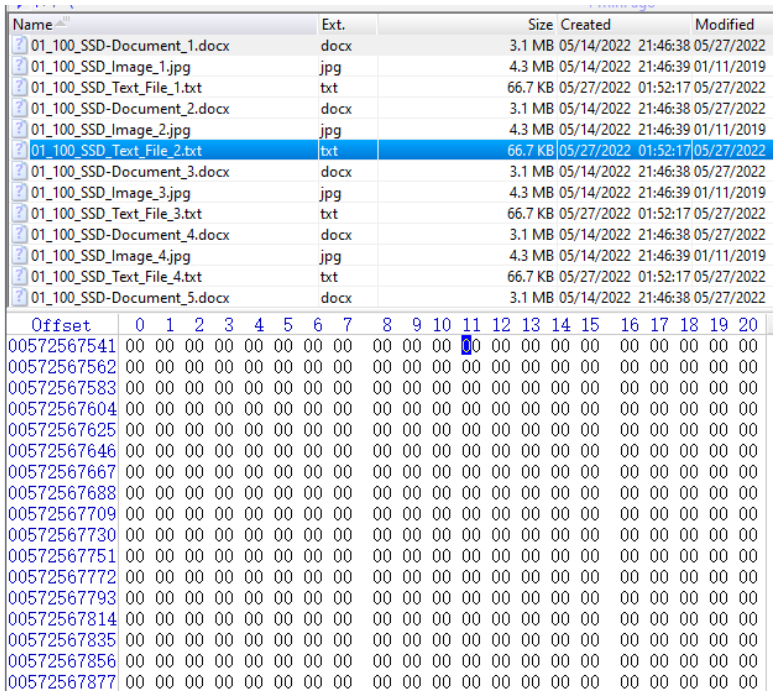


Abbildung 46: Experiment 1 – „Leere“ Daten durch TRIM

5.2.2 Experiment 2 – Wiederherstellung nach Löschung und Akquise „Offline“

Das nächste Experiment befasst sich wie im ersten Beispiel mit der Analyse von Daten, jedoch findet hierbei die Akquise im ausgeschalteten Zustand statt. Diese Art der Akquise, auch „Post-Mortem-Analyse“ genannt, wird bei forensischen Untersuchungen verwendet, wenn die zu untersuchenden Geräte nicht mehr aktiv im System laufen und ausgeschalten oder defekt sind. Der Vorteil dieses Zustandes ist die Möglichkeit der Durchführung unterschiedlicher Analyseverfahren, die simultan durchgeführt werden können.

Vorgehensweise

Die Vorgehensweise (siehe Abbildung 47) beginnt mit der Formatierung und Partitionierung der Datenträger mit dem Dateisystem NTFS. Die Speichermedien werden mit 50- oder 100-Prozent ihrer Speicherkapazität ausgelastet und anschließend vom System getrennt. Unmittelbar nach dem Löschen der Beweisdaten werden die Speichermedien vom System abgesteckt und wieder extern durch unterschiedlich Adapter ans System angeschlossen. Abschließend kann der Wiederherstellungsprozess gestartet werden, hierbei ist der TRIM-Befehl auf der SSD wieder aktiv.

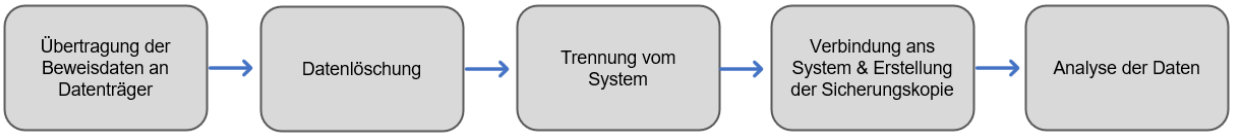


Abbildung 47: Experiment 2 – Vorgehensweise

Ergebnisse

Das Ergebnis zeigt auf, dass die Wiederherstellungsraten ident zu den Ergebnissen des ersten Experiments sind. Der Grund für das Ergebnis der SSD ist wieder die aktive TRIM-Funktion, denn die Trennung vom System hält den Datenträger nicht davon ab, den Löschvorgang abzuschließen. Nachdem ein Bereich durch den TRIM-Befehl als gelöscht markiert ist, kann der Garbage-Collection-Prozess nicht mehr verhindert werden. Bei Wiederaufnahme des Datenträgers ins System, nimmt der Prozess seine Arbeit wieder auf.

Datenträger	50% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten (z.B.: „leere“ Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
HDD	894	894	894	894	0	0	0
SSD	348	0	0	0	348	348	348
SD-Karte	360	360	360	360	0	0	0
USB-Stick	84	84	84	84	0	0	0

Tabelle 10: Ergebnis Experiment 2 – 50-Prozent Speicherauslastung

Datenträger	100% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten (z.B.: „leere“ Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
HDD	1797	1797	1797	1797	0	0	0
SSD	714	0	0	0	714	714	714
SD-Karte	717	717	717	717	0	0	0
USB-Stick	168	168	168	168	0	0	0

Tabelle 11: Ergebnis Experiment 2 – 50-Prozent Speicherauslastung

5.2.3 Experiment 3 – Wiederherstellung nach Löschung mit einer Leerlaufzeit von einer Minute

Experiment 3 basiert auf dasselbe Szenario des ersten Experiments, mit dem Unterschied, dass das System nach der Löschung für eine Minute im Leerlauf[5] belassen wird und anschließend der Wiederherstellungsprozess startet. Dadurch wird versucht einen Unterschied durch die Laufzeit im Verhalten der verschiedenen Geräte sowie die Menge an erfolgreich wiederhergestellten Dateien zu ermitteln. Das Ziel dieses Szenarios ist es festzustellen, ob eine bestimmte Leerlaufzeit, sich auf die Wiederherstellung der Daten auf Flash-Speicher sowie der HDD auswirkt.

Vorgehensweise

Die Vorgehensweise in diesem Fallbeispiel (siehe Abbildung 48) beginnt mit der Formatierung und Partitionierung der Datenträger mit dem Dateisystem NTFS. Darauffolgend werden die Speichermedien mit 50- und 100-Prozent ihrer Speicherkapazität mit Beweisdaten befüllt und für eine Minute im Leerlauf belassen. Unmittelbar nach dem Löschen der Dateien, wird der Wiederherstellungsprozess gestartet.

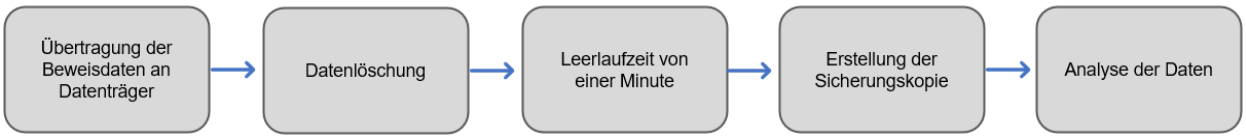


Abbildung 48: Experiment 3 – Vorgehensweise

Ergebnisse

Das Ergebnis des dritten Experiments zeigt keine Unterschiede zu den vorherigen Experimenten. Die Anzahl der wiederhergestellten Beweisdaten und Metadaten ist ebenfalls ident geblieben. Daraus lässt sich erschließen, dass durch die Leerlaufzeit von einer Minute sich keine Unterschiede bei der Wiederherstellung durch die drei Programme ermitteln lässt.

[5] Gesamtzeit, in der ein Gerät für eine bestimmte Zeitspanne eingeschaltet bleibt (mit aktiver Stromzufuhr), aber nicht benutzt wird.

Datenträger	50% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten (z.B.: „leere“ Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
HDD	894	894	894	894	0	0	0
SSD	348	0	0	0	348	348	348
SD-Karte	360	360	360	360	0	0	0
USB-Stick	84	84	84	84	0	0	0

Tabelle 12: Ergebnis Experiment 3 – 50-Prozent Speicherauslastung

Datenträger	100% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten (z.B.: „leere“ Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
HDD	1797	1797	1797	1797	0	0	0
SSD	714	0	0	0	714	714	714
SD-Karte	717	717	717	717	0	0	0
USB-Stick	168	168	168	168	0	0	0

Tabelle 13: Ergebnis Experiment 3 – 100-Prozent Speicherauslastung

5.2.4 Experiment 4 – Wiederherstellung nach Löschung - Leerlaufzeit von einer Stunde

Mit dem vierten Experiment wird die Leerlaufzeit auf eine Stunde erhöht, um zu ermitteln, ob diese Erhöhung zu einem anderen Ergebnis führt.

Vorgehensweise

Die Vorgehensweise in diesem Fallbeispiel (siehe Abbildung 49) beginnt mit der Formatierung und Partitionierung der Datenträger mit dem Dateisystem NTFS. Darauffolgend werden die Speichermedien mit 50- und 100-Prozent ihrer Speicherkapazität mit Beweisdaten befüllt und für eine Stunde im Leerlauf belassen. Unmittelbar nach dem Löschen der Dateien, wird der Wiederherstellungsprozess gestartet.

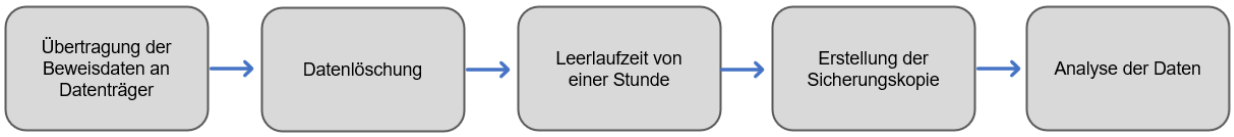


Abbildung 49: Experiment 4 – Vorgehensweise

Ergebnisse

Die Erhöhung der Leerlaufzeit auf eine Stunde bewirkt keine Unterschiede bei der Datenwiederherstellung. Gleichermaßen ist die Anzahl der „leeren“ Daten, die durch den SSD-Controller aufgrund der aktiven TRIM-Funktion zurückgegeben werden, im Vergleich zu den anderen Experimenten ident geblieben.

Datenträger	50% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten (z.B.: „leere“ Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
HDD	894	894	894	894	0	0	0
SSD	348	0	0	0	348	348	348
SD-Karte	360	360	360	360	0	0	0
USB-Stick	84	84	84	84	0	0	0

Tabelle 14: Ergebnis Experiment 4 – 50-Prozent Speicherauslastung

Datenträger	100% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten (z.B.: „leere“ Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
HDD	1797	1797	1797	1797	0	0	0
SSD	714	0	0	0	714	714	714
SD-Karte	717	717	717	717	0	0	0
USB-Stick	168	168	168	168	0	0	0

Tabelle 15: Ergebnis Experiment 4 – 100-Prozent Speicherauslastung

5.2.5 Experiment 5 – Wiederherstellung nach Löschung - Leerlaufzeit von 24 Stunden

Das fünfte Experiment wird mit der letzten Erhöhung der Leerlaufzeit mit 24 Stunden umgesetzt.

Vorgehensweise

Die Vorgehensweise beginnt mit der Formatierung und Partitionierung der Datenträger mit dem Dateisystem NTFS. Die Speichermedien werden mit Beweisdaten entsprechend befüllt und anschließend wieder gelöscht. Unmittelbar nach dem Löschen der Daten werden die Datenträger für 24 Stunden im Leerlauf belassen und der Wiederherstellungsprozess gestartet, hierbei ist der TRIM-Befehl auf der SSD aktiv. Mit folgender Abbildung wird der Prozess des fünften Experiments grafisch dargestellt:

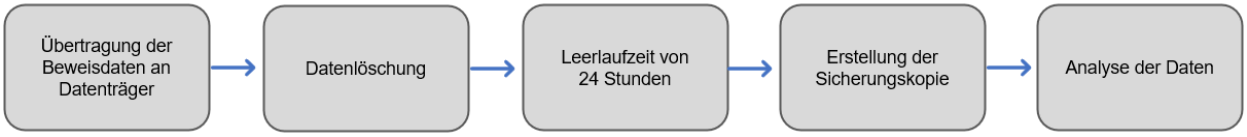


Abbildung 50: Experiment 5 – Vorgehensweise

Ergebnisse

Mit den Ergebnissen des fünften Experiments kommt hervor, dass eine Leerlaufzeit mit bis zu 24 Stunden keine Auswirkung auf die erfolgreiche Datenwiederherstellung bei den getesteten Geräten hat. Die einzige Ausnahme bilden die „leeren" Daten bzw. Metadaten der SSD, die durch die Garbage-Collection in der Leerlaufzeit teilweise entfernt wurden. Hierbei ist anzumerken, dass die Garbage-Collection durch verschiedene Hersteller unterschiedlich implementiert wird und aufgrund dessen einen eigenen Algorithmus haben kann, um leeren Daten endgültig aus dem Speicher der SSD zu löschen.

Datenträger	50% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten („leere"/defekte Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
HDD	894	894	894	894	0	0	0
SSD	348	0	0	0	305	305	305
SD-Karte	360	360	360	360	0	0	0
USB-Stick	84	84	84	84	0	0	0

Tabelle 16: Ergebnis Experiment 5 – 50-Prozent Speicherauslastung

Datenträger	100% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten („leere"/defekte Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
HDD	1797	1797	1797	1797	0	0	0
SSD	714	0	0	0	657	657	657
SD-Karte	717	717	717	717	0	0	0
USB-Stick	168	168	168	168	0	0	0

Tabelle 17: Ergebnis Experiment 5 – 100-Prozent Speicherauslastung

5.2.6 Experiment 6 – Wiederherstellung nach Formatierung

Experiment 6 befasst im Gegensatz zu den anderen Testfällen mit der Formatierung der Datenträger, mit dem Ziel der Ermittlung unterschiedlicher Ergebnisse als bei den vorherigen Experimenten.

Vorgehensweise

Die Vorgehensweise in diesem Experiment (siehe Abbildung 51) beginnt mit der Formatierung und Partitionierung der Datenträger mit dem Dateisystem NTFS. Darauffolgend werden die Speichermedien mit jeweils 50- und 100-Prozent ihrer Speicherkapazität ausgelastet. Unmittelbar nach der erneuten Formatierung der Geräte mit dem Dateisystem NTFS, startet der Wiederherstellungsprozess, hierbei werden die Datenträger für neue Erkenntnisse sorgfältig analysiert. Wie in den anderen Experimenten zuvor, ist die TRIM-Funktion auf der SSD aktiv im Einsatz.

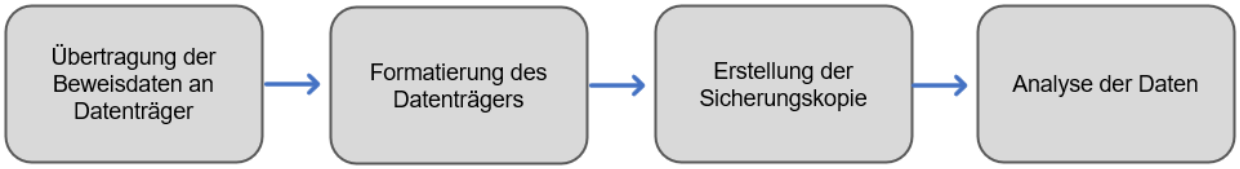


Abbildung 51: Experiment 6 – Vorgehensweise

Ergebnisse

Mit der Formatierung der Datenträger kommt es zu den ersten unterschiedlichen Ergebnissen. Bei der HDD-Festplatte konnten bei der Datenwiederherstellung mit 50-Prozent Speicherauslastung mit „Recuva“ 735 Dateien und mit „Autopsy“ 2 Dateien erfolgreich wiederhergestellt werden. Wie in Abbildung 54 dargestellt wird, hat das Tool „WinHex“ hingegen 101 Bild-Dateien wiederherstellen können, die in einem kleineren bzw. defektem Format waren. Bei 100-Prozent Speicherauslastung wurden mit „Recuva“ 1637 Dateien und mit „Autopsy“ 10 Dateien sowie zusätzlich mit „WinHex“ 156 defekte Dateien wiederhergestellt. Hierbei ist zu beachten, dass auch defekte Funde forensische Untersuchungen unterstützen können. Aufgrund dessen werden in diesem Experiment diese Rekonstruktionen in den Ergebnistabellen als „leere/defekte Daten“ kategorisiert aufgelistet. Die Ergebnisse des SSD-Speichers zeigen auf, dass nach der Formatierung keine Beweisdaten extrahiert, werden konnten. Die leeren Daten, die bei den vorherigen Experimenten akquiriert worden sind, waren in diesem Experiment nicht wiederherstellbar. Die Ergebnisse der SD-Karte (siehe Abbildung 52 und Abbildung 53) haben in diesem Experiment bei allen Tools hohe Wiederherstellungsraten erreicht, dabei konnten je nach Tool 55- bis 81 Prozent aller Daten rekonstruiert werden. Bei dem USB-Speicherlaufwerk war die Wiederherstellung mit allen forensischen Tools teilweise möglich (siehe Tabelle 18). Ähnlich zu den Ergebnissen der SD-Karte konnten hierbei 54- bis 83 Prozent der Daten wiederhergestellt werden, wobei bei 100-Prozent Speicherauslastung „Recuva“ ausschließlich 6 von 168 Dateien rekonstruieren konnte. Mit diesem Experiment sind erste unterschiedliche Ergebnisse durch die Verwendung verschiedener Tools bei gleicher Ausgangslage aufgekommen.

Datenträger	50% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten („leere“/defekte Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
HDD	894	735	2	0	0	0	101
SSD	348	0	0	0	0	0	0
SD-Karte	360	198	292	235	0	0	0
USB-Stick	84	4	47	45	0	0	0

Tabelle 18: Ergebnis Experiment 6 – 50-Prozent Speicherauslastung

Datenträger	100% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten („leere“/defekte Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
HDD	1797	1637	10	0	0	0	156
SSD	714	0	0	0	0	0	0
SD-Karte	717	555	579	495	0	0	0
USB-Stick	168	6	139	110	0	0	0

Tabelle 19: Ergebnis Experiment 6 – 100-Prozent Speicherauslastung

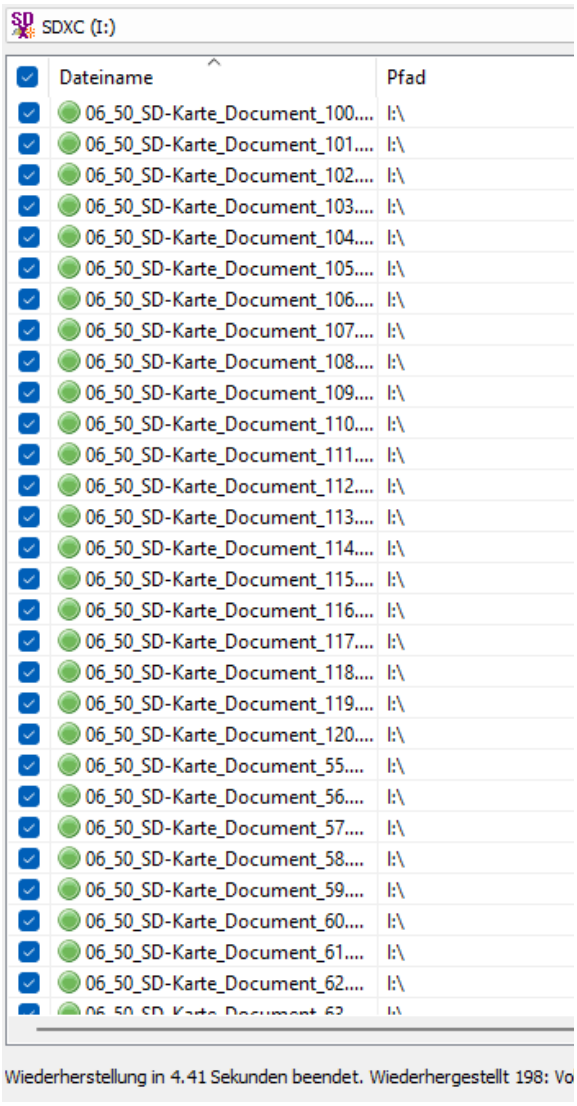


Abbildung 52: Experiment 6 – Wiederherstellung nach Formatierung – SD-Karte

Abbildung 53: Experiment 6 – Wiederherstellung nach Formatierung – SD-Karte – Teil 2

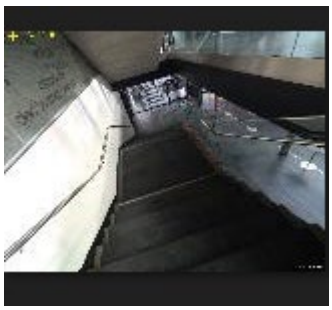


Abbildung 54: Experiment 6 – Wiederherstellung nach Formatierung mit „WinHex“ – HDD

5.2.7 Experiment 7 – Wiederherstellung nach Löschung – residente Daten

In diesem Experiment werden die Akquise und die Analyse von residenten Daten durchgeführt. Das Ziel dieses Experiments ist es, Erkenntnisse nach einer Löschung in Bezug auf die Datenwiederherstellung von residenten Daten zu erhalten. Hierbei liegt der Fokus auf der SSD, da in den vorherigen Experimenten bei der Löschung die normalen Beweisdaten nicht intakt waren bzw. leere Daten entstanden sind.

Vorgehensweise

Das Experiment beginnt mit der Formatierung und Partitionierung der Datenträger mit dem Dateisystem NTFS. Darauffolgend werden die Speichermedien mit 50- und 100-Prozent ihrer Speicherkapazität mit residenten Beweisdaten ausgelastet. Unmittelbar nach dem Löschen der Dateien, wird der Wiederherstellungsprozess gestartet (siehe Abbildung 55). Die TRIM-Funktion auf der SSD ist bei diesem Testfall aktiv im Einsatz.

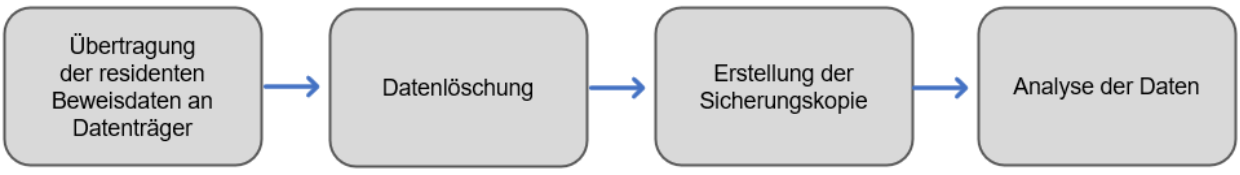


Abbildung 55: Experiment 7 – Vorgehensweise

Ergebnisse

Das Ergebnis des siebten Experiments zeigt auf, dass allen residenten Daten auf jedem Datenträger erfolgreich wiederhergestellt werden konnte. Nach einer Löschung sind residente Daten sind von der TRIM-Funktion nicht betroffen (siehe Abbildung 56), da sich der Inhalt dieser Dateien als Eintrag in der „Master File Table“ (MFT) befindet.

Datenträger	50% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten („leere“/defekte Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
HDD	305	305	305	305	0	0	0
SSD	118	118	118	118	0	0	0
SD-Karte	122	122	122	122	0	0	0
USB-Stick	29	29	29	29	0	0	0

Tabelle 20: Ergebnis Experiment 7 – 50-Prozent Speicherauslastung

Datenträger	100% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten („leere“/defekte Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
HDD	610	610	610	610	0	0	0
SSD	242	242	242	242	0	0	0
SD-Karte	244	244	244	244	0	0	0
USB-Stick	58	58	58	58	0	0	0

Tabelle 21: Ergebnis Experiment 7 – 100-Prozent Speicherauslastung

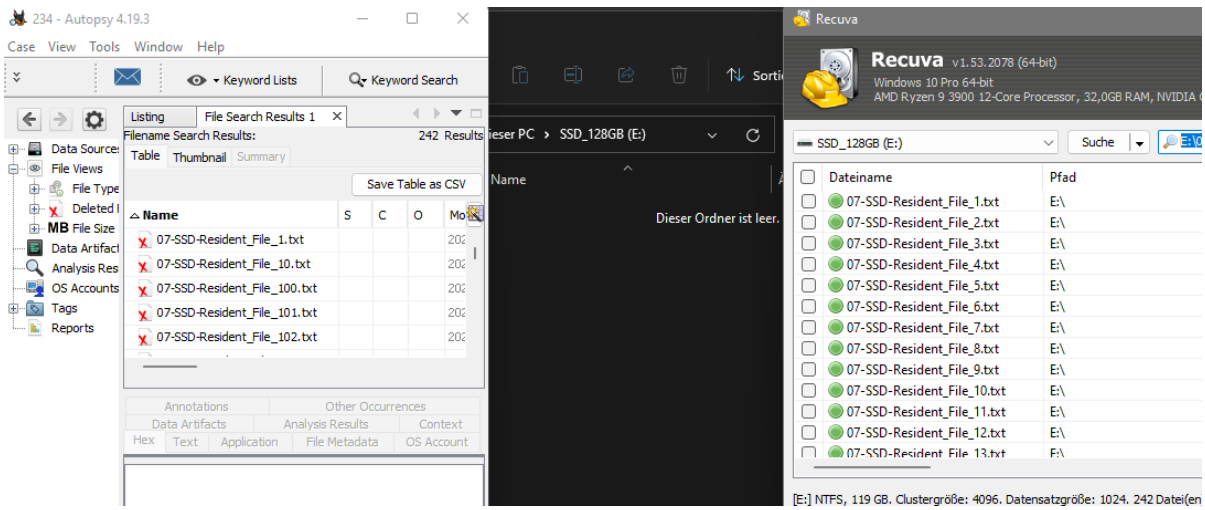


Abbildung 56: Experiment 7 – SSD – Ergebnis mit 100-Prozent Speicherauslastung

5.2.8 Experiment 8 – Wiederherstellung nach Formatierung – residente Daten

Das Ziel dieses Experiments ist es, Erkenntnisse nach einer Formatierung in Bezug auf die Datenwiederherstellung von residenten Daten zu erhalten.

Vorgehensweise

Die Vorgehensweise in diesem Experiment (siehe Abbildung 51) beginnt mit der Formatierung und Partitionierung der Datenträger mit dem Dateisystem NTFS. Darauffolgend werden die Speichermedien mit jeweils 50- und 100-Prozent ihrer Speicherkapazität mit residenten Daten ausgelastet. Unmittelbar nach der erneuten Formatierung der Geräte mit dem Dateisystem NTFS, startet der Wiederherstellungsprozess, hierbei werden die Datenträger für neue Erkenntnisse sorgfältig analysiert. Wie in den anderen Experimenten zuvor, ist die TRIM-Funktion auf der SSD aktiv im Einsatz.

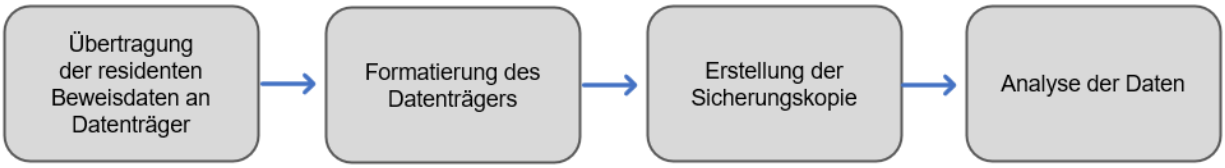


Abbildung 57: Experiment 8 – Vorgehensweise

Ergebnisse

Die Ergebnisse der Formatierung der Datenträger, die befüllt mit residenten Daten sind, zeigt auf, dass bei der HDD-Festplatte bei der Datenwiederherstellung mit „Autopsy“ und „WinHex“ bei beiden Speicherauslastungen keine intakten Daten gesichert werden konnte. Mit „Recuva“ hingegen wurden bei 50-Prozent Speicherauslastung 199 von 305 Dateien und bei 100-Prozent Speicherauslastung 504 von 610 Dateien fehlerlos wiederhergestellt. Die Ergebnisse des SSD-Speichers zeigen auf, dass nach der Formatierung keine residenten sowie leeren Daten extrahiert, werden konnten, da bei der Formatierung die „Master File Table“ überschrieben wird. Die Ergebnisse der SD-Karte haben Ähnlichkeiten zu den Ergebnissen der HDD, sowohl bei „Autopsy“ als auch bei „WinHex“ konnten keine Beweisdaten zurückgeführt werden. Wie in Tabelle 20 und Tabelle 21 dargestellt, konnten mit „Recuva“ bei 50-Prozent Speicherauslastung 13 von 122 Dateien (siehe Abbildung 58) und bei 100-Prozent Speicherauslastung 135 von 244 Dateien erfolgreich gesichert werden. Bei dem USB-Speicherlaufwerk hingegen war die Wiederherstellung bei beiden Speicherauslastungen erfolglos.

Datenträger	50% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten („leere“/defekte Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
HDD	305	199	0	0	0	0	0
SSD	118	0	0	0	0	0	0
SD-Karte	122	13	0	0	0	0	0
USB-Stick	29	0	0	0	0	0	0

Tabelle 22: Ergebnis Experiment 8 – 50-Prozent Speicherauslastung

Datenträger	100% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten („leere“/defekte Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
HDD	610	504	0	0	0	0	0
SSD	242	0	0	0	0	0	0
SD-Karte	244	135	0	0	0	0	0
USB-Stick	58	0	0	0	0	0	0

Tabelle 23: Ergebnis Experiment 8 – 100-Prozent Speicherauslastung

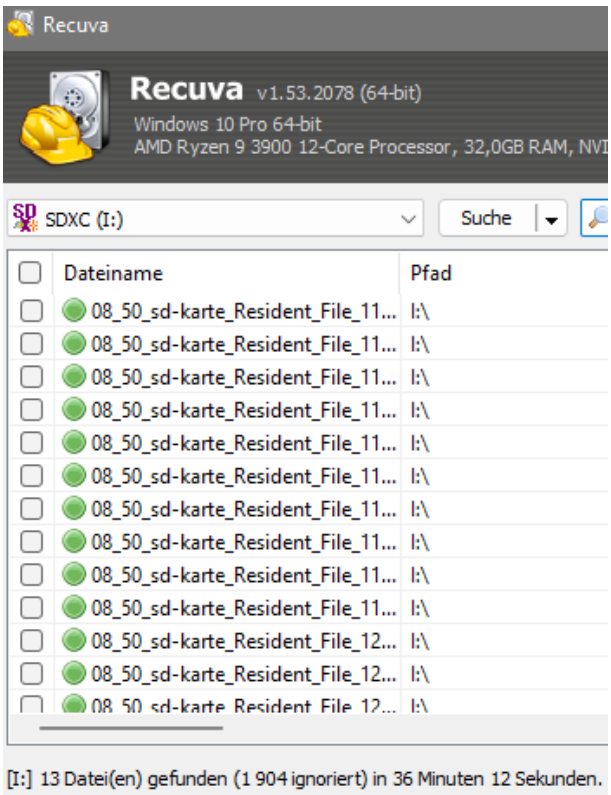


Abbildung 58: Experiment 8 – SD-Karte – 50-Prozent Speicherauslastung

5.2.9 Experiment 9 – Wiederherstellung nach Löschung – ohne TRIM

Ab dem neunten Experiment werden die Auswirkungen der TRIM-Funktion auf den Wiederherstellungsprozess von SSD-Speichermedien nach einer Löschung von Daten. Aufgrund dessen wird die TRIM-Funktion in diesem Experiment deaktiviert (siehe Abbildung 59), um dessen Einfluss auf die SSD besser zu verdeutlichen.

```
C:\WINDOWS\system32>fsutil behavior query DisableDeleteNotify
NTFS DisableDeleteNotify = 0  (TRIM-Vorgänge dürfen an Speichergeräte gesendet werden)
ReFS DisableDeleteNotify = 0  (TRIM-Vorgänge dürfen an Speichergeräte gesendet werden)

C:\WINDOWS\system32>fsutil behavior set DisableDeleteNotify NTFS 1
NTFS DisableDeleteNotify = 1  (TRIM-Vorgänge dürfen nicht an Speichergeräte gesendet werden)

Dieser Vorgang wird sofort wirksam (kein Neustart erforderlich)
```

Abbildung 59: Experiment 9 – Deaktivierung der TRIM-Funktion

Vorgehensweise

Wie in Abbildung 60 dargestellt wird, beginnt die Vorgehensweise mit der Formatierung und Partitionierung der SSD mit dem Dateisystem NTFS und wird mit 50- oder 100-Prozent der Speicherkapazität ausgelastet. Unmittelbar nach und der Löschung der Beweisdaten und der Erstellung der Sicherungskopien kann die Analyse gestartet werden, zusätzlich dazu ist die TRIM-Funktion auf der SSD deaktiviert.

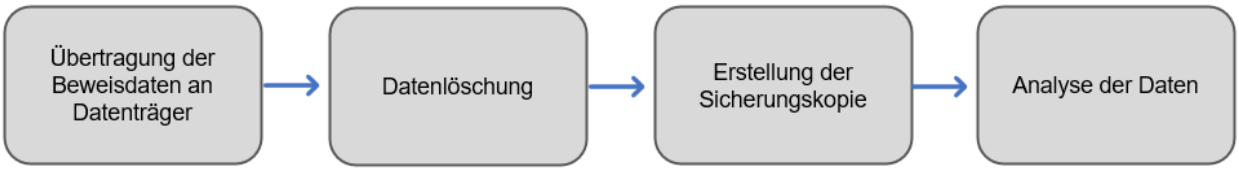


Abbildung 60: Experiment 9 – Vorgehensweise

Ergebnisse

Das Ergebnis des Experiments zeigt auf, dass auf der SSD alle gelöschten Beweisdaten bei beiden Kapazitätsauslastungen erfolgreich wiederhergestellt werden konnten und die Deaktivierung der TRIM-Funktion ein großer Faktor für die Datenwiederherstellung ist.

Datenträger	50% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten („leere“/defekte Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
SSD	348	348	348	348	0	0	0

Tabelle 24: Ergebnis Experiment 9 – 50-Prozent Speicherauslastung

Datenträger	100% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten („leere“/defekte Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
SSD	714	714	714	714	0	0	0

Tabelle 25: Ergebnis Experiment 9 – 100-Prozent Speicherauslastung

5.2.10 Experiment 10 – Wiederherstellung nach Formatierung – ohne TRIM

Dieses Experiment testet die Auswirkungen der TRIM-Funktion auf den Wiederherstellungsprozess von SSD-Speichermedien nach einer Formatierung.

Vorgehensweise

Die Vorgehensweise des Experiments (siehe Abbildung 61) beginnt mit der Formatierung und Partitionierung der SSD mit dem Dateisystem NTFS und wird mit 50- oder 100-Prozent der Speicherkapazität ausgelastet. Unmittelbar nach und der Formatierung des Datenträgers und der Erstellung der Sicherungskopien kann die Analyse gestartet werden, zusätzlich dazu ist die TRIM-Funktion auf der SSD deaktiviert.

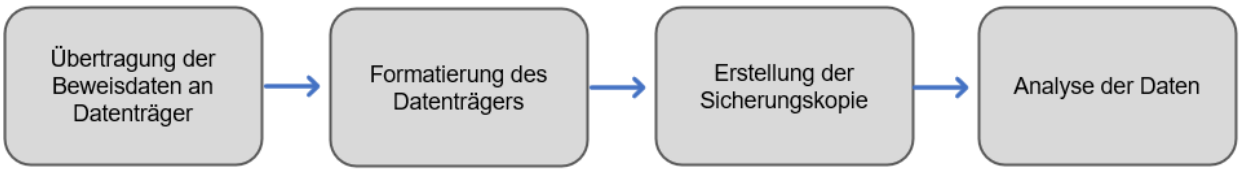


Abbildung 61: Experiment 10 – Vorgehensweise

Ergebnisse

Das Ergebnis des Experiments zeigt auf, dass auf der SSD ein Großteil der Beweisdaten bei beiden Kapazitätsauslastungen nach einer Formatierung erfolgreich wiederhergestellt werden können. Hierbei wurden mit dem Tool „Autopsy“ bei 50-Prozent Speicherauslastung 262 von 348 Dateien und bei 100-Prozent Speicherauslastung 565 von 714 Dateien wiederhergestellt, die wie in Abbildung 63 zu sehen ist unterschiedliche Namen aufweisen, jedoch inhaltlich, mit Ausnahme der Bild-Dateien (siehe Abbildung 64), ident zu den originalen Daten sind.

Datenträger	50% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten („leere“/defekte Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
SSD	348	187	0	116	0	262	0

Tabelle 26: Ergebnis Experiment 10 – 50-Prozent Speicherauslastung

Datenträger	100% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten („leere“/defekte Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
SSD	714	555	0	237	0	565	0

Tabelle 27: Ergebnis Experiment 10 – 100-Prozent Speicherauslastung

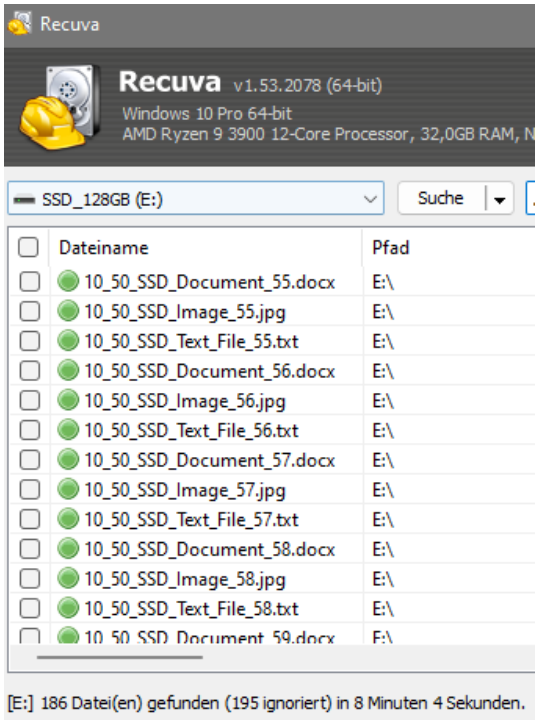


Abbildung 62: Experiment 10 – Ergebnis „Recuva“ – 50-Prozent Speicherauslastung

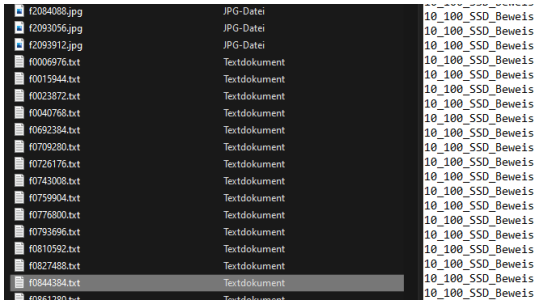


Abbildung 63: Experiment 10 – Ergebnis „Autopsy“ – 100-Prozent Speicherauslastung

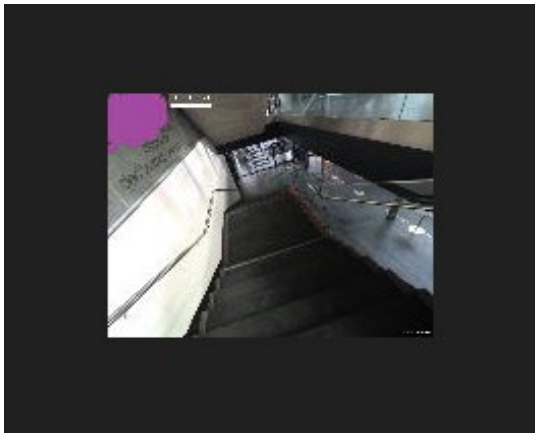


Abbildung 64: Experiment 10 – Wiederherstellung nach Formatierung mit „Autopsy“ – SSD

5.2.11 Experiment 11 – Wiederherstellung nach Löschung – residente Daten / ohne TRIM

Experiment 11 befasst sich mit dem Wiederherstellungsprozess von residenten Daten nach einer Formatierung des SSD-Datenträgers.

Vorgehensweise

Wie in Abbildung 65 dargestellt wird, beginnt die Vorgehensweise mit der Formatierung und Partitionierung der SSD mit dem Dateisystem NTFS und wird mit 50- oder 100-Prozent der Speicherkapazität mit residenten Daten ausgelastet. Unmittelbar nach und der Löschung der Daten und der Erstellung der Sicherungskopien kann die Analyse gestartet werden, zusätzlich dazu ist die TRIM-Funktion auf der SSD deaktiviert.

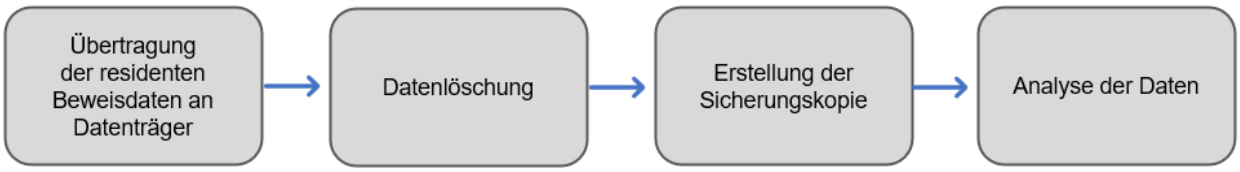


Abbildung 65: Experiment 11 – Vorgehensweise

Ergebnisse

Das Ergebnis des Experiments zeigt auf, dass auf der SSD alle residenten Beweisdaten bei beiden Kapazitätsauslastungen nach einer Löschung erfolgreich wiederhergestellt werden können. (siehe Abbildung 66)

Datenträger	50% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten („leere“/defekte Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
SSD	118	118	118	118	0	0	0

Tabelle 28: Ergebnis Experiment 11 – 50-Prozent Speicherauslastung

Datenträger	100% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten („leere“/defekte Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
SSD	242	242	242	242	0	0	0

Tabelle 29: Ergebnis Experiment 11 – 100-Prozent Speicherauslastung

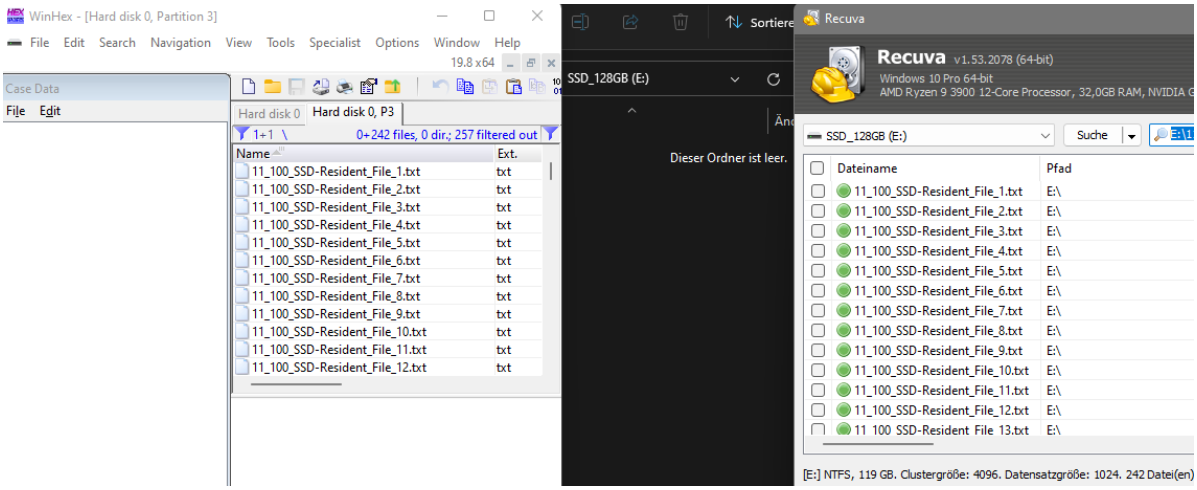


Abbildung 66: Experiment 11 – Ergebnis „WinHex“ und „Recuva“ – 100-Prozent Speicherauslastung

5.2.12 Experiment 12 – Wiederherstellung nach Formatierung – residente Daten / ohne TRIM

Das Ziel des letzten Experiments ist die Wiederherstellung residenter Beweisdaten nach einer Formatierung des SSD-Datenträgers.

Vorgehensweise

Die Vorgehensweise des Experiments (siehe Abbildung 67) beginnt mit der Formatierung und Partitionierung der SSD mit dem Dateisystem NTFS und wird mit 50- oder 100-Prozent der Speicherkapazität ausgelastet. Unmittelbar nach und der Formatierung des Datenträgers und der Erstellung der Sicherungskopien kann die Analyse gestartet werden, zusätzlich dazu ist die TRIM-Funktion auf der SSD deaktiviert.

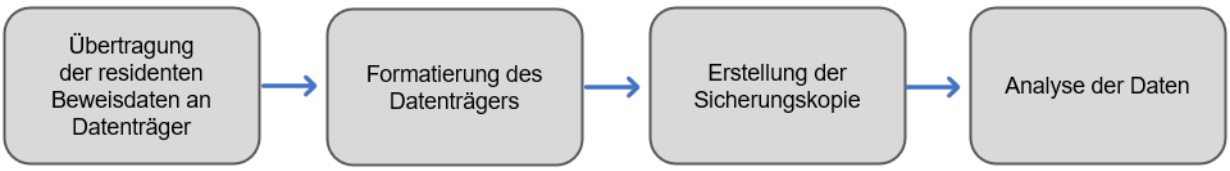


Abbildung 67: Experiment 12 – Vorgehensweise

Ergebnisse

Das Ergebnis des Experiments zeigt auf, dass auf der SSD lediglich mit „Recuva“ residente Beweisdaten bei beiden Kapazitätsauslastungen nach einer Formatierung erfolgreich wiederhergestellt werden können (siehe Tabelle 30 und Tabelle 31). Hierbei wurden bei 50-Prozent Speicherauslastung 12 von 118 Daten und bei 100-Prozent Speicherauslastung 135 von 242 Daten (siehe Abbildung 68) gesichert.

Datenträger	50% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten („leere“/defekte Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
SSD	118	12	0	0	0	0	0

Tabelle 30: Ergebnis Experiment 12 – 50-Prozent Speicherauslastung

Datenträger	100% Auslastung	Anzahl Wiederherstellung intakte Daten			Anzahl Wiederherstellung Metadaten („leere“/defekte Daten)		
	Gesamtanzahl der Daten	Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
SSD	242	135	0	0	0	0	0

Tabelle 31: Ergebnis Experiment 12 – 100-Prozent Speicherauslastung

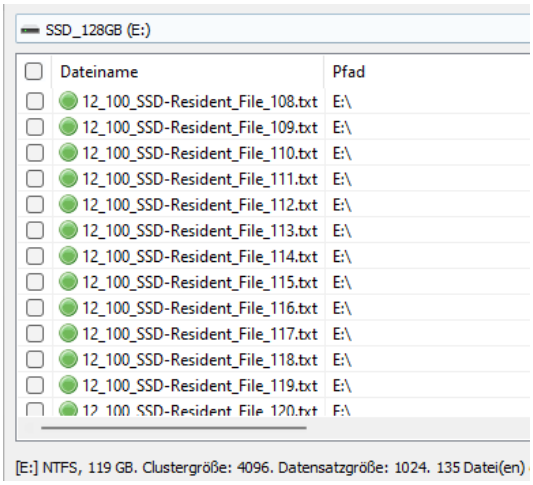


Abbildung 68: Experiment 12 – Ergebnis „Recuva“ – 100-Prozent Speicherauslastung

5.2.13 Übersicht der Ergebnisse

Folgende Tabelle gibt eine Gesamtübersicht auf die Möglichkeiten einer Datenwiederherstellung durch die Verwendung der forensischen Tools in Bezug auf die Ergebnisse des Experiments. Hierbei wird eine erfolgreiche Datenwiederherstellung (mindestens 1%) und die Wiederherstellung von Metadaten, die in einer separaten Spalte aufgezeigt wird, mit einem Häkchen markiert:

Nr.	Datenträger	Wiederherstellung von intakten Daten			Wiederherstellung von Metadaten		
		Recuva	Autopsy	WinHex	Recuva	Autopsy	WinHex
Experiment 1 Löschung und Akquise „live“	HDD	☑	☑	☑	-	-	-
	SSD	-	-	-	☑	☑	☑
	SD-Karte	☑	☑	☑	-	-	-
	USB-Stick	☑	☑	☑	-	-	-
Experiment 2 Löschung und Akquise „Offline“	HDD	☑	☑	☑	-	-	-
	SSD	-	-	-	☑	☑	☑
	SD-Karte	☑	☑	☑	-	-	-
	USB-Stick	☑	☑	☑	-	-	-

Experiment 3 Löschung und Leerlaufzeit 1 Minute	HDD	☑	☑	☑	-	-	-
	SSD	-	-	-	☑	☑	☑
	SD-Karte	☑	☑	☑	-	-	-
	USB-Stick	☑	☑	☑	-	-	-
Experiment 4 Löschung und Leerlaufzeit 1 Stunde	HDD	☑	☑	☑	-	-	-
	SSD	-	-	-	☑	☑	☑
	SD-Karte	☑	☑	☑	-	-	-
	USB-Stick	☑	☑	☑	-	-	-
Experiment 5 Löschung und Leerlaufzeit 24 Stunden	HDD	☑	☑	☑	-	-	-
	SSD	-	-	-	☑	☑	☑
	SD-Karte	☑	☑	☑	-	-	-
	USB-Stick	☑	☑	☑	-	-	-
Experiment 6 Formatierung	HDD	☑	☑	-	-	-	☑
	SSD	-	-	-	-	-	-
	SD-Karte	☑	☑	☑	-	-	-
	USB-Stick	☑	☑	☑	-	-	-
Experiment 7 Löschung und residente Daten	HDD	☑	☑	☑	-	-	-
	SSD	☑	☑	☑	-	-	-
	SD-Karte	☑	☑	☑	-	-	-
	USB-Stick	☑	☑	☑	-	-	-
Experiment 8 Formatierung und residente Daten	HDD	☑	-	-	-	-	-
	SSD	-	-	-	-	-	-
	SD-Karte	☑	-	-	-	-	-
	USB-Stick	-	-	-	-	-	-
Experiment 9 Löschung ohne TRIM	SSD	☑	☑	☑	-	-	-
Experiment 10 Formatierung ohne TRIM	SSD	☑	-	☑	-	☑	-
Experiment 11 Löschung ohne TRIM und mit residenten Daten	SSD	☑	☑	☑	-	-	-

Experiment 12 Formatierung ohne TRIM und mit residenten Daten	SSD	☑	-	-	-	-	-

Tabelle 32: Gesamtübersicht der Ergebnisse der verwendeten Tools

6. Diskussion

6.1 Forschungsfragen

Was sind die Unterschiede der Eigenschaften von SSDs bei der Analyse im laufenden Betrieb sowie im ausgeschaltetem/defekten Zustand im Vergleich zu HDDs?

Die Experimente 1 und 2 zeigen auf, dass durch die TRIM-Funktion bei der SSD keine Daten wiederhergestellt werden können, da durch den SSD-Controller bei einem Lesevorgang ein vordefinierter Wert zurückgegeben wird, dieser kann dabei, wie in Abbildung 46 zu sehen ist, aus Nullen bestehen. Bei der HDD hingegen sind alle Dateien fehlerfrei wiederhergestellt worden. Die Zustände haben bei diesen Experimenten keinen Unterschied bewirkt.

Was sind die Unterschiede der Eigenschaften von SSDs bei der Akquise im laufenden Betrieb sowie im ausgeschaltetem/defekten Zustand im Vergleich zu HDDs?

Die unterschiedlichen Zustände hatten keinen Einfluss auf die Ergebnisse. Hierbei ist anzumerken, dass das Ergebnis je nach Hersteller von SSDs unterschiedlich ausfallen kann, da verschiedene Implementierungen sowie Algorithmen verwendet werden können.

Wie sind die Unterschiede zwischen SSDs und HDDs in Bezug auf den Wiederherstellungsprozess nach einer Löschung von residenten und normalen Daten?

Das Ergebnis von Experiment 7 verdeutlicht, dass alle residenten Daten auf jedem Datenträger erfolgreich wiederhergestellt werden konnte. Nach einer Löschung sind residente Daten von der TRIM-Funktion nicht betroffen, da sich der Inhalt dieser Dateien als Eintrag in der „Master File Table“ befindet. Bei normalen Daten sind bei der SSD keine Daten wiederherstellbar gewesen, erst durch die Deaktivierung der TRIM-Funktion war es möglich, gelöschte normale Daten von der SSD wieder zu sichern. Die HDD kann residente und normale Daten nach einer Löschung problemlos wiederherstellen.

Welchen Unterschied macht die TRIM-Funktion auf Solid-State-Speichermedien bei der Akquise von gelöschten Daten?

Wie in den Experimenten 9, 10, 11 und 12 zu sehen ist, hat die TRIM-Funktion einen großen Einfluss auf den Akquise-Prozess, da durch die Deaktivierung der Funktion die SSD gelöschte Daten nicht mit vordefinierten Werten zurückgibt, sondern wiederherstellbar in den Zellen speichert. Eine aktive TRIM-Funktion hingegen, wird von einer Unterbrechung der Stromzufuhr bzw. Verbindung zum System nicht davon abgehalten, den Löschvorgang bei der nächsten Verbindung wieder fortzusetzen. Da der Garbage-Collection-Prozess im Hintergrund abläuft, haben auch „Write-Blocker“ keinen Einfluss auf diese Funktion.

6.2 Hypothesen

Daten auf einer SSD mit deaktivierter TRIM-Funktion bleiben nach dem Löschen genauso erhalten wie auf traditionellen Hard-Disk-Laufwerken.

Durch das Experiment 9 (siehe Kapitel 5.2.9) wurde die 1. Hypothese bestätigt, nach der Deaktivierung der TRIM-Funktion konnten alle Daten nach der Datenlöschung wiederhergestellt werden. Wie in Experiment 11 (Kapitel 5.2.11) zu sehen ist, können residente Daten ebenfalls erfolgreich wiederhergestellt werden.

Die Leerlaufzeit zwischen Löschung und Akquise von Daten hat keinen Einfluss auf den Wiederherstellungsprozess.

Diese Hypothese konnte nicht belegt werden, da der Einfluss der verschiedenen Leerlaufzeiten nicht genau messbar ist. Wie in Experiment 3, 4 und 5 (siehe Kapitel 5.2.3, 5.2.4 und 5.2.5) dargestellt wird, sind Daten bei der SSD unmittelbar nach dem Löschen dauerhaft gelöscht, lediglich Dateinamen können gesichert werden bzw. Daten mit „leerem“ Inhalt. Die einzige Ausnahme bilden die „leeren“ Daten der SSD, die durch die Garbage-Collection bei einer Leerlaufzeit von 24 Stunden teilweise entfernt wurden.

Daten von einer SSD können nicht wiederhergestellt werden, wenn bei dieser Festplatte die TRIM-Funktion aktiviert ist.

Die 3. Hypothese konnte nur teilweise belegt werden, da mit dem Experiment 7 (siehe Kapitel 5.2.7) bestätigt wurde, dass mit residenten Daten eine Wiederherstellung nach einer Datenlöschung trotz aktiver TRIM-Funktion möglich ist.

Das Formatieren einer Festplatte hat größere Auswirkungen auf die Akquise als das Löschen der Daten.

Die letzte Hypothese ist mit den Experimenten 6,8,10 und 12 (siehe Kapitel 5.2.6, 5.2.8, 5.2.10 und 5.2.12) bestätigt worden. Die Formatierung hat zusätzlich bei der SSD und beim USB-Stick größere Auswirkungen als bei der HDD und SD-Karte.

6.3 Diskussion der Ergebnisse

Durch die Ergebnisse dieser Studie wurden ein Großteil der aufgestellten Hypothesen durch vielseitige Resultate bestätigt. Diese Arbeit hat gezeigt, dass die wesentlichen Unterschiede der beiden Speichertechnologien auf die Funktionsweise der SSD zurückzuführen sind. Durch die begrenzte Anzahl der Schreib-/Löschzyklen wird die Zuverlässigkeit der SSD beeinträchtigt, die durch die Implementierung von Funktionen am SSD-Controller wie TRIM und Garbage-Collection ausgeglichen wird. Diese sorgen für deutliche Unterschiede in Bezug auf Datenrekonstruktion und Transparenz im Vergleich zu herkömmlichen Festplatten. Der aktive Einsatz dieser Eigenschaften wirkte sich auf die Erfassung bzw. Akquise von forensischen Daten beträchtlich aus. Da der innere Aufbau einer SSD ein Betriebsgeheimnis des Herstellers ist, kommt es bei der Implementierung der Funktionen am SSD-Controller zu unterschiedlichen Ansätzen, die nicht dokumentiert sind. Dies zwingt Forensiker/innen für eine erfolgreiche Datenwiederherstellung andere Maßnahmen zu ergreifen, wie die Entfernung und das Auslesen von Speicherchips. Bei solchen Maßnahmen ist die Einhaltung der Grundsätze der digitalen Forensik eine schwierige Herausforderung.

Im Gegensatz dazu konnten die auf einer HDD sowie auf Flash-Speicher wie USB-Sticks und SD-Karten gelöschten Daten vollständig und ordnungsgemäß wiederhergestellt werden. Bei SSDs mit aktivierter TRIM-Funktion hingegen war eine lückenlose Datenwiederherstellung nicht möglich, da alle gelöschten Daten als leere Blöcke aufscheinen, die mit Nullen befüllt sind. Eine Ausnahme waren residente Daten, die nach einer Löschung vollständig wiederhergestellt werden konnten, da sich der Inhalt dieser Dateien vollständig im

MFT-Eintrag befindet. Eine weitere wichtige Erkenntnis war die Tatsache, dass die Namen der „leeren“ Daten trotz Löschung sichtbar sind und im Rahmen einer forensischen Untersuchung ein potenzieller Hinweis auf Beweisdaten sein können. Durch die Deaktivierung der TRIM-Funktion verhalten sich SSDs wie HDDs und weisen dabei eine ähnliche Wiederherstellungsrate auf. Dies deutet darauf hin, dass durch den aktiven Zustand von TRIM herkömmliche Wiederherstellungsmethoden auf SSD-Laufwerken nicht mehr zielführend sind. Die Verwendung verschiedener Tools führt zu der Erkenntnis, dass trotz eines identischen Ausgangsszenarios unterschiedliche Ergebnisse erzielt werden können und deshalb die Wahl der forensischen Tools als eine zusätzliche kritische Komponente für den Erfolg digitaler forensischer Untersuchungen zu berücksichtigen ist.

6.4 Limitations/Future Work

Die Limitationen der vorliegenden Arbeit ergeben sich aus der Menge der verwendeten Geräte. Eine potenzielle Entdeckung einer Anomalie ist ohne Kenntnisse der inneren Funktionsweise der Firmware einer SSD grundsätzlich schwierig. Durch die Verwendung mehrerer SSD-Laufwerke von unterschiedlichen Herstellern können neue Kenntnisse gewonnen und das Verhalten der Implementierungen bei unterschiedlichen Experimenten gegebenenfalls auf bestimmte Hersteller zugeordnet werden. Dadurch können gewisse herstellerbezogene Ansätze für die Datenwiederherstellung entdeckt werden. Mit den Experimenten dieser Arbeit ist es gelungen, eine gemeinsame Meinung zu einigen anderen Studien [4, 16] zu vertreten. Diese Experimente zeigen, dass durch die Verwendung mehrerer Tools unterschiedliche Ergebnisse bei identischen Untersuchungen entstehen können. Die Experimente der vorliegenden Arbeit lassen viele Möglichkeiten für weitere Forschungen in Bezug auf die Verwendung von SSDs unterschiedlicher Hersteller sowie verschiedener Forensik-Tools offen.

7. Conclusio

Im letzten Abschnitt werden die Erkenntnisse der vorliegenden Arbeit zusammengefasst und die Resultate kritisch reflektiert.

Einer der größten Herausforderungen für die digitale Forensik in den letzten Jahren war der Wandel von der traditionellen Festplatte zu den schnellen und kleineren SSDs. Der verbreitete Einsatz von modernen Flash-basierten Speichermedien führte zu grundlegenden Unterschieden bei der Erfassung bzw. Akquise von forensischen Daten.

Das Kapitel der Grundlagen der digitalen Forensik zeigte, dass durch bestimmte Teilbereiche wie die Mobilgeräte-Forensik, mit dem Wandel des Datenspeichersystems zu kleineren Flash-Speichern, stets neue Anwendungsgebiete entstanden sind. Für die Nachvollziehung von Straftaten und das Übermitteln von unterstützenden Informationen, sind digitale Spuren oftmals die einzigen Ermittlungsansätze. Dies zeigte auf, dass sich die digitale Forensik in vielen Bereichen des täglichen Lebens erweitert hat. Die Einhaltung der Grundsätze wie die Integrität, Authentizität und ordnungsgemäße Beweismittelkette sind dabei zu wichtigen Grundvoraussetzungen für die Zulässigkeit und Glaubwürdigkeit von digitalen Beweismitteln vor Gericht geworden. Aus dem Kapitel geht ebenfalls hervor, dass die Flüchtigkeit von Daten die Ermittlungsmethode bestimmt. Dabei wurde zwischen Post-Mortem-Analyse, die ausgeschaltete Systeme bzw. persistente Daten sicherstellt, und Live-Response-Analyse, die flüchtige Daten von noch aktiven Systemen sammelt, unterschieden. Die Flüchtigkeit von Daten bestimmt dabei die Reihenfolge der Akquise von potenziellen Beweismitteln und ist ein großer Bestandteil der forensischen Untersuchung. In diesem Kontext wurde ebenfalls auf verschiedene Vorgehensmodelle hingewiesen, die als Basis für eine ordnungsgemäße Durchführung forensischer Untersuchungen dienen können.

Das Kapitel der technischen Grundlagen zeigt, dass es grundlegende Unterschiede zwischen den Speichermedien gibt. Datenwiederherstellungsprozesse, die bei der HDD zum Einsatz kamen, sind für die SSD nicht mehr zielführend. Aus diesem Abschnitt geht ebenfalls hervor, dass SSD-Controller das Herzstück eines Flash-Speichers mit grundlegenden Eigenschaften bzw. Funktionen sind. Da die Speicherzellen eines Flash-basierten Datenträgers nur eine begrenzte Lebensdauer haben, die mit Schreib-/Löschzyklen gemessen wird, sind Funktionen wie TRIM, Garbage-Collection und Bad-Block-Management, die als Hintergrundprozess laufen, für ein effizientes Speichermanagement von großer Bedeutung. Dabei führte das Fehlen eines Standards zu unterschiedlichen Ansätzen der Hersteller der verwendeten Funktionen und Algorithmen der SSD-Controller, welche im Detail dem Betriebsgeheimnis unterliegen. Seit der Entwicklung der SSD-Technologie ist dies eine Herausforderung für ermittelnde Personen im Bereich der digitalen Forensik. Das Kapitel „Related Work“ zeigt einen Überblick über ähnliche Werke und befasst sich mit deren Inhalten und Ergebnisse. Diese zeigten das gemeinsame Ergebnis auf, dass durch die Funktionen wie TRIM und Garbage-Collection forensische Untersuchungen erheblich beeinträchtigt werden.

Für die Beantwortung der Forschungsfragen und gestellten Hypothesen, ist eine Anzahl von Experimenten, basierend auf Szenarien der digitalen Forensik, durchgeführt worden. Hierbei wurden als Speichermedien eine SSD, HDD, SD-Karte und ein USB-Stick eingesetzt, die mit Beweisdaten befüllt worden sind. Durch die Experimente wurde aufgezeigt, dass aufgrund von Funktionen wie TRIM gelöschte Daten auf einer SSD nicht wiederhergestellt werden können. Dagegen bei Deaktivierung dieser Funktion sich SSDs wie HDDs verhalten und ähnliche Wiederherstellungsraten in den Experimenten aufweisen konnten. Eine Ausnahme waren residente Daten, die trotz einer aktiven TRIM-Funktion nach einer Löschung vollständig wiederhergestellt werden konnten. Das Verhalten in Bezug auf die Datenwiederherstellung bei der SD-Karte und dem USB-Stick war mehrheitlich identisch zur HDD. Daraus lässt sich schließen, dass der Schlüsselfaktor zu den grundlegenden Unterschieden und der Unvorhersehbarkeit bei der Datenwiederherstellung in der Firmware der SSD liegt.

Literaturverzeichnis

[1] A. Brockhaus, „Cybercrime as a Service (CaaS) – So funktioniert die professionalisierte Cyberkriminalität," isits AG International School of IT Security, November 2021. [Online]. Available: https://www.is-its.org/it-security-blog/cybercrime-as-a-service-caas-so-funktioniert-die-professionalisierte-cyberkriminalitaet. [Zugriff am 04 06 2022].

[2] K. A. Hahn, „Der „Smart-Ort" als Tatort," September 2017. [Online]. Available: https://www.kriminalpolizei.de/ausgaben/2017/september/detailansicht-september/artikel/der-smart-ort-als-tatort-wie-neue-digitale-spuren-die-ermittlungsarbeit-veraendern.html. [Zugriff am 25 Mai 2022].

[3] P. Ghodsnia, „Effective Use of SSDs in Database Systems," University of Waterloo, Ontario, Kanada, 2018.

[4] F. Geier, „The differences between SSD and HDD technology regarding forensic investigations," Linnaeus University, Sweden, 2015.

[5] D. Grossi, „What is Forensic Science? - Definition, History & Types," 01 2018. [Online]. Available: https://study.com/academy/lesson/what-is-forensic-science-definition-history-types.html. [Zugriff am 27 04 2022].

[6] G. Palmer, „A Road Map for Digital Forensic Research (Technical Report)," 08 2001. [Online]. Available: https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf. [Zugriff am 19 05 2022].

[7] S. V. N. Parasram, „Digital Forensics With Kali Linux," in *Perform data acquisition, digital investigation, and threat analysis using Kali Linux tools*, Birmingham - Mumbai, Packt, 2020, pp. 21-22.

[8] E. Casey, Digital Evidence and Computer Crime (3rd Edition), Academic Press, 2011.

[9] Council of Europe Portal, „Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedingsGuidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceeding," Council of Europe Portal, 30 01 2019. [Online]. Available: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0c. [Zugriff am 27 04 2022].

[10] S. Ludewig, „Die Sicherstellung und Auswertung des Smartphones – Kriminalpolitischer Anpassungsbedarf?," KriPoZ Onlineportal, September 2019. [Online]. Available: https://kripoz.de/2019/09/18/die-sicherstellung-und-auswertung-des-smartphones-kriminalpolitischer-anpassungsbedarf/. [Zugriff am 25 Mai 2022].

[11] D. Larry und D. Lars, „Digital Forensics for legal professionals," in *Understanding Digital Evidence from the Warratn to the Courtroom*, Massachusetts, USA, ELSEVIER, 2012.

[12] R. Luh, „Digital Forensics - Introduction," FH St. Pölten, 2021.

[13] A. Meister, „Digitale Forensik," Netzpolitik.org, 08 2018. [Online]. Available: https://netzpolitik.org/2018/digitale-forensik-mit-diesen-sieben-programmen-liest-die-polizei-smartphone-daten-aus/. [Zugriff am 01 05 2022].

[14] K. Kent, S. Chevalier, T. Grance und H. Dang, „https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf," NIST, 08 2006. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf. [Zugriff am 01 05 2022].

[15] Bundesamt für Sicherheit in der Informationstechnik (Deutschland), „IT-Grundschutz-Kataloge (15. Ergänzungslieferung)," 01 2016. [Online]. Available: https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf. [Zugriff am 17 05 2022].

[16] V. R. Kondam, *Comparing SSD Forensics with HDD Forensics,* St. Cloud State University, 2020.

[17] PasswordsGenerator.net, „MD5 Hash Generator," PasswordsGenerator.net, o.J.. [Online]. Available: https://passwordsgenerator.net/md5-hash-generator/. [Zugriff am 01 Mai 2022].

[18] PasswordsGenerator.net, „SHA1 Hash Generator," PasswordsGenerator.net, o.J.. [Online]. Available: https://passwordsgenerator.net/sha1-hash-generator/. [Zugriff am 01 Mai 2022].

[19] P. Sommer, „Downloads, Logs and Captures: Evidence from Cyberspace," Journal of Financial Crime, 1997.

[20] H. Baier und S. Gärtner, „Einführung in die digitale Forensik," Hochschule Darmstadt, Darmstadt, 2019.

[21] NIST, „Evidence Chain of Custody Tracking Form," o.J.. [Online]. Available: ahttps://www.nist.gov/document/sample-chain-custody-formdocx. [Zugriff am 18 Mai 2022].

[22] A. Geschonneck, Computer Forensik: Computerstraftaten erkennen, ermitteln, aufklären, Heidelberg: dpunkt.verlag GmbH, 2014.

[23] IT-Forensik Wiki, „SAP-Modell," 17 Februar 2020. [Online]. Available: https://it-forensik.fiw.hs-wismar.de/index.php/SAP-Modell. [Zugriff am 17 Mai 2022].

[24] G. Dreo, F. Tietze, P. Hillmann, M. Golling und B. Stelte, „Grundlagen der IT-Forensik," Universität München - Fakultät für Informatik, 2013.

[25] A. S. Gillis, „ComputerWeekly.de," 04 2022. [Online]. Available: https://www.computerweekly.com/de/definition/Festplatte-Hard-Disk-Drive-HDD. [Zugriff am 20 05 2022].

[26] IBM, „IBM 350 disk storage unit," IBM, o.J.. [Online]. Available: https://www.ibm.com/ibm/history/exhibits/storage/storage_350.html. [Zugriff am 19 05 2022].

[27] K. Gerecke und K. Poschke, „IBM System-Storage-Kompendium," [Online]. Available: https://marketing-de.techdata.com/blog/wp-content/uploads/2019/10/IBM_Storage_Kompendium_komprimiert.pdf. [Zugriff am 19 05 2022].

[28] IBM, „IBM 350 disk storage unit," [Online]. Available: https://www.ibm.com/ibm/history/exhibits/storage/images/PH0350A.jpg. [Zugriff am 19 05 2022].

[29] P. Cohen, „A History of Hard Drives," Backblaze.com, November 2017. [Online]. Available: https://www.backblaze.com/blog/history-hard-drives/. [Zugriff am 22 05 2022].

[30] R. Chaudhary und A. Kansal, „A perspective on the future of the magnetic hard disk drive (HDD) technology," Bharat Institure of Technology, Meerut, 2015.

[31] C. Pröll, „Die Festplatte," Rudolf Diesel FachschuleIAV2 , o.J..

[32] it-surfer.de, „Festplatte / HDD," it-surfer.de, 12 2015. [Online]. Available: http://www.it-surfer.de/hardware/grundlagen/festplatte-hdd/. [Zugriff am 20 05 2022].

[33] Elektronik Kompendium, „Festplatte / Harddisk," Elektronik-Kompendium.de, o.J.. [Online]. Available: https://www.elektronik-kompendium.de/sites/com/0610291.htm. [Zugriff am 20 05 2022].

[34] Elektronik Kompendium, „P-ATA / Ultra-ATA / EIDE," elektronik-kompendium.de, o.J.. [Online]. Available: https://www.elektronik-kompendium.de/sites/com/0501031.htm. [Zugriff am 21 05 2022].

[35] Elektronik Kompendium, „SATA / Serial-ATA," Elektronik Kompendium, o.J.. [Online]. Available: https://www.elektronik-kompendium.de/sites/com/0808061.htm. [Zugriff am 21 05 2022].

[36] K. Greve, „HDDs," Universität Hamburg, Oldendorf, 2016.

[37] „Logical organization of hard disk," DataRecoverySalon, November 2009. [Online]. Available: https://www.datarecoverytools.co.uk/2009/11/27/logical-organization-of-hard-disk/. [Zugriff am 22 05 2022].

[38] M. J. W. Zimmer, „Ein forensischer Leitfaden zu Spezialverfahren der Datenrettung von Festplatten unter Nutzung des PC3000-Express System," Mittweida, 2022.

[39] pc-erfahrung.de, „Festplatte - Technik, Aufbau, Funktionsweise und Bilder," 05 2018. [Online]. Available: https://www.pc-erfahrung.de/fileadmin/Daten/Bilder/festplatte_technik_04.gif. [Zugriff am 22 05 2022].

[40] Ayusharma0698, „Introduction to solid-state drive (SSD)," GeeksforGeeks, November 2021. [Online]. Available: https://www.geeksforgeeks.org/introduction-to-solid-state-drive-ssd/. [Zugriff am 22 05 2022].

[41] S. Schefer, „SSD - Solid State Drive," Universität Hamburg, Hamburg, 2011.

[42] ssd-ratgeber.de, „SSD – Entwicklungsgeschichte von Anfang bis Heute," ssd-ratgeber.de, o.J.. [Online]. Available: https://www.ssd-ratgeber.de/ssd-entwicklungsgeschichte-anfang-heute/. [Zugriff am 24 Mai 2022].

[43] K. Weber, „Über den Einfluss von SSD-Technologie auf die Datenträger Forensik," Friedrich-Alexander-Universität Erlangen-Nürnberg, 2016.

[44] R. Micheloni, A. Marelli und K. Eshghi, Inside Solid State Drives (SSDs) - Second Edition, Springer Nature Singapore Pte Ltd., 2018.

[45] Micron Technology, Inc., „What is the Difference Between RAM and ROM?," Micron Technology, Inc., 2018. [Online]. Available: https://www.crucial.com/articles/about-memory/what-is-the-difference-between-ram-and-rom#:~:text=RAM%2C%20which%20stands%20for%20random,stores%20instructions%20for%20your%20computer.. [Zugriff am 22 05 2022].

[46] S. Larrivee, „Solid State Drive Primer # 8 - Controller Architecture - Channels and Banks," Cactus Technologies Limited, 05 2015. [Online]. Available: https://www.cactus-tech.com/resources/blog/details/solid-state-drive-primer-8-controller-architecture-channels-and-banks/. [Zugriff am 22 05 2022].

[47] V. Regulapati, „Error Correction Codes in NAND Flash Memory," The University of Texas at Austin, Texas, 2015.

[48] M. Günsch, „Flash-Speicher: Tiefgefrorener HLC-NAND mit 6 Bit pro Zelle," ComputerBase, 08 2021. [Online]. Available: https://www.computerbase.de/2021-08/flash-speicher-tiefgefrorener-hlc-nand-mit-6-bit-pro-zelle/. [Zugriff am 05 2022].

[49] Y. Aiba, H. Tanaka, T. Maeda, K. Sawa, F. Kikushima, M. Miura, T. Fujisawa, M. Matsuo und T. Sanuki, IEEE Journal on Exploratory Solid-State Computational Devices and Circuits, vol.7, no.2, pp.159-167, 2021.

[50] Wikipedia, „Solid-State-Drive," Wikipedia, 2022. [Online]. Available: https://de.wikipedia.org/wiki/Solid-State-Drive. [Zugriff am 25 Mai 2022].

[51] J. Chang, „SLC vs. MLC NAND und die Auswirkungen der Fertigungsprozesse - White paper CTWP010," DACOM West GmbH, Haan, 2016.

[52] R. Sheldon, „Merkmale der Charge-Trap-Technologie bei 3D-NAND-Flash," ComputerWeekly.de, 08 2018. [Online]. Available: https://www.computerweekly.com/de/tipp/Merkmale-der-Charge-Trap-Technologie-bei-3DNAND-Flash. [Zugriff am 23 05 2022].

[53] Samsung, „Samsung Starts Mass Producing Industry's First 3D Vertical NAND Flash," Samsung Newsroom, 08 2013. [Online]. Available: https://news.samsung.com/global/samsung-starts-mass-producing-industrys-first-3d-vertical-nand-flash. [Zugriff am 25 05 2022].

[54] Micron Technology, Inc., „Micron Investor Day 2022," 05 2022. [Online]. Available: https://investors.micron.com/static-files/8d23a61f-0c3d-46bf-81a1-c466525afd82. [Zugriff am 25 05 2022].

[55] S. Larrivee, „Alles, was Sie schon immer über Solid State Drives wissen wollten," dacomwest, 2016.

[56] R. Micheloni, L. Crippa und A. Marelli, Inside NAND Flash Memories, Springer Science+Business Media, 2010.

[57] R. Micheloni, M. Alessia und E. Kam, Inside Solid State Drives (SSDs), Dordrecht: Springer Dortrecht Heidelberg New York London, 2013.

[58] S. Every, „Gefahr für gelöschte Daten: TRIM-Befehl bei Solid State Drives," Attingo Datenrettung GmbH, 02 2020. [Online]. Available: https://www.attingo.at/blog/gefahr-fuer-geloeschte-daten-trim-befehl-bei-solid-state-drives/. [Zugriff am 23 05 2022].

[59] Intel, „Advantages of TRIM and How to Use It with Your Intel® SSD," Intel, 03 2022. [Online]. Available: https://www.intel.com/content/www/us/en/support/articles/000006462/memory-and-storage/data-center-ssds.html . [Zugriff am 23 05 2022].

[60] I. Micron Technology, „What is trim and active garbage collection?," Micron Technology, Inc., o.J.. [Online]. Available: https://www.crucial.com/articles/about-ssd/what-is-trim#:~:text=What%20is%20SSD%20Trim%3F,of%20data%20can%20be%20erased.. [Zugriff am 23 05 2022].

[61] O. Afonin, „Life after Trim: Using Factory Access Mode for Imaging SSD Drives," Elcomsoft, 01 2019. [Online]. Available: https://blog.elcomsoft.com/2019/01/life-after-trim-using-factory-access-mode-for-imaging-ssd-drives/. [Zugriff am 25 05 2022].

[62] Micron Technology, Inc., „Wear-Leveling Techniques in NAND Flash Devices," o.J.. [Online]. Available: https://www.micron.com/-/media/client/global/documents/products/technical-note/nand-flash/tn2942_nand_wear_leveling.pdf. [Zugriff am 24 05 2022].

[63] Elelktronik-Kompendium.de, „SSD - Solid State Drive," Elelktronik-Kompendium.de, o.J.. [Online]. Available: https://www.elektronik-kompendium.de/sites/com/1105091.htm. [Zugriff am 25 05 2022].

[64] S. Chen, „What Types of ECC Should Be Used on Flash Memory?," 11 2007. [Online]. Available: https://static.aminer.org/pdf/PDF/000/220/160/symbol_error_correctin_codes_for_memory_applications.pdf. [Zugriff am 25 05 2022].

[65] S. Moulton, „Solid State Drives Destroy Forensics & Data Recovery Jobs," Las Vegas, 2011.

[66] A. E. s.r.o., „PC-3000 Flash," ACELab Europe s.r.o., o.J.. [Online]. Available: https://www.acelab.eu.com/pc3000flash.php. [Zugriff am 25 05 2022].

[67] J. Kahn, „This is Apple's special tool to help customers recover data from the MacBook Pro's non-removable SSD," 9to5mac.com, 11 2016. [Online]. Available: https://9to5mac.com/2016/11/24/apple-special-cdm-tool-macbook-pro-ssd-recover-repairs/. [Zugriff am 25 05 2022].

[68] V. Subramaniam, „Apple removes the Customer Data Migration Tool connector in the the 2018 MacBook Pro with Touch Bar," notebookcheck.net, 07 2018. [Online]. Available: https://www.notebookcheck.net/Apple-removes-the-Customer-Data-Migration-Tool-connector-in-the-the-2018-MacBook-Pro-with-Touch-Bar.318186.0.html. [Zugriff am 25 05 2022].

[69] Y. R. Kambalapalli, „Different Forensic Tools on a Single SSD and HDD, Their Differences and Drawbacks," St. Cloud State University - theRepository at St. Cloud State, 2018.

[70] _N4rr34n6_, „One byte makes the difference: MFT Resident File," Mai 2019. [Online]. Available: https://unminioncurioso.blogspot.com/2019/05/dfir-one-byte-makes-difference-mft.html#:~:text=A%20file%20is%20resident%20when,file%20record%20is%201024%20bytes.. [Zugriff am 26 05 2022].

[71] Accessdata, „Accessdata.com," https://accessdata.com/product-download/ftk-imager-version-4-7-1 .

[72] Piriform Software Ltd, „Recuva," Piriform Software Ltd, o.J.. [Online]. Available: https://www.ccleaner.com/de-de/recuva. [Zugriff am 25 05 2022].

[73] Piriform Ltd, „How does Recuva work?," Piriform Ltd, o.J.. [Online]. Available: https://support.piriform.com/hc/en-us/articles/204044084#how-does-recuva-work--0-0. [Zugriff am 04 06 2022].

[74] B. Carrier, „Autopsy," o.J.. [Online]. Available: https://www.sleuthkit.org/autopsy/. [Zugriff am 04 06 2022].

[75] „Autopsy User Documentation 4.19.3 - Ingest Modules," Basis Technology, o.J.. [Online]. Available: http://sleuthkit.org/autopsy/docs/user-docs/4.19.3//ingest_page.html. [Zugriff am 04 06 2022].

[76] Basis Technology, „Autopsy User Documentation - File Type Identification Module," Basis Technology, Oktober 2015. [Online]. Available: https://sleuthkit.org/autopsy/docs/user-docs/3.1/file_type_identification_page.html. [Zugriff am 04 06 2022].

[77] The Apache Software Foundation, „Apache Tika - a content analysis toolkit," The Apache Software Foundation, o.J.. [Online]. Available: https://tika.apache.org/. [Zugriff am 04 06 2022].

[78] Basis Technology, „Autopsy User Documentation - Embedded File Extraction Module," Basis Technology, Oktober 2015. [Online]. Available: https://sleuthkit.org/autopsy/docs/user-docs/3.1/embedded_file_extractor_page.html. [Zugriff am 04 06 2022].

[79] Basis Technology, „Autopsy User Documentation - Picture Analyzer Module," Basis Technology, Juni 2022. [Online]. Available: http://sleuthkit.org/autopsy/docs/user-docs/4.19.3/_e_x_i_f_parser_page.html. [Zugriff am 04 06 2022].

[80] Basis Technology, „Autopsy User Documentation - PhotoRec Carver Module," Basis Technology, Oktober 2015. [Online]. Available: https://sleuthkit.org/autopsy/docs/user-docs/3.1/photorec_carver_page.html. [Zugriff am 04 06 2022].

[81] Basis Technology, „Autopsy User Documentation - Keyword Search Module," Basis Technology, o.J.. [Online]. Available: https://sleuthkit.org/autopsy/docs/user-docs/3.1/keyword_search_page.html. [Zugriff am 04 06 2022].

[82] Internet Service GmbH, „Leistungsstarker Index Server," Internet Service GmbH, o.J.. [Online]. Available: https://www.typo3-solr.com/de/was-ist-solr/so-funktionert-solr/#:~:text=Leistungsstarker%20Index%20Server,Tomcat%20oder%20Jetty%20laufen%20muss.. [Zugriff am 04 06 2022].

[83] X-Ways Software Technology AG, „WinHex: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor," X-Ways Software Technology AG, o.J.. [Online]. Available: https://www.x-ways.net/winhex/index-m.html. [Zugriff am 04 06 2022].

[84] X-Ways Software Technology AG, „X-Ways Investigator," X-Ways Software Technology AG, o.J.. [Online]. Available: https://www.x-ways.net/investigator/index-d.html. [Zugriff am 04 06 2022].

[85] X-Ways Software Technology AG, „X-Ways Forensics: Integrierte Software für Computerforensik," X-Ways Software Technology AG, o.J.. [Online]. Available: https://www.x-ways.net/forensics/index-d.html. [Zugriff am 04 06 2020].

[86] computerlexikon.com, „Parsen," computerlexikon.com, Januar 2001. [Online]. Available: https://www.computerlexikon.com/begriff-parsen. [Zugriff am 04 06 2022].